

СНЕЦ ТАНЦЕР

№10(59) ● ОКТЯБРЬ ● 2005

ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

В поисках Wi-Fi Пособие для начинающего вардрайвера

Ты решил приобщиться к армии вардрайверов и стать еще одним воином беспроводных сетей? Мы подготовили подробную инструкцию для начинающего вардрайвера.

Стр.
12



Взлом Пентагона Как взломать закрытую сеть

Настоящие хакеры не знают границ и проникают в закрытые сети различных могущественных организаций. Как они это делают? Продемонстрируем технику взлома на примере серверов милитаристского Пентагона.

Стр.
72



МОБИЛЬНЫЙ ВЗЛОМ

Мобильные атаки и безопасность беспроводных устройств

БОНУС Тест Видеокарт

Стр.
108



В ЖУРНАЛЕ Все о беспроводных сетях **4**, Война на колесах **8**,
Мобильный ужас **38**, Червивый КПК **44**, SIM-SIM, откройся **48**, Секретов не будет **52**,
Власть SMS **56**, Арсенал для охоты **60**, Атака на Cisco IOS **66**, Взлом Пентагона **72**,
Трубки-сканеры **84**, Вам звонят из милиции **88**, Фрикинг по-жесткому **94**

НА CD AirSnort 0.2.7e ■ Cryptex
WarLinux 0.5 CD ISO ■ Ethereal 0.10.12
NetStumbler 0.4.0 ■ MiniStumbler 0.4.0
Kismet 2.8.1/3.0.1 ■ StumbVerter 1.50 ■ TCPDump 3.9.3
TrunkSniffer Pro 3.0 ■ httpprint ■ WiFiScanner 0.9.1



(game)land
ISSN 1609-1027



Let's Hi-Fi!!!

9 771609 102006 10 >

Создай свою реальность

с компьютером DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT



Включи DEPO Ego — и перед тобой откроется новая реальность твоих любимых компьютерных игр. Наслаждайся быстротой реакции и скоростью, исследуй распахнувшийся перед тобой мир высококачественной компьютерной графики и настоящего экшена. Теперь эта цифровая реальность может стать твоей благодаря компьютеру DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT.



DEPO Ego 360 TV:

- процессоры Intel® Pentium® 4 с технологией HT серии 6xx (2Mb cash второго уровня)
- чипсет Intel® 925XE с улучшенной архитектурой
- сверхбыстрая память DDR2
- новые возможности графики PCI-Express
- реалистичный объемный 8-канальный звук

Компания DEPO Computers Тел./факс: (095) 969-2215, www.depo.ru

Intel, Intel Inside, the Intel Inside Logo и Intel Pentium являются зарегистрированными товарными знаками Intel Corporation и её отделений в США и других странах. Microsoft и Windows являются зарегистрированными товарными знаками компании Microsoft и её отделений в США и других странах.



INTRO

Wi-Fi, GPRS, EDGE, Bluetooth... Развитие беспроводных технологий и портативных устройств дарит тебе настоящую мобильность и практически безграничные возможности. НО... С одной стороны, ты впервые становишься по-настоящему свободным. Интернет, электронная почта - теперь что угодно из этого доступно где угодно. С другой стороны, каждая новая мобильная технология делает тебя уязвимее. В этом году мир высоких технологий столкнулся с новой опасностью - вирусами для мобильных устройств. В одночасье были похищены конфиденциальные данные некоторых знаменитостей, новые трояны стали выводить из строя смартфоны. Ты тоже можешь стать жертвой, даже не заметив этого.

Мы подготовили этот Спец, чтобы ты мог свободно ориентироваться в мире высоких технологий. Мобильная оборона, мобильная защита - все это в "Мобильном взломе". Wi-Fi и Bluetooth-атаки, SMS-спам, SMS-убийцы, клонирование SIM-карт, фрикинг, вирусы для мобильных телефонов, смартфонов и КПК, уязвимости в операционных системах портативных устройств, как сделать трубку-сканер из обычного радиотелефона и как защититься от нее - вот далеко не полный перечень информации, которую ты найдешь в этом Спеце. Кроме того, ты узнаешь, как взломать маршрутизаторы Cisco, на которых держится весь интернет, и сделать это с ноутбука! А на нашем диске ты найдешь весь необходимый софт для реализации самых безумных планов.

Добро пожаловать в мир беспроводных технологий. Помни, что ты сможешь стать по-настоящему мобильным только если полностью уверен в собственной безопасности.

Ашот Оганесян

СОДЕРЖАНИЕ № 10 (59)

WIRELESSECURITY

4 Долой провода!

Все о беспроводных сетях

8 Война на колесах

Разберемся, что такое вардрайвинг (wardriving) и с чем его необходимо употреблять

12 В поисках Wi-Fi

Пособие для начинающего вардрайвера

18 Без проводов и без защиты

Разбираемся в уязвимостях беспроводных сетей

24 Майские жуки

Часто встречающиеся слабости и баги 802.11 беспроводных устройств

28 Защита воздуха

Безопасность беспроводных сетей

32 Узнаем по походке

Обнаружение и fingerprinting Bluetooth-устройств

ИНСТРУМЕНТЫ

60 Арсенал для охоты

Вооружись до зубов для вардрайвинга



66 Завоевание интернета

Атака на Cisco IOS

72 Взлом Пентагона

Как взломать закрытую сеть

78 Утилизируй мобильного друга

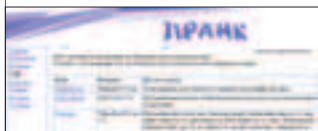
Обзор хакерских утилит для мобильных платформ

84 Трубки-сканеры

Все о взломе бесшнуровых телефонов

88 Вам звонят из милиции

Обзор софта для телефонных розыгрышей



90 За связь денег не берем

Все о бесплатных сервисах связи

94 Фрикинг по-жесткому

Фрикинг изнутри

SPECIAL delivery

98 Мобильная оборона

Как защитить себя от мобильного взлома



102 Обзор сайтов и софта

Что посмотреть о мобильном взломе на бескрайних просторах Сети

WIRELESSECURITY

4 В поисках Wi-Fi

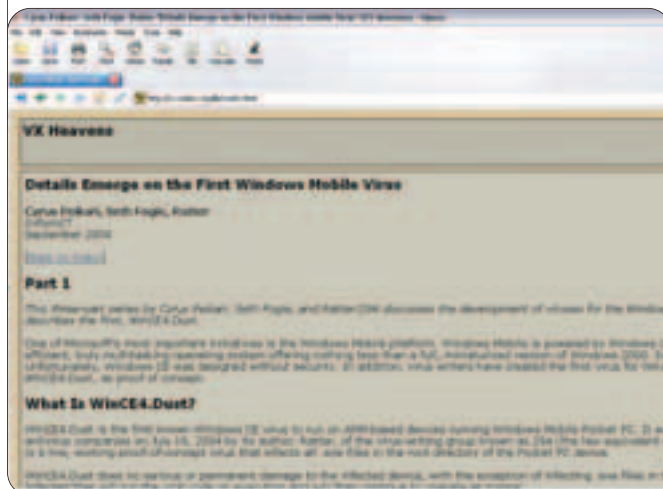
Пособие для начинающего вардрайвера



ВЗЛОМ УСТРОЙСТВ

38 Мобильный ужас

Вирусы нашли новую среду для обитания - мобильные девайсы



ВЗЛОМ УСТРОЙСТВ

38 Мобильный ужас

Вирусы нашли новую среду для обитания - мобильные девайсы



44 Червивый КПК

Первые вирусы, трояны для мобильных устройств

48 SIM-SIM, откройся

Все, что ты хотел знать о SIM-карте, но боялся спросить

52 Секретов не будет

Все о прослушивании мобильных телефонов



56 Власть SMS

SMS может больше, чем тебе кажется



ОФФТОПИК

HARD

108 Видеонападение!

Тестирование современных видеокарт

113 Матплата для железного экстремала

ECS PF5 Extreme

114 Паяльник

Стань PHREAK'ом: те самые коробочки

CREW

120 Е-мыло

Пишите письма

STORY

122 Овердрайв

ИНСТРУМЕНТЫ

44 Взлом Пентагона

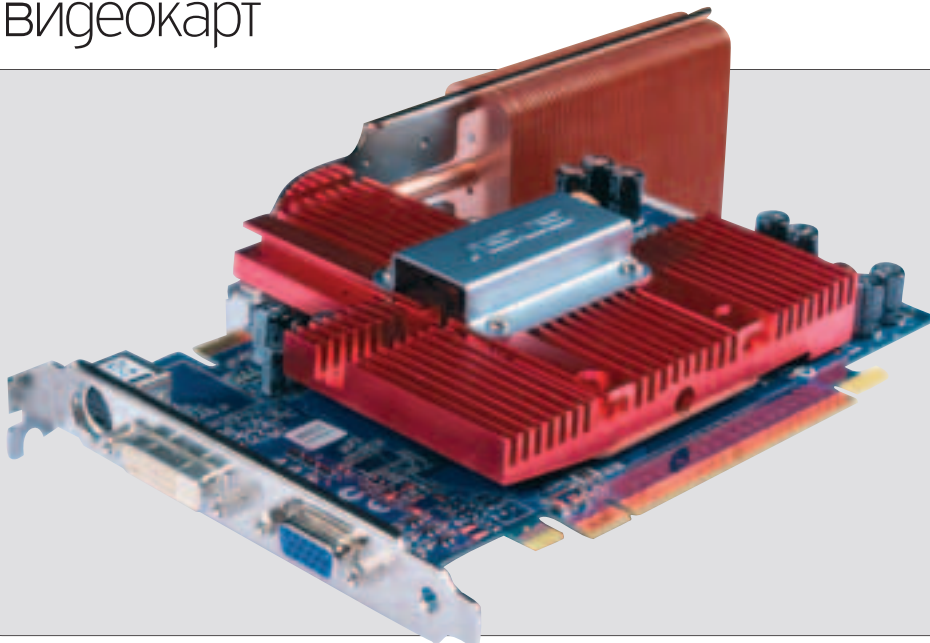
Как взломать закрытую сеть



HARD

106 ВИДЕОАТАКА!

Тестирование современных видеокарт



Редакция

» **главный редактор**
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)

» **выпускающие редакторы**

Ашот Оганесян
(ashot@real.xakep.ru),
Николай «Gorlum» Андреев
(gorlum@real.xakep.ru)

» **редакторы**

Александр «Dr.Klouniz» Позовский
(alexander@real.xakep.ru),
Андрей Каролик
(andrusha@real.xakep.ru)

» **редактор CD и раздела ОФФТОПИК**

Иван «SkyWriter» Касатенко
(sky@real.xakep.ru)

» **литературный редактор, корректор**

Валентина Иванова
(valy@real.xakep.ru)

Art

» **арт-директор**
Кирилл «KROt» Петров
(kegel@real.xakep.ru)

Дизайн-студия «100%КПД»

» **верстальщик**

Алексей Алексеев

» **художник**

Константин Комардин

Реклама

» **директор по рекламе ИД (game)land**

Игорь Пискунов (igor@gameland.ru)

» **руководитель отдела рекламы**

Ольга Басова (olga@gameland.ru)

» **менеджеры отдела**

Виктория Крымова (vika@gameland.ru)

Ольга Емельянцева (olgaeml@gameland.ru)

» **трафик-менеджер**

Марья Алексеева (alekseeva@gameland.ru)

тел.: (095) 935.70.34

факс: (095) 780.88.24

PR

» **директор по PR цифровой группы**

Глеб Лашков (lashkov@gameland.ru)

Распространение

» **директор отдела**

дистрибуции и маркетинга

Владимир Смирнов (vladimir@gameland.ru)

» **оптовое распространение**

Андрей Степанов (andrey@gameland.ru)

» **региональное розничное**

распространение

Андрей Наседкин (nasedkin@gameland.ru)

» **подписка**

Алексей Попов (popov@gameland.ru)

тел.: (095) 935.70.34

факс: (095) 780.88.24

PUBLISHING

» **издатель**

Сергей Покровский (pokrovsky@gameland.ru)

» **учредитель**

ООО «Гейм Лэнд»

» **директор**

Дмитрий Агарунов (dmitri@gameland.ru)

» **финансовый директор**

Борис Скворцов (boris@gameland.ru)

Горячая линия по подписке

тел.: 8 (800) 200.3.999

Бесплатно для звонящих из России

Для писем

101000, Москва,

Главпочтамт, а/я 652, Хакер Спец

Web-Site

<http://www.xakep.ru>

E-mail

spec@real.xakep.ru

Мнение редакции не всегда совпадает с мнением авторов. Все материалы этого номера представляют собой лишь информацию к размышлению. Редакция не несет ответственности за незаконные действия, совершенные с ее использованием, и возможный причиненный ущерб. За перепечатку наших материалов без спроса - преследуем.

Отпечатано в типографии «ScanWeb», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ № 77-12014 от 4 марта 2002 г.

Тираж 42 000 экземпляров. Цена договорная.

Степан Ильин aka Step (step@gameland.ru)

ДОЛОЙ ПРОВОДА

ВСЕ О БЕСПРОВОДНЫХ СЕТЯХ

История беспроводной передачи данных началась в далеком 1895 году, когда А.С. Попов изобрел первое радио. Принцип работы этого чуда техники такой: в передающей антенне создается переменный электрический ток высокой частоты, в окружающем пространстве он вызывает быстро изменяющееся электромагнитное поле, которое распространяется в пространстве в виде электромагнитной волны, достигает приемной антенны и вызывает в ней переменный ток той же частоты, на которой работает передатчик. Кто в 1895 году смог бы подумать, что этот же принцип будет использоваться для передачи данных на скорости в несколько мегабит в секунду?



С ЧЕГО НАЧИНАЛСЯ WI-FI

■ Так уж повелось, что, когда заходит речь о беспроводной передаче данных, сразу вспоминаешь технологию Wi-Fi. Ее развитие началось в далеком 1997 году, когда международная организация IEEE (Институт инженеров электричества и электроники) ратифицировала небезызвестный стандарт 802.11, четко определивший понятия беспроводной сети, используемых ею частот, характеристики устройств и параметры соединения между ними.

Устройства Wi-Fi могут работать в двух режимах. Первый, Ad-hoc, подразумевает, что беспроводная сеть состоит всего из двух беспроводных девайсов, они соединяются друг с другом напрямую (соединение "точка-точка"), то есть без участия какого-либо промежуточного оборудования. Такой режим позволяет создать полноценную сеть со всеми сопутствующими сервисами и возможностями, однако он подходит для соединения только двух клиентов.

Совсем по-другому сложилась ситуация с Infrastructure: многочисленные клиенты общаются друг с другом с помощью специального коммутирующего устройства - точки доступа (Access Point, AP). Такой режим позволяет не только организовать беспроводную сеть из нескольких устройств, но еще и спланировать между собой несколько Wi-Fi-сетей, а также наладить мост на обычную локалку. Что касается скорости такого соединения, то для стандарта 802.11 она составляет 1-2 Мбит/с. При этом используется рабочая частота от 2,400 МГц до 2,483 МГц, а также один из двух принципиально разных методов кодирования: FHSS и DSSS.

