Phrack RU issue 011

Русская версия Phrack, выпуск 011. Полный текст статей с кодом и таблицами.

Темы выпуска: сети, маршрутизация, TCP/IP, Cisco, телефония и телеком-инфраструктура; культура Phrack, новости сцены, loopback, prophile и хакерские манифесты; Unix/Linux, BSD, Windows NT и администрирование систем; криптография, генераторы случайных чисел, протоколы и приватность.

Материалы выпуска: Оглавление; Phrack Pro-Phile VIII; PACT: транслятор кодов доступа с префиксом; Взлом систем голосовой почты; Простое шифрование данных; Введение; Взлом Prime-систем, части I, II, III (I и II — исправленные); Методы телефонной сигнализации; ЭЛЕКТРОННЫЙ СЕРИЙНЫЙ НОМЕР: СОТОВОЕ «СИТО»?; Верификация занятой линии; Scan Man: возвращение к теме; Phrack World News.

Больше крутых материалов в моём телеграм канале @grogrigs

Оглавление

Автор: Taran King

17 февраля 1987 года

Добро пожаловать в одиннадцатый выпуск электронного журнала Phrack Inc. В этот раз я был немного пунктуальнее с выходом номера (да, всего лишь на 3 дня опоздал!). Выпуск складывался не так легко, как хотелось бы, — ряд людей было трудно застать или получить от них материалы, однако я заполнил пустующие места другими файлами. Если вам говорили, что ваш материал выйдет в этом номере, — свяжитесь со мной, чтобы он появился в двенадцатом выпуске. В этом издании Phrack Inc. представлены следующие файлы:

Taran King
Sysop of Metal Shop Private

Phrack Pro-Phile VIII

Автор: Taran King

17 февраля 1987 г.

Добро пожаловать в Phrack Pro-Phile VIII. Phrack Pro-Phile создан для того, чтобы рассказывать вам, пользователям, о старых или особо известных и скандальных личностях. В этом месяце я представляю вам одного из старейших и наиболее заметных фрикеров прошлого...

Wizard of Arpanet

Wizard of Arpanet — один из представителей старшего поколения фрикеров и хакеров. В числе его главных достижений — управление BBS Inner Circle и Secret Service.

```
                    Handle: Wizard of Arpanet
                  Call him: Eric
              Past handles: The Hacker and The Priest
             Handle Origin: A real programmer on Arpanet was called The
                            Wizard and Eric took his handle from him.
             Date of Birth: 02/26/69
  Age in 9 days of this writing: 18 years old
                    Height: 6'1"
                    Weight: 150 lbs
                 Eye color: Blue
                Hair color: Dishwaterish blond
                 Computers: Atari 400, Commodore 64
          Sysop/Co-sysop of: Secret Service
```

Wizard of Arpanet начинал как обычный пользователь BBS. В какой-то момент он позвонил на Central Processing Unit — местную для него доску, — где обнаружил странные номера. Он попробовал подключиться к ним через модем, но оказалось, что это дозвонные номера Sprint. Системный оператор CPU объяснил ему, что к чему, и он начал звонить на общенациональные BBS. В продвижении ему помогли следующие доски: Twilight Zone (сисоп которой написал T-Net), OSUNY, Dragon's Lair и Delta BBS. Wizard организовал несколько групп, которые (от самой ранней до самой поздней) включали: PHA (Phreakers and Hackers of America) — в неё входили Deep Throat, Phreak King и Psycho Killer; The Inner Circle (первая версия) — с участием Shockwave Rider и Satan Knight, он же Redrum; и The 2nd Inner Circle — с участием The Cracker, Mr. America, Napoleon Bonapart, Stainless Steal Rat, Big Brother, Mr. Xerox, Bootleg, Maxwell Wilke, Mandrake The Magician и Zaphod Beeblebrox.

Эрик получил номер Arpanet от Dark Dante, а доступ к MIT Research System обнаружил через TAC News. Однажды ночью он завладел примерно 50–60 аккаунтами на Unix и сменил все пароли на WIZARD.

Stainless Steal Rat — сисоп Delta BBS — вместе с The Myth как-то приехал из Нью-Джерси на выходные, и они остановились у Джона Максфилда. Они побывали в его офисе. Wizard попросил Максфилда разрешить воспользоваться компьютером, чтобы распечатать кое-что, — и напечатал несколько материалов из списка адресов Stanford Artificial Intelligence для Arpanet. Джон был поражён. «Вот это да, — сказал он, — у меня теперь есть неопровержимые улики против тебя.» (TK: это может быть не дословная цитата.) После этого на следующей же неделе он устроил нашему другу Эрику облаву. Помимо этого, у Эрика было немало материалов по AUTOVON от

некоего человека из Вашингтона, и он начал изучать линии FTS (Federal Telephone System), о которых узнал — кто бы мог подумать — от того же Джона Максфилда. Они также нашли стандартные пароли TeleMail, получили учётные записи администраторов и развернули собственную BBS на системах Nassau и Coca-Cola, а также везде, где только было возможно. И вдруг всё рухнуло в одночасье: Mandrake решил обрушить часть TeleMail. Появилось Федеральное бюро расследований. ФБР следило за Эриком на протяжении шести месяцев в поисках улик против него. И они их нашли. Серьёзных последствий не было, но ему пришлось нанять адвоката, и история получила огласку в прессе. Спустя 90 дней всё изъятое, за исключением нескольких документов, было возвращено. В эти 90 дней Эрик работал консультантом по компьютерной безопасности в банке, получая 200 долларов в час (всего два часа...).

Единственные «фрикеры», с которыми он встречался лично, — это Stainless Steal Rat и Cable Pair.

Эрик упоминался в местных теленовостях, в газетах, в USA Today, NY Times, Washington Post, в книгах и в Британской энциклопедии (смотри статью «Хакер»).

Интересы: музыка (предпочтительно джаз, регги, новая волна), восточная философия (дзен-буддизм), книги Джека Керуака (великого битника), бесцельные поездки на машине, постепенное превращение в социального затворника, физика и греческие математики.

Любимое у Эрика

Женщины: поиск идеала (Карен Уайлдер).
Еда: китайская кухня.
Автомобили: BMW 320-I.
Художник: Сальвадор Дали.
Планы на ближайшие месяцы: следующие полтора года — поездка в Монреаль в апреле на неделю отдыха, затем возвращение в прекрасный Детройт и продолжение учёбы в старшей школе Эйзенхауэра.

Самые памятные события

Внезапное осознание того, что всё, что ты делал три года назад, было глупостью.
Превращение в нового человека.
Обретение нравственных принципов, новых идей и нового взгляда на мир.

Люди, которых стоит упомянуть

Tuc — за то, что рассказал ему о боксе.
Tom Tone — за то, что позвонил ему на его первой конференции.
Magnetic Surfer — за то, что поговорил с ним впервые после того, как Sherwood Forest исчез из эфира.
John Maxfield — за встречу с ним.
Stainless Steal Rat — за встречу с ним... вместе с Джоном Максфилдом.
Dark Dante — один из легендарных фрикеров.

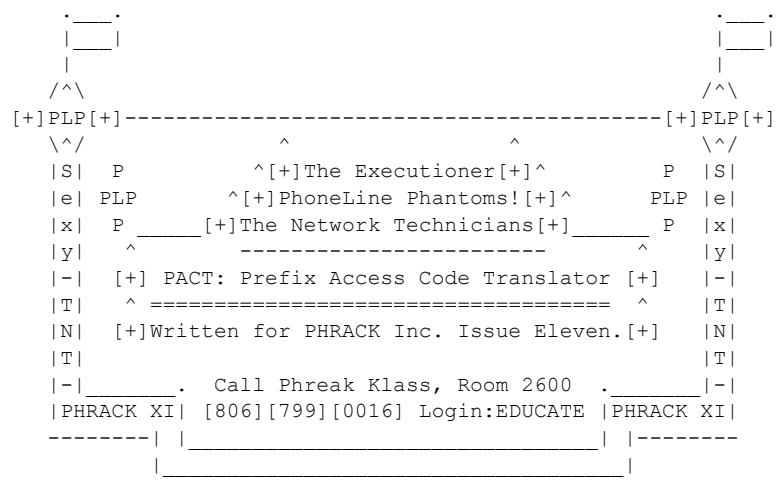
Всегда следуй инстинкту, а не желанию, иначе пожалеешь — ведь так ты лжёшь самому себе.

Надеюсь, файл вам понравился. Ждите новых Phrack Pro-Phile в самом ближайшем будущем. ...А теперь — традиционный вопрос, который задаётся всем участникам интервью.

Среди фрикеров, которых вы встречали, можно ли считать большинство из них компьютерными задротами? Нет, говорит Эрик, — он считает их новой породой интеллектуалов. Спасибо за ваше время, Эрик.

Taran King
Sysop of Metal Shop Private

PACT: транслятор кодов доступа с префиксом



Автор: The Executioner / PLP / TNT (PhoneLine Phantoms / The Network Technicians)

Функция PACT (Prefix Access Code Translator — транслятор кодов доступа с префиксом) обеспечивает предварительную трансляцию данных для функций, использующих коды доступа с особым префиксом. Стандартный план нумерации и набора номера требует, чтобы индивидуальные абоненты и клиенты малого бизнеса использовали набор кодов доступа с префиксом для активации функций. PACT предоставляется на уровне отдельного офиса и **не** применяется для обработки вызовов клиентов Centrex.

Когда клиент инициирует вызов, для хранения данных о нём используется регистр вызова. Клиент набирает префикс и двузначный код доступа (таблица A). PACT анализирует набранные цифры и определяет, какое действие необходимо выполнить. Если введён неназначенный код, будет воспроизведено сообщение об ошибке (переадресация или специальный сервис). При корректном коде выполняется соответствующее действие.

PACT состоит из головной таблицы PACT и транслятора кодов доступа с префиксом. Функция PACT позволяет использовать специальные символы в качестве префикса: `*` и `#`. На дисковых телефонных аппаратах вместо них используются `11` и `12` соответственно. После префикса необходимо набрать двузначный код. Эта комбинация интерпретируется в терминах типа и подтипа (таблица B).

Таблица A — Коды доступа

Код доступа	Описание функции
2X — 3X (x=0–9)	Расширение до 2- или 3-значных кодов (зарезервировано на будущее)
4X, 5X, 7X	Локальные службы сигнализации (LASS)
72	Активация переадресации вызовов
73	Деактивация переадресации вызовов

74	Однозначный ускоренный набор
75	Двузначный ускоренный набор
#56	Цифровая коммутируемая связь (CSDC)

Субтранслятор всегда строится длиной в 100 слов. Слово — это двоичный код, который при целостной передаче является командой; одно слово соответствует одному двузначному коду доступа. Субтранслятор содержит PTW (Primary Translation Word — первичное слово трансляции). PTW содержит тип функции, подтип функции и индекс подтипа функции, которые определяют значение набранного кода. Подтип функции допускает четыре таблицы подтипов для типа функции 31 (LASS). Индекс 0 — для LASS, индекс 1 — для LASS с оплатой за использование, индексы 2 и 3 в настоящее время не используются.

Таблица B — Типы и подтипы функций

Тип функции: 0 — Не назначен

Тип функции: 1 — Однозначный сокращённый набор

• Подтип 0: Ускоренный вызов (Speed Call)
• Подтип 1: Изменение списка ускоренного вызова
• Подтип 2: Недопустимый

Тип функции: 2 — Двузначный набор

• Подтипы: аналогично типу функции 1

Тип функции: 3 — Цифровая коммутируемая связь (CSDC)

• Подтип 1: Служба CSDC 56 кбит/с

Тип функции: 4 — Трёхсторонняя конференция с оплатой за использование

Тип функции: 5 — Отмена ожидания вызова (Cancel Call Waiting)

Тип функции: 20 — Активация переадресации вызовов

Тип функции: 21 — Деактивация переадресации вызовов

Тип функции: 22 — Сервис учёта проекта (Autoplex)

Тип функции: 26 — Выбор оператора межзоновой связи клиентом (Inter LATA carrier)

Тип функции: 27 — Защита голоса/данных (Voice/Data Protection)

Тип функции: 28 — MDS — служба сообщений рабочего стола (Message Desk Service)

• Подтип 0: Активация MDS
• Подтип 1: Деактивация MDS

Тип функции: 30 — Пул ресурсов передачи данных для жилых абонентов (Residence Data Facility Pooling)

Тип функции: 31 — Локальные службы сигнализации (LASS)

Индекс 0:

• Подтип 0: AR — автоматический обратный вызов входящих

• Подтип 1: AR — автоматический обратный вызов исходящих
• Подтип 2: AR — активация входящих/исходящих
• Подтип 3: AR — деактивация
• Подтип 4: Активация трассировки вызова по инициативе клиента
• Подтип 5: Активация отличительного сигнала вызова (Distinctive Alert — ВКЛ)
• Подтип 6: Активация ICLID (определитель номера входящего абонента)
• Подтип 7: Активация избирательного отклонения вызовов (SCR — ВКЛ)
• Подтип 8: Активация избирательной переадресации вызовов (SCF — ВКЛ)
• Подтип 9: Активация режима «Частный вызов»
• Подтип 10: Отличительный сигнал — ВЫКЛ
• Подтип 11: ICLID — ВЫКЛ
• Подтип 12: SCR — ВЫКЛ
• Подтип 13: SCF — ВЫКЛ
• Подтип 14: Частный вызов — ВЫКЛ
• Подтип 15: Отличительный сигнал — переключение ВКЛ/ВЫКЛ
• Подтип 16: ICLID — переключение ВКЛ/ВЫКЛ
• Подтип 17: SCR — переключение ВКЛ/ВЫКЛ
• Подтип 18: SCF — переключение ВКЛ/ВЫКЛ
• Подтип 19: Частный вызов — переключение ВКЛ/ВЫКЛ
• Подтип 20: Избирательный приём вызовов (SCA) — ВКЛ
• Подтип 21: SCA — ВЫКЛ
• Подтип 22: SCA — переключение ВКЛ/ВЫКЛ
• Подтип 23: Ограничение компьютерного доступа (CAR) — ВКЛ
• Подтип 24: CAR — ВЫКЛ
• Подтип 25: CAR — переключение ВКЛ/ВЫКЛ
• Подтипы 26–31: Зарезервированы для будущих функций LASS

Индекс 1 — Pay Per View (платный просмотр):

• Подтип 0: Размещение заказа
• Подтип 1: Отмена заказа

Функция PACT крайне важна для работы служб LASS. Именно PACT позволяет сообщать коммутатору о желаемом действии. Без PACT взаимодействие между абонентом и его центральной станцией (CO) было бы невозможным. PACT является фундаментом для использования кодов доступа.

```
============================================================
= If you have any questions or comments, please leave mail =
= either on Phreak Klass Room 2600 or at 214-733-5283.     =
============================================================
= (c) The Executioner/PLP/TNT                              =
============================================================
```

Взлом систем голосовой почты

Автор: Black Knight from 713

Голосовая почта — относительно новая концепция, о которой пока мало говорят. Это очень полезный инструмент как для делового человека, так и для фрика. Принцип работы следующий: тот, кто хочет с вами связаться, звонит на номер — как правило, 1-800 — и вводит с тонального набора номер вашего почтового ящика, после чего может оставить вам сообщение. По словам бизнес-экспертов, это практически полностью устраняет проблему «телефонных догонялок». Чтобы прослушать сообщения, достаточно позвонить на тот же номер, ввести определённый код — и вы сможете услышать сообщения, перенаправить их и воспользоваться прочими функциями почтового ящика.

