Phrack RU issue 003

Русская версия Phrack, выпуск 003. Полный текст статей с кодом и таблицами.

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

Материалы выпуска: Phrack Inc. Выпуск третий; Системы ROLM; Phrack Inc. Том 1, выпуск 3, файл 3 из 10; Системы сигнализации по всему миру; Частная аудитория; Fortell Systems; Электронный подслушиватель; Изготовление электрошоковой дубинки; Введение в АТС (PBX); Phreak World News II.

Больше крутых материалов в моём телеграм канале @grogrigs

Phrack Inc. Выпуск третий

Дата выпуска: 1 февраля 1986 года
Автор индекса: Cheap Shades

Файлы, содержащиеся в этом выпуске Phrack Inc.:

1. Index — Cheap Shades
2. Rolm systems — Monty Python
3. Making shell bombs — Man-Tooth
4. Signalling systems around the world — Data Line
5. Private audience — Overlord
6. Fortell systems — Phantom Phreaker
7. Eavesdropping — Circle Lord
8. Building a Shock Rod — Circle Lord
9. Introduction to PBX's — Knight Lightning
10. Phreak World News II — Knight Lightning

Если у вас есть оригинальный файл, который вы хотели бы опубликовать в будущем выпуске Phrack Inc., оставьте E-Mail Taran King, Knight Lightning или мне на любой системе, где мы бываем.

Если вы не можете нас найти, попробуйте связаться с кем-нибудь из Metal Shop, чтобы выйти на нас.

```
Later,
Cheap Shades
```

Системы ROLM

Автор: Monty Python

Цель этого файла — рассказать, с чем вы будете иметь дело, если наткнётесь на такую систему или если знаете компанию, которая её использует. Здесь нет невероятно глубоких деталей, и кое-каких вещей не хватает. Это не руководство по взлому системы, а попытка дать понять, с чем вы столкнётесь. Текст должен пробудить интерес к системе.

Так что же, чёрт возьми, такое ROLM?

ROLM — это «Business Communications System», которую IBM купила несколько месяцев назад, пытаясь эффективнее конкурировать с AT&T и получить большую долю рынка в большом генеральном плане стать «Big Daddy Blue» вместо «Ma Bell».

Это очень сложная система с такими возможностями, как PhoneMail, Super-PBX, local area networks, публичные и частные сети данных, desktop communications и call management.

Сердце системы — контроллер, называемый **CBX**, то есть **Computerized Business Exchange**. Он управляет всей сетью, доступной через ROLM. С 1983 года CBX был переработан и обновлён до **CBX II**. Это PBX, но с гораздо большими возможностями; см. «Introduction to PBX's», доступный на вашей местной BBS. Именно это и является предметом гордости ROLM. Система на световые годы опережает обычный PBX.

CBX II

CBX II — ядро сети ROLM. Он управляется компьютером и масштабируется от одного узла со 165 каналами до 15 узлов, предоставляющих 11 520 двусторонних каналов.

Небольшой бизнес может иметь модель с максимумом 16 пользователей, но система может расти до 10 000 пользователей, хотя это было бы довольно редко и чертовски дорого.

К ней можно обращаться с внешних линий, то есть так же, как это сделали бы вы, а также с hardwired units. В системе есть коммутация, предотвращающая busy signals на порту. Скорость зависит от установленной системы: либо более нового и быстрого ROLMbus 295, либо более старого стандартного ROLMbus 74. Точные детали см. в service manuals.

Чем больше система, тем она быстрее. Её можно настраивать для разных полос пропускания разных компонентов: telex, voice, data, mainframe, LAN, video — да, настоящие picturephones — и всего, что подключено к системе.

Похожие задачи также можно группировать на одном канале на высокой или низкой скорости. Если используется multiplexing, максимальная скорость составляет 192 000 bps; при использовании одного интерфейса верхняя возможная скорость — умопомрачительные 37 000 000 bps. На мой взгляд, это скорее украшение и не слишком практично, поэтому обычно используется multiplexing. Вот это разница по сравнению с 300 бод.

Используя сеть CBX II, вы можете найти почти любой вид mainframe: от HP до DEC, VAX и IBM 327 series.

Примечание: существует меньшая версия этой системы, называемая **VSCBX**.

PhoneMail

Это одна из маленьких прелестей системы, с которой действительно интересно возиться. Я позвонил в штаб-квартиру ROLM в Калифорнии, чтобы задать конкретные вопросы о ROLM, изображая исследователя, и получил большую беготню по отделам.

Может быть, вы продвинетесь дальше, чем я. Их номер:

```
408-986-1000
```

Номер PhoneMail извне:

```
800-345-7355
```

Приятный компьютерно-сгенерированный голос просит ввести extension number, который есть у каждого сотрудника, а затем ввести знак #. После этого нужно ввести пароль.

Если сделать примерно 3 или 4 неверные попытки ввода extension или пароля, система автоматически позвонит на другой номер — вероятно, в assistance, чтобы выяснить, почему была неудачная попытка входа. Я не играл с этим особенно много, поэтому оставляйте почту Monty Python с тем, что найдёте.

После ввода authorization number с правильным паролем появятся дополнительные варианты: оставить сообщения другим людям и так далее. Можно слушать свои сообщения, пересылать их другому человеку, оставлять одно и то же сообщение нескольким людям, менять приветственное сообщение и так далее.

Сервис предназначен для business-type pigs, которые ни минуты не сидят на месте, будто постоянно на speed.

Сценарий PhoneMail

Допустим, мистер Greed уходит встретиться со своей секретаршей в мотеле, но ему обязательно нужно получить важное сообщение от мистера Rasta, который ввозит 3 миллиона долларов во Flake, и нельзя доверить это человеку, который должен был бы принять сообщение, то есть человеку, временно заменяющему его секретаршу с огромной грудью, которую сейчас валяет этот грязный старый толстяк.

Мистер Greed дал бы мистеру Rasta свой телефонный номер, и тот был бы перенаправлен в сеть PhoneMail, где услышал бы сообщение, оставленное мистером Greed для всех звонящих. Мистер Rasta оставил бы своё сообщение и повесил трубку.

Затем мистер Greed мог бы позвонить на:

и ввести свой extension authorization number и пароль. Или, если он вернулся в офис, он мог бы получить сообщение там через DeskTop communications.

Сообщения можно доставлять без ошибок, голосом самого человека и без того, чтобы другие люди знали об этом. Поэтому кто-то с достаточными знаниями мог бы использовать неиспользуемую учётную запись как собственный сервис без ведома остальных.

DeskTop communications

ROLM разработала интегрированное устройство Computer/Telephone для использования с Desktop communications. Оно связано с CBX II через телефонные линии, а значит доступно снаружи вам и мне. Оно не hardwired, хотя может приближаться к hardwired speed.