FHSS (Frequency-Hopping Spread Spectrum) - это так называемый метод частотных скачков, который распределяет передаваемые данные по 75-ти каналам частотой 1 МГц. А в чем фишка? Передача осуществляется по единственному каналу одновременно, при этом смена канала осуществляется по схеме, которая случайна, но заранее известна участникам обмена. Такой подход позволяет уменьшить возможные помехи в эфире, так как данные передаются только в том случае, если обе стороны настроены на одну и ту же частоту. Приемник должен слушать эфир и в нужный момент переходить на нужную частоту, чтобы правильно принимать данные.

При этом данные передаются по одному каналу всего 400 мс.

DSSS (Direct-Sequence Spread Spectrum) - это уже совершенно другой метод кодирования, который основывается на использовании набора избыточных битов на каждую переданную единицу информации. Этот набор называется chipping-кодом и состоит из 11-ти дополнительных битов, генерируемых по специальному алгоритму, известному приемнику и передатчику. Если во время передачи один из переданных битов был поврежден, то его можно легко восстановить с помощью 11-ти дополнительных и обойтись без повторной отправки данных. А значит, можно обойтись сигналом очень малой мощности, не мешающим другим приемо-передающим устройствам: они не знают алгоритма, по которому создается набор избыточных битов, и поэтому считают их шумом обычным и почти не влияющим на работу. Все данные, закодированные по схеме DSSS, передаются по 14-ти перекрывающимся друг друга каналам частотой 22 МГц, но в каждый момент времени используется только один из них.

Из-за такой двойственности стандарта, который допускает совершенно разные методы кодирования, обнаружилась первая серьезная проблема. Устройства на базе DSSS были абсолютно несовместимы с теми, что использовали FHSS. Да и скорости "до двух Мбит/с" были далеки от идеала. Но прогресс не остановился в деле дополнения стандартов новыми подробностями, и уже в 1999 году было утверждено новое расширение стандарта беспроводной передачи данных - IEEE 802.11b.

БЫСТРЕЕ, СИЛЬНЕЕ, НАДЕЖНЕЕ

■ Основное преимущество нового стандарта - значительно увеличенная пропускная способность в 11 Мбит/с. Правда, из-за некоторой специфики это значение является чисто теоретическим, а максимум, которого удастся добиться на практике, равен примерно 5,9 Мбит/с по протоколу TCP и 7,1 Мбит/с по UDP. Подобных показателей удалось достичь за счет полного перехода на метод кодирования DSSS. До этого момента на рынке было немало девайсов, которые использовали FHSS, стоимость их производства была на порядок меньше, но в то же время они были безнадежно ограничены в максимальной пропускной способности.

Content:

4 Долой провода!

Все о беспроводных сетях

8 Война на колесах

Разберемся, что такое вардрайвинг (wardriving) и с чем его необходимо употреблять

12 В поисках Wi-Fi

Пособие для начинающего вардрайвера

18 Без проводов и без защиты

Разбираемся в уязвимостях беспроводных сетей

24 Майские жуки

Часто встречающиеся слабости и баги 802.11 беспроводных устройств

28 Защита воздуха

Безопасность беспроводных сетей

32 Узнаем по походке

Обнаружение и fingerprinting Bluetooth-устройств

WIRELESSECURITY



Логотип Wi-Fi

Переход на схему кодирования DSSS прошел очень плавно, для производителей не составило труда адаптировать свои DSSS-девайсы для поддержки обновленного стандарта и молниеносно вывести их на рынок. Примерно в это же время звонким словом Wi-Fi (Wireless Fidelity) назвали ветку стандартов 802.11 и основали организацию Wireless Ethernet Compatibility Alliance (ныне Wi-Fi Alliance), которая стала метатщательно отслеживать все появляющиеся на рынке девайсы и проверять их совместимость, а тем самым - ликвидировать один из существенных недостатков 802.11.

Оборудование 802.11b все чаще стали использовать по схеме "точка-мультиточка". В свою очередь точки доступа (AP'шки) на базе 802.11b становились намного функциональнее. В связке с всесторонними (omni) антеннами они стали творить чудеса. Именно тогда начали появляться первые хотспоты, которые использовали несколько точек доступа и позволяли абоненту незаметно переключаться между ними в зависимости от месторасположения. Так, если клиент попадал в зону действия сразу двух или нескольких AP'шек, то его беспроводной адаптер автоматически подключался к той, которая имела наиболее стабильный и

сильный сигнал. В то же время мощность сигнала других точек доступа и количество ошибок в передаче постоянно отслеживались, и если какая-то точка доступа предлагала более комфортные условия, то подключение осуществлялось уже к ней. Эта функция роуминга между AP'ками очень похожа на механизм сотовой связи. Ты никогда не замечаешь, когда перемещаешься от одной базовой станции к другой, - телефон сам подключается к лучшей из них (но не всегда удачно).

Параллельно с этим нашлись умельцы, которые быстро приспособили 802.11b и в организации дальних линков. С помощью параболических антенн с высоким коэффициентом усиления (17-21 дБ) стало возможным наладить связь даже на несколько километров, правда, для этого требовались прямая видимость, качественные оборудование и кабель от внешних антенн до Wi-Fi-девайсов.

Столь универсальное применение Wi-Fi стало возможным благодаря функции динамической корректировки скорости (Adaptive Rate Selection). Wi-Fi-устройство может начать передавать данные на скорости 11 Мбит/с, но позже снизить ее до 5,5; 2 или вообще 1 Мбит/с, если сигнал будет недостаточно сильным. На малых скоростях используются более простые методы кодирования. Они менее эффективны, но используют избыточное кодирование и меньше подвержены влиянию посторонних шумов, потере пакетов, ослаблению сигнала. Важно, что скорость изменяется динамически, то есть она не только понижается, но и повышается, как только это позволит состояние канала. Для протокола 802.11b существуют также расширения, которые позволяют увеличить скорость до 22, 33 и даже 44 Мбит/с, но ни один из них не был полностью одобрен в IEEE, а необходи-



Точка доступа с двумя антеннами - идеальный вариант для дома

мость в них отпала сразу после появления расширения 802.11g.

802.11G И 802.11A

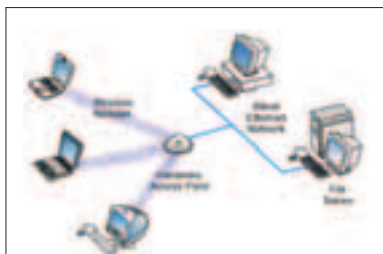
■ 802.11g, ставший стандартом де-факто и являющийся им до сих пор, был принят еще в далеком 2001 году. Это был самый настоящий прорыв: с помощью совершенно нового метода модуляции сигнала инженерам из IEEE удалось многократно увеличить скорость передачи данных. Теоретический максимум скорости устройств на базе 802.11g составляет 54 Мбит/с, что уже вполне сравнимо со скоростями обычных проводных ЛВС. Секрет в том, что новый метод модуляции сигнала (OFDM - метод ортогонального разделения частот) делит передаваемый сигнал на 48 отдельных несущих частот и передает данные одновременно по каждому из них. Помимо этого используется четыре контрольных частоты, с помощью которых осуществляется проверка целостности данных. Столь эффективное использование спектра позволило добиться огромной плотности битов и передавать данные на очень высоких скоростях.

В погоне за скоростью специалисты IEEE не забыли о принципе совместимого оборудования. Все новые 802.11g-устройства поддерживают старый метод модуляции (ССК) и полностью совместимы с девайсами на базе уже устаревшего 802.11b. Благодаря этому 802.11b могут легко работать в сетях 802.11g (но не быстрее 11 Мбит/с), а адаптеры 802.11g - снижать скорость передачи данных для работы в старых сетях 802.11b.

»



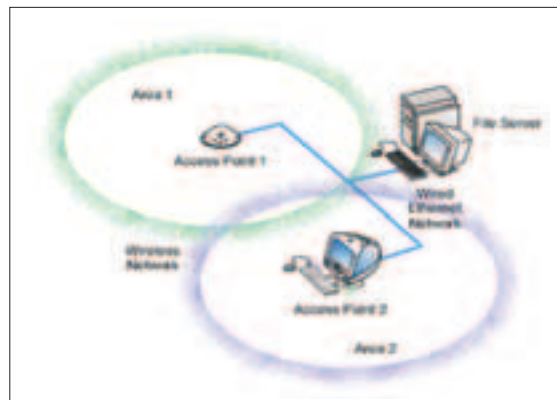
Схема подключения Ad-hoc: устройства подключаются друг к другу напрямую



В режиме Infrastructure устройства взаимодействуют друг с другом посредством точки доступа

WARNING!

■ Антенны точек доступа являются источниками высокочастотного излучения. И пусть мощность излучаемого сигнала ничтожна, старайся не находиться в непосредственной близости от рабочей антенны (даже если очень хочется), особенно если она имеет высокий коэффициент усиления или используется в связке с усилителем.



Функция роуминга позволяет перемещаться от одной AP к другой без обрыва соединения



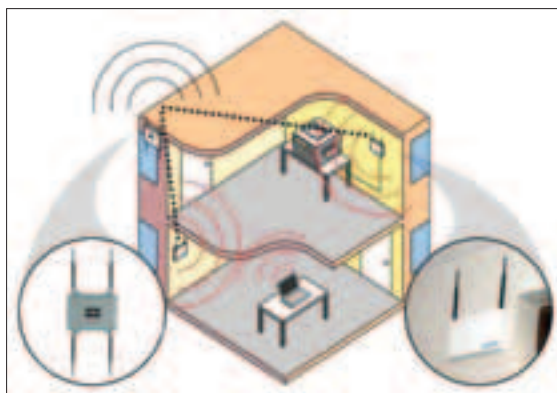
Wi-Fi-модуль для КПК

Метод ортогонального разделения частот стал стандартным и для расширения 802.11a, рабочими частотами которого являются диапазоны 5,15-5,25 ГГц, 5,25-5,35 ГГц и 5,725-5,825 ГГц. Переход на столь высокие частоты позволил еще больше увеличить эффективность беспроводной передачи данных. Пусть максимальная пропускная способность 802.11a остается на уровне 802.11g и не превышает 54 Мбит/с, но средняя скорость - значительно выше. Еще один плюс - меньшая интерференция радиочастот.

Радиооборудование доступно, использование частоты 2,4 ГГц контролируется слабо, как результат - нарождающаяся армия пиратов. Многочисленные наводки и помехи от "нелегалычиков" мешают полноценно работать даже тем людям и организациям, которые имеют на это официальные разрешения. Оборудование для 5 ГГц стоит существенно дороже, поэтому пока практически не используется пиратами. К тому же Wi-Fi использует высокую частоту, поэтому значительно ограничивает свои возможности и скрывает от нас многие свои прелести.

ЗА СЕМЬЮ ЗАМКАМИ

Любая беспроводная сеть намного более беззащитна перед атаками извне, чем обычная проводная локалка, - это очевидно. Физически подключиться к проводам, проложенным внутри здания, чаще всего практически невозможно, а перехватить радио-



Wi-Fi сегодня успешно используется как внутри помещений, так и для организация дальних линков вне зданий

ПОЛЕЗНЫЕ ССЫЛОЧКИ

- www.wi-fi.org/OpenSection/FAQ.asp - официальный FAQ по Wi-Fi.
- interfaces.by.ru/80211g.htm - подробное описание стандарта IEEE 802.11g.
- interfaces.by.ru/bluetooth.htm - подробно о Bluetooth.
- www.bluetooth.org/spec - полная спецификация технологии Bluetooth.
- www.freewifi.ru - база данных по хотспотам в России.



Взлом WEP - дело нескольких минут

сигнал - небольшая проблема. Специалисты из IEEE позаботились о безопасности Wi-Fi-канала, поэтому расширение 802.11b поддерживает специальную криптографическую защиту WEP (Wired Equivalent Privacy). Весь передаваемый поток данных с помощью WEP шифруется по алгоритму RC4, при этом используется 40- или 104-битный ключ, дополненный 24-битным иницирующим вектором (IV), который передается между устройствами в открытом виде. Такой подход первоначально считали довольно надежным, однако со временем в нем нашли массу изъянов (читай этот Спец гальше). Отчасти эти изъяны компенсировал список контроля доступа (Access Control List), реализованный на базе большинства точек доступа. Если соответствующая функция была включена, то AP'ка принимала подключения только от известных беспроводных устройств, однако и это не могло гарантировать полной безопасности.

2003 год, появившаяся в нем технология WPA (Wi-Fi Protected Access) и ее множественные достоинства прекратили этот беспорядок. Если WEP шифрует весь поток данных одним и тем же ключом, то WPA использует отдельный ключ для каждого (!) переданного пакета. Даже если хакер перехватит часть потока, ему вряд ли удастся расшифровать его. Более того, точка доступа с включенным режимом WPA будет блокировать все попытки клиентского подключения по

тех пор, пока не произойдет аутентификация на уровне логина и пароля. После этого для клиента будет сгенерирован специальный 128-разрядный ведущий ключ, который будет отослан по безопасному протоколу TKIP (Temporal Key Integrity Protocol). Новая система аутентификации (Certificate Authority Server) гарантирует, что беспроводное устройство, к которому производится подключение, действительно является тем, за кого себя выдает, а средство проверки целостности сообщений (Message Integrity Checker - MIC) в значительной мере исключает атаки Man-in-the-Middle. Но это еще не все. В 2004 году Wi-Fi Alliance опубликовал пресс-релиз второго поколения WPA, который использует еще более сложный метод шифрования AES (Advanced Encryption Standard) и удовлетворяет самым высоким требованиям к безопасности.

ЗУБЫ РЕЖУТСЯ

Думаю, технология Bluetooth (IEEE 802.15.3) в представлении не нуждается. Если с Wi-Fi успели познакомиться еще галеко не все, то ощутить прелести Синего Зуба удалось почти каждому. Сразу напрашивается вопрос: "Откуда такое странное название?" Говорят, технология Bluetooth названа в честь датского короля Харальда Голубого Зуба, прозванного так из-за темного переднего зуба. В X веке этому монарху удалось объединить территории современных Норвегии, Дании и Шве-

ции. Если проводить аналогию, то технология Bluetooth должна объединить оборудование самых различных отраслей (компьютеры, мобильные технологии, автомобили и т.п.).

Идея разработки Bluetooth возникла в 1994 году, когда команда исследователей Ericsson Mobile Communications положила начало изучению мало-мощной беспроводной технологии, действующей в узком диапазоне, для экономии кабелей между мобильными телесфонами и компьютерами, наушниками и другими устройствами. Позже к этой разработке присоединились такие бренды, как IBM, Intel, Nokia и Toshiba. Множественность компаний, участвующих в разработке, и недостаточно документированная первая версия спецификации Bluetooth привели к появлению несовместимых между собой прототипов. Для того чтобы дважды не наступать на одни и те же грабли, в 1997 году была учреждена специальная группа SIG (Special Interest Group), которая занялась разработкой и продвижением единой спецификации Bluetooth, а также следила за соблюдением стандартов. Сейчас в число ее членов входят несколько десятков известнейших компаний. Примечательно, что технологию Bluetooth может беспрепятственно использовать любой производитель, поэтому встроенные модули Bluetooth уже не являются диковинкой, а повсеместно интегрируются во всевозможные устройства. Через год-два все мобильные телефоны, ноутбуки и КПК будут оснащаться модулями связи этого стандарта.