Большинство систем голосовой почты (VMS) устроены схожим образом. Способов хранения голоса существует несколько. Первый: голос записывается в цифровом формате, сжимается, а при воспроизведении восстанавливается в исходное звучание. Второй метод — более медленный и требующий больше места, но дешевле в реализации — хранит голос на магнитной ленте того же типа, что используется для хранения данных на компьютере, и воспроизводит её на медленной скорости. При таком подходе голос не требует никакой обработки и звучит естественно, пока лента движется с постоянной скоростью. В некоторых новых VMS голос записывается в цифровом формате и считывается с магнитной ленты со скоростью около 2400 бит в секунду.

Существует множество различных типов и версий систем голосовой почты. Ниже рассматриваются одни из лучших и наиболее доступных из них.

Centagram

Это системы с прямым дозвоном (вводить номер ящика не нужно). Чтобы попасть на одну из них, сначала нужно знать номер хотя бы одного ящика в системе. Все остальные ящики будут находиться на том же префиксе — достаточно перебирать их до тех пор, пока не найдётся такой, где говорится, что вызываемый абонент недоступен. Как правило, это означает, что ящик ещё никому не назначен. До того как приятный женский голос предложит оставить сообщение, нажмите `#`. Система запросит пароль. Обычно пароль совпадает с последними четырьмя цифрами номера ящика либо является простым числом вроде 1000, 2000 и т.д. После входа система очень дружелюбна и выводит меню с доступными опциями. Если пустых ящиков не найти или хочется большего, можно попробовать взломать ящик системного администратора — как правило, это 9999 на том же префиксе. Этот ящик позволяет прослушивать чужие сообщения, а также создавать и удалять ящики.

Sperry Link

Очень неплохие системы. Обычно доступны по номеру 800. Получить ящик здесь сложнее всего, поскольку нужно подобрать идентификатор пользователя (отличающийся от номера ящика) и пароль. Если при ответе система говорит: «This is a Sperry Link voice station. Please enter your user ID» — придётся перебирать идентификаторы. На большинстве систем Sperry это пятизначное число. Если же система отвечает: «This is an X answering service» — нужно сначала нажать `*#`, чтобы появился запрос номера пользователя. Получив действующий идентификатор, необходимо угадать пароль — на большинстве систем он состоит из 4 цифр. После входа система также очень

дружелюбна и предлагает множество различных опций.

RSVP

Пожалуй, одна из худших VMS, зато получить ящик здесь проще всего. При ответе можно нажать `*` для просмотра каталога ящиков системы (их не более 23). При нажатии `#` выводится меню опций, а при выборе любой из них система запрашивает идентификационный номер. На системах RSVP идентификатор почти всегда совпадает с номером ящика, который всегда состоит из 2 цифр.

A.S.P.E.N.

Системы голосовой почты Aspen производства Octel Telecommunications — на мой взгляд, лучшие из существующих VMS. Чтобы получить ящик в Aspen, нужно найти свободный. Свободный ящик распознаётся по фразе: «You entered XXXX. Please leave a message at the tone». Затем нажмите `#`; когда система запросит номер ящика, введите номер найденного свободного ящика, и приятный женский голос проведёт вас через все этапы настройки. Сначала система объяснит, что можно делать с ящиком, а затем предложит: «Please enter the temporary password assigned to you by your system manager». Этот пароль обычно состоит из 4 цифр и совпадает с номером ящика — например, 1000 и т.д. После входа доступны многочисленные возможности. Можно создать список рассылки: если нужно отправить одно сообщение нескольким людям, достаточно ввести номер списка — и все ящики, входящие в него, получат сообщение. Можно также настроить звонок от системы с уведомлением о новых сообщениях. В Aspen есть так называемые «информационные почтовые ящики» — только для прослушивания; они могут быть защищены паролем, который звонящий должен ввести перед прослушиванием приветствия. В системах Aspen также есть ящик системного менеджера, дающий практически полный контроль над всей системой: прослушивание чужой почты, создание и удаление ящиков и многое другое.

Спасибо за прочтение этого файла. Если хотите связаться со мной через голосовую почту, звоните 1-800-222-0311 и нажмите `*2155`.

```
//--Black Knight from 713--\\
|     for PHRACK XI (1987)  |
\\--++--++--++--++--++--++-//
```

Простое шифрование данных

<или цифровая электроника 101>

Автор: The Leftist

Пролог

Прошло немало времени с тех пор, как я писал свои практические статьи. На этот раз я переключился с химии на электронику. Надеюсь, в будущем я буду писать ещё больше материалов в том же духе. Кроме того, я разработал более сложное устройство шифрования, которое, возможно, опубликую позже.

Вы держите BBS и боитесь, что «федералы» залогинятся и хитростью выманят у вас пароль? Хотите точно контролировать, кто подключается к вашей доске? Тогда эта статья — для вас.

Компоненты

• 1 батарейка на 9 вольт
• 1 микросхема 74HC/HCT04 — CMOS шестиканальный инвертор (около 50 центов)

Базовые знания электроники не помешают, а ещё пригодится проводка. Если хотите сделать всё по-настоящему, можно раскошелиться и купить разъём для батарейки на 9 В.

Примечание: хотя разводить всё на травлёной печатной плате не обязательно, сделать это вполне просто, и результат получается гораздо аккуратнее.

Принцип работы

Данные, приходящие в модем и исходящие из него, передаются в виде единиц и нулей. Они представляют высокие и низкие уровни сигнала, которые компьютер распознаёт как допустимые данные. Если поменять все единицы на нули, а нули на единицы, получится простой способ шифрования данных. Именно это и делает шестиканальный инвертор: увидев 0, он выдаёт 1, а увидев 1 — выдаёт 0.

Таким образом, нужно поставить инвертор на линию передачи и инвертор на линию приёма. На компьютере, с которым вы соединяетесь, тоже должны быть инверторы на линиях приёма и передачи, — иначе вы увидите только мусор! Я постарался изложить всё как можно проще для тех, кто далёк от технических деталей.

Подключение

Возьмите микросхему и посмотрите на неё. На одном из торцов должна быть небольшая выемка. Держите её так, как показано на схеме:

```
  (80 столбцов)


          _____________________________
           |                           |
          14 13 11 12 10 9 8           |
           |  |  |  |  | |  |          |
           _________________            |
          |                 |          |_ к плюсу батарейки
          \   74hc/hct04    |
          /                 |
          |_________________|            к минусу батарейки
           |  |  |  |  |  | |             |
           1  2  3  4  5  6 7_____________|
           |  |  |  |
           |  |  |  |_____________________________________к порту компьютера
           |  |  |_____________________________________от модема
           |  |_____________________________________________________к разъёму модема
           |_____________________________________________________ от порта компьютера
```

Подключите +9 В к выводу 14, а минус — к выводу 7. На этой микросхеме шесть инверторов; нам понадобятся только два из них.

Найдите провод, идущий от компьютера к линии передачи данных модема. Разрежьте его и подключите один конец к выводу 1, а другой — к выводу 2. Затем найдите линию приёма данных и тоже разрежьте её. Один конец подключите к выводу 3, другой — к выводу 4. Вот, в общем-то, и всё. Если хотите задействовать остальные инверторы на микросхеме, вот полная распиновка:

Вывод(ы)	Название и назначение
1, 3, 5, 9, 11, 13	Входы данных
2, 4, 6, 8, 10, 12	Выходы данных
7	Земля (GND)
14	VCC

Помните: такое же устройство должно быть установлено и на модеме BBS, и у пользователя, который к нему подключается. Я проверял это на Smartmodem — работает. Если у вас внутренний модем, реализовать схему будет несколько сложнее.

Введение

Автор: Taran King

Система DAIS II производства Computer Consoles Incorporated

Computer Consoles Incorporated (CCI) производит различное аппаратное обеспечение, используемое совместно с коммутаторами телефонных компаний, а также в других направлениях их деятельности, включая собственные Unix-совместимые вычислительные системы.

DAIS II — это Distributed Automatic Intercept System (Распределённая автоматическая система перехвата). Она используется для оповещения абонента в случае, когда набранный номер не обслуживается. Именно это вы слышите, набрав неверный номер: три тональных сигнала, за которыми следует автоматическое объявление, или же подключается оператор ONI (Operator Number Identification — идентификация номера оператором), который спрашивает: «Какой номер вы набирали?»

Информация для этого файла получена преимущественно из учебного руководства, присланного мне компанией CCI. С ними можно связаться по телефону 800-833-7477 или 716-482-5000, либо написать по адресу: 97 Humbolt Street, Rochester, NY, 14609.

Перехват вызовов

Пожалуй, каждый человек, когда-либо пользовавшийся телефоном, так или иначе сталкивался с пресловутыми тремя тональными сигналами, после которых следует громоздкое объявление об отключённом или недействующем номере. В этом файле подробно рассматривается принцип работы всей системы.

После набора недействующего номера коммутатор телефонной компании класса 5 (Class 5 End Office) направляет вызов в DAIS II.

Вызовы с ANI

Если коммутатор конечного офиса оснащён оборудованием Automatic Number Identification (ANI — автоматическая идентификация номера), оно определяет цифры набранного номера и передаёт их в систему перехвата.

Система получает набранный номер от конечного офиса, извлекает соответствующую информацию из базы данных перехвата, формирует сообщение и воспроизводит его абоненту в виде автоматического объявления. Такие объявления могут быть стандартизированными или адаптированными под нужды независимых телефонных компаний. Если абоненту требуется дополнительная помощь, он может оставаться на линии и дождаться оператора.

Вызовы с ONI

Когда конечный офис устарел и не оснащён оборудованием ANI, к работе непосредственно подключаются операторы. Они также вступают в действие при сбоях в работе ANI или DAIS II.

При поступлении вызова ONI (Operator Number Identification) DAIS II направляет его оператору. Оператор спрашивает у абонента набранный номер и вводит его в KDT (Keyboard Display Terminal — терминал с клавиатурой и дисплеем). После нажатия командной клавиши система выполняет поиск информации о номере в базе данных перехвата, формирует сообщение и воспроизводит автоматический ответ. Если абоненту потребуется дополнительная помощь, оператор вновь выходит на линию.

Оператор может вернуться на линию по ряду причин:

Неудачный поиск (Unsuccessful Searches) — получив набранный номер от оборудования ANI или от оператора, DAIS II выполняет поиск в базе данных, чтобы найти соответствующее перехваченному вызову сообщение. База данных содержит все 10 000 номеров для каждой АТС в зоне обслуживания. Если поиск завершить не удаётся, значит, номер был введён неверно либо в системе возникла неисправность. Вызов переводится на оператора, а на экране KDT отображается перехваченный номер (включая код NPA) и сообщение о причине, по которой поиск не завершился. Если номер был введён с ошибкой, оператор исправляет его; в противном случае оператор просит абонента набрать номер повторно.

Прерванные объявления (Aborted Announcements) — если поиск прошёл успешно, но автоматическое объявление по какой-либо причине не может быть воспроизведено, вызов переводится на оператора. На экране KDT отображаются перехваченный номер, необходимые сведения для устного ответа и сообщение «VERBAL REPORT». В этом случае оператор зачитывает сообщение абоненту вместо того, чтобы запускать автоматический ответ.

Повторное подключение (Reconnects) — если абонент остаётся на линии для получения дополнительной информации после прослушивания автоматического объявления, система направляет вызов оператору. На экране KDT оператора отображается набранный номер и прочие сведения, уже сообщённые абоненту в предыдущем объявлении. Оператор может ответить устно или повторно активировать автоматическую систему. DAIS II допускает до 4 повторных подключений на один вызов, однако фактически доступное их число варьируется от 0 до 3. При одном подключении оператор обязан ответить устно.

Разделённые переадресации (Split Referrals) — если номер был изменён и заменён двумя новыми номерами, такая ситуация называется «разделённой переадресацией». При обнаружении в базе данных двух и более номеров DAIS II направляет абонента к оператору, отображая на экране KDT старый номер и новые варианты. Оператор уточняет, какой именно номер ищет абонент, и нажимает командную клавишу для запуска объявления либо сообщает информацию устно.

Поиск операторами

Могут возникать ситуации, когда абоненту требуется больше информации, чем было предоставлено автоматическим объявлением, или он считает полученные сведения недостоверными. DAIS II предоставляет операторам постоянный доступ к базам данных перехвата и справочной службы (DA), при условии что системный администратор, определяющий допустимый объём использования функции перекрёстного поиска, разрешает это.

Компоненты системы

Коммутаторы класса 5 (Class 5 End Offices) телефонных компаний содержат коммутационное оборудование, направляющее вызовы в DAIS II. Если офис оснащён оборудованием ANI, коммутатор передаёт набранные цифры в систему перехвата в виде многочастотных тональных сигналов (MF). Конечные офисы направляют вызовы в DAIS II по выделенным (прямым) соединительным линиям (трункам). Эти прямые транки могут обслуживать либо трафик ANI, либо трафик ONI, но не оба одновременно.