Если бы вы смогли достать один из таких computer/phones, думаю, дома и в обычной жизни вы нашли бы ему очень полезное применение. Но получить доступ к сети можно и без специальных функций телефона, вроде one-touch dialing, разработанного для тупого ленивого бизнесмена.

Через сеть можно получать доступ к базам данных компании, mainframes, другим людям — почти ко всему, как если бы вы находились прямо там и сказали секретарю сделать это за вас. Используется специальное программное обеспечение для компьютеров или computer/phone, но его можно импровизировать, и оно является лишь помощником.

Система использует специальный протокол. Автор оригинала не знает, какой именно, и предлагает попытаться достать устройство через мусор sales office.

Самое интересное в том, что всё связано через телефонные линии, а не RS-232C. Значит, где-то есть access port.

Оригинал предлагает искать номера вокруг офиса, использующего ROLM. Чтобы понять, использует ли компания ROLM, автор предлагает составить список местных компаний и звонить им под видом ROLM Customer Support с сообщением о жалобе в их CBX II network. Если компания отвечает, что не использует ROLM или CBX II, автор предлагает извиниться и идти дальше. Альтернативно он предлагает представиться ROLM Corp. и спросить, заинтересована ли компания в использовании ROLM для объединения своей системы в сеть: если система уже есть, они, вероятно, так и скажут; если нет, можно дать фиктивный номер или, если вы «хороший», номер местного sales office.

Пример экрана

Но знаете, что действительно отлично? Сетевой интерфейс сделан с расчётом на человека с Computer IQ около нуля. Команды написаны простым английским. Вот демонстрационный экран из их брошюры:

```
CALL, DISPLAY or MODIFY

Display groups

ACCESSIBLE GROUPS:
  [00] PAYROLL       [01] MODEM       [02] IBMHOST
  [03] DOWJONES      [04] DECSYSTM    [05] MIS-SYSTM
  [06] DALLAS        [07] SALES

CALL, DISPLAY OR MODIFY?
Call Payroll

CALLING 7717  <which would be the ID code for the PAYROLL file>
CALL COMPLETE

**PAYROLL SYSTEM** <or whatever they want to call it>
 ENTER ACCOUNT CODE:
```

Видите, ничего не запутано: всё довольно самоочевидно. Может быть больше одного человека, желающего сделать то же, что и вы; в таком случае вас поставят в очередь на задачу.

Похоже, что владельцы IBM лучше всего подходят для ROLM hacking, потому что ROLM принадлежит IBM, а используемые в сети PC — это IBM. Человек с более простым phone/terminal не смог бы получить доступ к чему-то вроде их DEC mainframe или подобной системы.

Позвонив внутрь, вы не смогли бы запустить приложение, если у вас нет специального интерфейса, но вы могли бы получить доступ к database — а это способен сделать любой dumb terminal.

Однако существуют security levels. Поэтому тот, у кого есть привилегированная учётная запись, может получить доступ к большему числу вещей, чем тот, у кого её нет. Например, Joe Schmoe из Sales не смог бы попасть в Payroll.

Похоже, что для доступа не-IBM машин к некоторым частям сети нужен интерфейс, чтобы выглядеть как RolmPhone.

Чрезмерное число плохих попыток входа, которые могут быть истолкованы как linking error, уведомит network manager. Если он увидит, что аппаратной ошибки нет, то рано или поздно — если он хоть немного опытен — подумает о хакерах.

PBX

У ROLM есть вещь под названием **Integrated Call Management**, далее ICM. При проектировании ICM, должно быть, учли возможные злоупотребления в обычных PBX. Поэтому туда добавили **Call Screening**.

Это позволяет компании ограничивать звонки на определённые номера и prefixes. Звонки на нерабочие номера или в определённые районы могут отсеиваться, за исключением одного конкретного номера, который вы хотите разрешить.

Есть выбор между codeless screened PBX и PBX, где учётные записи назначены каждому сотруднику, а набираемые ими номера записываются на эту учётную запись.

Могут существовать привилегированные учётные записи, где большой объём звонков останется относительно незамеченным. Но автор не считает, что крупномасштабное злоупотребление этой системой было бы простым или практичным.

Звонки автоматически маршрутизируются через тот сервис, где тарифы дешевле для набранного направления, что довольно круто. PBX также доступен извне через Direct Inward System Access, что делает его пригодным для abuse.

А что если в этой зоне есть Equal Access? Это не имеет значения: CBX автоматически получит доступ к сервису, и вам не придётся об этом беспокоиться. Автор добавляет, что для hack/phreak это вообще не важно, потому что они всё равно не платят за звонок.

Но есть важное «но»: используется **Call Detail Recording**, где записывается информация обо всех входящих и исходящих звонках.

Заключение

В этот файл вложено не так много исследований, но его набор занял некоторое время, и вся информация, насколько автор знает, верна. Любой может расширить этот файл во вторую часть.

Он был написан, чтобы просветить людей об этой системе, и автор надеется, что это хотя бы немного помогло.

Sysops могут размещать этот файл, если **никакие credits не изменены**. Это означает и Phrack Inc., и личные credits. Дайте нам шанс.

Скоро, на телефоне рядом с вами: **The Return of The Flying Circus**. Ищите.

```
Later On,
```

Monty Python
01/11/86

Phrack Inc. Том 1, выпуск 3, файл 3 из 10

```
                ==Phrack Inc.==
          Volume One, Issue Three, Phile 3 of 10


        ////////////////////\\\\\\\\\\\\\\\\\\\\
        ::::                                ::::
        ::::    "БОМБЫ ИЗ ДРОБОВЫХ ПАТРОНОВ" ::::
        ::::               из               ::::
        ::::    "Бедный человек Джеймс Бонд" ::::
        ::::           Курта Саксона        ::::
        ::::                                ::::
        :::: напечатано --] Man-Tooth [--   ::::
        ::::                                ::::
        \\\\\\\\\\\\\\\\\\\\////////////////////
```

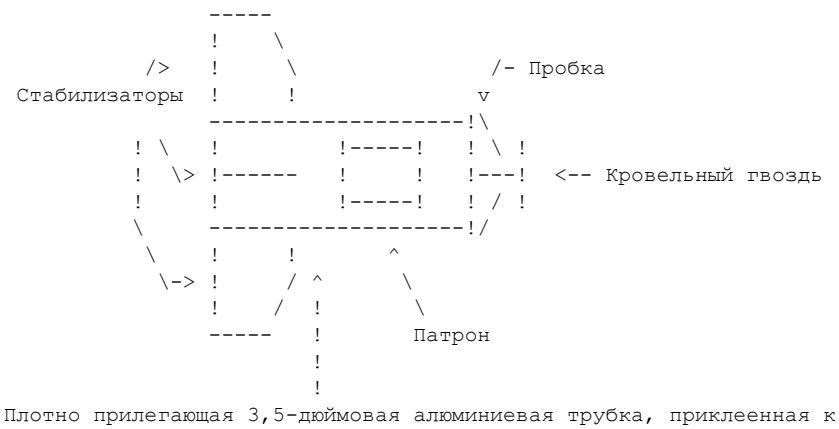
Эти маленькие прелести ласково известны как "орехокрушители" (nut busters). Это просто дробовые патроны, заключённые в картонные гильзы с приклеенными картонными стабилизаторами. На капсюльный конец патрона приклеивается маленькая пробка с просверленным отверстием. В отверстие вставляется кровельный гвоздь достаточно плотно, чтобы он оставался на месте, но достаточно свободно, чтобы при ударе вонзиться в капсюль.