Диапазон частот 2400-2483.5 МГц, используемый Bluetooth, выбран не случайно. В большинстве стран он не нуждается в лицензировании, поэтому может свободно использоваться. Ты подметил, что выбранные частоты в точности повторяют Wi-Fi. Да, ты прав. Однако использование одинакового диапазона частот практически не влияет на их совместную работу. Чтобы избежать конфликтов, Bluetooth использует очень слабый сигнал всего в один милливатт. Модули связи этого стандарта не создают помех не только для Wi-Fi, но и для сторонних Bluetooth-соединений еще и потому, что в основе технологии лежит механизм псевдослучайного переключения частот. Любое устройство, оснащенное Bluetooth-модулем, одновременно работает только на одном из 79-ти каналов и переключается между ними 1600 (!) раз в секунду. Частота, на которую будет происходить переключение, заведомо известна как приемнику, так и передатчику, - таким образом осуществляется непрерывная связь. Как и в протоколе IP, данные в Bluetooth посылаются отдельными пакетами, в которых, помимо информационного поля и адреса назначения, как раз содержится информация о частоте, на которой будет пере-

дан следующий пакет. Длина используемых пакетов относительно небольшая, так что максимальная реальная пропускная способность Bluetooth'a составляет всего 721 Кбит/с. Что касается радиуса действия, то она зависит от класса Bluetooth-модуля:

- * Class 1 - go 100 м;
- * Class 2 - go 20 м;
- * Class 3 - go 10 м.

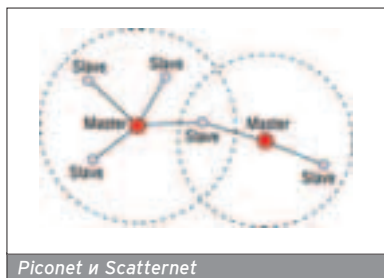
НЕ ВСЕ ТАК ПРОСТО

■ Широко распространено ошибочное мнение, что Bluetooth-соединение может производиться только по схеме "точка-точка". Так же, как и для Wi-Fi, вполне возможна схема с одновременным подключением нескольких устройств - для этого и существуют точки доступа Bluetooth, которые поряточно представлены на рынке. Устройство, к которому осуществляется подключение, называется ведущим (master), а все подключаемые - ведомыми (slave). Такое распределение ролей неслучайно: master всегда выполняет функции координатора, то есть управляет частотной и пакетной синхронизацией, следит за связью, уровнем сигнала и т.п. К одному master'у может быть подключено одновременно до семи активных slave'ов, обменивающихся данными, а также множество неактивных, ожидающих, пока для них освободится место. Все вместе они образуют структуру Piconet. В Piconet'e может быть только один master, однако любой подключенный к ней slave может быть master'ом в другом Piconet'e. Получается, что несколько Piconet'ов могут быть объединены в одну структуру - Scatternet.

Каждое Bluetooth-устройство имеет уникальный 48-битный сетевой MAC-адрес, который полностью совместим с форматом стандарта 802.11. Для того чтобы инициировать беспроводное подключение, Bluetooth-модуль должен просканировать эфир и выцепить оттуда адреса подходящих девайсов. Для этого он посылает специальный запрос - если по соседству работают активные устройства, то они могут ответить на него или не ответить в зависимости от выбранного режима:

Discoverable mode - в этом режиме устройства всегда отвечают на полученный запрос.

Limited discoverable mode - девайсы отвечают на запросы только в ограниченное время или при соблюдении других условий, которые были обозначены хозяином.




Piconet и Scatternet

Non-discoverable mode - устройства, на которых установлен этот режим, на запросы не отвечают.

Если какое-то из найденных устройств готово принять соединения, то оба Bluetooth-устройства начинают договариваться о параметрах связи (частота, статус каждого из них и т.д.), после чего соединение устанавливается.

Особого внимания заслуживает вопрос о том, насколько защищен Bluetooth. Изначально Bluetooth разрабатывался как безопасный вид связи, то есть он включал в себя безопасную аутентификацию, шифрование и контроль качества обслуживания (QoS, Quality of Service). Действительно, в спецификации имеется три режима защиты. При первом, Non secure, любые защитные функции отключены, а соответственно, лучше вообще не использовать этот режим. Второй - это режим Service Level Enforced Security, подразумевающий использование защиты после успешной установки соединения. И, наконец, третий - это Link Level Enforced Security, обеспечивающий безопасность на этапе инициализации и установки соединения. Второй и третий режимы могут использоваться одновременно и, по идее, обеспечивают максимальный уровень защиты. В их основе лежит так называемый сеансовый ключ, которые генерируются в процессе соединения двух устройств и используется для последующей идентификации и шифрования передаваемых данных. Однако такой подход также имеет недостатки и изъяны, в которых виновата открытость Bluetooth. Сетевой трафик может быть перехвачен, причем для этого даже не нужно использовать какие-либо специфические устройства. Вполне подойдут КПК или ноутбук, оснащенные Bluetooth-модулем. Так или иначе, проблемы с безопасностью пытаются решить, и в каждой новой спецификации Bluetooth, которая открыто лежит на сайте www.bluetooth.org, описываются все новые средства и приемы. Более того, некоторые приложения, использующие Bluetooth, применяют свою собственную защиту и мощное шифрование, что позволяет создавать неплохо защищенные соединения.

БУДУЩЕЕ ЗА НАМИ

■ Тема беспроводных сетей и безопасности сейчас особенно актуальна. Несколько лет назад мы не знали, что такое сотовый телефон, а сейчас не знаем, что бы делали без него. С беспроводными сетями ситуация примерно та же: оборудование постоянно дешевеет, модули связи интегрируются даже в бюджетные варианты ноутбуков и КПК, на них обратили внимание производители авто, их используют на производстве. Долой провода! 

Андрей Каролик (andrusha@real.hacker.ru) и Крис Касперски aka мышцх

ВОЙНА НА КОЛЕСАХ

РАЗБЕРЕМСЯ, ЧТО ТАКОЕ ВАРДРАЙВИНГ (WARDRIVING) И С ЧЕМ ЕГО НЕОБХОДИМО УПОТРЕБЛЯТЬ

Немногие знают, что такое вардрайвинг, хотя он существует давно. В отличие от привычных способов взлома, научиться вардрайвингу намного проще, так как для него не требуются специфические знания дизассемблирования, необходимые при взломе программ. Тем не менее, профессиональных вардрайверов единицы, и те шифруются. В этом номере мы приоткроем занавес и расскажем о вардрайвинге.



ЧТО ТАКОЕ ВАРДРАЙВИНГ

■ Вардрайвингом (англ. wardriving - дословно "военное вождение" или "война на колесах") называется охота на точки доступа Wi-Fi (никаких зверей при этом убивать не нужно), на те самые точки доступа, которые предназначены для беспроводного подключения к локальной сети или интернету. Цель вардрайвера - найти чужую точку и захватить контроль над ней. Реально вардрайвинг зародился в 50-х годах прошлого века (он еще назывался охотой на пис) и представлял собой вполне легальный вид радиоспорта с четко установленными правилами и международными состязаниями. На пересеченной местности в укромной норе закладывался радиопередатчик, периодически издающий сигналы (писа), а спортсмены, вооруженные приемниками с направленной антенной, должны были найти ее. С началом перестройки все это умерло. Теперь никому не интересно корпеть над паяльником, изобретая все новые и новые технические решения, и скакать, как козел :). Современное поколение предпочитает охотиться на добычу попроще, используя полностью готовое оборудование и программное обеспечение.

РАЗРАБОТЧИКИ VS. ВАРДРАЙВЕРЫ

■ Стандартный 64-битный ключ шифрования легко взламывается лобовым перебором. Учитывая, что фактическая длина секретного ключа составляет всего лишь 40 бит, в среднем достаточно перебрать 549.755.813.888 комбинаций. При скорости перебора в сотню миллионов ключей в секунду (посильная скорость для современных процессоров) атака займет час-полтора. Злоумышленнику достаточно перехватить один зашифрованный пакет, а затем терзать его до тех пор, пока контрольная сумма расшифрованного пакета не совпадет с ICV. Стучаться на точку доступа при этом совершенно не обя-

зательно. А с учетом существования четырех секретных ключей, продолжительность полного цикла перебора несколько возрастает, однако не столь радикально.

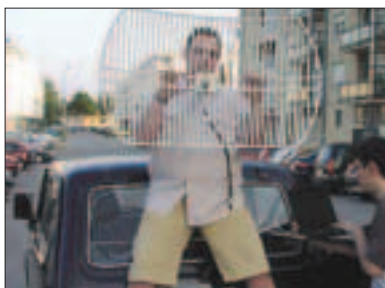
Для предотвращения лобовой атаки производители беспроводного оборудования увеличили длину секретной части ключа до 104 бит, попутно породив проблему обратной совместимости. Добавь сюда 24 бита вектора инициализации и получишь так называемое 128-битное шифрование. Подобрать 104-битный ключ вслепую уже нереально: при прежней скорости перебора в среднем на это уходит 2.817.001.333.840.509.768.000 часов, или 3.215.754.947.306.518 веков, что значительно превышает не только оставшееся время существования Солнца, но и Вселенной в целом :). Однако хакерам удалось найти более короткий путь, сократив время взлома в миллиарды раз.

В августе 2001 года три криптоаналитика (Scott Fluhrer, Itsik Mantin и Adi Shamir) опубликовали свою подрывную статью "Слабые места алгоритма

распределения ключей RC4" ("Weaknesses in the Key Scheduling Algorithm of RC4"), которая мгновенно стала знаменитой и опрелогела название всего семейства атак этого типа, - FMS-attack (по первым буквам фамилий первооткрывателей Fluhrer-Mantin-Shamir). Они обнаружили существование крупных классов слабых (weak) ключей, в которых крошечная часть битов ключа оказывает значительное влияние на зашифрованные данные. Поскольку в формировании эффективного ключа участвует вектор инициализации, генерируемый произвольным образом, в общий шифропоток неизбежно попадает некоторое количество слабых ключей. Собрав достаточный объем трафика, злоумышленник отбирает пакеты, зашифрованные слабыми ключами (такие пакеты называются слабыми или интересными). Каждый слабый пакет с 5% степенью вероятности восстанавливает один байт секретного ключа, поэтому общее количество пакетов, которые атакующий должен собрать для реализации атаки, в первую



Комплект вардрайвера: GPS и адаптер с внешней антенной



очередь зависит от степени его везучести. В среднем для взлома требуется порядка шести миллионов зашифрованных пакетов. В зависимости от интенсивности трафика и пропускной способности канала, на это уходит от нескольких часов до нескольких дней, хотя в некоторых случаях атака успешно заканчивается уже через несколько минут. И это при 104-битном ключе! Так работает AirSnort и многие другие хакерские утилиты, которые любой злоумышленник может свободно скачать из Сети.

Если обмен данными между легальными клиентами и точкой доступа незначителен или практически отсутствует, злоумышленник может заставить жертву генерировать большое количество трафика, даже не зная секретного ключа. Достаточно просто перехватить правильный пакет и, не расшифровывая, ретранспировать его вновь. ARP-запрос вызовет неизбежный ARP-ответ. Отличить ARP-запросы от всех остальных пакетов очень просто: `frame.pkt_len == 68` и `wlan.da == FF:FF:FF:FF:FF:FF`. Обычно для передачи запросов используется отдельная WLAN-карта (при этом расстояние между антеннами приемной и передающей карт должно составлять, по меньшей мере, 15 сантиметров), хотя некоторые карты ухитряются перехватывать трафик и одновременно с этим бомбардировать жертву пакетами.

Хакеры лаборатории Hikari of DasBoden Labs усилили FMS-алгоритм, сократив количество необходимых пакетов с шести миллионов до 500 тысяч. А в некоторых случаях 40/104-битный ключ взламывается всего с тремя тысячами пакетов, что позволяет атаковать даже домашние точки



Замечательная маечка для фанатов своего дела

доступа, не напрягая их избыточным трафиком. Усиленный алгоритм атаки реализован в утилите `dwergrack`, входящей в состав пакета `BSD-airtools`, а также в другом хакерском инструментарии.

Разработчики оборудования отреагировали вполне адекватным образом, изменив алгоритм генерации векторов инициализации так, чтобы слабые ключи уже не возникали. Даже `dwergrack`'у требовалось перехватить свыше 10 миллионов пакетов, но даже в этом случае успешная расшифровка ключа не гарантирована. Устройства, выпущенные после 2002-2003 года, скорее всего, уже защищены от FMS-атаки, а более дорогие модели решают эту проблему обновлением прошивки (правда, не все производители выпустили такое обновление). Но даже сегодня, в середине 2005 года, в эксплуатации находится множество уязвимых устройств, особенно на периферии, куда уходят все нереализованные складские запасы. Тем не менее, ситуация сложилась так, что хакерам пришлось искать новые пути для атак.

В августе 2004 года хакер по имени Kogek продемонстрировал исходный код нового криптоанализатора, взламывающего даже сильные векторы инициализации. Для восстановления 40-битного ключа ему требовалось всего 200 000 пакетов с уникальными векторами инициализации, а для 104-битного - 500 тысяч. Количество пакетов с уникальными векторами в среднем составляет порядка 95% от общего количества зашифрованных пакетов, так что для восстановления ключа атакующему потребуется совсем немного времени. Данный алгоритм реализован в `shopper'e`, `aircrack'e`, `WepLab'e` и других хакерских утилитах.

В новом оборудовании, построенном по технологии WPA (Wi-Fi Protected Access - защищенный Wi-Fi-доступ), вновь была усилена защищенность беспроводных устройств. На место WEP пришел TKIP (Temporal Key Integrity Protocol - протокол краткосрочной целостности ключей), генерирующий динамические ключи, сменяющиеся друг друга с небольшим интервалом времени. Для совместимости с существующим оборудованием TKIP использует тот же самый потоковый алгоритм шифрования, что и WEP, - RC4, но в каждый зашифрованный пакет теперь укладывается специальный 8-байтный код целостности сообщения, рассчитанный по алгоритму Michael и предотвращающий ретрансляцию подложных пакетов. Процедура аутентификации осуществляется по протоколу EAP (Extensible Authentication Protocol - расширенный протокол аутентификации), который использует либо а) RADIUS-сервер (Remote Authentication Dial-In User Service - служба дистанционной ау-



Направленная антенна

тентификации пользователей по коммутируемым линиям); либо б) предустановленный общий ключ PSK (pre-shared key). В процессе аутентификации сервер генерирует парный мастер-ключ (PMK - Pairwise Master Key) и передает его клиенту. Несмотря на относительную новизну этой технологии, в комплект `aircrack'a` уже входит специальный модуль `WZCOOK`, отображающий PMK-ключ :). Для несанкционированного подключения к точке доступа, защищенной технологией WPA, этого оказалось вполне достаточно. Впрочем, атакующий модуль недостаточно отлажен и в некоторых случаях не срабатывает.