При использовании концентраторов транков транки от концентраторов к DAIS II могут обслуживать вызовы ANI, ONI или оба типа — в зависимости от типов транков, поступающих в концентраторы от конечных офисов. Тип вызова — ANI или ONI — определяется по MF-сигналам, передаваемым концентраторами.

Если требуется участие оператора (при ONI или необходимости дополнительной помощи), DAIS II направляет вызов на ACD (Automatic Call Distributor — автоматический распределитель вызовов) телефонной компании — коммутационное устройство, распределяющее вызовы между доступными операторами.

База данных перехвата хранится на диске в ARS (Audio Response System — система речевого ответа). Поиск в базе данных перехвата выполняют процессоры ARS, известные как Audio Response Controllers (ARC — контроллеры речевого ответа). Если для обработки вызова необходим оператор, блок Marker Decoder Unit (MDU) предоставляет ARC информацию о маршрутизации ACD.

Контроллеры AICC (DAIS II Automatic Intercept Communications Controllers) обеспечивают передачу сообщений между ARC и подсистемами DAIS II. Подсистема перехвата, размещённая в одном месте с базой данных, называется CAIS (Colocated Automated Intercept System — совмещённая автоматизированная система перехвата). Подсистема, удалённая от базы данных, именуется LAIS (Local Automated Intercept System — локальная автоматизированная система перехвата). Каждая подсистема способна воспроизводить автоматические объявления без использования дорогостоящих транков для маршрутизации ANI-вызовов в централизованный перехватывающий офис. Только вызовы, требующие участия оператора, направляются по транкам на узел ARS. Поскольку эти транки удерживаются лишь на время идентификации номера оператором и освобождаются до начала воспроизведения объявления, потребность в транках снижается. Автоматическое объявление всегда воспроизводится подсистемой перехвата.

На каждом узле CAIS или LAIS находятся Trunk Time Switch (TTS — временной коммутатор транков) и аудиоблоки DARU (DAIS II Audio Response Units). Транки перехвата от концентраторов и коммутаторов класса 5 оканчиваются на TTS. При поступлении ONI-вызова на один из этих транков TTS направляет его на ACD. При поступлении ANI-вызова TTS передаёт набранный номер в ARC. После того как ARC извлекает соответствующее сообщение из базы данных, он возвращает эту информацию в TTS, который подключает порт DARU к транку, на котором поступил вызов. Затем DARU воспроизводит автоматическое объявление и передаёт его абоненту. Аппаратура ARS генерирует исключительно объявления справочной службы (DA), тогда как аппаратура DAIS II — исключительно объявления о перехвате.

AICC обеспечивает маршрутизацию сообщений между ARC и TTS. Для повышения надёжности системы требуются два блока. Каждая пара AICC может взаимодействовать с четырьмя подсистемами CAIS или LAIS.

AICC схожи с контроллерами ACC (Audio Communications Controllers) в системе ARS, однако вместо LACIM используют модуль бисинхронной связи BSCM (Bisynchronous Communications Module).

Один AICC может оснащаться до 8 модулями BSCM, каждый из которых обслуживает одну синхронную линию связи до TTS. Выбор моделей BSCM зависит от расположения AICC относительно узлов CAIS/LAIS. Для связи с ARC используются стандартные модули SLIM (Subscriber Line Interface Modules).

Временной коммутатор транков (TTS)

TTS включает два типа компонентов: периферийные модули (PM) и общие блоки управления (CC).

Модуль PM содержит печатные платы, обеспечивающие связь между ANI-транками конечного офиса и ARC, а также между ONI-транками и ACD. Работой PM управляет блок CC.

Стойка PM содержит платы пяти типов: многочастотные приёмники (MFR), аналоговые интерфейсные блоки абонентских линий (ALFE), интерфейсы T1 (T1FE), контроллеры доступа к периферийным модулям (PMAC) и многофункциональные периферийные устройства (MPPD).

Приёмники MFR преобразуют перехваченный номер из многочастотных тональных сигналов в ASCII-цифры для ANI-вызовов; для ONI-вызовов, поступающих через концентратор транков, MFR декодируют сигналы концентратора, указывающие на тип вызова. На основании тональных сигналов MFR определяет тип вызова: обычный, аварийный и т. д.

Блоки ALFE преобразуют входящие аналоговые данные в цифровую форму для коммутации в цифровой сети, а также выполняют обратное преобразование — из цифровой в аналоговую — для исходящих сигналов. Входящие ALFE обеспечивают связь между TTS и аналоговыми транками от коммутаторов класса 5. Исходящие ALFE обеспечивают связь между TTS и аналоговыми транками к ACD.

ALFE подразделяются на два подтипа — для входящих и исходящих линий: ALFE-A (содержит логику управления, терминацию шины PCM и порты для 8 транков) и ALFE-B (содержит порты для 16 транков, но требует сопряжения с ALFE-A для использования логики управления и шины PCM на объединительной плате). ALFE-A может использоваться без ALFE-B, но не наоборот.

Входящие ALFE поддерживают сигнализацию E&M 2-wire, E&M 4-wire, reverse battery и 3-way. Исходящие ALFE поддерживают сигнализацию E&M 2-wire, reverse battery и high-low.

Интерфейсы T1FE обеспечивают связь между TTS и потоками T1 типа D3 от конечных офисов, а также связь между портами платы VOCAL блока DARU и TTS. Каждая плата имеет 24 порта для обработки одного потока T1, несущего 24 голосовых канала.

Контроллер PMAC построен на базе микропроцессора Motorola 68000 и управляет потоками данных внутри PM, координируя их.

Платы MPPD обеспечивают терминацию шины и системные тактовые сигналы для цифровой сети. Модуль MPPD содержит главные и резервные тактовые генераторы, синхронизированные с частотой входящего потока T-1, а также собственный генератор для работы в случае отсутствия или потери синхронизации T-1.

Помимо этого, MPPD формирует сигналы вызова, сигнал «занято» и сигналы переадресации, слышимые абонентом, а также отправляет zip-сигнал (предупреждающий) оператору.

Блок CC управляет взаимодействием компонентов PM и DARU. Он содержит ODDB (Office Dependent Data Base — база данных конфигурации офиса) — системную таблицу, описывающую конфигурацию TTS. CC использует ODDB для определения типа входящего транка: ANI или ONI.

CC устанавливает пути в цифровой сети для координации ресурсов CAIS/LAIS. Он получает сообщения от PMAC, хранит информацию, необходимую для возврата ответа на нужный транк, и управляет маршрутизацией сообщений к ARC или оператору и от них. Он также синхронизирует TTS с Directory Assistance System (DAS — система справочного обслуживания) для обеспечения связи оператора с абонентом.

CC является автономным процессором серии Power, содержащим центральный процессор CPU-2 на основе микропроцессора Motorola 68000. Процессор также оснащён распределённой логикой управления памятью, подсистемой ввода-вывода и подсистемой дисков и лент. Каждый блок CC включает жёсткий диск Winchester, накопитель на четвертьдюймовой ленте и дополнительное вспомогательное оборудование.

Аудиоблок DAIS II (DARU)

DARU содержит платы VOCAL, воспроизводящие автоматические объявления, синтезируемые из словаря, хранящегося в ОЗУ. Узел CAIS/LAIS содержит от 1 до 3 блоков DARU, каждый с 48 портами.

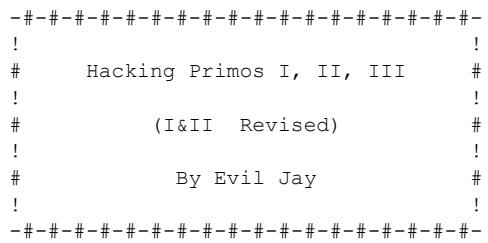
Если в узле CAIS/LAIS установлено более одного DARU, блоки объединяются в цепочку (multi-drop). Один DARU всегда связан с ARC (непосредственно или через модемы и телефонные линии), чтобы при необходимости можно было загрузить словарь объявлений из ARC.

:=:

Значительная часть информации в этом файле скопирована дословно из учебного буклета, присланного мне компанией CCI. Их документация чрезвычайно подробна и хорошо написана, а при внимательном прочтении вполне доступна для понимания. Многие сведения поначалу кажутся запутанными из-за обилия аббревиатур и технических терминов, однако если последовательно раскрывать аббревиатуры по всему тексту, можно разобраться в их значении. Если что-то остаётся непонятным, попробуйте рассмотреть это в контексте использования телефонной компанией — как правило, назначение и функция устройства или понятия становятся очевидными. Надеюсь, этот файл оказался вам полезным, и вы продолжите читать материалы Phrack Inc., чтобы глубже понять систему, которой мы пользуемся и с которой сталкиваемся в повседневной жизни. Конструктивные замечания и предложения приветствуются — как напрямую, так и иными способами.

Taran King

Взлом Prime-систем, части I, II, III (I и II — исправленные)



Автор: Evil Jay

Примечание автора

Чёрт! Я посмотрел на свой первый файл после его выхода и обнаружил массу опечаток, ошибок и прочих косяков — мне было жутко стыдно. У меня не было времени его отредактировать, а параллельно я писал второй файл — про получение привилегий. Я отдал оба файла Taran King'y, который объединил их в один. Поэтому я смиренно прошу прощения за все ошибки в том файле. В этом файле я переработаю старый материал и добавлю ещё несколько способов получить доступ, а заодно приведу список самых базовых команд для начинающих. Как я и говорил раньше, если есть вопросы — ищите меня на любой борде, где я сейчас обитаю. Рад буду услышать от вас.

Получение доступа с нуля

В прошлом файле я допустил ошибку, написав, что FAM не является значением по умолчанию. FAM — это значение по умолчанию, однако системные администраторы могут его отключить.

Чтобы получить список всех возможных учётных записей в системе, всё очень просто. Они находятся в каталогах MFD. Введите:

```
A MFD <MFD #>  (без угловых скобок)
```

Или просто:

```
A MFD
```

Затем введите `LD` и нажмите Enter. Вы увидите список файлов, а ниже — список каталогов с соответствующим заголовком «Directories». Эти каталоги и есть допустимые пользовательские идентификаторы. Однако, судя по всему, в каталоги, содержащие символ `*`, войти нельзя.

Получение более высокого доступа — исправленный вариант

SYS1 — это наивысший системный уровень. Это означает, что если только команды не требуется вводить с терминала супервизора, с учётной записью, имеющей доступ SYS1, обычно можно

делать что угодно. Также уточню: наивысший уровень доступа не обязательно будет называться SYS1 — он может называться SYSTEM или как-то иначе.

Вам нужен файл с расширением `.CPL` — ищите его в любом из каталогов SYS1. Когда найдёте, выполните `SLIST` для этого файла. Ищите строку вида:

```
A <ИМЯ КАТАЛОГА> <ПАРОЛЬ>
```

Например:

```
A LIB XXX
```

`LIB` — это имя каталога (пользовательский идентификатор).

`XXX` — пароль к этому каталогу (пользовательскому идентификатору).

Получив эти данные, войдите в систему с именем каталога и паролем. Если повезёт, вы получите доступ к этой учётной записи. Я заметил, что у многих высокоуровневых учётных записей иногда стоит пароль `XXXXXX` или `X`. Попробуйте — я не уверен, являются ли они реальными паролями по умолчанию или нет.

Ладно, с правками покончено! Теперь ещё несколько способов получить доступ...

Троянский конь

Если у вас уже есть доступ, вы можете, а можете и не иметь возможности редактировать файл в каталоге с высоким уровнем доступа. Если не получается — попробуйте описанный выше метод и постарайтесь взломать учётную запись более высокого уровня.

Для начала вам нужно изучить Command Processing Language (CPL). Введите `HELP CPL`, чтобы получить список команд, а затем экспериментируйте и попробуйте написать собственные программы. Если под рукой нет мануала — посмотрите на другие CPL-программы в каталогах, к которым у вас есть доступ. Освоив CPL, вам достаточно отредактировать CPL-файл в каталоге с высоким уровнем доступа. Добавьте в программу свои команды высокого уровня. Затем замените старый файл, разлогиньтесь и ждите, пока операторы не решат запустить вашу программу. Надеюсь, если всё пойдёт хорошо, ваши процедуры помогут вам добиться желаемого. Тем не менее было бы неплохо, чтобы ваш «троян» записывал в ваш каталог файл, который сообщал бы, был ли он запущен. Различным видам троянских коней я посвящу отдельные материалы в следующих выпусках Phrack.

Оказавшись на Prime-системе, получить другие учётные записи довольно просто, так что не переживайте об этом. Просто беспокойтесь о том, как попасть туда в первую очередь. Терпение здесь абсолютно необходимо, поскольку многие системы (особенно версии 19 и выше) имеют тенденцию обрывать соединение после первой неверной пары идентификатор/пароль.

Основные команды для начинающих

Ниже приведён список базовых команд, которые можно использовать, оказавшись в Prime-системе. Я не буду подробно описывать каждую команду — вы сами сможете это сделать, введя:

```
HELP <ИМЯ КОМАНДЫ>
```

```
SLIST <FILENAME>
```

Выводит содержимое файла в каталоге. Введите полное имя файла (вместе с расширением).

```
ATTACH <DIRECTORY NAME>
```

Подключает вас к другому каталогу. Для подробного описания введите `HELP ATTACH`.

```
LD
```

Выводит список всех файлов и подкаталогов в каталоге.

```
RLS -ALL
```

Команды накапливаются в стеке, и после заранее определённого их количества вы получите сообщение о том, что «находитесь на уровне команд XX». Эта команда освобождает все накопившиеся команды из стека.

```
CPL <FILENAME>
```

Запускает файл с расширением `.CPL`.

```
COMINPUT <FILENAME>
```

Запускает файл с расширением `.COM`.

```
SEG <FILENAME>
```

Запускает файл с расширением `.SEG`.

```
STATUS USERS
```

Выводит список пользователей и другую информацию о текущих подключениях к системе.

```
STATUS
```

Выводит состояние системы и другую информацию.

```
EDIT  (или ED)
```

Текстовый редактор.

```
CHANGE_PASSWORD <OLD PASSWORD>
```

Делает именно то, что написано.

```
DELETE <FILENAME>
```

Удаляет файл.

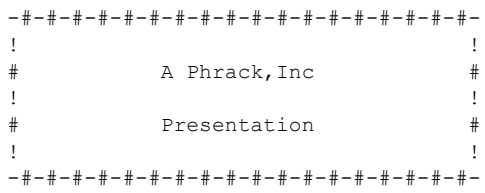
```
LOGOFF
```

Думаю, это и так очевидно.

```
LOGIN
```

Выводит вас из системы и возвращает к процессу входа — при условии, что администраторы не запретили вложенные входы.