Поскольку патрон не заперт в патроннике ружья, он, естественно, не вызовет такого же уровня разрушений. Но если он взорвется между ног парня, он может рассчитывать на то, что станет сопрано.

Эти бомбы бросают по одной или горстями в воздух над возбуждённой толпой. Вес патрона и стабилизация хвостовиками заставляют "орехокрушитель" лететь вертикально вниз.

Он оказывает потрясающий эффект, поскольку его появление обычно становится неожиданностью. Угроза новых бросков гарантированно разгонит любую толпу.

Он взрывается не только на мостовой, но и при ударе о голову или плечо человека. Ночью невозможно проследить источник его появления.



Плотно прилегающая 3,5-дюймовая алюминиевая трубка, приклеенная к патрону.

БОМБА ИЗ ДРОБОВОГО ПАТРОНА

Остроумное применение обычному дробовому патрону — как бомба в глушитель. Патрон просто проталкивается в выхлопную трубу автомобиля с помощью жесткой проволоки, пока не упадет в глушитель. Через несколько минут езды патрон взрывается, полностью разрушая глушитель и вызывая у водителя болезненного рода панику.

Системы сигнализации по всему миру

Для тех, у кого есть желание совершать международные звонки, эта информация может быть интересна.

Благодарности: TAP и Nick Haflinger.

CCITT 1

Старая международная система, теперь уже умершая. Использовала тон 500 Hz, прерываемый на 20 Hz, то есть ring, для односторонних линейных сигналов.

CCITT 2

Предложенный «международный стандарт», который так и не прижился широко. Использовал 600 Hz, прерываемые 750 Hz. Всё ещё используется в Австралии, Новой Зеландии и Южной Африке.

CCITT 3

Ранняя in-band система, которая использует 2280 Hz и для line, и для register. В оригинале это отмечено двойным восклицательным знаком. Использовалась во Франции, Австрии, Польше и Венгрии.

CCITT 4

Вариант CCITT 3, но использует 2040 Hz и 2400 Hz для end-to-end передачи line и register. Используется для международного трафика в Европе, но не может использоваться с TASI, также известным как multiplex или «эта проклятая обрезка».

CCITT 5

Самая популярная система и та, что используется в США. 2400 Hz и печально известные 2600 Hz используются для link-to-link, а не просто для end-to-end line signals. Registers обрабатываются через DTMF, то есть touchtones.

Автор спрашивает:

> *Кто-нибудь знает, что делает 2400?*

CCITT 5 bis

То же, что выше, но тон 1850 Hz используется для TASI locking и передачи line signals.

CCITT 6

Самая новая и худшая для фрикеров. Она использует цифровые данные, отправляемые out-of-band, чтобы управлять соединением. Другими словами, соединение устанавливается и billing начинается **до** того, как вы можете получить управление.

CCITT 5R1

Региональная система вроде CCITT 5, но она не использует загадочные 2400 Hz и не может использовать multiplexer.

CCITT 5R2

Вероятно, это интерфейс к AUTOVON, поскольку он использует тоны с интервалом 120 Hz для DTMF вместо 200 Hz. Кроме того, 3825 Hz является blow-off tone вместо 2600 Hz.

«Дополнительные» тоны

```
1700 + 700  = Inward Operator
1700 + 900  = Delay operator; также в TSPS/STP
              ("Zero Plus" call from a coin phone)
1700 + 1100 = KP1 (start recognition of special tones)
1300 + 1700 = KP2 (end recognition of special tones)
```

12-85
Data Line
CIS 72767,3207
TWX 650-240-6356

Частная аудитория

(Базовый курс в искусстве подслушивания)

Автор: The Overlord

Часть I: Закон

Федеральный закон:
Раздел 605 главы 47 Кодекса США запрещает перехват сообщений или разглашение перехваченных сообщений, за исключением лиц, перечисленных в разделе 119 главы 18 (часть Закона об общем контроле над преступностью и безопасности улиц 1968 года). Этот закон гласит, что «не является незаконным по настоящему закону для оператора коммутатора, или должностного лица, сотрудника или агента любого общего носителя связи, чья коммутационная система используется при передаче проводной связи, перехватывать или раскрывать перехваченные сообщения».

Всё это юридическое дерьмо говорит о том, что если вы не работаете в телефонной компании, то вы не можете прослушивать чужие линии. Если вы всё же решитесь и вас поймают, это может стоить вам до 5 лет жизни и $10 000. Все вы, конечно, решите, что это означает: если вы прослушиваете чужую линию, вас накажут... неверно! Вы не можете прослушивать и собственную линию. Наказание за это, скорее всего, не более чем лёгкий выговор — если вас вообще поймают, — но знать это полезно... а теперь к делу.

Часть II: Прослушивание

Каждый хотя бы раз хотел услышать, что говорит по телефону друг, директор школы, королева выпускного бала или сосед. Существует несколько простых способов подключиться к телефонной линии. Ни один из представленных методов не потребует проникновения в дом. Всё можно сделать с заднего двора. Я расскажу о четырёх методах прослушивания — в порядке возрастания сложности.

1. «Бежевая коробка»: бежевая коробка (или bud box) широко известна как «телефон монтажника». Её чрезвычайно просто сделать, и это самый лёгкий в использовании метод. Она представляет собой обычный телефон, у которого отрезан модульный разъём для розетки и к красному и зелёному проводам прикреплены два зажима-«крокодила». Способ применения: зайти во двор к человеку, которого хотите прослушать, и подключиться к его линии. Лучше всего это делать у телефонной распределительной коробки Bell, которая обычно находится рядом с газовым счётчиком. Она держится, как правило, на одном винте и очень легко открывается. Внутри вы увидите 4 винта с прикреплёнными проводами. Если в доме одна линия, подключите красный провод к первому винту, зелёный — ко второму. После этого вы окажетесь на линии «прослушиваемого» и будете слышать любой разговор. Настоятельно рекомендую убрать динамик из используемого вами телефона, чтобы «прослушиваемый» не слышал каждый ваш звук. Если в доме две линии, вторая находится на третьем и четвёртом винтах. Если вы всё подключили

правильно, но на линию не попали, скорее всего провода перепутаны. Поменяйте красный на второй винт, а зелёный — на первый. Если разговора нет, может возникнуть проблема: вы не сможете долго ждать, а пока вы на линии, «прослушиваемый» не может позвонить — это нежелательно. Переходим к методу два.