Стандарт IEEE 802.11i описывает более продвинутую систему безопасности (известна под именем WPA2), основанную на криптоалгоритме AES. Готовых утилит для ее взлома в открытом виде пока не наблюдается, так что с этой технологией можно чувствовать себя в безопасности. По крайней мере, какое-то время она продержится :). Обладателям устаревшего оборудования настоятельно рекомендуем пробить VPN-туннели (Virtual Private Network - виртуальная частная сеть), задействовать SSL-шифрование или подключить любые другие способы защиты, изначально ориентированные на небезопасные каналы передачи данных.

ВАРДРАЙВИНГ - НЕ СОВСЕМ ВЗЛОМ

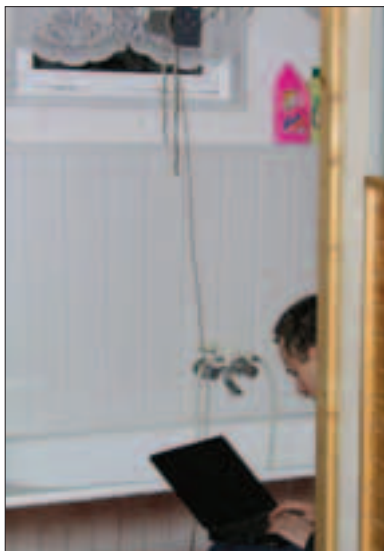
■ Вардрайвинг - это не обязательно "взлом". Часто атакующий ограничивается тем, что находит открытую точ- ➤

Вардрайвинг - охота на точки доступа Wi-Fi и получение контроля над ними.

Вардрайвингом занимаются скорее для спортивного интереса, чем для получения ценной информации. Иногда и просто ради халяжного доступа в интернет.



Еще один комплект для занятия вардрайвингом



Вардрайверу неважно где вардрайвить, хоть в ванне, хоть в туалете

ку доступа, но не подключается к ней. Во-вторых, вардрайвинг ни внешне, ни внутренне не похож на дисасемблирование защищенных программ или написание вирусов. Это делает занятие вардрайвингом непохожим на другие способы взлома в привычном для нас понимании. В вардрайвинге намного больше романтики, чем, например, в сексе с отладчиком :). С другой стороны, если ломать программы умеют единицы, то стать классным вардрайвером сможет практически любой.

КТО ЗАНИМАЕТСЯ ВАРДРАЙВИНГОМ

■ Вардрайвингом занимаются в основном романтики :), хотя отмечены единичные случаи хищения кредитных карт и другой конфиденциальной информации через WLAN. У вардрайвера вряд ли может возникнуть много амбиций, скорее, азарт и спадострастное чувство, что ты кого-то поймел. Подавляющее большинство атакующих действуют без злого умысла, воспринимая это как шалость или интеллектуальную игру. Но встречаются и настоящие охотники за чужим трафиком, из которого можно извлечь различную конфиденциальную информацию (пароли на почтовые ящики, номера кредитных карт и т.д.), и просто желающие подключиться к интернету за чужой счет.

Кто-то вардрайвит за деньги, но таких немного. Даже в Штатах точки доступа еще не распространены настолько, чтобы на их взломе было возможно добывать пропитание. Тех, кто конструирует уникальное железо, - единицы. Тех, кто пишет софт, - десятки. Сотни или даже тысячи пользуются готовым железом/софтом, а еще больше тех, кто просто интересуется этим занятием, но не рискует вардрайвить на практике. Мы относимся к последним :).

Использование готового снаряжения не требует теоретической подго-

товки, выходящей за рамки навыков владения мышью, зато физическая подготовка весьма желательна, так как вычисленных вардрайверов в нашей стране практически никогда не передают в прокуратуру - только "братков" к ним посылают.

Источник информации для вардрайверов - форумы, в которых можно найти и свежие хакерские программы, и хитрые приемы взлома, и все остальное. Эрудитии продвинутого пользователя будет вполне достаточно. Но для написания атакующего софта требуется глубокая теоретическая подготовка и интуиция. Над проблемой взлома корпят не только программисты, но и криптографы, причем последние обычно работают на легальной основе и публикуют свои научные труды, которые уже перерабатывают программисты.

ИНСТРУМЕНТЫ ВАРДРАЙВЕРА

■ Если говорить об оснащении вардрайвера, то, как правило, это карманный компьютер или ноутбук, снабженный WLAN-картой на основе чипсета Prism (его поддерживает подавляющее большинство программ), внешней антенной (обычно направленного типа) и соответствующим ПО. Добротная антенна направленного типа, снабженная усилителем мощности, уверенно держит связь на расстояниях до 1,5-2 км, а в некоторых случаях и больше.

Такую антенну вместе с усилителем можно купить совершенно легально. Их выпускает Hyper Technology, Broadcast Warehouse, "Радиал" и многие другие компании. Среди хакеров большой популярностью пользуется направленная антенна HG2415Y типа Radome-Enclosed (компания HyperLink Technology), которую мож-

но заказать по интернету. Рассчитанная на стационарный монтаж, она, тем не менее, неплохо чувствует себя на фотографическом штативе или даже на обыкновенном ружейном прикладе, превращающем ее в мобильный инструмент для слежения за подвижными жертвами. Параболические антенны действуют на расстояниях, ограниченные, фактически, лишь горизонтом видимости, но они катастрофически немобильны, а для хакера самое главное - вовремя сместиться с места взлома. В общем, для вардрайвинга подходит практически любая антенна направленного типа на 2,4 ГГц (она же антенна стандарта IEEE 802.11b/802.11g или WLAN).

Из программного обеспечения понадобятся: сканер, сниффер и взломщик паролей. Их можно найти практически под любую платформу. На Pocket PC обычно используется связка MiniStumbler/Sniffer Portable/Airscanner Mobile. MiniStumbler обнаруживает присутствие сети в данной точке, измеряет интенсивность сигнала, отображает SSID/MAC-адреса и определяет, задействовано WEP-шифрование или нет. Sniffer Portable и Airscanner Mobile грабят все пролетающие мимо пакеты и записывают их в файл, который затем переносится на ноутбук или настольный ПК и пропускается через взломщик паролей (процессорных ресурсов карманного компьютера для взлома паролей за разумное время пока негостаточно).

Распространенный сниффер под Linux и BSD - Kismet, изначально ориентированный на исследовательские цели. Он поддерживает массу оборудования и беспроводных протоколов, удобен в использовании и к тому же абсолютно бесплатен. Перехватывает сетевой

Пока еще не научились ломать стандарт IEEE 802.11g. Но долго ли он продержится?

Для вардрайвинга, по сути, нужны только ноутбук, направленная антенна и специальный софт.

Вардрайвингом занимаются в основном романтики.



Ноут - первый спутник вардрайвера

трафик, показывает SSID- и MAC-адреса, подсчитывает количество пакетов со слабыми векторами инициализации и т.д. Из взломщиков паролей в последнее время реально работают только aircrack и WepLar, причем первый работает значительно лучше.

Пог Windows перехват беспроводного трафика реализуется гораздо сложнее, и кроме снифера потребуются модифицированные версии драйверов для WLAN-карты. Из коммерческих сниферов можно порекомендовать Airoreel, из некоммерческих - утилиту airdump (входит в состав aircrack, портирована под Windows). Еще можно использовать Sniffer Pro.

На Mac'ax весь хакерский инструментариум собран в одном флаконе - утилита KisMAC, настолько простая, что ей сможет пользоваться даже ребенок. Здесь есть и сетевой сканер, и снифер, и парольный переборщик (brute force), и криптоанализатор слабых векторов инициализации. Предусмотрена даже такая мелочь, как планировщик, позволяющий осуществлять атаки по расписанию :).

КАК ОХОТИТЬСЯ

■ Можно, например, просканировать периметр своего обитания, поднявшись на балкон и вооружившись параболической антенной на 2,4 ГГц. Представь: сидишь себе в засаде, пьешь пиво, сканируешь периметр и ждешь, когда жертва попадет в силки. Через неделю, максимум через две, оперативная обстановка будет изучена, и что тогда? А тогда карманный компьютер или ноутбук - и вперед на



Вардрайверы за работой

колеса. Если колес нет, вполне подойдет троллейбус или трамвай. Они и внимания меньше привлекают, и за дорогой следить не надо.

НА ЗАПАДЕ И У НАС

■ Конечно, западные и азиатские тусовки более многочисленны и прогривнуты. У нас, несмотря на мягкий климат никем не соблюдаемых законов, вардрайвинг распространяется довольно сдержанно. Отчасти это объясняется апатичностью отечественной публики, отчасти ориентацией не на процесс, а на результат.

Каждый оценивает крутость вардрайвера по-своему. Настоящие профи шифруются и молчат. Этап самоутвер-

ждения у них остался позади, зато иметь проблемы с законом или "братками" им неохота. Они посещают тематические форумы, но практически не оставляют сообщений. В самых жарких дискуссиях, как правило, участвуют новички, соревнующиеся, "кто больше взломает".

А что с безнаказанностью? Да у нас вообще высокий уровень преступности. Суды переполнены намного более важными делами, чем какой-то там вардрайвинг, а сотрудники милиции заняты вопросами собственного пропитания. Но даже честный следователь не может начать дело, пока не будет заявления от истца и каких-нибудь доказательств. В практическом плане для истца это означает постоянные поездки в суд, длительные разбирательства по поводу наличия всех сертификатов, комплекса охранных мер и т.д. На Западе такие шалости не проходят и уже есть реальный пример того, как засудили вардрайвера.

Направленные антенны продаются совершенно легально.

Вряд ли тебя посадят за вардрайверство, но могут серьезно "наехать".

Каждый оценивает крутость вардрайвера по-своему. Настоящие профи шифруются и молчат.



Крутая антенна в багажнике автомобиля

СОМНИТЕЛЬНАЯ МОБИЛЬНОСТЬ

■ Может показаться, что вардрайвинг безопаснее банального стационарного взлома, так как сам вардрайвер становится мобильнее и его сложнее вычислить физически. Напротив. Стационарный взлом через цепочку надежных прокси или сотовый телефон, купленный с рук, а после звездного часа закатанный в асфальт, вполне безопасен, и хакера обычно вяжут уже на продаже ворованной информации. Вардрайвер привлекает больше внимания. Вокруг уважаемых зданий полно камер, фиксирующих номера машин, и простых охранников хватает, а у них на эти вещи глаз наметан. Так что мобильность мобильностью, а питать иллюзий на этот счет не стоит. 

Антон Карпов (toxa@real.hacker.ru), Сергей Земланский (sergey.zemlansky@gmail.com)

В ПОИСКАХ WI-FI

ПОСОБИЕ ДЛЯ НАЧИНАЮЩЕГО ВАРДРАЙВЕРА

И так, ты решил приобщиться к армии вардрайверов и стать еще одним воином беспроводных сетей. Чтобы ты не начинал с нуля и не заморачивался вопросами "что взять, где взять", мы подготовили подробную инструкцию для начинающего вардрайвера.



ЖЕЛЕЗО

■ Ясно, что без ноутбука не обойтись. Тут единственное требование - время автономной работы, оно должно быть максимальным. Самые долгоиграющие ноутбуки - построенные на платформе Intel Centrino. И Linux, и FreeBSD полностью поддерживают эту технологию, так что очень рекомендуется изучить мануалы и настроить свою ось на энергосберегающий режим (для контроля соответствующих параметров можно использовать `cpufreqd` в Linux и `powerd` во FreeBSD). В условиях активной работы правильно настроенный ноут может прожить автономно до трех-четырех часов. Очень приветствуется запасной комплект аккумуляторов. Впрочем, никто не мешает тебе приобрести адаптер для подключения ноутбука к автомобильному прикуривателю :). Что же касается встроенной беспроводной карты, то она устроит лишь самого неприяательного вардрайвера, и вот почему. Во-первых, Linux и FreeBSD начали полноценно поддерживать Centrino'вские карты (`ipw2100` и `ipw2200`) сравнительно недавно. Во-вторых, встроенная в ноутбук антенна, безусловно, сможет улавливать определенное количество пакетов, но любая, даже самая захудалая внешняя антенна даст эффект на несколько порядков лучше. Не стоит и упоминать о том, что мож-

но вести речь о реальном подключении к AP встроенными средствами лишь при непосредственной близости к точке доступа, а это убивает саму суть вардрайвинга. Соответственно, нужно покупать хорошую беспроводную PCMCIA-карту с разъемом под внешнюю антенну и саму антенну. Или даже две.

БЕСПРОВОДНЫЕ КАРТЫ И ВАРДРАЙВИНГ

■ Что же имеется в виду, когда говорят о "подходящей для вардрайвинга" карте? В первую очередь, поддержка операционной системой специального режима Monitor. Как известно, беспроводное устройство может работать штатно в двух режимах: BSS (Basic Service Set) aka Infrastructure - клиент подключен к Сети с использованием точки доступа (как правило, беспроводные сети строятся именно по такому принципу); и IBSS (Independent Basic Service Set) aka ad-hoc - клиент подключен

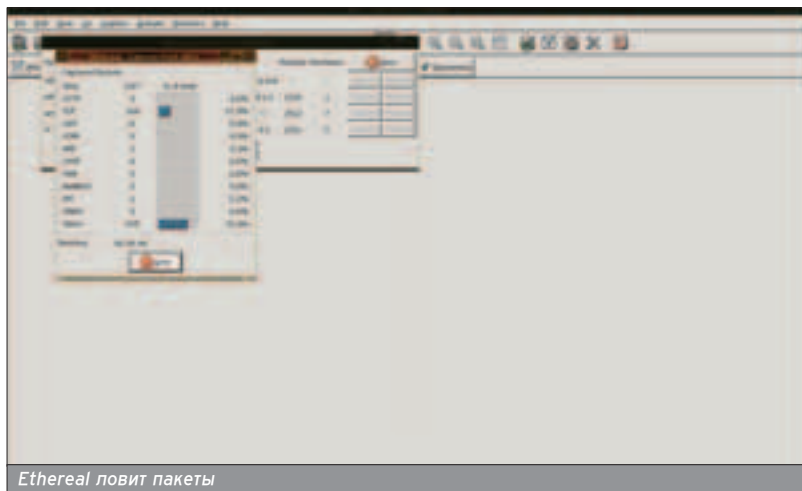
без использования точки доступа (связь "точка-точка", например, когда необходимо связать по сети два ноутбука, чтобы обменяться файлами). Соответственно, драйвер устройства обязан, как минимум, поддерживать два режима конфигурации. Но ни один из них не годится для прослушивания эфира. Простой перевод интерфейса в `promisc mode` ничего не даст: карта будет ловить все пакеты, но предназначенные лишь для той сети, на которую она настроена.