Это очень небольшой список, но он, вероятно, сильно поможет начинающему, когда он впервые зайдёт в систему. Надеюсь, этот выпуск вам понравился... Ждите «Взлом Prime-систем, часть IV» в Phrack № 12. Возможно.



Методы телефонной сигнализации

Автор: Doom Prophet

Этот файл объясняет основные методы сигнализации, используемые в телефонной системе, и предназначен для общего понимания. Приведённый ниже текст не является высокотехническим, поскольку файл рассчитан на базовое понимание и адресован менее опытным фрикам. Тем не менее более опытные читатели могут воспользоваться им как обзором материала.

Аналоговый сигнал

Аналоговые сигналы — это сигналы с непрерывно и плавно изменяющейся амплитудой или частотой. Речевые сигналы относятся именно к этому типу, если принять во внимание тон, высоту и уровень громкости, меняющиеся в зависимости от говорящего. Когда человек говорит в микрофон телефона, голосовые сигналы состоят из акустической энергии, которая затем преобразуется в электрическую для передачи по линии связи.

Аналоговые несущие средства передачи могут работать через различные среды: воздушные провода, многопроводные кабели, коаксиальные кабели или волоконно-оптические кабели. Медный провод наиболее широко применяется в абонентских шлейфах.

Техника, позволяющая передавать множество сигналов по одному и тому же тракту передачи, называется мультиплексированием. Аналоговые сигналы используют частотное разделение каналов — FDM (Frequency Division Multiplexing).

Цифровой сигнал

Вместо того чтобы обрабатывать голосовой сигнал как аналоговый, он преобразуется в цифровой и на всём протяжении процесса передачи обрабатывается цифровыми схемами. Когда сигнал достигает АТС, обслуживающей вызываемый телефон, он обратно преобразуется в аналоговый для воспроизведения исходной голосовой передачи.

Импульсно-кодовая модуляция (ИКМ, или PCM — Pulse Code Modulation) — это когда двоичный сигнал передаётся в последовательной форме. Двоичное кодирование представляет биты или двоичные разряды на уровнях 0 и 1. Эти уровни имеют строго определённые временны́е отношения друг с другом. Временно́е разделение каналов — TDM (Time Division Multiplexing), иногда сокращаемое как MUX, — это тип мультиплексирования, применяемый при цифровой передаче.

Металлический канал

Металлические средства передачи несут только один канал голосовой частоты (VF — Voice Frequency). Как правило, металлический канал используется для подключения деловых или жилых линий к АТС. Коаксиальный кабель может применяться для передачи как аналоговых и цифровых,

так и металлических сигналов.

Полоса пропускания VF-каналов составляет 4000 Гц — от 0 до 4000 Гц. Однако внутриполосный диапазон голосовой частоты находится между 200 и 3400 Гц. Сигналы, выходящие за пределы этого диапазона частот, но всё ещё остающиеся внутри VF-канала, являются внеполосными сигналами. Внеполосный эквивалент тона 2600 Гц составляет 3700 Гц. Количество VF-каналов варьируется в зависимости от используемых средств передачи.

CCIS — общеканальная межстанционная сигнализация

CCIS (Common Channel Interoffice Signalling) — система, в которой управляющие или супервизорные сигналы передаются по отдельному каналу данных между коммутационными узлами. Каналы CCIS работают на скорости 4800 бит/с (бод). Точки транзита сигнальной информации (Signal Transfer Points) в коммутаторе передают супервизорную информацию по выделенному каналу. Это не позволяет супервизорным тонам с абонентских станций регистрироваться в телефонной сети как изменение состояния транка.

Сигнализация с переполюсовкой батареи (Reverse Battery Signalling)

Когда вызываемый абонент отвечает, полярность и состояние проводников Ring и Tip инвертируются, чтобы указать состояние соединения. Условия для вызова, который ещё не принят: земля на Tip и батарея (ток батареи АТС протекает через линию) на Ring. Когда вызываемый абонент отвечает, реле коммутационного оборудования изменяют направление тока в шлейфе вызывающего абонента: батарея подаётся на Tip, а земля — на Ring; это состояние сохраняется на протяжении всего разговора.

Провода E и M

Провода, соединяющие коммутационное оборудование с транковыми схемами, называются E и M — от «receive» (приём) и «transmit» (передача). Провод E отражает состояние дальнего или терминирующего конца транка. Земля на проводе E указывает, что сигнал получен с другого конца; провод E разомкнут, когда транк свободен. Провод M отражает состояние ближнего конца транка: он заземлён, когда транк свободен, и переходит в состояние батареи, когда вызываемый абонент снимает трубку. Этот метод сигнализации используется на длинных межстанционных и коротких платных транковых соединениях.

Следует отметить, что AC-сигнализация — это сигнализация переменным током; она используется в межтерминальной сети, на межстанционных и коротких платных транках. DC (постоянный ток) применяется на двухпроводных или внутристанционных соединениях, а также на местных межстанционных транках.

Однотональная сигнализация (SF — Single Frequency)

Однотональная сигнализация — это внутриполосная система сигнализации на частоте 2600 Гц. Когда четырёхпроводный транк свободен и оснащён внутриполосной SF-сигнализацией, тон 2600 Гц передаётся в обоих направлениях. Когда транк захватывается на исходящей стороне, провод M переходит из состояния земли в состояние батареи. Это убирает супервизорный тон 2600 Гц с исходящей пары. Потеря 2600 Гц обнаруживается на дальнем конце блоком SF-сигнализации, который переводит провод E дальнего конца из разомкнутого состояния в заземлённое, заставляя коммутационное оборудование реагировать. Когда на провод M ближнего конца снова подаётся земля (восстанавливая тон 2600), начинается импульсная передача адресной информации.

Многотональная сигнализация (MF — Multi-Frequency)

Метод MF-импульсации использует сигналы переменного тока в диапазоне голосовых частот и передаёт адресную информацию между АТС комбинациями из 2 из 5 возможных частот. MF применяется для отправки адресной информации, как упоминалось ранее. Для управления транком и супервизии по-прежнему требуются другие методы сигнализации. Существует шесть MF-частот, составляющих MF-коды. Они расположены с интервалом в 200 Гц в диапазоне 700–1700 Гц. Одновременно передаются две частоты — отсюда и термин «многотональный».

MF-импульсация инициируется ручными клавиатурными устройствами, коммутатором TSPS или MF-исходящими отправителями в ESS и Xbar. MF-импульсация очень быстрая и происходит только в момент установления соединения. KP (Key Pulses — ключевые импульсы) используются как сигнал начала MF-импульсации. ST (STart tones — стартовые тона) используются как сигнал окончания MF-импульсации.

В качестве примера MF-сигнализации рассмотрим платный транк коммутатора, подключённый к АТС типа Xbar. Оператор выбирает свободный транк и нажимает кнопку KP на клавиатуре, сигнализируя удалённому отправителю или оборудованию регистровой связи подключиться к MF-приёмнику. Лампа S на клавиатуре загорается, когда дальний конец готов принимать MF-импульсы. После набора цифр вызываемого номера оператор нажимает кнопку ST, что сигнализирует об окончании импульсации, отключает клавиатуру от шнурового тракта оператора и гасит лампы KP и S.

На терминирующей АТС два MF-тона каждой цифры усиливаются и ограничиваются в блоке MF-приёмника, связанного со входящим отправителем и регистровой схемой. Частоты выделяются канальными фильтрами MF-приёмника и затем детектируются. Возникающее постоянное напряжение срабатывает соответствующие канальные реле для продолжения процесса установления вызова.

ЭЛЕКТРОННЫЙ СЕРИЙНЫЙ НОМЕР: СОТОВОЕ «СИТО»?

Перепечатано из ноябрьского выпуска журнала Personal Communications Technology за 1985 год с разрешения авторов и издателя — FutureComm Publications Inc., 4005 Williamsburg Ct., Fairfax, VA 22032, 703/352-1200.

«СПУФЕРЫ» МОГУТ ОБМАНЫВАТЬ ПОЛЬЗОВАТЕЛЕЙ И ОПЕРАТОРОВ

Автор: Geoffrey S. Goodfellow, Robert N. Jesse и Andrew H. Lamothe, Jr.

В чём заключается главная проблема безопасности сотовых телефонов? Может быть, в конфиденциальности переговоров? Нет.

Несмотря на то что конфиденциальность вызывает определённые опасения, она меркнет на фоне куда более серьёзной угрозы — спуфинга.

«Спуфинг» — это процесс, при котором некий агент («спуфер») выдаёт себя за другого человека, предъявляя ложные данные, как правило с целью мошенничества. Этот обман невозможно предотвратить в рамках действующих американских стандартов сотовой связи, и он способен породить серьёзные проблемы — если только отрасль не примет меры по устранению существующих лазеек.

По сравнению со спуфингом привычная проблема конфиденциальности выглядит не столь опасной. В худшем случае большинство сотовых абонентов просто рассердятся, узнав, что их разговоры были прослушаны. Меньшая часть пользователей действительно может пострадать в деловом или личном плане, если их конфиденциальные переговоры окажутся скомпрометированы. Для них оборудование голосового шифрования становится всё более доступным — при условии готовности платить за него.

Таким образом, несмотря на то что технологии для защиты чувствительных переговоров от прослушивания уже существуют, сотовые системы не могут — ни при каких затратах — помешать злоумышленникам тарифицировать звонки на чужие счета. Эта проблема для отрасли не нова. Хотя сотовая связь представляет собой современную высококачественную мобильную услугу, в фундаментальном плане она ненамного безопаснее более старых форм мобильной телефонии.

История уязвимости к спуфингу

Самая ранняя форма мобильной телефонии — ручная Мобильная Телефонная Служба (MTS) без шумоподавления — была уязвима для перехвата и прослушивания. Чтобы совершить звонок, пользователь прослушивал эфир в поиске свободного канала. Найдя его, он нажимал кнопку микрофона и запрашивал соединение: «Оператор, говорит Мобильный 1234, соедините меня, пожалуйста, с 555-7890». Оператор записывал звонок на счёт номера 1234 — и это же мог сделать любой другой, кто слушал канал, что открывало возможность для спуфинга и мошенничества.

MTS со шумоподавлением лишь незначительно скрывала проблему: в обычных условиях пользователи не слышали чужих переговоров. Однако мошенничество оставалось простым делом для тех, кто ненадолго отключал шумоподавление, чтобы подслушать чужой номер счёта.

Сервисы мобильной телефонии с прямым набором, такие как Улучшенная Мобильная Телефонная Служба (IMTS), несколько усложнили задачу: идентификация абонента осуществлялась автоматически, а не путём голосового обмена с оператором. При каждом исходящем вызове мобильный телефон передавал свой идентификационный номер на обслуживающую базовую станцию с помощью той или иной разновидности частотной манипуляции в звуковом диапазоне (AFSK) — что было уже не так просто перехватить и расшифровать.

Для совершения мошенничества в системе IMTS требовалась модификация мобильного устройства — перестановка перемычек в радиоблоке или использование специальных комбинаций клавиш на более поздних аппаратах — с целью перепрограммирования устройства на передачу несанкционированного идентификационного номера. На некоторых пультах управления мобильными устройствами даже устанавливались удобные переключатели-роллеры, облегчавшие частую смену ANI (Автоматической Идентификации Номера).

Эволюция сотовой связи

Сотовая связь претерпела значительные изменения по сравнению с предшественниками. Сигнализация между мобильными устройствами и базовыми станциями использует высокоскоростные цифровые методы и включает множество различных типов цифровых сообщений. Как и прежде, сотовый телефон содержит собственный Мобильный Идентификационный Номер (MIN), который программируется продавцом или сервисным центром и может быть изменён, например при продаже телефона новому пользователю. Помимо этого, американский стандарт сотовой связи предусматривает второй номер — «Электронный Серийный Номер» (ESN), призванный уникально и навсегда идентифицировать мобильное устройство.

Согласно Промежуточному Стандарту IS-3-B Ассоциации электронной промышленности (EIA), Спецификация совместимости сотовых мобильных и базовых станций (июль 1984 г.): «Серийный номер представляет собой 32-битное двоичное число, уникально идентифицирующее мобильную станцию в любой сотовой системе. Он должен быть установлен на заводе и не подлежать лёгкому изменению в полевых условиях. Схема, обеспечивающая серийный номер, должна быть защищена от несанкционированного доступа и вмешательства. Попытки изменить схему серийного номера должны приводить мобильную станцию в нерабочее состояние».

ESN был призван решить две проблемы, которые отрасль наблюдала в более старых системах.

Во-первых, число абонентов, которых могли обслуживать старые системы, во многих регионах существенно уступало спросу, что побуждало группы пользователей совместно использовать один мобильный номер (мошеннически), настраивая несколько телефонов на передачу одного и того же идентификатора. Операторы утрачивали возможность индивидуального учёта пользователей и прогнозирования и контроля трафика в своих сетях.

Во-вторых, системы не имели возможности автоматически обнаруживать использование похищенного оборудования, поскольку злоумышленники могли легко изменить передаваемый идентификатор.

Теоретически обязательные свойства ESN позволяют сотовым системам проверять, что конкретный MIN использует только зарегистрированное устройство, а ESN похищенных аппаратов могут быть навсегда заблокированы (внесены в «чёрный список»). Это улучшение по сравнению со старыми системами, однако уязвимости сохраняются.

Лёгкость подделки ESN

Хотя концепция неизменяемого ESN заслуживает похвалы в теории, на практике в ней обнаруживаются слабые места. Многие сотовые телефоны сконструированы так, что «попытки изменить схему серийного номера» вовсе не приводят мобильную станцию в нерабочее состояние. Мы лично наблюдали, как в одном из аппаратов без каких-либо затруднений заменяли чип ESN — после чего устройство продолжало безупречно работать.

Где можно достать чипы ESN для такой замены? Нам известен один недавний случай в районе Вашингтона, округ Колумбия, когда ESN был «куплен» у сотрудника местного сервисного центра в обмен на полграмма кокаина. В довершение ко всему большинство производителей используют для хранения ESN стандартные микросхемы постоянной памяти (ROM), которые легко приобрести, запрограммировать или скопировать.