2. Диктофон: этот метод, пожалуй, самый распространённый, и он также не требует особых умений. Существует масса способов записывать разговоры. Два наиболее простых: либо прикрепить «телефонный индукционный датчик» (Radio Shack, $1.99) к используемой бежевой коробке, подключив его к гнезду микрофона небольшого диктофона и оставив на запись, либо подключить диктофон напрямую к линии. Для этого возьмите штекер от плеера, отрежьте наушники, выберите один из двух проводов наушников и зачистите его. Внутри обнаружится ещё один провод — зачистите и его, прикрепите к ним зажимы-«крокодилы» и следуйте инструкции по бежевой коробке для записи разговора. Чтобы экономить плёнку, воспользуйтесь диктофоном с голосовой активацией (Radio Shack, $59) или, если у вашего диктофона есть разъём «remote», купите в Radio Shack «контроллер записи телефона» за $19 — он включает диктофон, когда трубка снята, и выключает, когда положена. Эта маленькая коробка подключается прямо в розетку (разумеется, через модульный разъём), поэтому лучше не отрезать модульный разъём. Обойдите это ограничение, если можно. Если нет — просто постарайтесь обеспечить хорошее соединение. При записи желательно прятать диктофон (по возможности в коробке Bell), но так, чтобы было удобно менять кассеты.

3. Беспроводной микрофон: это «жучок». Он передаёт сигнал с телефона на радиоприёмник (FM-диапазон). Возможно, вы помните Mr. Microphone (от Kaytel); такие беспроводные микрофоны продаются в Radio Shack за $19. Их легко собрать и подключить. Существует так много разных моделей, что почти невозможно дать точные инструкции. Чаще всего нужно отрезать элемент микрофона и прикрепить два провода к первому и второму винтам. В зависимости от марки линия МОЖЕТ оказаться «постоянно снятой с рычага». Это плохо, но, повозившись немного, вы должны добиться нужного результата. У этого метода два недостатка. Первый: бедолага, которого прослушивают, может услышать себя на «FM 88, the principal connection». Второй — радиус действия. Магазинные передатчики имеют ОЧЕНЬ короткий радиус. Рекомендую собрать доработанную версию, которую я представлю в части четвёртой (к тому же она дешевле). А теперь — лучший из всех методов...

4. «Easy-talks»: этот метод сочетает в себе лучшие качества всех прочих методов. У него лишь один недостаток... Вам нужен комплект рации «Easy-talk». Они оснащены голосовой активацией и стоят около $59. Их можно найти в магазинах игрушек и «высокотехнологичных» каталогах. Думаю, подойдут любые рации с голосовой активацией, но я пробовал только Easy-talks. Сначала определите, какая рация будет «передатчиком», а какая — «приёмником». Лучше использовать для передачи ту, у которой сигнал сильнее, даже если она лучше и принимает. Выпаяйте динамик «передатчика» и микрофон «приёмника». Идите к коробке, установите рацию в режим «VOX» и подключите провода микрофона (как в методе три) к первому и второму винтам в коробке. Вернитесь домой и слушайте на своей рации. Если ничего не происходит, значит сигнал телефона недостаточно сильный для активации передачи. В этом случае есть два варианта. Первый: добавить несколько проводов заземления к разъёмам микрофона. Это наименее заметно, но если не поможет — нужен усилитель, например плеер с двумя гнёздами для наушников. Вставьте первый штекер в линию и в одно из гнёзд плеера. Затем максимально увеличьте громкость (не нажимая воспроизведение). После этого подключите второй штекер для наушников к проводам микрофона и во второй разъём для наушников плеера. Уложите всё это в коробку и закройте её. Должно сработать. Это даёт вам личную радиостанцию для прослушивания: когда надоест — можно выключить, а со спикера рации можно и записывать!

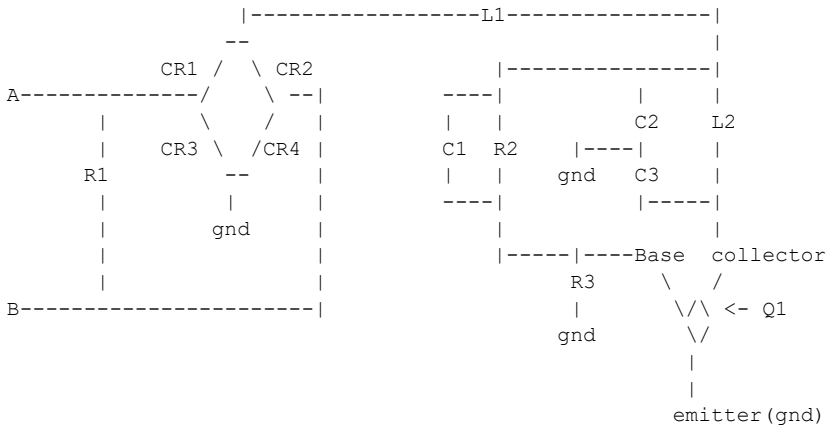
Часть IV: Схема беспроводного передатчика

Это крошечный передатчик, построенный на одном генераторе Колпитца, питающемся от телефонной линии. Поскольку сопротивление, которое он создаёт на линии, составляет менее 100 Ом, он никак не влияет на работу телефона и не может быть обнаружен телефонной компанией или прослушиваемым. Поскольку это маломощное устройство без антенны для излучения, оно является законным с точки зрения FCC (то есть соответствует части 15 правил и регламентов FCC). Однако его применение всё равно незаконно — просто само устройство законно. Это объясняется позже в части 15: «ни одно лицо не должно использовать такое устройство для подслушивания, если только это не разрешено всеми сторонами разговора» (тогда это ведь и не подслушивание, не так ли?). Устройство использует четыре диода для образования «мостового выпрямителя». Он вырабатывает переменное постоянное напряжение, изменяющееся в соответствии с автосигналами на линии. Это напряжение питает транзистор генератора, подключённый к радиосхеме. Отсюда можно настроить его на любой нужный канал. Остальное будет объяснено ниже...