Как же находить сами сети? Для этого существует режим монитора (Monitor mode), при котором карта не ассоциируется ни с какой сетью и ловит все доступные ей "пролетающие мимо" фреймы. Поддержка драйвером этого режима в Linux/BSD во многом определяется открытостью спецификаций на карту. К примеру, проблем с Monitor'ом не имеют карты на чипсете Prism-II/Prsim-2.5/Prism-3, Orinoco, Atheros, Ralink. Intel же не торопится открывать спецификации

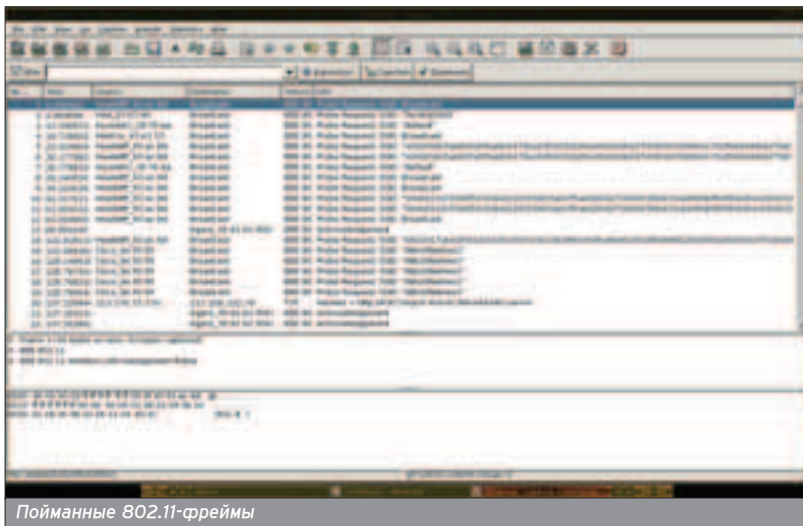
Простой перевод интерфейса в `promisc mode` ничего не даст: карта будет ловить все пакеты, но предназначенные лишь для той сети, на которую она настроена.



Вардрайвер :)



Ethereal ловит пакеты



Пойманные 802.11-фреймы



Панельный интерфейс Kismet

(драйверы под Linux пишет группа разработчиков, подписавшая с компанией NDA, Non-Disclosure Agreement, и получившая документацию на карту на условиях неразглашения; драйвер под BSD пишется на основе Linux'ового, а также методом reverse engineering), поэтому до недавнего времени были проблемы с поддержкой этой картой Monitor mode и, соответственно, с поддержкой ее специализированным софтом вроде Kismet'a. Помимо подходящего

чипсета, рекомендуется выбирать карту и по наличию стандартного разъема для подключения внешней антенны.

АНТЕННЫ И ВАРДРАЙВИНГ

■ Не секрет, что чем мощнее антенна, тем сильнее сигнал. Для вардрайвера эта прописная истина принимает решающее значение: используя слабую антенну (например встроенную в ноутбук), можно ловить сигнал и даже перехватывать некоторые па-

кеты, но мощностей может не хватить для подключения к сети. Чтобы не стать жертвой типичной ситуации "вижу полно сетей, но ни к одной не могу подключиться", опытные вардрайверы приобретают внешние антенны, подключаемые к беспроводным картам через стандартный разъем. Антенны бывают самые разные: от небольшой пирамидки в 15-20 сантиметров до огромной полутора-метровой трубы. Все они делятся на две категории: ненаправленные (omnidirectional) и направленные (directional). Первый тип - это, по сути, то же, что и встроенные в ноутбук или PCMCIA-карту, только мощнее. Насколько мощнее, определяется конкретной антенной. Очевидно, что чем мощнее антенна, тем больше точек доступа вардрайвер обнаружит при одном и том же перемещении. Отыскав "вкусную" точку, он меняет антенну на направленную, которая, как пушка, "стреляет" узким направленным лучом на большие расстояния. Откалибровав антенну в пространстве так, чтобы направление на AP было как можно более точным, вардрайвер получает идеальный сигнал и может добраться даже до слабых офисных "пипирок", стоящих в глубине комнаты.

Но что делать, если антенны нет? Во-первых, можно попробовать собрать ее из подручных средств (скажем из банки от чипсов, пример сборки такой antenna/can antenna можно посмотреть здесь:

www.cruftbox.com/cruft/docs/cantenna.html) - в устройстве антенны нет ничего хитрого. Во-вторых, стоит вызвать из спячки смекалку и тактику: если антенна не идет к вардрайверу, он идет к антенне. Я имею в виду довольно типичную схему, в которой два соседних здания, например расположенные через дорогу, соединены одной беспроводной сетью. Как правило, для такой схемы по обеим сторонам ставится по узконаправленной антенне, и, окажись ты посередине, даже с самой захудалой встроенной антенной связь будет отличной.

СОФТ

■ Подобрав подходящее железо, экипируемся необходимым софтом. Софта категории wireless tools довольно много, достаточно заглянуть на www.networkintrusion.co.uk/wireless.htm, чтобы убедиться в этом. Но, как правило, вардрайвер обходится двумя-тремя любимыми утилитами. Для *nix-систем это, конечно же, kismet, aircrack и etherreal.

Для начала точку доступа нужно обнаружить. Именно это, но и не только, призван делать Kismet (www.kismetwireless.net) - пассивный беспроводной сканер для 802.11a/b/g-сетей. Продуманность архитектуры (сервер запускается на одной машине, клиенты с графическим интерфейсом

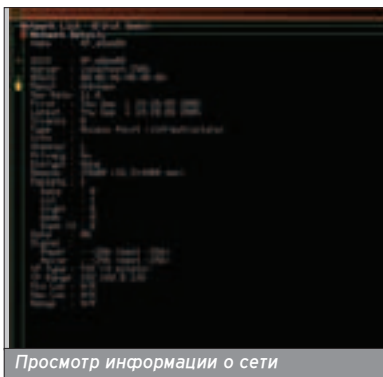
www.chronicle-sofawardriver.org - хроники вардрайвера, дневник прожженного беспроводного охотника.

www.netstumbler.org - форум, посвященный не только одноименной утилите, но и вардрайвингу в целом.

Очевидно, что чем мощнее антенна, тем больше точек доступа вардрайвер обнаружит при одном и том же перемещении.

ЧТО ТАКОЕ ХОТСПОТ?

■ Хотспот (англ. hotspot) - публичная точка доступа в интернет, например в кафе или ресторане, пользование ей предоставляется бесплатно (как бонус к кофе с пирожным) или как платная дополнительная услуга. Как правило, информация о присутствии в помещении беспроводной сети афишируется самим заведением, и потому особого интереса для вардрайверов не представляет.



Просмотр информации о сети

запускаются со сколь угодно многих машин и соединяются с сервером, выводя полученную им информацию и исключительная функциональность обеспечили этой программе популярность: Kismet умеет получать исчерпывающую информацию об AP, такую как тип сети, наличие шифрования, производитель AP, SSID, определять скрытые сети (в которых отключен Broadcast SSID) и точки доступа, сконфигурированные максимально небезопасно (по умолчанию); Kismet легко интегрируется с другим софтом, например IDS Snort или GPS-навигатором. Наконец, эта софтина пишет отличные логи и поддерживает множество беспроводных карт.

Установку Kismet для твоего любимого дистрибутива Linux или BSD рассматривать не буду, на самый крайний случай все способны набрать магическое `./configure && make && make install`. Но go установки задайся таким животрепещущим вопросом, как драйверы беспроводной карты. В случае с BSD все предельно просто: либо карта поддерживается базовой системой, либо нет :). В случае же Linux, как правило, вменяемый драйвер пишет сторонняя группа разработчиков. Например, для Intel'овских карт существуют проекты <http://ipw2100.sourceforge.net> и <http://ipw2200.sourceforge.net>, для карт на чипсете Atheros - проект MADWi-Fi (<http://madWi-Fi.sourceforge.net>) и т.д. Словом, до начала "беспроводных работ" вардрайверу необходимо найти подходящий драйвер, следуя указаниям на сайте соответствующего проекта. Кроме того, для управления параметрами карты под Linux потребуются пакет wireless-tools, тогда как в BSD все делается той же утилитой `ifconfig`, как и для обычных интерфейсов.

После установки Kismet'a следует провести минимальные настройки. Правим `kismet.conf`:

```
suiduser=toxa
```

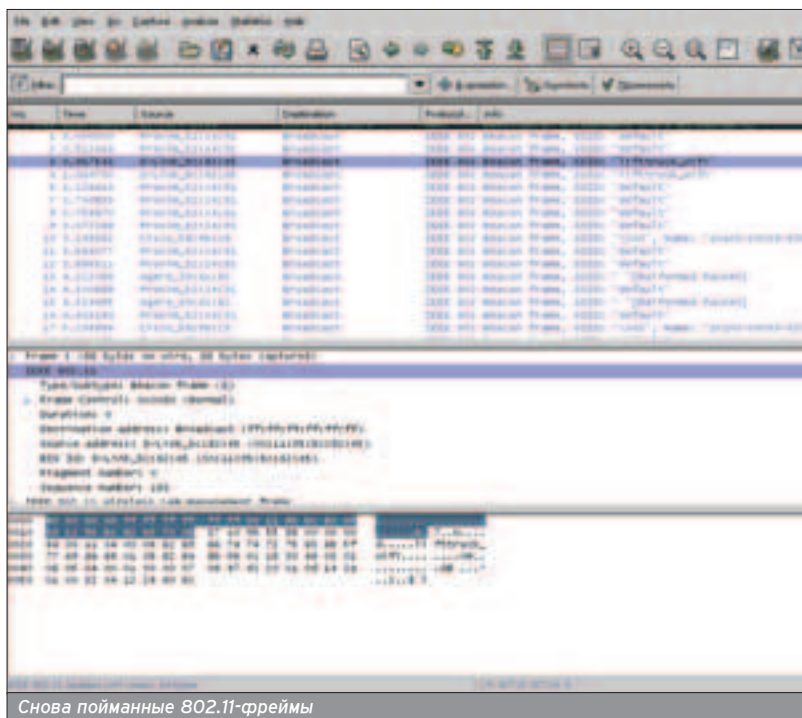
Не рекомендуется пускать Kismet с привилегиями суперпользователя. При запуске от рута он инициализирует интерфейс и понижает привилегии до указанного пользователя. Как правило, здесь указывают имя поль-

ЧТО ТАКОЕ GPS?

■ GPS - global positioning system, система глобального позиционирования. Применяется для очень точного позиционирования на местности при помощи специального устройства (GPS-модуля), который синхронизируется со специальным GPS-спутником, возвращающим на землю твои координаты. Таким образом, их постоянное обновление позволит гаджету, например, построить маршрут и высветить его на карте. Или показать на карте района все точки доступа и зоны покрытия сетей, пойманных во время сеанса вардрайвинга.



Обнаруженные сети



Снова пойманные 802.11-фреймы

www.wi-fiplanet.com - довольно полезная подборка статей о Wi-Fi.

<http://gkismet.sourceforge.net> - графический GTK/Perl-фронтенд к Kismet.

www.dachb0den.com/projects/bsd-air-tools.html - качественный, хотя и морально устаревший набор утилит для обнаружения беспроводных сетей и взлома WEP-ключа специально для BSD-систем.

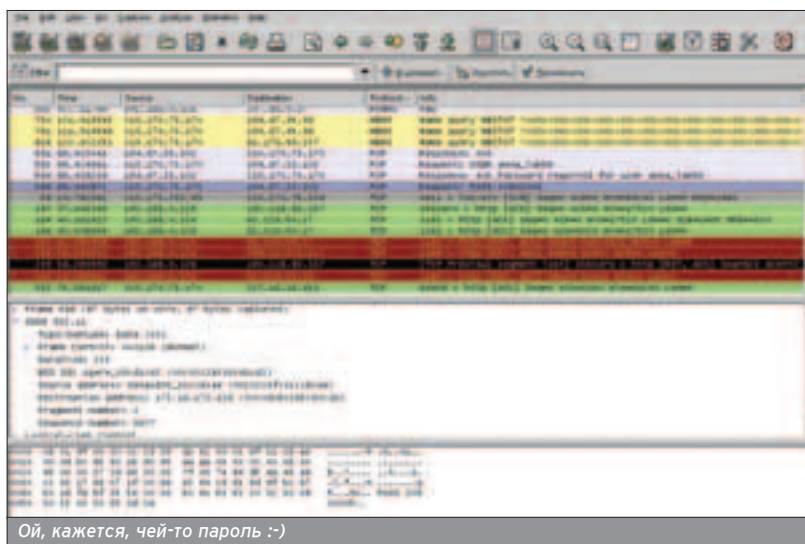
Kismet легко интегрируется с другим софтом, например IDS Snort или GPS-навигатором.

КАК РАБОТАЮТ WI-FI-СКАНЕРЫ?

■ Типичный сканер (stumbler) переводит карту в monitor mode и начинает прыгать по каналам (channel hopping) в надежде обнаружить на каком-нибудь канале точку доступа. Поймав сигнал, сканер ловит в первую очередь специфические а) беспроводные фреймы (аутентификационные, информационные), на основе их анализа делает вывод о типе сети, наличии в ней WEP-шифрования, SSID, производителе AP и т.д.; и б) фреймы данных, на основе которых сканер судит об адресации в сети и клиентах.

Большинство сканеров работают в полностью пассивном режиме (ловят пакеты и ничего более), но некоторые, с целью получения большей информации о сети, могут производить и активное обнаружение, обмениваясь с AP пакетами.

|||||||



зователя, который будет запускать Kismet. В моем случае это toxa.

`source=radiotap_bsd_b,wifi,prismsource`

Эта запись формата "драйвер_карты, имя_интерфейса,имя" указывает сканеру загружать соответствующие драйверы для данной карты и в дальнейшем оперировать этим по определенным именам. Так как основная платформа разработки Kismet - Linux, то в случае с этой осью типом карты может быть prism2, orinoco, atheros или любой другой поддерживаемый драйвер. Под BSD это не работает, но существует универсальный "метадрайвер" под названием Radiotap. В указанном случае Kismet как раз запущен на FreeBSD, потому указан драйвер radiotap_bsd_b, имя интерфейса - wifi (в Linux, естественно, будет eth0/eth1/etc), и все это названо prismsource. Нужно заметить, что поддержка radiotap появилась лишь в current-версиях FreeBSD/NetBSD и впервые - в OpenBSD 3.7, так что в случае использования какого-либо релиза из ветки 5.x могут быть проблемы. Про устаревшую серию 4.x я вообще молчу :). Пример записи под Linux для карточек на чипсете

Orinoco: `source=orinoco,eth1,orinoco`
`source.`

`enablesource=prismsource`

Эта запись активизирует вышеописанную конфигурацию. Так, если используются разные карты, можно указать сколько угодно записей вида `source` и включать их по мере необходимости. Более подробную информацию о настройке Kismet см. в <http://kismetwireless.net/documentation.shtml>.