Аналогичным образом — в духе исследования — один западный сотовый оператор скопировал ESN с устройства одного производителя на другое устройство того же типа и модели, создав тем самым два аппарата с абсолютно одинаковыми идентификаторами.

Доска объявлений ESN

Для многих телефонов чипы ESN легко достать, запрограммировать и установить. Но откуда потенциальный мошенник узнает, какие номера использовать? Следует помнить: чтобы получить обслуживание в системе, сотовое устройство должно передать действительный MIN (телефонный номер) и, как правило, соответствующий серийный номер, хранящийся в базе данных сотового коммутатора.

При наличии нужного оборудования пару ESN/MIN можно снять прямо из эфира, поскольку мобильное устройство передаёт её при каждом исходящем вызове. Сервисные центры способны перехватывать эту информацию с помощью тестового оборудования, автоматически принимающего и декодирующего сигналы на обратных каналах — от мобильного к базовой станции.

Сервисные центры хранят в своих файлах записи ESN/MIN по проданным и обслуживаемым устройствам, а у операторов такие данные имеются по всем абонентам. Нечестные на руку сотрудники могут поставить под угрозу безопасность телефонов своих клиентов.

По всей видимости, «торговля» скомпрометированными парами ESN/MIN будет во многом напоминать то, что сегодня происходит в сфере дальней телефонии с номерами кредитных карт AT&T и кодами счетов альтернативных операторов дальней связи (таких как MCI, Sprint и Alltel). Коды передаются среди знакомых, публикуются на компьютерных «досках объявлений» и становятся товаром для профессиональных преступных структур.

Пользователи, на чьи счета совершается мошенничество, в конце концов могут — а могут и не — заметить счета, превышающие ожидаемые, и после жалобы оператору получить новые номера. Однако, как и в сфере дальней телефонии, эта «ротация» номеров (деактивация) не будет происходить достаточно быстро, чтобы сделать злоупотребление невыгодным. Поймать пиратов с поличным будет ещё сложнее, чем в проводной телефонии, — из-за присущей мобильной радиосвязи мобильности.

Компьютерные энтузиасты и любители электроники — люди смекалистые. Зачем мошеннику, ворующему сотовый трафик, «прожигать ПЗУ» и возиться с железом только ради установки новых идентификаторов в телефон? Никаких геркулесовых технологий не требуется, чтобы «хакнуть» телефон и обеспечить программирование ESN/MIN с клавиатуры — примерно как роллерные переключатели на IMTS-телефонах, описанные выше.

Те, кто не столь подкован технически, вероятно, смогут воспользоваться услугами предприимчивых продавцов по почте, которые будут предлагать наборы для модификации сотовых телефонов в мошеннических целях — примерно как сегодня некоторые продают оборудование для телефонного мошенничества и декодеры платного телевидения.

По меньшей мере один производитель уже предлагает устройства с программируемыми с клавиатуры номерами MIN. Хотя эта возможность предназначена исключительно для удобства дилеров и сервисных центров и потому не описана в пользовательской документации, осведомлённые и/или настойчивые конечные пользователи, скорее всего, узнают нужные комбинации. Разумеется, это не позволяет изменить ESN, однако лёгкая перепрограммируемость MIN сама по себе создаёт огромную брешь в современных условиях роуминга.

«Роллс-Ройсом» этого порочного увлечения мог бы стать некий «Cellular Cache-Box» («сотовый кэш-бокс»). Он мониторил бы обратные каналы установки соединения и перехватывал пары ESN/MIN из эфира, сохраняя список в памяти. Его владелец звонил бы, как с обычного сотового телефона. Cache-Box автоматически выбирал бы пару ESN/MIN из своего каталога, использовал её один раз и затем удалял, распределяя мошенничество по многим счетам. Ни клиент, ни оператор вряд ли смогли бы обнаружить злоупотребление — а тем более поймать виновного.

Как показывает история компьютерной отрасли, нет ничего невероятного в том, что стремительный рост телекоммуникаций и сотовой связи сделает оборудование доступным для широкого круга экспериментаторов. Уже сегодня на рынке подержанных товаров появляются сотовые телефоны первого поколения, а новые аппараты во многих регионах можно купить менее чем за 1000 долларов.

Каков масштаб потерь?

Абонентов, на счета которых приходят мошеннические начисления, конечно, нельзя обязать их оплачивать. Во что обойдётся мошенничество оператору? Если речь идёт только о плате за эфирное время в домашней сети, предельные затраты оператора на предоставление этой услуги не столь высоки, как в случае с оплатой дальних переговоров. При дальних переговорах оператор несёт прямые денежные потери. Ситуация наиболее тяжёлая, когда спуфер выдаёт себя за роумингового пользователя. По большинству действующих на сегодняшний день межоператорных роуминговых соглашений ответственность за расходы несёт домашний оператор пользователя (реального или подделанного), который оказывается должен живые деньги за дальние переговоры и эфирное время.

Мы не пытались прогнозировать денежные потери от этих махинаций, поскольку фактических данных недостаточно для ответственного предположения. Ознакомление с нынешними оценками мошенничества при дальних переговорах должно убедить скептиков в серьёзности угрозы.

Решения

Описанные нами проблемы относятся в основном к двум типам. Во-первых, схема ESN в большинстве современных мобильных устройств не является защищённой от вмешательства — и уж тем более не является абсолютно защищённой. Во-вторых, что важнее, решительный злоумышленник имеет полный доступ ко всей информации, необходимой для спуфинга, просто прослушивая радиоизлучения реальных мобильных устройств, поскольку идентификационные данные (ESN/MIN) не шифруются и остаются неизменными при каждой передаче.

Производители могут смягчить первую проблему, создавая мобильные устройства, более реалистично соответствующие процитированным выше требованиям EIA. Вторая проблема также решаема с помощью существующих технологий. Хорошо известные методы шифрования позволили бы мобильным устройствам идентифицировать себя в обслуживающей сотовой системе, не передавая при этом каждый раз один и тот же цифровой поток. В рамках такой схемы злоумышленник, перехвативший одну передачу, не смог бы просто ретранслировать тот же шаблон и добиться его повторного принятия.

Дополнительным преимуществом шифрования стала бы разумная защита сведений о связи — цифровой части каждой транзакции, идентифицирующей, кто кому и когда звонит.

Недостаток любого подобного решения состоит в том, что оно требует определённой доработки Спецификации совместимости мобильных и базовых станций, а значит — нового программного или аппаратного обеспечения как для мобильных устройств, так и для базовых станций. Сложная логистика разработки нового стандарта, его внедрения и максимально возможной адаптации существующего оборудования представляет серьёзное препятствие, усугублённое необходимостью продолжать поддерживать незашифрованный протокол в переходный период — возможно, бессрочно.

Тем не менее необходимость решения этой проблемы станет очевидной. Хотя на сегодняшний день нам не известно ни одного задокументированного случая сотового мошенничества, уязвимость действующих стандартов и опыт работы с аналогичными технологиями позволяют нам утверждать: оно неизбежно. Промедление с принятием решительных мер обернётся для отрасли куда более дорогостоящей дилеммой. XXX

Geoffrey S. Goodfellow — старший научный сотрудник Лаборатории компьютерных наук в SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025, 415/859-3098. Специалист в области компьютерной безопасности и сетевых технологий, активный участник процессов стандартизации в сотовой отрасли. Давал показания в Конгрессе по вопросам безопасности и конфиденциальности в телекоммуникациях, является соавтором книги о культуре компьютерного «хакинга».

Robert N. Jesse (2221 Saint Paul St., Baltimore, MD 21218, 301/243-8133) — независимый консультант, специализирующийся в области безопасности и конфиденциальности, операционных систем, телекоммуникаций и технологического менеджмента. Активный участник процессов сотовой стандартизации. Ранее — старший сотрудник Университета Джонса Хопкинса, где получил степень BES/EE.

Andrew H. Lamothe, Jr. — исполнительный вице-президент по инженерным вопросам в Cellular Radio Corporation, 8619 Westwood Center Dr., Vienna, VA 22180, 703/893-2680. Сыграл ключевую роль в международном развитии сотовых технологий. До прихода в American TeleServices десять лет проработал в Motorola, где проектировал и вводил в эксплуатацию опытную сотовую систему для района Балтимор/Вашингтон, ныне управляемую компанией Cellular One.

Более поздняя заметка указывает, что один из операторов может терять порядка 180 000 долларов в месяц...

Верификация занятой линии

Автор: Phantom Phreaker

Этот файл описывает, как оператор TSPS выполняет BLV (Busy Line Verification — верификацию занятой линии) и EMER INT (Emergency Interrupt — экстренное прерывание) на занятой линии по запросу абонента, желающего «вклиниться» в разговор. Я написал этот файл в надежде развеять все заблуждения относительно верификации занятой линии и экстренных прерываний.

BLV — это «верификация занятой линии» (Busy Line Verification), то есть определение того, занята линия или нет. BLV — телефонный термин, однако это явление также называют Verification, Autoverify, Emergency Interrupt, «вклиниться в линию», REMOB и другими именами. BLV реализуется на базе TSPS, использующей систему управления на основе хранимых программ (Stored Program Control System, SPCS) под названием Generic 9. До появления TSPS в 1969 году процедуру верификации выполняли операторы ручных коммутаторов. Внедрение BLV через TSPS повлекло за собой усиление защитных функций операторских систем. Аппаратное и программное обеспечение Generic 9 SPCS было впервые введено в эксплуатацию в Тусоне, Дейтоне и Колумбусе (Огайо) в 1979 году. К настоящему времени практически каждая TSPS работает по программе Generic 9.

Фактическую верификацию выполняет оператор TSPS. Предположим, абонент A находится в зоне кода 815, а абонент B — в зоне кода 314. A набирает 0, чтобы дозвониться до TSPS своей зоны кода — 815. Затем A сообщает оператору о желании произвести экстренное прерывание на номер B: 314+555+1000. Оператор TSPS зоны 815, принявшая вызов A, не может выполнить прерывание вне своей зоны обслуживания, поэтому она звонит оператору Inward для зоны кода 314 по схеме KP+314+TTC+121+ST, где TTC — код транзитного toll-центра, обязательный в ряде районов. Таким образом, TSPS зоны 815 соединяется с оператором TSPS зоны 314, однако индикатор на консоли последней сообщает ей, что вызов поступает по маршруту Inward. Оператор зоны 815 сообщает, что ей нужно экстренное прерывание на 314+555+1000, и называет имя своего абонента — например, Дж. Смит. После этого оператор Inward зоны 314 (которая по сути тоже является TSPS) набирает номер B обычным способом — Operator Direct Distance Dialing (ODDD). Если линия не занята, оператор Inward зоны 314 сообщает об этом TSPS зоны 815, а та в свою очередь информирует абонента A, что линия 314+555+1000 свободна и он может позвонить обычным образом. Если же запрошенная линия (в нашем случае 314+555+1000) занята, происходит следующее и начинается процедура BLV и EMER INT. Оператор Inward зоны 314 захватывает верификационный транк (BLV trunk) до toll-офиса, обслуживающего местную петлю запрашиваемого номера (555+1000). При этом ещё одна функция TSPS сверяет запрошенный номер со списком линий, недоступных для верификации, — таких как радиостанции, полиция и т. д. Если номер абонента находится в этом списке, верификация невозможна и оператор сообщает об этом клиенту.

Далее оператор нажимает клавишу VFY (VeriFY) на консоли TSPS, и оборудование выдаёт в BLV-транк последовательность KP+0XX+PRE+SUFF+ST. Здесь KP — Key Pulse (ключевой импульс); 0XX — «защитный код», предотвращающий перекрёстное подключение транков; PRE — префикс запрашиваемого номера (555); SUFF — суффикс запрашиваемого номера (1000); ST — STart (старт), сигнализирующий верификационному транку об окончании передачи MF-цифр. Защитный код существует для того, чтобы обычный транк сети toll (используемый в обычных звонках) случайно не подключился к верификационному транку. Если бы такого кода не было и перекрёстное подключение произошло, кто-нибудь, звоня другу в том же зоне кода, мог бы неожиданно оказаться в середине чужого разговора. Однако верификационный транк ожидает

последовательность 0XX, тогда как обычный вызов через toll-транк не начинается с 0XX.

(Пример: вы живёте по номеру 914+555+1000 и хотите позвонить на 914+666+0000. Маршрутизация вашего вызова будет выглядеть как KP+666+0000+ST. BLV-транк не может принять 666 вместо правильного префикса 0XX, и поэтому выдаст звонящему сигнал занятости/перегрузки.)

Также следует отметить, что последовательность, выдаваемая в BLV-транк, не может содержать код зоны. Именно поэтому, если абонент запрашивает прерывание в другой зоне кода (NPA), оператор TSPS обязана обратиться к оператору Inward той зоны, который имеет возможность выдать сигнал в нужный транк. Попытка TSPS зоны 815 выполнить прерывание на транке зоны 314 окончится неудачей. Это доказывает, что для каждой NPA существует собственная BLV-сеть: получив доступ к BLV-транку, вы сможете использовать его только для прерываний внутри той NPA, в которой этот транк расположен.

BLV-транки «охотятся» за нужными транками до нужного коммутатора End Office класса 5, обслуживающего данную местную петлю. Одна и та же последовательность передаётся по BLV-транкам до тех пор, пока не будет найден BLV-транк, обслуживающий toll-офис, к которому относится нужный End Office.

Как правило, предусмотрен один BLV-транк на 10 000 линий (то есть на один телефонный район). Таким образом, если toll-офис обслуживает десять End Office, он обслуживает 100 000 местных петель и имеет 10 BLV-транков, ведущих от TSPS к этому toll-офису.