СПИСОК КОМПОНЕНТОВ

Элемент	Описание
C1	47-Pf ceramic disk capacitor
C2,C3	27-Pf mica capacitor
CR1,CR2,CR3,CR4	germanium diode 1n90 or equivalent
R1	100 ohm, 1/4 watt 10% composition resistor
R2	10k, 1/4 watt 10% composition resistor
R3	.7k, 1/4 watt 10% composition resistor
L1	2 uH radio frequency choke (see text)
L2	5 turns No.20 wire (see text)
Q1	Npn rf transistor 2N5179 or equivalent

L1 можно собрать, намотав примерно 40 витков провода No.36 с эмалевой изоляцией на резистор мегаом, 1/2 Вт. Точное значение L1 не критично. L2 изготавливается путём намотки 5 витков провода No.20 на оправку диаметром 1/4 дюйма. После намотки оправку можно убрать. Просто припаяйте катушку на плату — она должна хорошо держаться. Также убедитесь, что Q1 установлен правильно: эмиттер, база и коллектор должны попасть в нужные отверстия. Принципиальная схема достаточно проста для понимания. Несмотря на необычно большое количество точек заземления, она работает.



Необычная особенность этого жучка, о которой мы ещё не говорили, заключается в том, что он подключается только к одному проводу (красному или зелёному). Идите к коробке, отсоедините красный провод, который УЖЕ был на винте 1, и подключите его к проводу «A» жучка. Затем подключите провод «B» к самому винту. Частоту, на которой сигнал выйдет на FM-канале, можно регулировать, сжимая или растягивая витки катушки L2. Настройка займёт несколько минут, зато устройство очень универсально. Вы можете менять частоту по желанию и легко записывать с

радиоприёмника.

Часть V: Полезные советы

Прежде всего, с первым методом — бежевой коробкой — вы можете заметить, что через используемый телефон можно также набирать номера. Не рекомендую этого делать. Если вы всё же решитесь и совершите нечто заметное — например, организуете трёхчасовую конференц-связь на 30 человек, — убедитесь, что эти люди либо уехали из города, либо мертвы. В целом при прослушивании линии нужно быть осторожным. Я сначала проверяю всё на своей линии, а затем устанавливаю устройства поздно ночью. Не рекомендую оставлять диктофон включённым на весь день. Включайте его, когда нужно, и убирайте, когда закончили. Что касается записи, думаю, что наличие диктофона на линии периодически посылает сигнал в телефонную компанию. Зато если вы пишете не напрямую с линии (например, с радио), то даже самое сложное оборудование не сможет определить, что вы ведёте запись. Также убедитесь, что при установке устройства люди НЕ разговаривают по телефону. Установка сопровождается множеством шорохов, щелчков и помех. Этого, как правило, лучше избегать. Не нужно большого ума, чтобы просто позвонить в дом перед установкой. Если занято — подождите. (Это, разумеется, не относится к «полуночным вылазкам».)

В целом, если использовать здравый смысл и быть *ОЧЕНЬ* осторожным, шансы попасться невелики. Никогда не думайте, что вы неуязвимы, и не трезвоните о своих делах. Держите это при себе — и отлично проведёте время.

-[OVERLORD]-

Благодарности:

The CircleLord
TARAN KING
Knight Lightning
The Forest Ranger
P-80 systems

Следите за продолжением: более продвинутые методы прослушивания, способы обнаружения и верификация — в ближайшем будущем.

Fortell Systems

Автор: Phantom Phreaker
Дата: 6 января 1986 года
BBS: The Alliance, `618-667-3825`

Fortell systems, похоже, являются системами для мониторинга линий. Их можно использовать только для мониторинга линий внутри собственного NPA.

Одна Fortell-система находилась по номеру:

```
716-955-7750
```

Когда вы звоните, вы услышите:

```
Hello. This is the Taradyne Fortell system. Please enter ID code
```

ID для этой системы:

```
722877*
```

После ввода этого кода через DTMF система спросит:

```
please enter line number
```

Здесь вводится `PRE+SUFF` номера, который нужно проверить внутри NPA Fortell.

После ввода номера система повторит введённый номер и спросит:

```
please enter mode
```

Режимы

```
1 - Calling on other line
2 - Calling on test line
3 - Line test results
```

Mode 1

Если выбрать mode 1, доступны следующие команды:

```
1 - Fault location
2 - Other testing
7 - Test ok, Monitor
8 - Hang up
9 - Enter next line number
```

Если здесь ввести `7`, система повторит выбранное и попросит ID code, которым может быть любой шестизначный номер, за которым следует `*`.

Затем система наберёт номер и скажет:

```
Subscriber busy-busy-monitor test in progress
conversation on line-short on line
```

После этого доступны варианты:

```
2 - Monitor test
3 - Overide and test
4 - Wait for idle
```

Если ввести `2`, то есть Monitor Test, система снова сообщит busy status.

Если ввести `3`, она выполнит override или скажет:

```
Not available in this CO
```

Если ввести `4`, Wait for idle, система будет ждать, пока линия станет idle.

Fault Location

Если в главном списке выбрать `1`, Fault Location, будут доступны варианты:

```
1 - Open location
3 - Short location
4 - Cross location
5 - Ground location
8 - Hang up
```

Если выбрать `2`, Other testing, доступны команды:

```
2 - Loop Ground OHMS
3 - Dial tone test
5 - Pair ID
8 - Hang up
```

Mode 2

Если выбрать mode 2, доступны варианты:

```
2 - Other testing
7 - Test ok, Monitor
8 - Hang up
9 - Enter next line number
```

Система повторит выбранное. Если здесь выбрать `2`, доступны команды:

```
2 - Loop Ground Omhs
8 - Hang up
```

Если выбрать `7` в главном списке после mode 2, система попросит ID, которым является любой шестизначный номер с `*` в конце. Затем она наберёт и проверит номер.

Если номер занят, система скажет:

```
Subcriber busy-monitor-test in progress-
conversation on line-short on line-please hang up-waiting for idle
```

После этого можно просто ввести `*`, чтобы вернуться к главному списку команд.

Mode 3

Если выбрать mode 3 и ранее уже выполнялся тест, система выдаст результаты теста. Если тест не выполнялся, она сообщит:

```
No test results available
```

В любой момент можно вернуться к главному списку команд, введя `*`.