После конфигурирования остается только перейти в каталог, в который доступна запись пользователю, указанному в директиве `suiduser`, и запустить Kismet:

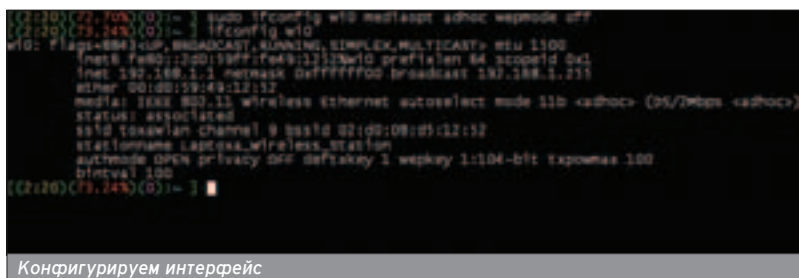
`# kismet`

Запустится сервер, который по умолчанию слушает 127.0.0.1:2501, а затем и клиент, который тут же подключится к серверу. Клиент имеет удобный ncurses-based интерфейс, что правильно: в целях экономии заряда батарейки вардрайвер не станет запускать X-сервер на своем ноутбуке. Обнаруженные AP тут же высвечиваются со всей необходимой информацией (имя и тип сети, наличие шифрования, канал, количество пойманных пакетов, IP-диапазон). Kismet имеет отличный встроенный help, и нет смысла пересказывать его здесь.

Но "обнаружить сеть" не всегда означает "легко получить доступ к ней". Помимо "желтых" (означаю- ➤



Структура пакета



Конфигурируем интерфейс

ших, согласно цветовому кодированию в Kismet'e по умолчанию, сеть без шифрования) или даже "красных" сеток (AP с настройками по умолчанию), вардрайвер встречает и "зеленые" - те самые, где WEP=Yes. Но это его не останавливает: тут на сцену выходит вторая любимая игрушка вардрайвера - aircrack.

Как известно, в протоколе WEP существуют фундаментальные уязвимости, и вскоре после их обнаружения появилось множество утилит, взламывающих ключ на основе анализа перехваченных пакетов. Вместе с методами взлома совершенствовались и утилиты, и последнее их поколение - набор aircrack

(www.cr0.net:8040/code/network/aircrack), в который входят утилиты airodump, aireplay, aircrack и aircrack-ng. Помимо непосредственного взлома WEP-ключа, они умеют внедрять в беспроводную сеть злонамеренные пакеты и расшифровывать зашифрованный трафик. Но нас сейчас интересует только взлом ключа. Как известно, это лишь дело времени, так как достаточно поймать необходимое количество пакетов. Первоначально такие утилиты, как dweirdump, aircrack-ng, aircrack-ng, требовали до нескольких гигабайт трафика. Но aircrack'у нужно существенно меньше - около 500 тыс. пакетов для взлома 128-битного ключа (несколько часов в хорошо загруженной сети). Накопить их можно утилитой airodump из пакета aircrack. К сожалению, она работает только под Linux. Но aircrack'у подогат и дампы, например Kismet'a.

Повим пакеты на четвертом канале и пишем дампы в outfile:

```
# airodump eth1 outfile 4.
```

А затем натравливаем на него aircrack:

```
$ aircrack outfile
```

Дополнительные опции расписаны на сайте утилиты. Если собрано достаточное количество пакетов, то через некоторое время (от минуты до получаса) aircrack радостно сообщит: "KEY FOUND!"

Наконец, уже после внедрения в сеть вардрайверу необходимо получить удобное средство анализа перехватываемых пакетов. В качестве такого sniffера можно посоветовать Ethereal - мощную утилиту, способную сортировать трафик по прикладным протоколам и выдирать вкусные пакеты с авторизационными данными.

ВСЬ МИР НА ЛАДОНИ

■ Типичный вардрайвер путешествует на автомобиле по местам, потенциально богатым на точки доступа, - промышленные районы, центр города, улицы с офисными зданиями

ЧТО ТАКОЕ "СКРЫТАЯ СЕТЬ"?

■ Существует специальный тип управляющих фреймов - так называемые beacon frames. В них содержится вся информация о сети: SSID, номер канала, на котором слушает AP, и т.п. Эти фреймы призваны сообщать клиентам, что сеть жива и все хорошо. Но, помимо клиентов сети, рядом могут оказаться и злоумышленники, а выкладывать всю информацию для кого попало небезопасно. Как известно, для того чтобы подключиться к сети, нужно, как минимум, знать ее идентификатор (SSID). По этой причине многие производители точек доступа включили в свои продукты возможность его исключения из beacon-фреймов (то есть disable Broadcast SSID). Это полумера, и ее легко обойти: как только легитимный клиент соединяется с точкой, SSID все равно передается, таков дизайн протокола, и аутентификационный фрейм также легко перехватить. Так что "демаскировка" скрытой сети - лишь дело времени.

Существует множество управляющих фреймов, каждый из которых предоставляет свою частичку информации о сети. Беглое описание можно посмотреть тут: www.wi-fiplanet.com/tutorials/article.php/1447501.



Официальный сайт Kismet

Мы в Питере, проехавшись со слабенькой антенной по нескольким крупным проспектам, нашли около двухсот AP.

ми. Мы в Питере, проехавшись со слабенькой антенной по нескольким крупным проспектам, нашли около двухсот AP. Но как запомнить, где и какая сеть встретилась? Куда возвращаться, чтобы накопить пакеты? И тут на помощь приходит GPS.

Помимо функций обнаружения и анализа беспроводных сетей, Kismet обладает возможностью взаимодействия со стандартным *nix-демоном для работы с GPS - gpsd (<http://gpsd.sourceforge.net>). Для последующей визуализации

сетей на карте в состав Kismet'a включена утилита gpsmap. К возможностям этой программки относятся такие вещи, как отображение маршрута, примерной зоны покрытия сети, мест перехвата пакетов, легенд сети. Во время работы Kismet с gpsd в файлы net.xml и gps.xml записываются все данные об обнаруженных сетях, например SSID, вендор точки доступа, доступность сети в настоящее время, наличие шифрования, а также координаты найденных точек



доступа и прочие географические и топографические параметры, необходимые для дальнейшей визуализации сетей.

Для корректной работы grpsmap необходимы карты местности, которые можно скачать с публичных источников. В данный момент grpsmap может использовать карты с NullMap, MapBlast, MapPoint, TerraServer, Tiger, Earthamap, Terraserver Торо. Мы рекомендуем либо карты с Earthamap (что и предлагается по умолчанию), либо с TerraServer, которая представляет собой не векторное изображение, а фотографию со спутника наподобие известного Google maps (<http://maps.google.com>).

Что же нужно, чтобы увидеть работу grpsmap воочию? Допустим, вардрайвер уже прокатился по городу, поймал множество сеток, они отобразились в логах, а теперь ему хочется посмотреть, где располагались точки доступа с привязкой к конкретной карте. Тогда он запускает:

```
$ grpsmap -S 4 --metric GPS_nor
```

Флаг -S определяет, откуда grpsmap попытается стянуть карту местности. Возможны следующие варианты: -1 = отсутствие карты (правда, не совсем ясно, зачем в этом случае тогда мы все это затеваем); 0 = Map-blast; 1 = MapPoint(broken); 2 = Terraserver; 3 = Tiger Census; 4 = Earthamap; 5 = Terraserver Topographic. Разработчиками рекомендован пункт 4. Флаг --metric обозначает, что grpsmap попытается стянуть карты в метрической системе, так как по умолчанию в нем используется измерение в милях. Также к интересным возможностям grpsmap относятся отслеживание на карте маршрута (опция --draw-track), отображение цветом силы сигнала передающего AP (--draw-power-zoom), указание SSID-сети (--draw-leg-end) и еще куча разных возможностей по настройке внешнего вида итоговой карты.

КАК ЗАЩИТИТЬСЯ?

■ До сих пор стандарт безопасности беспроводных сетей 802.11i не получил широкого распространения. Так что и по сей день проверенным средством остается шифрование всего трафика на уровне протокола. Принудительное использование ipsec защитит сеть от посторонних посетителей и сохранит конфиденциальность передаваемой информации. Менее надежный вариант, который, правда, затруднит проникновение в сеть, - использование фильтрации клиентов на точке доступа по жесткой привязке MAC-IP.

В общем, защититься можно, методы уже разработаны. О некоторых из них читай в этом же номере в еще одной статье моего авторства.



№ 1 MEMORY

Откройте для себя непревзойденную мощность X.

HyperX от компании Kingston Technology



Феноменальная мощность!
Память Kingston® HyperX® — это высокочастотная, быстродействующая память следующего поколения, разработанная специально для наиболее взыскательных пользователей ПК и любителей компьютерных игр. Память HyperX обеспечивает полное раскрытие всех возможностей вашего компьютера. К тому же вы получаете легендарное качество Kingston, бесплатную техническую поддержку и гарантию на весь срок эксплуатации. Дополнительную информацию смотрите по адресу kingston.com/hyperx или обращайтесь к указанным ниже дистрибуторам.

Kingston
TECHNOLOGY
HYPERX

Компания "Ак-цент Микросистемс" : (095) 232-0281 • sales@ak-cent.ru • www.ak-cent.ru
Alliance Marketing Group, LLC : (095) 796-9356 • info@alliancegroup.ru • www.alliancegroup.ru
Asbis Russia : (095) 933-1133 • memory@asbis.ru • www.asbis.ru
Eltex Computer Solutions (ITC Company) : (095) 786-6908 • (812) 324-6134 • www.eltex.ru • www.itcmemory.com
PatriArch Approved Memory : (095) 216-7201 • sales@memory.ru • www.memory.ru
Trinity Logic : (095) 787-1416 • info@tl-c.ru • www.tl-c.ru



©2005 Kingston Technology Company, Inc. 17600 Newhope Street, Fountain Valley, CA 92708 USA. Все права защищены. Все товарные знаки являются зарегистрированными товарными знаками их соответствующих владельцев.

Ермолаев Евгений aka Saturn (saturn@linkin-park.ru)

БЕЗ ПРОВОДОВ И БЕЗ ЗАЩИТЫ

РАЗБИРАЕМСЯ В УЯЗВИМОСТЯХ БЕСПРОВОДНЫХ СЕТЕЙ

Когда речь заходит о технологии Wi-Fi, признаком хорошего тона считается упоминание о низком уровне безопасности в сетях, построенных на ее основе. Сегодня даже далекие от вопросов сетевой безопасности люди знают, что Wi-Fi - это небезопасно. Но многие ли знают, как использовать это знание себе во благо?

Беспроводные сети должны быть защищены надежнее, чем кабельные. Необходимость обеспечения надежной защиты передаваемой информации продиктована прежде всего использованием радиоканала. Для перехвата информации в традиционной сети злоумышленник должен получить физический доступ к кабелю. В случае же с беспроводными решениями ему достаточно попасть в зону действия сети, прихватив с собой недорогое радиооборудование. Вот почему во многих стандартах связи, использующих радиоволны в качестве физической среды, предусмотрены программные средства защиты от несанкционированного доступа к информации. Есть ли таковые в 802.11 и насколько они уязвимы?

МЕХАНИЗМЫ ЗАЩИТЫ СТАНДАРТА IEEE 802.11

■ К сожалению (или к счастью), разработчики прототипа Wi-Fi почти не заботились обеспечением его безопасности. Мало ли других сложных и интересных задач? В течение семи лет (с 1990 по 1997 год) решались вопросы методов передачи данных,

увеличения пропускной способности, совместимости оборудования и т.п. Стоит ли удивляться, что изначально единственной защитой был системный идентификатор (SSID), передающийся в открытом виде? Более того, чтобы повысить комфорт при использовании чужой сети, была введена возможность широковещания сетевого имени (SSID Broadcast), которая по умолчанию используется на большинстве современных точек доступа. Еще одной преградой для чукотских хакеров и простых хулиганов стал контроль доступа по MAC-адресам. На точке доступа есть возможность задать список адресов, которым разрешена или запрещена авторизация. В лучших традициях

802.11 MAC-адрес передается в открытом виде. Следующей ступенью, на которую поднялась безопасность Wi-Fi, стал протокол WEP (Wired Equivalent Privacy).

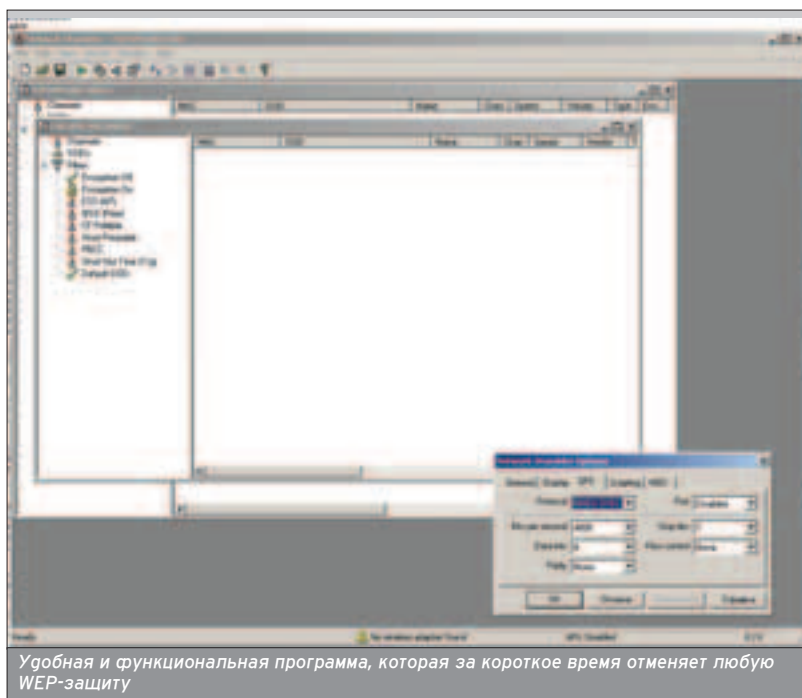
WEP - ЗАЩИТА ОТ СЛУЧАЙНОГО ПРОНИКНОВЕНИЯ

■ Основа протокола - поточный шифр RC4, разработанный Рональдом Райвестом в 1987 году. Этот алгоритм является симметричным и получил широкое распространение благодаря своему высокому быстродействию. Для оценки криптостойкости RC4 необходимо сказать несколько слов об используемом методе шифрования.

Для перехвата информации в традиционной сети злоумышленник должен получить физический доступ к кабелю.



Рональда Райвест, разработчик RC4



Удобная и функциональная программа, которая за короткое время отменяет любую WEP-защиту

ОПИСАНИЕ АЛГОРИТМА RC4

■ Алгоритм RC4 был разработан в 1987 году и в течение семи лет оставался закрытым. Подробные сведения о его конструкции предоставлялись только после подписания договора о неразглашении. Однако в сентябре 1994 года алгоритм появился в Сети.