Нажав клавишу VFY, оператор может слышать, что происходит на линии (модемный сигнал, голос или постоянный сигнал, свидетельствующий о снятой трубке), и предпринимать соответствующие действия. Впрочем, слышимость не абсолютная: схема подавления речи внутри операторской консоли вносит шум в линию, пока оператор выполняет VFY. Этот шум призван не позволять операторам подслушивать чужие разговоры, однако он не настолько силён, чтобы помешать оператору определить, идёт ли разговор, присутствует ли модемный сигнал или тональный сигнал. Если оператор слышит постоянный сигнал, она может лишь сообщить абоненту, что телефон снят с рычага или на линии неисправность, и ничего с этим не поделать. В случае абонентов A и B оператор Inward зоны 314 сообщает об этом TSPS зоны 815, а та — клиенту. Если на линии идёт разговор, оператор нажимает клавишу EMER INT (EMERgency INTerrupt — экстренное прерывание) на своей консоли. Это добавляет оператора в трёхстороннее соединение на занятой линии. Клавиша EMER INT также отключает схему подавления речи и включает предупредительный тон, который слышит вызываемый абонент. Этот тон, воспроизводящийся каждые 10 секунд, сообщает абоненту, что на линии присутствует оператор. Правда, в некоторых районах предупредительный тон отсутствует. Затем оператор говорит: «Это номер XXX-XXXX?», называя префикс и суффикс номера, который первоначально запросил клиент. Абонент подтверждает, что оператор попала на нужную линию. После этого оператор говорит: «Вас хочет соединить оператор с абонентом (имя клиента). Вы принимаете вызов?» Это даёт абоненту возможность ответить «Да» и принять звонок: звонящий подключается, а прежний собеседник отсоединяется. Если абонент отвечает «Нет», оператор сообщает клиенту, запросившему прерывание, что вызываемый абонент не принял вызов. Оператор также может просто уведомить занятую сторону, что с ней хотят связаться, попросить обе стороны положить трубки, а затем сообщить клиенту, что линия свободна. Либо оператор может соединить звонящую и прерванную стороны без разрыва соединения.

Стоимость данной услуги (по крайней мере в моём районе): 1,00 доллара — за запрос оператору прервать телефонный разговор, чтобы вы могли дозвониться; 0,80 доллара — за запрос оператору проверить, занят ли нужный телефон из-за технической проблемы или из-за разговора. Если на линии нет разговора, верификация проводится бесплатно.

Когда абонент, инициировавший экстренное прерывание, получит телефонный счёт, запись о плате за прерывание будет выглядеть примерно так:

```
12-1   530P     INTERRUPT  CL       314 555 1000  OD     1              1.00
```

Здесь 12-1 — 1 декабря текущего года; 530P — время обращения к оператору с запросом прерывания; INTERRUPT CL — тип произошедшего события, то есть звонок с прерыванием; 314 555 1000 — запрошенный номер; OD — Operator Dialed (набор оператором); 1 — продолжительность звонка в минутах; 1.00 — сумма за прерывание. Формат может различаться в зависимости от вашего района и телефонной компании.

Ещё один момент, который я не упомянул в связи с операторами TSPS. Там, где применяется схема удалённой транкинговой коммутации (Remote Trunking Arrangement), а также там, где она не применяется, вас могут соединить с оператором TSPS в совершенно другой зоне кода. В таком случае TSPS в чужой NPA (Foreign NPA) вызовет оператора Inward вашей домашней NPA (Home NPA, HNPA), если запрошенная вами линия EMER INT находится в вашей HNPA. Если же линия, на которой вы запрашиваете EMER INT, находится в той же NPA, что и TSPS, с которой вы соединились, оператор Inward не потребуется и ответивший оператор сможет выполнить всю процедуру самостоятельно.

Верификационные транки, по всей видимости, доступны только оператору TSPS/Inward. Тем не менее были сообщения о людях, выполнявших экстренные прерывания с помощью синих коробок (blue boxes). Я не знаю, как осуществить EMER INT без помощи оператора, и не уверен, возможно ли это вообще. Если вы действительно хотите поучаствовать в BLV/EMER INT, позвоните оператору Inward, разыграв роль оператора TSPS, которому нужно EMER INT на заранее определённой занятой линии. Биллинг обрабатывается на локальной TSPS, поэтому при выполнении этой процедуры вам не потребуется указывать номер для выставления счёта.

Если вы найдёте ошибки в этом файле, пожалуйста, сообщите мне об этом; если вы располагаете какой-либо дополнительной информацией, которую я не включил, — комментарии приветствуются.

— Конец файла —

Scan Man: возвращение к теме

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                        *>=-{ Phrack World News }-=<*                PWN
PWN                                                                     PWN
PWN                                  Issue X                            PWN
PWN                                                                     PWN
PWN                        Written, Compiled, and Edited                PWN
PWN                             by Knight Lightning                     PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

---

19 января 1987 года

Ниже приводится перепечатка из второго выпуска информационного бюллетеня TeleComputist:

SCAN MAN — ФЕД ИЛИ ФРИК? (Другая сторона)

TeleComputist публикует заявление Scan Man'a, сделанное им для нашего издания в ответ на материал Phrack World News, который ранее вышел в восьмом выпуске Phrack. Те, кто читал ту статью, знают: в ней излагалась информация и перехваченная служебная записка, в которых Scan Man'у вменялась слежка за хакерами и передача кодов со своей BBS (P-80 Systems, Чарльстон, Западная Виргиния, 304/744-2253) в качестве сотрудника TMC. Обращаем внимание: данное заявление следует читать вместе со статьёй о Scan Man'е из восьмого выпуска Phrack — только так можно составить полное представление о ситуации.

Scan Man начал своё заявление с того, что отрицает работу на TMC. По его словам, он трудился в нью-йоркском отделении Telecom Management — компании с головным офисом в Майами. Его еженедельно перевозили из Чарльстона (Западная Виргиния) в Нью-Йорк, где он проводил от четырёх до пяти дней. На время работы Telecom Management предоставляла ему арендованные апартаменты для руководящего состава. Его должность в компании — системный аналитик, «...и только», — заявил Scan Man. Он также подчеркнул, что никогда не скрывал факт работы в Нью-Йорке и даже оставлял соответствующие сообщения на своей BBS.

Далее он заявил, что не имел никакого отношения к аресту Shawn'a (из Phreaker's Quest, ранее известного как Captain Caveman), произведённому TMC в Лас-Вегасе. По словам Scan Man'a, у него нет никаких связей с лас-вегасским отделением TMC, и там его попросту не знают. Он добавил, что Shawn ни разу не ответил на его прежние сообщения, в которых он запрашивал коды TMC, а сами сообщения о TMC никак с ним не связаны. Scan Man утверждал, что не имеет никакого отношения к TMC — франчайзинговой структуре, где даже разные подразделения не связаны между собой ни чем, кроме названия.

Scan Man сообщил, что позвонил Полин Фрейзер и уточнил у неё, что именно она сказала Салли Райд [:::Space Cadet] — инсайдеру, раздобывшей сведения для восьмого выпуска Phrack. По его словам, Полин ничего не сообщила самозванке (Салли Райд) и лишь отправила её к сотруднику TMC по имени Кевин Гриффо. Scan Man также отметил, что Салли Райд позвонила Полин Фрейзер в тот же день, когда он получил уведомление об увольнении, и прокомментировал это так: «Если выяснится, что между этими событиями есть связь — полетят головы!»

После этого Scan Man перешёл к собственным контраргументам, начав с дат, указанных в восьмом выпуске Phrack. Он утверждал, что даты неверны, и в подтверждение сослался на то, что Бен

Грейвз был уволен за шесть месяцев до разговора с Салли Райд. Затем Scan Man задался вопросом: почему Салли Райд так долго тянул с разоблачением? Напоследок он сделал такое заявление: «Это чёртово позорище — социальная иерархия в мире фриков!» Иными словами, по его мнению, Салли Райд слил информацию лишь ради повышения собственного статуса в тусовке.

На этом всё и закончилось. TeleComputist публикует заявление Scan Man'a, чтобы представить обе стороны истории. Мы не выносим суждений и не принимаем ничьей стороны.

Перепечатано с разрешения информационного бюллетеня TeleComputist, выпуск 2

Итак, это была версия Scan Man'a — которую у него было несколько месяцев, чтобы придумать. Теперь разберём её по пунктам.

«Его еженедельно перевозили из Чарльстона (Западная Виргиния) в Нью-Йорк, где он проводил от четырёх до пяти дней».

Неужели это не влетало в копеечку? Каждую неделю — и «предоставляла арендованные апартаменты для руководящего состава»... Он, видимо, был крайне ценным активом для Telecom Management, раз на него тратили такие деньги. Любопытно, что он жил в Чарльстоне (Западная Виргиния), где, как ни странно, расположено отделение TMC, и при этом еженедельно летал в Нью-Йорк.

«Scan Man заявил, что не имеет никаких связей с TMC в Лас-Вегасе».

Допустим. Но заметьте: он не сказал, что не имеет связей с TMC в Чарльстоне. И если у него не было связей с TMC в Чарльстоне — почему его имя фигурировало во внутренней документации компании? Почему все те сотрудники знали его и, мягко говоря, не питали к нему симпатии?

«Scan Man отметил, что Салли Райд позвонила Полин Фрейзер в тот же день, когда он получил уведомление об увольнении».

Но как вообще между этими событиями может быть какая-либо связь, если Scan Man работает на Telecom Management, «не имеет связей с TMC» и «не работает на TMC»? Если TMC и Telecom Management действительно независимы друг от друга, то всё, что Салли Райд сказала Полин Фрейзер, не могло никак повлиять на него. Если только он изначально не работал на TMC.

«...подтвердив это тем, что Бен Грейвз был уволен за шесть месяцев до разговора с Салли Райд».

Во-первых, PWN не указывал дату увольнения Бена Грейвза из TMC. Во-вторых, что важнее: откуда Scan Man так хорошо осведомлён о делах TMC, если работает на «Telecom Management» и «...не имеет никаких связей с TMC»?

Остальные его заявления крайне спорны и ничем не подкреплены. Что касается вопроса, почему Салли Райд так долго ждал — он вовсе не ждал: он обратился ко мне в конце мая — начале июня 1986 года. Я принял решение ничего не предпринимать, поскольку доказательств было недостаточно. После трёх месяцев расследования доказательств стало достаточно, и статья была опубликована.

Этой попыткой замести следы Scan Man лишь подкинул новых аргументов тем, кто сомневается в правдивости его слов.

Особая благодарность информационному бюллетеню TeleComputist

Cracker сломался?

21 декабря 1986 года

«Компьютерный взломщик пропал — жив он или мёртв»

Том Горман, Los Angeles Times

Эскондидо, Калифорния. Ранним утром в конце сентября компьютерный хакер Билл Ландрет встал из-за своего IBM PC — на экране которого застыло незаконченное предложение — и вышел через парадную дверь дома своего приятеля.

С тех пор его никто не видел и ничего о нём не слышал.

Власти разыскивают его, потому что он — «Cracker»: в 1984 году осуждённый за взлом ряда наиболее защищённых компьютерных систем США, в том числе электронной почтовой сети GTE Telemail, где он читал переписку NASA и Министерства обороны.

Ему назначили три года испытательного срока. Теперь его куратор не знает, где он находится.

Его литературный агент разыскивает его, потому что он — Билл Ландрет-писатель: уже получивший гонорар за успешно изданную книгу о компьютерном взломе и просрочивший сдачу рукописи второй.

Институт внутренних аудиторов разыскивает его, потому что он — Билл Ландрет-докладчик, который должен был через несколько месяцев рассказать этой организации, как защитить компьютерные системы от таких людей, как он сам.

Сьюзан и Галливер Фурмайл разыскивают его, потому что он — старший из их восьми детей. Они не видели его с мая 1985 года, когда переехали из Пауэя на севере округа Сан-Диего — сначала на Аляску, а затем на Мауи, где живут сейчас.

Его друзья разыскивают его, потому что он — сумасбродный Билл Ландрет с IQ 163, который уже проделывал подобные фокусы и «исчезал» в ночи — но никогда больше чем на пару недель, и уж точно не на три месяца. Они встревожены.

Некоторые полагают, что Ландрет, которому 21 год, покончил с собой. Есть явные свидетельства того, что он это обдумывал — прежде всего бессвязное восьмистраничное эссе, написанное им летом.

Письмо было напечатано на компьютере, распечатано и оставлено в комнате, чтобы кто-нибудь нашёл. В нём говорилось об эволюции человечества, перспективах бессмертия и победы над старением, ядерной войне, противостоянии коммунизма и капитализма, алчности общества, смысле жизни, компьютерах, превосходящих человека по творческому потенциалу — и, наконец, о самоубийстве.

Последняя страница гласит:

> *«В момент, когда я пишу это, я, очевидно, ещё жив. Однако я планирую уйти из жизни прежде, чем кто-либо прочтёт эти строки. Замысел таков: я покончу с собой примерно в день своего 22-летия...»*

Далее в письме объяснялось:

> *«Мне было скучно в школе, скучно колесить по стране, скучно, когда меня брало ФБР, скучно в тюрьме, скучно писать книги, скучно скучать. Вероятно, будет скучно и умирать — но это мой риск.»*

Но затем в письме говорилось:

> *«С тех пор как я написал вышесказанное, мои планы несколько изменились... Суть в том, что я собираюсь взять оставшиеся деньги в банке (всё, что у меня есть в ликвидной форме) и сделать последнюю попытку наполнить жизнь смыслом. Попытка будет короткой, и я подозреваю, что если она удастся — никто из нынешних моих друзей меня не узнает. Если не удастся — весть о моей смерти, по всей видимости, разойдётся сама собой. (Я не стану её скрывать.)»*

День рождения Ландрета — 26 декабря, и его лучший друг не рассчитывает увидеть его снова.

«Мы шутили о том, что можно узнать о жизни — особенно если не веришь в Бога и не видишь в ней особого смысла», — сказал Том Андерсон, 16-летний старшеклассник школы Сан-Паскуаль в Эскондидо, примерно в 50 километрах к северу от Сан-Диего. Андерсон тоже осуждён за компьютерный взлом и находится на испытательном сроке.

Андерсон — последний, кто видел Ландрета. Это было около 25 сентября — точную дату он не помнит. Ландрет провёл неделю в доме Андерсона, чтобы вдвоём пользоваться его компьютером: IBM PC Андерсона был конфискован властями, а сам он хотел закончить собственную книгу.

По словам Андерсона, они с Ландретом также работали над заявкой на фильм о своих похождениях.

«Он начал набрасывать заявку на компьютере, а я пошёл в душ», — рассказал Андерсон. «Когда я вышел — его уже не было. Заявка обрывалась на полуслове. И с тех пор я его не видел.»

По всей видимости, Ландрет взял с собой лишь ключ от дома, паспорт и то, что было на нём надето.