Ввод `9` в нескольких местах возвращает к началу, где система просит:

enter line number

PP - 01/06/86

Электронный подслушиватель

Автор: Circle Lord

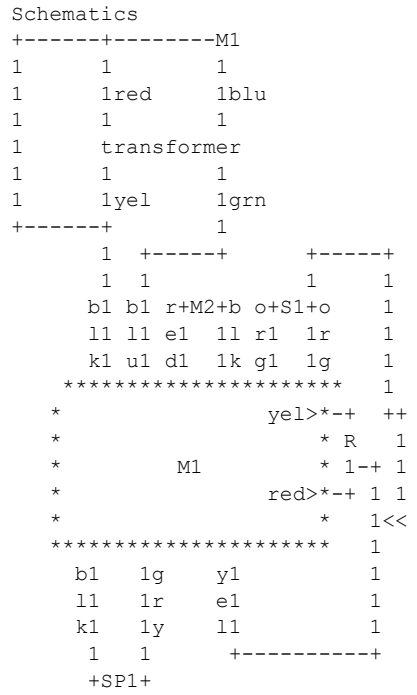
Вы когда-нибудь задумывались о покупке одного из тех высокочувствительных микрофонов, которые часто рекламируются в журналах по электронике, но считали, что это слишком дорого и слишком мало, чтобы украсть? Схема, представленная в этом файле, даст вам информацию, необходимую для самостоятельной сборки подобного устройства за значительно меньшие деньги.

Эти аудиоустройства для прослушивания, пожалуй, одни из самых горячих штучек в подполье благодаря своей способности улавливать голоса сквозь толстые стены. Вы также можете подключить провода динамика к магнитофону и записывать весь разговор. Как несложно догадаться, они отлично подходят для шантажа учителя, одноклассника, директора школы, соседа или любого другого человека, от которого вам что-то нужно...

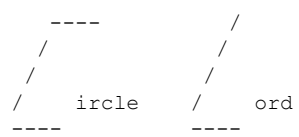
Список деталей

```
-=EM-------------------------
M1    Amplifier Module. (Lafayette 99C9037 or equiv.)
M2    9-VDC battery.
M3    Microphone
R1    20K poteniometer with spst switch.
S1    Spst switch on R1
SP1   8-ohm speaker
T1    Audio transformer (Radio Crap part  273-1380)
```

Схема



S1 здесь находится на потенциометре.
M3 может представлять собой капсюль от наушника.


ircle
ord

Изготовление электрошоковой дубинки

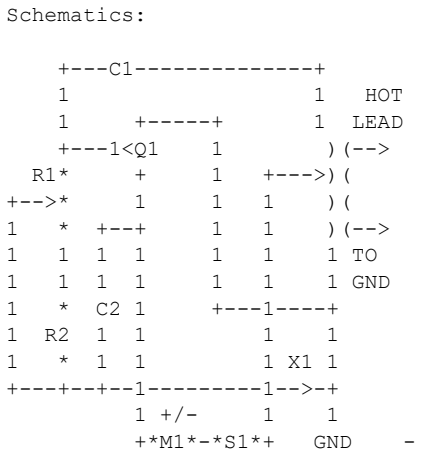
Автор: Circle Lord

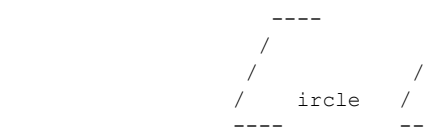
Эта удобная небольшая схема является ключом к генерации ТЫСЯЧ вольт электричества для отпугивания нападающих (заметьте — во множественном числе). Всё это вырабатывается от мощного источника питания в 6 вольт и легко помещается в трубчатый корпус. Изначально использовавшаяся как зарядник для электрического забора, эта схема может применяться и в других целях: например, для зарядки целого ряда школьных шкафчиков, ряда театральных кресел или металлических трибун в спортивном зале. Подробнее об этом — позже.

Для сборки вам понадобится транзистор GE-3, трансформатор на 6,3 В и горсть запасных деталей из старых радиоприёмников. Величина удара тока определяется положением потенциометра R1 — переменного резистора на 15 000 Ом. Подсказка: для максимального удара установите R1 на максимум!

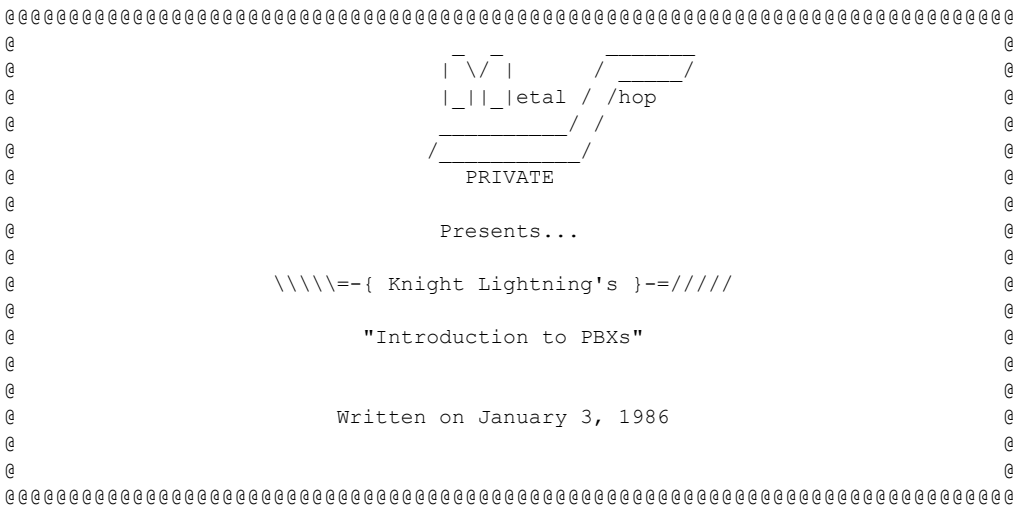
```
************************************************************
Item    *  Description
************************************************************
 C1      * 500uF, 10-WVDC electrolytic capacitor
 C2      * 2000uF, 15-WVDC electrolytic capacitor
 M1      * 6-VDC battery
 M2,M3   * Leads
 Q1      * GE-3 transistor (2n555 will also do)
 R1      * 15K potentiometer
 R2      * 160-ohm resistor
 S1      * Spst switch
 T1      * 6.3-VAC filament transformer (Triad F-14x or equiv.)
 X1      * 1N540 diode

************************************************************
```

Схема





Введение в АТС (PBX)



Автор: Knight Lightning

Данный файл является личным продолжением статьи об АТС из глоссария телекоммуникаций MCI.

Телефонная станция, обслуживающая отдельную организацию и имеющая соединения с публичной телефонной сетью, называется учрежденческо-производственной автоматической телефонной станцией (УПАТС), или в английской терминологии — Private Branch Exchange (PBX). АТС выполняет функцию коммутации, соединяя любой внутренний номер частной организации с внешней линией. По существу, АТС — это частная коммутационная станция, связывающая группу телефонов внутри отдельной организации. Вызовы, направленные за пределы этой группы, соединяются с центральной станцией телефонной компании через соединительные линии (транки). АТС может обслуживаться оператором организации, либо коммутация может осуществляться автоматически. Другими терминами, которые обычно используются как синонимы PBX, являются: Private Automatic Branch Exchange (PABX), Private Automatic Exchange (PAX) и Computerized Branch Exchange (CBX). Хотя изначально эти термины применялись для обозначения конкретных структур коммутаторов, сегодня они нередко используются как взаимозаменяемые.