RC4 является алгоритмом компании RSA Data Security, основанным на потоковом шифре. Такие шифры преобразуют открытый текст в криптограмму по одному биту

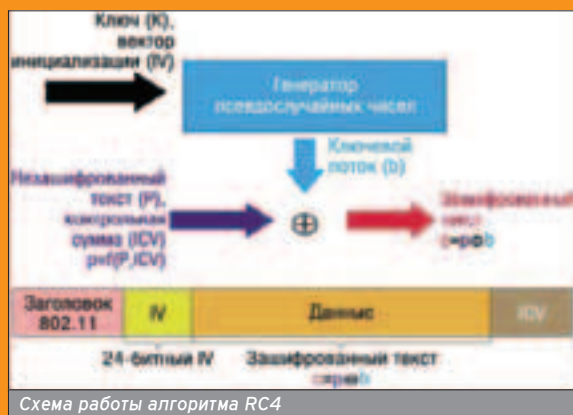


Схема работы алгоритма RC4

за операцию. Генератор потока ключей выдает поток битов $k_1, k_2, k_3, \dots, k_n$. Этот поток ключей и поток открытого текста $p_1, p_2, p_3, \dots, p_n$ подвергается операции XOR ("исключающее или"), в результате чего получается зашифрованный текст. Для дешифровки та же операция выполняется с зашифровкой и с потоком ключей. Безопасность такой системы полностью зависит от генератора ключей. Дело в том, что в большинстве случаев используются псевдослучайные числа, и так повышается вероятность повторений. Генератор настоящих случайных чисел и длинные ключи могут сделать этот алгоритм довольно стойким.

Свойства алгоритма:

- Адаптивность для аппаратных средств, использование в алгоритме только простейших вычислительных операций, которые реализуются во всех процессорах.
- Высокая скорость работы алгоритма. Это свойство позволило RC4 завоевать широкую популярность. На данный момент он реализован в десятках коммерческих продуктов, например Lotus Notes, Apple Computer's AOCE, Oracle Secure SQL, а также является частью спецификации стандарта сотовой связи CDPD.
- Компактность исходного кода в различных реализациях.
- Низкие требования к памяти.
- Простота выполнения.

Man-in-the-Middle - это одна из немногих атак, которая позволяет получить доступ даже к хорошо защищенной сети.

Как я уже говорил, алгоритм является симметричным, соответственно, для шифрования и расшифровки используется один и тот же ключ, который передается по защищенным каналам связи. При расшифровке данных автоматически выполняется аутентификация, так как предполагается, что ключ известен лишь двум лицам: отправителю и получателю. Плюсом такого подхода является скорость, минусом - низкая криптос-

тойкость. Симметричные алгоритмы особо уязвимы к атакам типа Man-in-the-Middle. В протоколе WEP используется шифрование с помощью 40- или 104-битного ключа, который является статической частью шифра. Как правило, пользователю предлагается два метода введения ключа: HEX-числа и ASCII-символы (для 40-битного ключа - 10-значное HEX-число или пять символов ASCII; для 104-битного - 26 и 13 соответственно). К

статической части добавляется динамическая составляющая, которая носит имя вектора инициализации (Initialisation Vector - IV) и весит 24 бита. Таким образом, полная длина ключа равна 64 или 128 битам (о чем и заявляют производители). В последнее время все чаще встречаются продукты, в которых реализована поддержка ключей с длиной до 256 бит, однако это не сильно повышает стойкость алгоритма, поскольку увеличение длины ключа происходит за счет статической части.

ВЗЛОМ WEP

■ Существует несколько разновидностей атак, которые могут быть эффективны против защиты WEP.

Атаки на отказ в обслуживании (DoS-атаки)

Как всегда, подобной рода атаки направлены на достижение неработоспособности сети или какой-либо ее части. В случае с беспроводными сетями такие атаки особо эффективны благодаря физической среде взаимодействия различных уровней OSI. Особенности Wi-Fi-сетей делают DoS-атаки возможными на всех уровнях, в том числе на физическом, при этом очень трудно доказать сам факт проведения DoS. Например, никто не мешает создать сильные помехи в частотном диапазоне 2,4 ГГц, то есть и сеть из строя вывести, и атакующего скомпрометировать. Самая большая проблема на канальном уровне - возможность спуфинга точек доступа. Причина в том, что для связи клиентское оборудование обычно выбирает точку доступа с наиболее качественным сигналом. Подменить базовую точку доступа не составит труда: для этого нужно обеспечить сильный сигнал в выбранной зоне и узнать SSID жертвы. После такого "клонирования" злоумышленник перехватывает весь трафик, а в результате не только будет получен отказ в обслуживании, но и появится возможность со временем получить WEP-ключи.

Man-in-the-Middle

Подобная атака может быть очень эффективна благодаря симметричности алгоритма RC4. Суть Man-in-the-Middle состоит в прослушивании передач между двумя хостами, при этом исключено присутствие атакующего в соединении. На основе такой атаки можно имитировать другой хост, перехватывать трафик для дальнейшего анализа и т.д. Кроме того, Man-in-the-Middle - это одна из немногих атак, которая позволяет получить доступ даже к хорошо защищенной сети. Прежде чем начать атаку, необходимо собрать как можно больше информации, например SSID-, IP- и MAC-адреса клиента и точки доступа, соответствие запроса и отклика и т.д. »

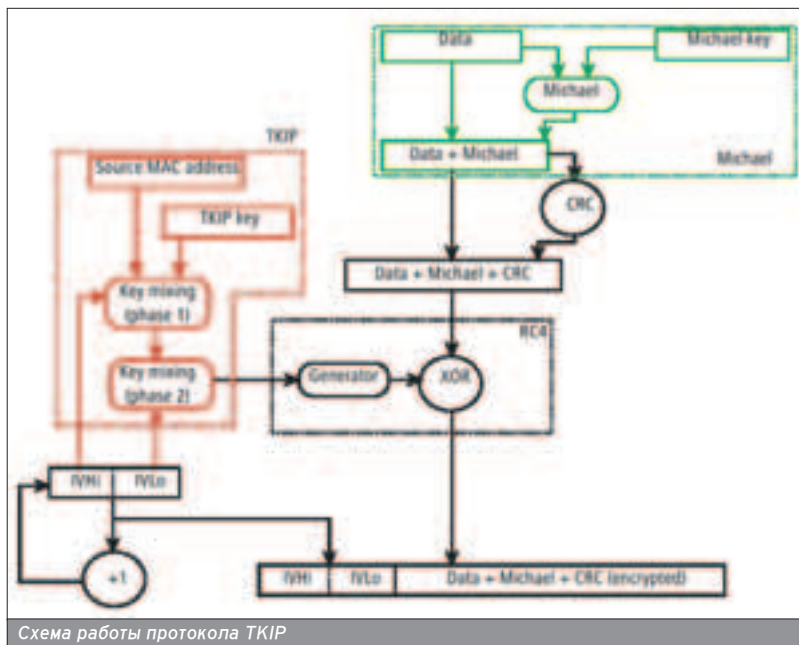


Схема работы протокола TKIP

WPA - это протокол, использующий усовершенствованную схему шифрования данных RC4 на основе TKIP с обязательной процедурой аутентификации средствами 802.1x.

Далее злоумышленник бросит все силы на то, чтобы а) обмануть точку доступа, выдавая себя за авторизованного клиента; и б) обдурить клиента, выдавая себя за точку доступа. Желаемым результатом атаки типа "человек посередине" является вытеснение авторизованного клиента и "общение" с базой от его имени.

Вардрайвинг

Вкратце, этот метод состоит в сканировании эфира с целью нахождения точек. Вардрайверы могут довольно эффективно охотиться за "вражескими" сетями, при этом "запоминая" самые интересные. Какой бы метод ни был использован, для получения доступа к сети, защищенной WEP, нужно получить ключ. Чтобы получить ключ, используем основную уязвимость протокола - вектор инициализации (IV). Его длина - 24 бита, что дает нам 2^{24} уникальных вариантов. Если известны все значения вектора, то получить статическую часть ключа проще пареной репы. Поскольку IV динамически изменяется во время работы (проще говоря, каждый пакет несет новое значение), то для успешного взлома необходимо собрать достаточное количество пакетов (от 50 000 до 200 000). Чем активнее идет обмен трафиком внутри сети, тем быстрее можно собрать необходимую информацию. Однако можно ускорить про-

цесс искусственным генерированием трафика.

ПРАКТИКА

Итак, нам понадобится один или несколько ноутбуков, Wi-Fi-адаптер (или несколько) и направленная антенна средней мощности. Будем считать, что сеть уже найдена и связь с точкой доступа достаточная для бесперебойного обмена данными. Цель

атаки - узнать необходимую информацию о сети, перехватить достаточное количество пакетов, вычислить статическую часть WEP-ключа. Для этого будем использовать...

УТИЛИТЫ ДЛЯ ВЗЛОМА WEP

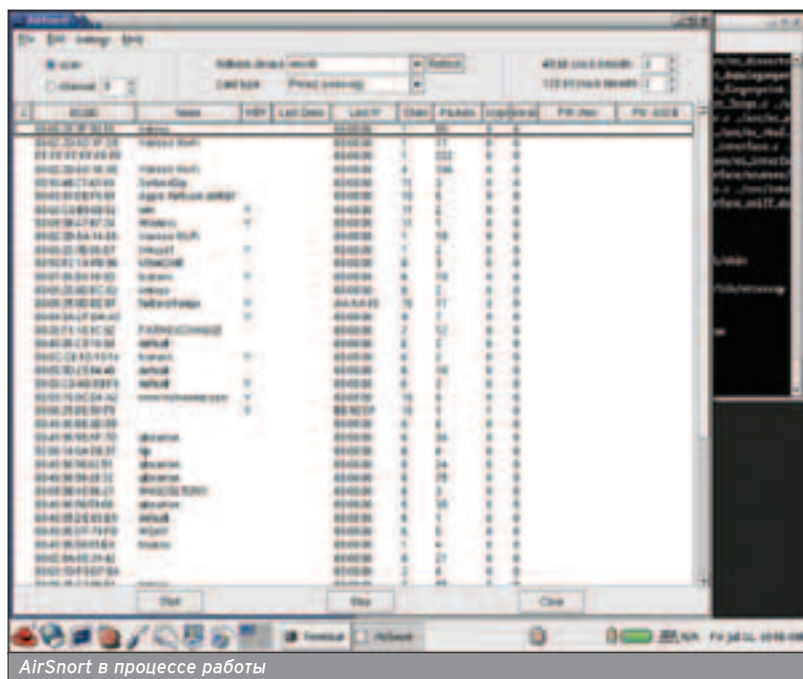
Стоит сказать, что среди представленных ниже утилит присутствуют как готовые решения, позволяющие найти информацию о сети и одновременно умеющие перехватывать и анализировать пакеты, так и узко специализированные софтины.

После того как в середине 2001 года была опубликована статья о методе взлома WEP, как грибы после дождя стали появляться утилиты, автоматизирующие этот процесс. Одна из самых известных - AirSnort.

AirSnort - это инструмент для определения ключей шифрования, реализующий атаку Fluhrer-Mantin-Shamir (FMS). Вычисляет ключ шифрования, перехватив достаточное количество зашифрованных пакетов. AirSnort проста в использовании и эффективна, однако для взлома WEP требуется очень большое количество собранных пакетов (5-10 млн). Из плюсов можно назвать небольшой размер (благодаря реализации для Linux) и незаметную работу.

Следующий шаг, который сделали хакеры, - увеличение скорости FMS-атаки. Результатом стала dwerfcrack, которая отличается от AirSnort лишь более высоким быстродействием. Долгое время суть метода оставалась прежней, и взлом затягивался на длительное время, хотя уже тогда WEP казался все более мертвым, чем живым. Однако последний гвоздь в гроб эквивалента кабельной защиты забил некий KoreK, написавший NetStumbler.

Теперь для атаки на ключ WEP не нужно собирать миллионы пакетов, и



AirSnort в процессе работы

СТАНДАРТ IEEE 802.1X

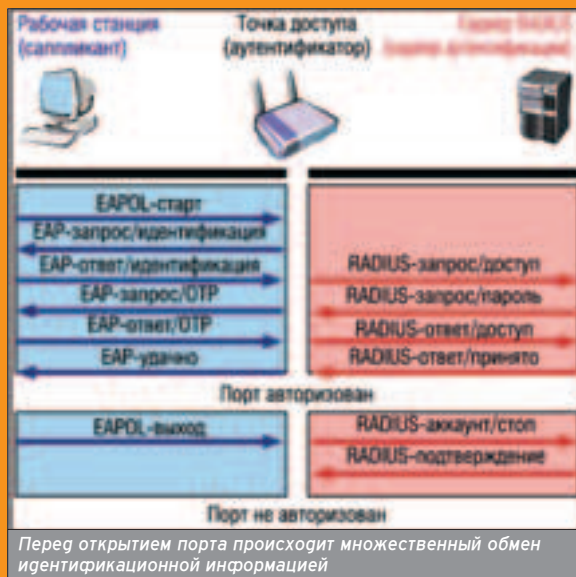
■ IEEE 802.1X - стандарт, основанный на трех компонентах (протокол расширенной аутентификации EAP - Extensible Authentication Protocol;

протокол защиты транспортного уровня TLS - Transport Layer Security; сервер RADIUS - Remote Access Dial-In User Service) и позволяющий производить эффективный контроль доступа на

уровне пользователей. Применение 802.1x связано с тремя основными элементами:

1. Саппликант - пользователь, который нуждается в сетевой аутентификации;
2. Сервер аутентификации - обычно RADIUS-сервер, который производит фактическую аутентификацию;
3. Аутентификатор - посредник между двумя уже названными элементами, предоставляющий доступ в сеть (в случае с беспроводной сетью этим элементом, как правило, является точка доступа). В общем случае (One Time Password) процесс аутентификации происходит следующим образом. Пользователь делает запрос на соединение с аутентификатором (реже наоборот), далее последний требует идентификационную информацию. После получения этих данных аутентификатор отправляет их серверу. Затем сервер запрашивает подлинность саппликанта. В случае положительного ответа сервер посылает специальный служебный сигнал, после чего аутентификатор открывает пользователю порт для доступа и отправляет сообщение о завершении процедуры.

Данный стандарт зарекомендовал себя как довольно эффективное и безопасное решение вопроса аутентификации клиентов и сейчас широко применяется как в кабельных, так и в беспроводных сетях. Подробнее читай там же, где читал я, - на www.itanium.ru и <http://itc.ua>.



Злоумышленник может легко вывести из строя сеть на базе WPA, просто посылая каждую секунду два пакета со случайными ключами шифрования.

неважно, зашифрованы ли они. Новый метод статического криптоанализа позволил сократить время подбора ключа в несколько раз. Единственная характеристика, используемая для анализа, - количество уни-

кальных векторов инициализации. Кроме того, утилита написана под Windows и имеет простой, интуитивно понятный интерфейс, так что теперь взлом Wi-Fi-сетей стал доступным для каждого. Кроме непосред-

ственного анализа пакетов, утилита предоставляет много интересной информации о "жертве": имя сети, излучаемая мощность, производитель точки доступа, состояние DHCP-сервера, диапазон IP-адресов, MAC-адрес точки и еще много данных о том, что происходит в эфире. Есть возможность записать координаты точки доступа, если они предоставлены внешним GPS-устройством.

На сегодняшний день существует более продвинутая версия NetStumbler - chooper. Кроме решений, основанных на статистическом анализе, существуют средства для старого доброго брутфорса. Самые известные - это WepLab, WepAttack. Сейчас уже очевидно, что взлом WEP - это задача, которая не требует почти никаких особенных знаний и навыков. Гораздо интереснее протокол безопасности WPA (Wi-Fi Protected Access - защищенный доступ Wi-Fi).