Поначалу исчезновение Ландрета не встревожило Андерсона. В конце концов, это был тот самый Ландрет, который летом уехал в Мексику, не предупредив никого — включая друзей, с которыми виделся накануне вечером.

Но тревога нарастала. 1 октября Ландрет не явился на выступление перед группой аудиторов в Огайо, за которое ему причиталось 1000 долларов плюс расходы. Ландрет мог вести беспорядочный быт и пренебрегать финансовыми документами, но уж в соблюдении договорённостей о выступлениях он был надёжен — так говорили его друзья и литературный агент Билл Гладстоун, отметивший также, что рукопись второй книги была должна поступить ещё в августе, но так и не пришла.

Рукопись так и не появилась, и Ландрет так и не объявился.

Стив Бёрнап, ещё один близкий друг, рассказал, что летом Ландрет стал безразличен ко всему. «Казалось, ему уже ни до чего нет дела.»

Для PWN набрал Druidic Death
Из Dallas Times Herald

Берегитесь охотников за хакерами

Декабрь 1986 года

Ламонт Вуд, Texas Computer Market Magazine

Если хотите ощутить себя шпионом в собственной стране, вам необязательно вступать в ЦРУ, МИ-5 или КГБ. Можно, как Джон Максфилд из Детройта, охотиться за хакерами.

Максфилд — консультант по компьютерной безопасности, владелец компании BoardScan, которая отслеживает хакеров в интересах корпоративных клиентов. Он периодически получает угрозы

убийством и насмешливые звонки от своих «жертв», в среде которых известен как «охотник за хакерами», и снимает трубку с осторожностью.

Уильям Тенер, возглавляющий службу информационной безопасности в подразделении TRW, Inc., занимающемся информационными услугами, хотя лично ему никто не угрожал, был вынужден привлечь специалистов по искусственному интеллекту из аэрокосмической отрасли для защиты корпоративных файлов. TRW — лакомая цель для хакеров: компания хранит персональные кредитные досье примерно на 130 миллионов американцев и 11 миллионов организаций — данные, которыми многие хотели бы завладеть.

По оценкам Максфилда, за последние четыре года проблема хакерства выросла в десять раз и теперь удваивается ежегодно. «Практически в любую систему может проникнуть четырнадцатилетний подросток с оборудованием на 200 долларов», — сетует он. «Мне попадались дети девяти лет, занимавшиеся взломом. Если это по силам таким малышам — представьте, что может взрослый.»

По оценкам Тенера, в стране действует до 5000 частных компьютерных BBS, из которых около 2000 — хакерские. Остальные используются для самых разных целей: клубные новости, связь с клиентами или просто хобби. Из этих 2000 примерно два десятка посещаются «элитными» хакерами, и некоторые имеют защиту не хуже пентагоновской, утверждает Максфилд.

Точное число самих хакеров не поддаётся оценке хотя бы потому, что пользователи досок перекрываются между собой. Информация также передаётся с доски на доску. Максфилд рассказывает, что видел коды доступа, опубликованные на восточном побережье, которые менее чем через час появлялись на западном — пройдя через десяток досок. И уже через несколько часов после появления нового номера где-либо его пробуют сотни хакеров.

«Сегодня каждый выскочка с Commodore 64 и модемом может этим заниматься — ради удовольствия быть центром притяжения запретных знаний», — вздыхает один нью-йоркец, известный под именами «Richard Cheshire» или «Cheshire Catalyst» — ни то, ни другое не является его настоящим именем. Cheshire — один из первых компьютерных хакеров, ещё с тех времён, когда главной мишенью была сеть Telex; он был редактором TAP — бюллетеня для хакеров и телефонных фриков. Характерно, что сам TAP стал ранней жертвой хакерского нашествия. «У хакерских детишек появились свои BBS, и TAP им стал не нужен — мы морально устарели», — вспоминает он.

Так кто же эти хакеры и чем они занимаются? По наблюдениям Тенера, большинство из них — мальчики от 14 до 18 лет с хорошими компьютерами, нередко способные, из среднего класса, хорошо успевающие в школе. За ними закрепилась слава одиночек — пожалуй, потому что они часами сидят за терминалом, — хотя среди них попадались и общительные хакеры-спортсмены.

Максфилда, однако, тревожит то, что к этому делу всё активнее подключаются взрослые и уголовники. Основная часть хакерских действий — «кража услуг»: бесплатный доступ к CompuServe, The Source и другим онлайн-сервисам или корпоративным системам. Но хакеры всё глубже погружаются в мошенничество с кредитными картами.

Максфилд и Cheshire описывают одну и ту же схему: хакеры роются в мусорных баках рядом с офисами компаний, чьи компьютеры хотят взломать, в поисках руководств или любых документов с кодами доступа. Иногда находят нужное — но попутно обнаруживают копии кассовых чеков по кредитным картам, из которых можно выудить номера. Эти номера используются для телефонных заказов товаров — как правило, компьютерного железа — с доставкой на пустующий дом в округе или туда, где днём никого нет. Дальше нужно лишь оказаться на месте, когда приедет курьер.

«Мы наблюдаем это лишь последний год», — говорит Максфилд. «Но теперь мы видим взрослых, которые руководят бандами подростков, ворующих для них номера карт. Взрослые перепродают товар и отстёгивают детям процент.»

Лучше всего красть номер у богатого и известного человека — но поскольку это обычно невозможно, желательно заранее проверить кредитный рейтинг жертвы: торговец проверит его, прежде чем одобрить крупную покупку. Именно здесь TRW становится такой лакомой целью — в компании хранятся кредитные досье. А в них нередко указаны номера всех прочих кредитных карт жертвы, отмечает Максфилд.

Родители хакеров, как правило, понятия не имеют, чем занят их сын — он сидит в комнате, играет, ну и что такого? Тенер вспоминает случай, когда родители пожаловались сыну на огромный телефонный счёт за один месяц. В следующем месяце счёт вернулся к норме. Родители успокоились. А мальчик тем временем просто перевёл звонки на украденную телефонную кредитную карту.

«Когда мальчишку ловят и ведут в полицию, родители, как правило, возмущаются на власти — они по-прежнему считают, что Джонни просто играл у себя в комнате. До тех пор, пока не узнают, во сколько обошлись его игры — 50 000 или даже 100 000 долларов. Но если не считать суммы ущерба, я ни разу не видел родителей, которых всерьёз беспокоило бы нарушение чужой частной жизни — они просто думают, что Джонни очень умный», — говорит Тенер.

TRW, как правило, возбуждает дело против хакеров, когда обнаруживает свои файлы или данные доступа на каком-либо BBS. Тенер говорит, что компания обычно требует возмещения расходов на расследование — в среднем около 15 000 долларов.

Истории об ущербе от хакеров нередко преувеличены. Тенер рассказывает о широко освещавшихся случаях, когда пойманные хакеры хвастались взломом TRW, хотя на самом деле никакого взлома не было. Но Максфилд рассказывает о двух четырнадцатилетних хакерах, которые независимо друг от друга взламывали одну и ту же корпоративную систему и пользовались ею. Поссорившись, они принялись стирать файлы друг друга и заодно уничтожили сторонние файлы — восстановление обошлось примерно в миллион долларов. Поскольку оба были несовершеннолетними, никто из них не понёс наказания.

По словам Тенера, большинство пойманных хакеров находят себе другое занятие. Некоторые по достижении совершеннолетия устраиваются работать именно в те компании, которые прежде взламывали. Тенер говорит, что рецидивисты редки, но Максфилд знает одного: четырнадцатилетнего, впервые попавшегося в тринадцать.

Максфилд и Тенер оба отслеживают BBS, а Максфилд даже располагает сетью двойных агентов и осведомителей внутри хакерского сообщества. Тенер использует программы на основе искусственного интеллекта для анализа дневного трафика в поисках подозрительных паттернов. TRW обрабатывает около 40 000 запросов в час и имеет около 25 000 подписчиков. Но всё это не устраняет глубинной проблемы.

«Настоящая проблема в том, что эти системы плохо защищены, а некоторые вообще защитить невозможно», — говорит Максфилд.

Cheshire соглашается. «Многие компании не представляют, на что способны эти ребята», — говорит он. «Если бы доступ был хоть немного труднее, дети перешли бы к другой системе.» Относительно других мер он замечает, что в MIT студентов-компьютерщиков с первых занятий учат, как «уронить» систему. И как следствие — никто этого не делает.

Но старожила Cheshire (как и Максфилда) больше всего раздражает то, что весь этот феномен — хакеры, взломщики, вандалы, воры — противоречит идеологии первых хакеров, стремившихся исследовать системы, а не разрушать их. Cheshire определяет исходную «хакерскую этику» как убеждение в том, что информация — это ценный ресурс, которым следует делиться. На практике это означает: пользователи должны добавлять данные в файлы, а не уничтожать их, или вносить функциональность в программы, а не пиратствовать.

«Эти дети хотят сделать себе имя и думают, что для этого нужно сделать что-то грязное. Но ничуть не хуже это удалось бы чем-то умным — например, оставить на системе отчёт об ошибке», — говорит он.

Тем временем Максфилд считает, что с этой проблемой нам, по всей видимости, придётся жить как минимум до перехода телефонных сетей на цифровые технологии — а они должны лишить хакеров анонимности, сделав отслеживание звонков простым делом.

До тех пор, разумеется, пока кто-нибудь не придумает, как взламывать цифровые телефонные сети. — TCM

Для PWN набрал Druidic Death

Phrack World News

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                        *>=-{ Phrack World News }-=<*                PWN
PWN                                                                     PWN
PWN                                  Issue XI                           PWN
PWN                                                                     PWN
PWN                        Written, Compiled, and Edited                PWN
PWN                             by Knight Lightning                     PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Knight Lightning

Компьютерные доски объявлений — 8 января 1986 года

Материал новостного выпуска телеканала KTVI Channel 2, Сент-Луис

Примечание: Карен и Расс — ведущие KTVI. Все комментарии в скобках [] принадлежат мне. —KL

Карен: Если Санта-Клаус подарил вам на Рождество компьютер — будьте осторожны: вы можете наткнуться на кое-что, к чему совсем не готовились. Компьютерные доски объявлений распространились по всей стране тысячами за последние несколько лет, и теперь некоторые люди всерьёз обеспокоены тем, что электронные сообщения вышли из-под контроля.

Расс: В простейшем определении компьютерная доска объявлений — это программа или сообщение, доступное с других компьютеров по телефонным линиям. Любой, у кого есть домашний компьютер и модем, может получать и отправлять сообщения на такие доски. По всей стране их тысячи, однако некоторые из них вызывают нешуточный переполох. [Глубокая мысль, Расс.]

```
[Flash to a picture of a geeky looking teenager]
```

Познакомьтесь с Джейсоном Реббе — шестнадцатилетним компьютерным вундеркиндом, который несколько месяцев назад случайно наткнулся на доску объявлений под названием Dr. Doom's Castle. [Прости, что перебиваю, Расс, но почему этот парень — «вундеркинд»? Только потому что у него есть компьютер? Расс, присмотрись повнимательнее — разве Джейсон не сидит перед Commodore-64? Именно так. И ещё одна деталь: BBS «Dr. Doom's Castle» не имеет никакого отношения к Dr. Doom (512) или Danger Zone Private.] Доктор Дум даёт инструкции по изготовлению бомб и оружия [Львы, тигры и медведи, ой-ой-ой!]. Джейсон нашёл рецепт дымовой бомбы и попытался собрать её на кухне — ничего не вышло. [Ха-ха-ха.]

Джейсон: Сначала я услышал взрыв в подвале — вот тогда-то и понял, что что-то пошло не так. Я думал, что будет здорово однажды устроить это там, где много народу, — просто как шутку или розыгрыш. [Да, это было бы K-Rad, d00d!] Я не ожидал, что взорву весь дом.

Расс: Джейсон не пострадал, однако ремонт кухни обошёлся примерно в 2 тысячи долларов. Отец Джейсона воспринял случившееся болезненно.

Боб Холлуэй: Слово «злой» — это не про то, что я тогда чувствовал. Я вышел далеко за рамки злости.

Расс: Мистер Холлуэй позвонил в Southwestern Bell и AT&T, чтобы выяснить, что можно предпринять в отношении досок объявлений вроде Dr. Doom's Castle. Ответ: ничего. Бюро по

алкоголю, табаку и огнестрельному оружию сказало то же самое.

Дэниел Хоггарт (Бюро по алкоголю, табаку и огнестрельному оружию): Публикация подобной информации не является нарушением закона. Нарушение возникает лишь тогда, когда кто-то фактически следует инструкциям и реально собирает взрывное устройство.

Расс: Другая доска объявлений, которая становится всё более заметной в наши дни, — это «Арийская нация». Одна такая доска в Чикаго сообщает: «Если вы антикоммунист — вы попали по адресу... с другой стороны, если вы заражены такими мифами, как иудео-христианство, то вы определённо набрали не тот номер».

Стэн Андерман (Антидиффамационная лига): Некоторые из этих проявлений крайней ненависти — попытка создать среду, в которой насилие стало бы приемлемым.

Расс: Как и большинство компьютерных досок, сообщение «Арийской нации» является законным и подпадает под законодательство о свободе слова. Тем не менее в ближайшую сессию конгресса запланировано рассмотрение законопроекта, запрещающего подобные доски объявлений.

Но пока что хакерам не стоит особо удивляться, если на экране их компьютерного терминала появится что-нибудь необычное. [Кхм, Расс, вы снова за своё. Далеко не все пользователи компьютеров — хакеры.]

Перепечатано для нужд PWN Рыцарем-Молнией (Knight Lightning)

MIT Unix: жертва или агрессор? — 23 января — 2 февраля 1987 года

Является ли система MIT невинной жертвой хакерского произвола — или всего лишь очередной ловушкой для доверчивых хакеров, застигнутых с поличным?

Всё началось так...

(Некоторые публикации слегка отредактированы для соответствия теме)

MIT
Ник: Druidic Death
Дата: 0:49, пн., 20 января 1986 г.

В последнее время я копаюсь в MIT'овском VAX'е физического факультета.