АТС могут использовать один из трёх основных методов коммутации: шаговый (SxS), координатный (X-bar) и управляемый компьютером — для выполнения базовой функции коммутации. Однако помимо обнаружения вызовов и установления канала связи между двумя телефонами АТС способны делать гораздо большее.

Общее управление, нередко именуемое центральным процессором (CPU), управляет коммутационной матрицей, соединяющей абонентские точки и транки. Коммутационная матрица АТС выполняет ту же задачу, что и оператор на ручном коммутаторе или центральная станция с общим управлением. Однако CPU получает инструкции из «хранимой программы», которая содержит команды для таких действий, как обнаружение вызовов, маршрутизация по наилучшему доступному пути и запись тарификационной информации. Эти компьютеризированные электронные коммутаторы применяются для выполнения как стандартных, так и уникальных функций, которые были попросту непрактичны или даже невозможны при использовании электромеханических коммутаторов.

Так же как и в публичной коммутируемой сети, коммутаторы АТС устанавливают соединение между аппаратами, или «клавишными телефонными аппаратами». Все мы знакомы с клавишными телефонными аппаратами — знаем ли мы их по названию или нет. Это офисные телефоны с

шестью кнопками, расположенными под наборным диском: красная кнопка с надписью «удержание» и пять кнопок или линий с мигающими индикаторами.

Системы с АТС и клавишными аппаратами обладают большой гибкостью при планировании потребностей, поскольку позволяют настраивать коды для выполнения функций, необходимых в конкретных ситуациях. Более того, АТС может быть запрограммирована таким образом, что каждый отдельный внутренний номер в системе сможет воспользоваться возможностями, соответствующими именно его деловым нуждам.

Некоторые из функций, доступных в АТС и клавишных системах: переадресация вызовов — позволяет переводить внутренние или внешние вызовы с одного телефона на любой другой аппарат в системе; автоматическая кнопочная сигнализация — отображает состояние всех телефонов в системе с помощью световых индикаторов и кнопок; односторонняя голосовая страница — на которую можно ответить, набрав номер оператора с ближайшего телефона в системе; постановка в очередь (camp-on) — при которой вызов на занятый телефон автоматически ожидает освобождения линии; а также возможности внутренней и внешней конференц-связи, позволяющие внешним абонентам проводить конференции с несколькими внутренними пользователями.

Некоторые функции автоматически обрабатывают входящие телефонные вызовы. Автоматическое ожидание вызова не только удерживает звонки на занятый внутренний номер до его освобождения, но и уведомляет вызываемого абонента об ожидающем звонке, а также информирует звонящего о том, что он находится на удержании. Автоматическая переадресация вызовов будет направлять звонки сотрудникам, временно находящимся в местах, отличных от их кабинетов, при условии, что они «сообщили» АТС о своём местонахождении. Автоматическое распределение вызовов автоматически направляет входящий вызов на первый свободный внутренний номер — полезная функция в ситуациях, когда любой из группы сотрудников организации может адекватно ответить на входящие звонки. Ещё один пример — автоматический обратный вызов, позволяющий абоненту, попавшему на занятую линию, попросить АТС перезвонить ему, когда линия освободится.

Другие функции предоставляют такие услуги, как ночной ответ на телефонные звонки, мониторинг телефонного трафика и подключение к сети или выделенной линии (hot-line). Приведённые примеры — лишь небольшая часть возможностей компьютеризированных АТС.

Краткое руководство по использованию АТС

Это очень краткое описание того, как пользоваться АТС и чего от неё ожидать.

По существу, вы звоните на АТС и должны ввести код длиной от 4 до 6 цифр (примечание: некоторые АТС не требуют кодов). Затем вы услышите сигнал готовности (гудок). Отсюда в обычных условиях вы набираете:
`9 + 1 (или 0) + NPA-PRE-SUFF` для звонков на дальнее расстояние, или `8` для местных звонков.

Наиболее распространённое применение АТС — звонок в Alliance Teleconferencing, службу телеконференций AT&T. Для этого наберите:
`0700-456-1000, 1002, 1003, 2000, 2001, 2002.`

Примечание: коды АТС, как правило, очень простые и обычно состоят из 4 цифр.
Например: 0000, 1111, 1234 и т.д.

Следите за готовящимся файлом об Alliance Teleconferencing...

Это была презентация от Knight Lightning...

@@@

Phreak World News II

Составил: Knight Lightning

Опровержение

Мы в Phrack Inc. с уважением отзываем все заявления, сделанные в прошлом выпуске относительно Stronghold East Elite и LOD. Мы сожалеем о любых неудобствах, которые это могло вам причинить.

Phreaks Against Geeks

Эта группа была сформирована в шутку The W(hack)o Cracko Brothers Inc. на конференции в декабре 1985 года. Учредителями были TWCB, taRfruS, Blue Adept, The Clashmaster и ещё несколько человек. С тех пор Catcher in the Rye и Slovak пытались вступить.

Позже в том же месяце Boston Strangler и Micro Man сформировали PAP, что означает **Phreaks Against Phreaks Against Geeks**. Среди других противников PAG были Hack Attack, The Detective, Kleptic Wizard и The Overlord 313. Неизвестно, входят ли эти люди теперь в PAP.

Вся эта ерунда фактически началась на Dartmouth System и в основном является местной ссорой фрикеров в районе Boston, NPA 617.

Brainstorm получает 10 мегабайт

Наконец, после нескольких месяцев обещаний, Brainstorm (ELITE) теперь имеет 10-мегабайтный hard drive. По состоянию на 1 января 1986 года Modern Mutant очистил userlog Brainstorm, и начался набор участников.

Примечание: чтобы стать участником Brainstorm, нужно пройти небольшой и более-менее лёгкий filter. Среди новых возможностей Brainstorm — online games: Karate, Football и hacking simulation.

Anarchy Inc. распущена

Anarchy Inc., когда-то очень известная организация авторов g-phile, была распущена. В основном потому, что большинство её участников теперь учатся в колледже.

Dartmouth Conferences будут отменены?

Это сообщение выдавалось 9 января 1986 года, когда пользователь пытался присоединиться к конференции.

> *XCaliber, Fantasie, Spectre и так далее недоступны до завтра. Из-за давления со стороны Kiewit и некоторых пользователей конференции отключены на один день.*

> *Надеемся, это напомнит некоторым людям, что конференции являются публичным сервисом со стороны нескольких людей, а не «правом». Недавние злоупотребления конференциями сделали заботу о них почти большей проблемой, чем они стоят. Эти злоупотребления также заставили некоторых пользователей жаловаться Kiewit. Слишком много жалоб — и они могут исчезнуть совсем. Если все будут стараться поддерживать конференции достаточно чистыми и свободными от злоупотреблений, жизнь станет намного проще. Спасибо за ваше время и извините за отсутствие конференций.*

```
You are no longer connected to conference "XYZ".
```

Позже Corwin разозлился из-за password abuse и убил почти все пароли не-Dartmouth студентов. Также ходит слух, что он снял DUNE BBS, однако Apollo Phoebus говорит, что это временно и DUNE скоро снова поднимется.

Арест сотрудника MCI

Сотрудники MCI создавали фальшивые учётные записи, а затем накручивали огромные счета. Позже они либо кредитовали эти учётные записи, либо говорили, что абонент сообщил о code abuse. Любой сотрудник, пойманный на этом, был уволен.

Другой способ, которым эти сотрудники обманывали компанию, состоял в сообщении о code abuse на собственных учётных записях. Однако MCI Security, используя CNA, быстро поймала этих сотрудников.

Примечание: MCI Security заявила, что единственный реальный способ поймать злоумышленников телефонной компании — звонить по номерам, куда они звонили, и спрашивать, кого они знают из тех, кто совершал эти звонки.

Информация предоставлена через MCI Security.

Слияние MCI и IBM

MCI Telecommunications Company слилась с IBM и их телефонной индустрией SBS. Это была попытка объединить их как сильных союзников против AT&T.

```
IBM computers           Vs. AT&T computers
MCI Telecommunications  Vs. AT&T Telecommunications
```

Изменения, возникающие из-за этого слияния, если они будут, неизвестны, но в течение нескольких лет ничего не ожидается.

Жизнь и преступления W(hack)o Cracko Brothers

Дата — где-то декабрь 1984 года. Peter пишет code hacker для Hayes и говорит Tim **не** использовать его на Sprint, потому что Sprint трассирует. Позже той ночью Tim получает звонок от Scan Man, sysop P-80.

Scan Man сказал, что ему нужно, чтобы TWCB взломали для него несколько Sprint codes, потому что у него не было времени или Hayes. Tim сделал это для него на Sprint extender `314-342-8900`.

Он оставил программу работать всю ночь и весь следующий день, пока был в школе. Sprint отследил его. В 9:00 следующего утра агенты FBI, AT&T, Western Union, GTE и Southwestern Bell прибыли в дом TWCB.

Их впустили внутрь; с собой они принесли камеры, магнитофоны и другое оборудование. Увидев это, Peter подул в upstairs extension и отменил dialing program, но только после того, как агенты убедились, что это правильное место.

Всё компьютерное оборудование TWCB было конфисковано, а Tim вскоре после того, как его забрали из школы, был доставлен downtown. Peter был болен и остался дома. Позже Tim был отпущен под опеку матери.

Каждый получил probation и 100 часов county service.

Это было тогда.

Недавно TWCB попали под расследование по следующим поводам: употребление и торговля наркотиками, burglary, forgery и fraudulent use of a credit card.

```
Peter:
  8 Class A Felony charges
  1 Class A Misdemeanor charge
  1 Class B Misdemeanor charge

Tim:
  6 Class A Felony charges
  2 Class B Misdemeanor charges
```

Примечание: некоторые из этих misdemeanors связаны с невозвратом библиотечных книг.

Также говорили, что Tim был в тюрьме 11 раз. Оба участника TWCB теперь зачислены в reform school.

Информация в этой статье предоставлена TWCB, прямо и/или косвенно.

Blue Adept: ушёл навсегда

Blue Adept, известный как all-around loser и Dartmouth impersonator, решил попробовать blue boxing. По какой-то причине он решил позвонить напрямую на out-of-state trunk.

Позже в том месяце Blue Adept и его родители получили телефонный счёт примерно на 386 долларов. Это привело к тому, что ему запретили пользоваться телефоном.

Через некоторое время после этого инцидента Blue Adept получил приглашение присоединиться к конференции. Его не было дома, но родители решили остаться на линии и послушать.

Blue Adept больше не разрешено участвовать в конференциях, и все звонки ему теперь screened.

Overlord 313 арестован: отчим сдаёт его

Отчим Overlord постоянно проверял его компьютер, чтобы посмотреть, что на нём и что рядом. На прошлой неделе он заметил credits в файле Overlord о wiretapping, который можно увидеть в этом выпуске Phrack.

Он сообщил о находке матери Overlord. Она поговорила с ним, и он пообещал прекратить свои злые дела. Отчим не поверил ему ни на секунду.

Отчим отправляется в командировку, где встречает Ma Bell executive Don Mitchell. Он задаёт разные вопросы об использовании MCI dialups и Alliance Teleconferencing и рассказывает, что его пасынок делает все эти вещи и даже больше. Don настоятельно предлагает сообщить об этом телефонной компании.

```
1-13-86

HE DOES
```

На данный момент против Overlord не было предпринято никаких юридических действий.

Информация предоставлена The Overlord of 313.

Maelstrom 305 арестован

Хотя я не вправе раскрывать всю информацию об этом аресте, я упомяну основные факты.

Maelstrom взломал Southern Bell Data Network (SBDN). Эта система оказалась местной для него, поэтому он не стал использовать extender. К сожалению, в этой системе также был ANI, Automatic Number Identification.

Его компьютер и другое оборудование, а также все его файлы были конфискованы как доказательства.

Информация предоставлена The Maelstrom of 305.

Whackoland BBS

Эта BBS теперь поднята и уверенно работает. Её sysops, конечно же, TWCB Inc.

```
300/1200 Baud
40 Megs
314-256-8220
```

У неё уникальные возможности, отличные mods и Elite Sections. Звоните сегодня.

Примечание: будет оставлено только 100 пользователей, так что если вы совсем новичок, пожалуйста, не беспокойтесь звонить.

R.I.P. Broadway Show

Broadway Show BBS в Нью-Йорке теперь закрыта, а Broadway Hacker скоро будет в Washington DC. Эта BBS на C-64 была одной из лучших в своё время, но позже стала местом обитания rodents.

Из её пепла возникает новая BBS, однако её название на момент написания ещё не опубликовано. Broadway Hacker будет sysop этой BBS примерно неделю, а затем передаст её новому sysop. Его имя пока неизвестно, вероятно, потому что у него ещё нет handle.

Хотя новая BBS будет выглядеть легальной и иметь некоторые legal sections, на самом деле это phreak BBS, и её стоит проверить.

```
718-615-0580
```

Speed Demon Elite закрыта?

Эта BBS, sysop которой был Radical Rocker, внезапно исчезла, оставив звонящему сообщение об отключении линии. Другой информации нет.

Это всё для Phreak World News этого выпуска. Если у вас есть какие-нибудь новости:

```
Knight Lightning / Taran King / Cheap Shades
```