Недавно туда залез кто-то ещё и навредил файлам. Однако MIT сказал, что всё равно доверяет нам — мы можем звонить им дальше. Номер:

```
617-253-XXXX
```

Мы должны соблюдать следующие условия, иначе нас выгонят; для нас создадут отдельный аккаунт «hacker».

```
<1>  Использовать только GUEST, RODNEY и GAMES. Никаких других
     аккаунтов, пока хакерский не создан. На этих аккаунтах нет паролей.

<2>  Обязательно правильно завершать сеанс. Control-D. Это UNIX-система.

<3>  Не звонить с 9:00 до 17:00 по восточному стандартному времени,
     чтобы не загружать систему.

<4>  Писать GEORGE только по вопросам UNIX (или C). И оставлять свои
     псевдонимы, чтобы он знал, кто мы такие.
```

Unix
Ник: Celtic Phrost
Дата: 16:16, пн., 20 января 1986 г.

Спасибо, Дет, за MIT'овский компьютер — я несколько недель пытался туда пробраться. Вот ещё один, с которым можно поиграть:

```
617/258-XXXX
login: GUEST
```

Или используй команду WHO при входе, чтобы увидеть другие аккаунты. Я давно не заходил в эту систему, так что не уверен, работает ли GUEST и сейчас, — но с помощью WHO ты должен увидеть аккаунт GUEST, который нужен для подачи заявки на собственный аккаунт.

— Phrost

Unix
Ник: Celtic Phrost
Дата: 17:35, пн., 20 января 1986 г.

Окей, прости, только что вспомнил аккаунт для регистрации — это: OPEN. Уф, как гора с плеч!

— (облегчённый) Celtic Phrost

На том MIT'овском компьютере, что указал Дет, есть ещё несколько аккаунтов по умолчанию:

```
LONG    MIKE    GREG    NEIL    DAN
```

Остальное найдите сами. И пожалуйста, люди, НЕ ТРОГАЙТЕ ПАРОЛИ!

MIT
Ник: Druidic Death #12
Дата: 1:16, пт., 23 января 1987 г.

MIT — это круто. Если ещё не звонили — попробуйте. Только ПОЖАЛУЙСТА, соблюдайте их маленькие правила! Если кто-то косячит, сисоп шлёт жалобы мне. Загляните в мою директорию через гостевой аккаунт — просто наберите `cd Dru`. Прочитайте первый файл.

MIT
Ник: Ctrl C
Дата: 12:56, сб., 24 января 1987 г.

Аккаунты MIT Unix без паролей: `617-253-XXXX`

```
ALEX   BILL   GAMES   DAVE   GUEST   DAN   GREG   MIKE   LONG   NEIL   TOM   TED
BRIAN   RODNEY   VRET   GENTILE   ROCKY   SPIKE   KEVIN   KRIS   TIM
```

И ПОЖАЛУЙСТА, не меняйте пароли...

— =>Ctrl C<=

MIT снова
Ник: Druidic Death
Дата: 13:00, ср., 28 января 1987 г.

Так, народ, MIT взбешён — кто-то нарушил договорённость, и там этому совсем не рады. Я был тем, кто заключил эту «сделку» с ними. Они даже дали мне голосовой номер для общения с сисопами.

Они просили всего три вещи — разумные и выполнимые: не подрывать безопасность больше, чем мы уже подорвали; нормально завершать сеанс и не оставлять запущенных процессов; звонить только в нерабочее время — и тогда мы могли бы сколько угодно пользоваться GUEST-аккаунтами.

Кто-то хорошенько постарался и добавил себя в группу «daemon» — это только для суперпользователей — под именем «celtic». Интересно, кто бы это мог быть? Я ни на кого не злюсь, но хотел бы и дальше пользоваться MIT'овскими компьютерами. Они и сами были рады, что мы там сидим, — но сейчас стали параноить. Кто бы ни звонил туда, кроме меня, — ведите себя нормально, ладно? Они даже дали мне голосовой телефон для разговора с их сисопами. Как часто такое бывает?

Немного раздражён, но не зол...

DRU'

Нехорошо, Celtic.
Ник: Evil Jay
Дата: 9:39, чт., 29 января 1987 г.

Лично я не понимаю, зачем вообще кому-то нужны привилегии суперпользователя на этой системе. Зайдя туда один раз, понимаешь: смотреть там особо не на что... Но так или иначе.

— EJ

Снова в переделке...
Ник: Celtic Phrost
Дата: 14:35, пт., 30 января 1987 г.

...Меня подставили!! Я не добавлял себя ни в какую группу «daemon» на MIT UNIX. Я заходил туда один раз, и должен признать — вышел без выхода из системы, но это произошло из-за глючной программы, из которой я никак не мог выбраться, что бы ни пробовал. Уверен, что вреда этим не причинил.

— Phrost

Крупные проблемы
Ник: Druidic Death
Дата: 12:20, сб., 31 января 1987 г.

Всё, серьёзный разговор. Какой-то неустановленный человек вошёл на PDP11/34 физического факультета по номеру `617-253-XXXX` и грубейшим образом нарушил нашу «договорённость». Эту сделку заключал я. Они даже дали мне прямой голосовой номер.

В один прекрасный день я позвонил на другой физический компьютер — офисный AT — и обнаружил, что кто-то создал аккаунт в суперпользовательской группе DAEMON с именем «celtic». После этого Брайан вызвал меня в чат и попросил позвонить ему. Тогда он вежливо сообщил мне, что «в связи с несанкционированным злоупотреблением системой сделка расторгнута».

Он отнёсся к этому спокойно и сказал, что сожалеет о произошедшем. Затем я позвонил Джорджу — тому, кто заключал сделку — и он сообщил: некий человек, назвавшийся «Celtic Phrost», вошёл в систему и удалил почти годичный объём данных по искусственному интеллекту из базы

исследований по ядерному синтезу.

Излишне говорить, что я был потрясён. Я сказал, что он не должен верить, будто это кто-то из наших, — насколько мне известно, все соблюдали договорённость. Тогда Джордж (в крайней злобе) потребовал все наши имена, чтобы сообщить о нас в ФБР. Он назвал нас разными нехорошими словами — короче говоря, был ОЧЕНЬ!! [дважды подчёркнуто] ЗОЛ! Я его понимаю. Честно говоря, я не виню Celtic Phrost — вполне может быть, что его подставили.

Но есть ещё кое-что: Джордж считает, что Celtic Phrost и Druidic Death — одно и то же лицо, то есть думает, что *я* его предал. По сути, он просто не понимает, как устроено хакерское сообщество.

Сделка отменена, они намерены преследовать всех, кого поймают. Поскольку Джордж — брат моего лучшего друга, я не только потерял приятеля, но и рискую скоро столкнуться с юридическими проблемами. Про аспирантуру в MIT теперь можно забыть. Кто бы ни нанёс им этот ущерб — надеюсь, ты доволен. Ты очень хорошо всё испортил для кучи людей.

Celtic, у меня нет оснований считать, что ты там напакостил. Но нет и оснований думать обратное. Я тебя ни в чём не обвиняю, но КОМУ БЫ это ни сделал — он заслуживает расстрела, по-моему. До того как эти данные были уничтожены, они вплотную приближались к управляемому термоядерному синтезу с лазерно-литиевым методом — более эффективному, чем стандартный водородный. Ну что ж, теперь придётся начинать с нуля.

Понимаю, в это трудно поверить — чтобы такие данные хранились на подобной системе. Но они были тупыми и во многих других отношениях. Оставить суперпользовательский аккаунт без пароля? Подумайте сами.

Возможно, они и преувеличивали. Но так или иначе, ущерб, судя по всему, реальный.

MIT
Ник: Phreakenstein
Дата: 1:31, вс., 1 февраля 1987 г.

Чёрт! Не знаю, но кто бы это ни был — думаю, ему стоило бы объявиться (такому суперкрутому элитному d00d'y).

Я в MIT не заходил, но это было весьма глупо с их стороны — вообще подпускать к себе хакеров. Я бы особо не беспокоился — они сами вас пустили, и всё, что нужно доказать: у вас не было мотива это делать.

— Phreak

Интересно...
Ник: Ax Murderer #15
Дата: 18:43, вс., 1 февраля 1987 г.

Очень сомневаюсь, что это был кто-то с нашей системы. Тут элитная доска, и все пользователи вроде как нормальные люди, знающие, что делать можно, а что нельзя. Может, кто-то из наших позвонил на другую систему и там всё это слил? Ну нет... расстреляли бы мало — придумаем что-нибудь поинтереснее.

Ax Murderer

Это было глупо
Ник: Druidic Death #12
Дата: 21:21, вс., 1 февраля 1987 г.

Мне кажется — или, по крайней мере, так я это понял — они изначально рассчитывали, что на системе будут хакеры, и считали, что так смогут в основном обезопасить себя.

Не думаю, что это был Celtic Phrost — не верю, что он способен на такое скотство. Но не могу утверждать наверняка. Когда писал тот пост, я был здорово зол на всё происходящее. Теперь успокоился. Psychic Warlord сказал мне кое-что по голосовому несколько дней назад — заставило меня задуматься. А что, если это была подстава с самого начала? MIT не сообщает мне конкретики о том, что якобы произошло, Celtic Phrost всё отрицает, а главное — что именно сказал мне Джордж:

«Мы можем простить тебя за то, что ты сделал, если ты пообещаешь завязать и никогда больше этого не делать — и просто назовёшь нам всех своих друзей, которые были в системе».

Поначалу я не обратил особого внимания на это замечание. Теперь начинаю задумываться...

Само собой, я никого не сдал. (И кого мне было сдавать??? хехе)

DRU'

Ну и ладно
Ник: Solid State
Дата: 23:40, вс., 1 февраля 1987 г.

Если они серьёзно насчёт ФБР — не стоит это игнорировать. В последнее время в Стэнфорде я заметил немало следователей, которые там крутятся. В основном это связано со взломами, которые были этим летом.

Так или иначе — если крупный университет вроде MIT говорит, что может подключить ФБР, — будьте начеку, но без паники.

SOLID STATE

Комментарии...
Ник: Delta-Master
Дата: 7:15, пн., 2 февраля 1987 г.

Не удивился бы, если это было что-то вроде подставы — такое уже бывало.

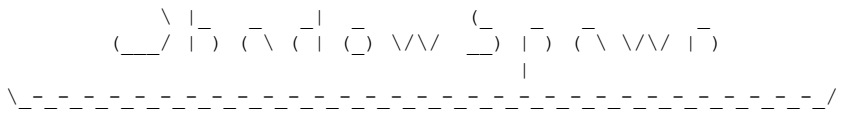
Delta-Master

Ну и ладно...
Ник: Evil Jay
Дата: 8:56, пн., 2 февраля 1987 г.

Думаю, вы все ошибаетесь. MIT'овские линии существуют давно и хорошо известны в определённых кругах. Любой, у кого есть g-file, мог подобрать пароль к системе — так что, похоже, кто-то просто поигрался там и случайно воспользовался Phrost'ом как козлом отпущения. Ну и ладно...

— EJ

Все публикации взяты из:



"We're not ELITE... we're just cool as hell."

Информация предоставлена прямо и косвенно участниками:

Ax Murderer / Celtic Phrost / Ctrl C / Delta-Master / Druidic Death
Evil Jay / Phreakenstein / Solid State

Phortune 500: новейшая организация мира фрикинга — 16 февраля 1987 года

Для тех, кому хоть немного интересно: Phortune 500 — это группа любителей телекоммуникаций, чья цель — распространять информацию и расширять собственные знания в мире телекоммуникаций. Новая группа была основана:

Brew Associates / Handsomest One / Lord Lawless / The Renegade Chemist
Quinton J. Miranda / Striker / The Mad Hacker / The Spiker

Эти восемь человек составляют также Совет директоров (Board of Directors, BOD). Они не претендуют на звание *элиты* в смысле величайших хакеров мира, но к отбору членов подходят достаточно взыскательно. Им нравятся люди, которые знают понемногу обо всём и обладают талантами, уникальными именно для них.

Один из завершённых проектов Phortune 500 — система индивидуальных паролей типа AE под названием TransPhor. Написана и создана Brew Associates. Прошла бета-тестирование на «The Undergraduate Lounge» (сисоп — Quinton J. Miranda). В ближайшие несколько месяцев ожидается публичный релиз.

Phortune 500 работает около 4 месяцев и уже выпустила два собственных информационных бюллетеня. «The Phortune 500 Newsletter» — нечто вроде журнала «People» в мире современных изданий. В то время как одни издания рассматривают глубокие технические аспекты нашего мира коммуникаций, их бюллетень старается осветить более лёгкую сторону, попутно включая материалы, которые авторы считают «технически значимыми». Третий выпуск должен выйти до конца этого месяца.

```
           *>=-> The Phortune 500 Membership Questionnaire <-=<*

  Note:  The following information is of a totally confidential nature.  The
         reason you may find this so lengthy and in depth is for our knowledge
         of you. We, with Phortune 500, feel as though we should know
         prospective members well before we allow them into our organization.
         Pending the answers you supply us, you will be admitted to Phortune 500
         as a charter member.  Please answer the following completely...
  ..........................................................................

  Handle                          :
  First Name                      :
  Voice Phone Number              :
  Data Phone Number               :
  City & State                    :
  Age                             :
  Occupation (If Applicable)      :
  Place of Employment (Optional)  :
  Work Phone Number   (Optional)  :
  Computer Type                   :
```

```
Modem Type                      :
Interests                       :
Areas Of Expertise              :
References (No More Than Three) :
Major Accomplishments (If Any)  :
.....................................................................
Answer In 50 Words Or Less;

^*^  What Is Phortune 500 in Your Opinion?

^*^  Why Do You Want To Be Involved With Phortune 500?

^*^  How Can You Contribute to Phortune 500?
.....................................................................

Please answer each question to the best of your ability and then return to any
Phortune 500 Board of Directors Member Or a Phortune 500 BBS:

           The Private Connection (Limited Membership) 219-322-7266
           The Undergraduate AE   (Private Files Only) 602-990-1573
```

Информация предоставлена Quinton J. Miranda и Советом директоров Phortune 500

Быстрая заметка PWN

В Университете Род-Айленда, судя по всему, действует некий агент-нелегал от Bay Bell. Говорят, он дежурит в библиотеке и следит за теми, кто берёт технические журналы Bell. Затем задаёт вопросы вроде: «Зачем вам это?», «Вы знаете, что такое 2600 Гц?» и т. п. В университете он не числится и, разумеется, ни на какие занятия не ходит. [Звучит как байка... ну и ладно — KL.]

Информация от Asmodeus Rex (21.01.87)