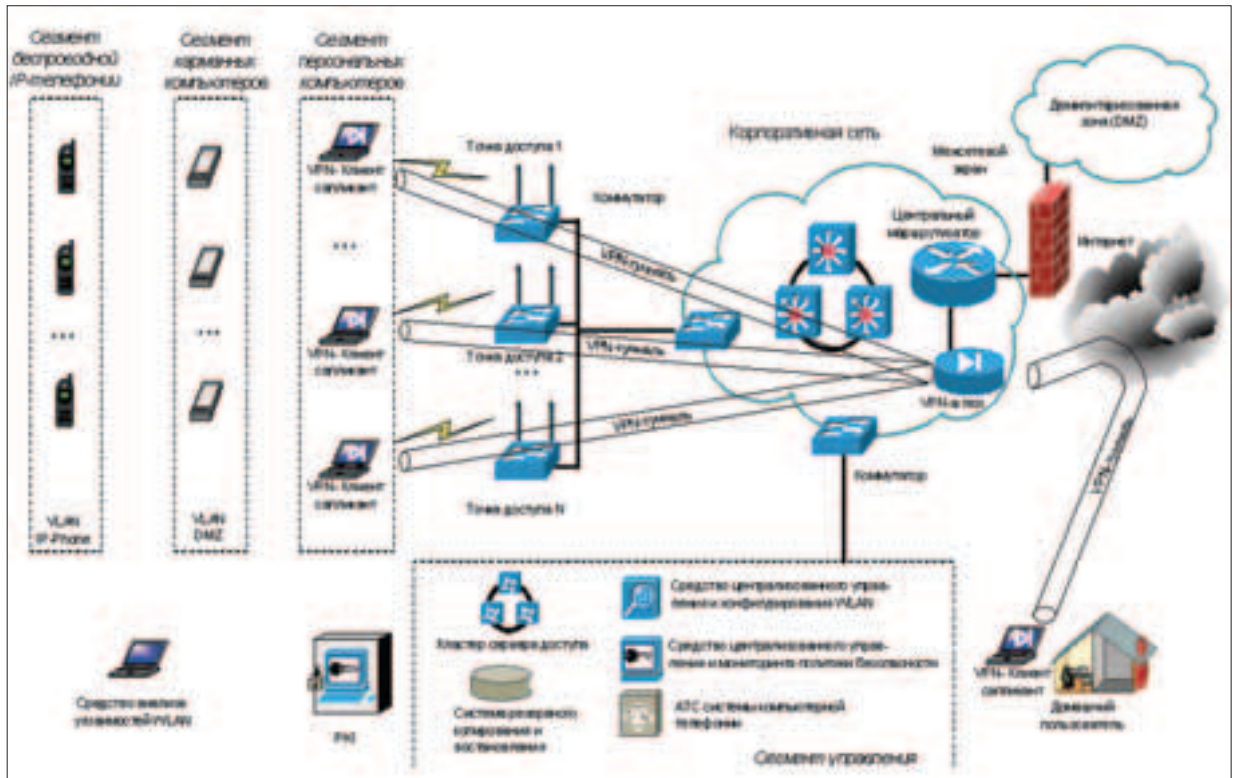
WPA - ВЫЗОВ БРОШЕН

■ Протокол WPA, утвержденный консорциумом Wi-Fi в 2002 году, направлен на устранение слабых мест беспроводных сетей на основе WEP. С другой стороны, WPA не является чем-то абсолютно новым по сравнению с WEP и использует, фактически, тот же RC4, но в иной реализации. Обо всем по порядку!

Итак, WPA - это протокол, использующий усовершенствованную схему шифрования данных RC4 на основе TKIP (Temporal Key Integrity Protocol) с обязательной процедурой аутентификации средствами 802.1x.

Протокол TKIP используется для обеспечения безопасности и целостности WPA. Он также использует RC4, однако вектор инициализации здесь имеет длину в 48 бит. Для каждого передаваемого пакета генерируется новый ключ, а контроль целостности сообщений ведется с помощью контрольной суммы MIC (Message Integrity Code). Базовый размер ключа увеличен до 128 бит. По сравнению с WEP, полностью изменена процедура генерации ключа. Теперь ключ получается из трех компонентов: базовая составляющая, MAC-адрес передающего узла и номер передаваемого пакета.

Базовая составляющая ключа является динамической и генерируется каждый раз, когда клиент устанавливает соединение с точкой доступа. Для формирования базового ключа используются следующие данные: хэш-функция секретного сеансового ключа (пароля, заданного пользователем), псевдослучайное число, MAC-адрес. В конечном итоге клиент и точка доступа получают сеансовый ключ в результате аутентификации по протоколу 802.1x. Стоит сказать, что при разработке WPA первоочередной задачей была совместимость »



Примерно так может выглядеть защищенная сеть

802.11i, скорее всего, не станет таким же универсальным и надежным средством защиты, каким когда-то стал VPN.

с WEP и создание условий работы нового средства защиты на старом оборудовании. Именно этим объясняется применение все того же RC4, а не AES, например. Однако, несмотря на преимущество, протокол WPA избавился от многих уязвимостей, присущих WEP.

УЯЗВИМОСТИ WPA

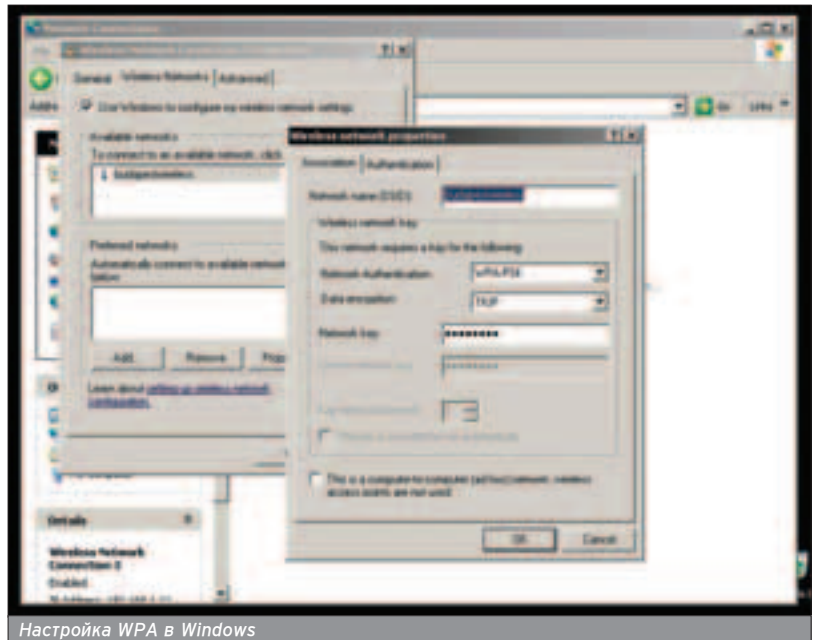
■ Самым страшным сном для протокола WPA, несомненно, являются атаки на отказ в обслуживании (DoS). Злоумышленник может легко вывести из строя сеть на базе WPA, просто посылая каждую секунду два пакета со случайными ключами шифрования. Вражеская точка доступа, приняв эти пакеты, решает, что произведена попытка несанкционированного доступа, и закрывает все соединения, чтобы не допустить использования сетевых ресурсов сторонним лицом. Уязвимость к DoS-атакам на физическом уровне также высока - здесь никаких изменений по сравнению с WEP. А гелла с атаками, направленными на получение ключа, намного хуже, хотя они не безнадежны. Роберт Московиц, технический директор ICSA Labs, опубликовал доклад, в котором описывается вот такая стратегия атаки на WPA-сети. Большинство програм-

мных реализаций WPA строят криптографический ключ для шифрования на основе введенного пользователем пароля и сетевого имени (либо MAC-адреса), которое является общедоступным. Информация, зашифрованная этим ключом, свободно передается по Сети. Методом брутфорса подбирается исходный пароль. В

данном случае пароль длиной менее 20-ти символов считается потенциально опасным. Конечно же, речь идет только о тех случаях, когда WPA используется в режиме pre-shared mode. Кроме того, WPA, так же как и WEP, не имеет защиты против "клонирования" точек доступа.

IEEE 802.11i - СЕМЬ БЕД, ОДИН ОТВЕТ?

■ Этого стандарта безопасности ждали. Очень долго и с большими надеждами. Наконец, после четырех лет ожидания, 24 июня 2004 года он был принят, и для определенных кругов это было событие года. Однако 802.11i во многом похож на WPA (поз-



Настройка WPA в Windows



Крутая направленная антенна

тому 802.11i иногда называют WPA2). Однако есть несколько кардинальных отличий. Во-первых, вместо RC4 используется AES. Он появился совсем недавно и обладает хорошей криптостойкостью (на данный алгоритм пока нет известных атак), а его симметрическая природа делает его достаточно быстрым.

Появились такие понятия, как надежно защищенная сеть (RSN) и на-

дежно защищенное сетевое соединение (RSNA). Добавлен механизм CCMP, состоящий из связки алгоритма шифрования AES и кода CBC-MAC. CCMP выполняет две важные задачи: обеспечение конфиденциальности и аутентификация. В рамках стандарта 802.11i алгоритм CCMP является обязательным, тогда как TKIP - опциональным (для совместности со старыми устройствами). По-

жалуй, последнее важное отличие от WPA - поддержка быстрого роуминга между точками доступа. Если рассмотреть принципиальные отличия 802.11i от предыдущего протокола, становится понятно, что разница в степени защиты невелика. Можно констатировать тот факт, что 802.11i, скорее всего, не станет таким же универсальным и надежным средством защиты, каким когда-то стал VPN.

Уже сейчас можно назвать несколько типов атак, к которым WPA2 проявляет особую слабость:

- Традиционные для беспроводных сетей атаки на физическом уровне.

- Использование служебных фреймов для подмены MAC-адреса. Такая атака возможна благодаря тому, что при передаче служебной информации точка доступа и клиент не выполняют процедуру аутентификации.

- Атаки посредством запросов IEEE 802.1x. Дело в том, что стандарт 802.11i не умеет отклонять запросы на аутентификацию, поэтому точку доступа можно перегрузить.

ЕСТЬ ЛИ ЗАЩИТА В 802.11I?

- Ответ на вопрос заголовка - "га". На сегодняшний день связка "WPA+VPN" (а тем более WPA2+VPN) делает беспроводную сеть достаточно защищенной для передачи даже особо ценной информации. Однако многие ли устанавливают подобную защиту?

По данным исследования, проведенного лабораторией сетевой безопасности компании "ИнформЗащита", только 5% сетей в Москве используют технологии WPA или 802.11i. Более 2/3 сетей не защищены ничем! На остальных настроен дырявый WEP. Делай выводы.

Стандарт 802.11i не умеет отклонять запросы на аутентификацию, поэтому точку доступа можно перегрузить.

Идеальное телевидение
GO TV VIEW
www.gotview.ru

GOTVIEW TV BOX CRYSTAL

Поддержка стереозвука в форматах NICAM и A2 для телепередач
Поддержка разрешения до 1280x1024
Функция предпросмотра 9 каналов
Автоматическое определение кодировки сигнала
Цифровые фильтры уменьшения шума и повышения резкости изображения

GOTVIEW PCI 7135

Высококачественный чип Philips SAA7135
Поддержка стереозвука телепрограмм в форматах NICAM и A2
Расширенная обработка звука: частота дискретизации до 48kHz, эквалайзер, регулировка баланса, Dolby ProLogic, Visual Dolby Surround (полнодвухканальный звук)

Стандарты: PAL / SECAM / NTSC
Полностью русифицированное программное обеспечение
Эфирное и кабельное TV

GOTVIEW USB2.0 DVD Deluxe

Внешний USB2.0 ТВ-тюнер с коаксиальным 15-ти битным видеовыходом, 8-и битным аудиовыходом Philips SAA7135
Поддержка звука в форматах A2 и NICAM
Видеозахват и аппаратное MPEG сжатие до 15 Mbit/sec, видеоконтраст
Настраиваемые аппаратные фильтры: шумоподавление
Аппаратный 3-х полосный эквалайзер с сохранением настроек для каждого канала

GOTVIEW PCI DVD

Высококачественный видеочип с аппаратным сжатием до 15 Мбит/сек и аппаратным фильтром подавления шума
Поддержка стереозвука телепрограмм в формате NICAM и A2

GOTVIEW USB пульт

Дистанционное управление мультимедийными программами воспроизведения звуковых, DVD, MP4 файлов, презентаций, управление официальными приложениями, запуск и остановка программ по желанию пользователя. Работа в режиме звуковой клавиатуры или мыши.

ULTRA Computers (095) 775-7566, 729-5255, 729-5244 (812) 336-3777 (Санкт-Петербург)
SUNRISE (095) 542-8070
ProNET Group (095) 789-3846, 789-3847
DESTEN Computers (095) 970-0007
FORUM Computers (095) 775-7759
ABC Компьютер (095) 107-9049, 741-9111 (бесплатная доставка)
MEJUN (095) 727-1222, 727-1220 (доставка по России)
Систек (095) 781-2384, 784-6658, 737-3125, 784-7224
Скорпион (812) 320-7160, 449-0573 (Санкт-Петербург)
R-Style (8312) 46-3517, 46-1622, 46-1623 (И.Новгород)
Радиоконтакт-Компьютер (095) 741-6577
ХОПЕР (095) 235-3500, 235-5417, 235-1667, 737-0377 доб. 40-28
Сатурн (095) 148-0101
УКРАИНА GOTVIEW (044) 237-5928, 516-8471, 517-8218 (Киев)
Беларусь "Ронгбук" (017) 284-1001, 284-2198
Савеловский рынок лавильоны: A44, 2D16, D32.

Eto'o

МАЙСКИЕ ЖУКИ

ЧАСТО ВСТРЕЧАЮЩИЕ СЛАБОСТИ И БАГИ 802.11 БЕСПРОВОДНЫХ УСТРОЙСТВ

Можно много писать об ошибках в протоколе WEP, использовании слабых ключей, перехвате воздушного трафика, атаках Man-in-the-Middle и прочей классике взлома Wi-Fi. Но обойти стороной тему ошибок в конкретных устройствах, в конкретных реализациях стандартов - нельзя, хотя бы потому что ты, ломая беспроводные сети, всегда имеешь дело с конкретным девайсом, а не абстрактной моделью, знакомой только по описанию "на бумаге". И у каждого устройства свои слабости и баги, знать о которых нужно любому Wi-Fi-взломщику.



ВОЗМОЖНЫЕ СЛАБЫЕ МЕСТА

■ Думаю, мы сразу начнем с места в карьер и обсудим возможные места, в которых могут скрываться слабости и уязвимости.

Как ты знаешь, помимо Wi-Fi-карточек, существует и множество других, более независимых устройств: видеорекамеры с портом 802.11, точки доступа, беспроводные маршрутизаторы и умные пылесосы. Совершенно понятно, что оборудовать каждый такой девайс набором устройств, необходимым для удобной настройки и администрирования, очень дорого да и обычно неудобно. В самом деле, довольно глупая затея - присобачить к точке доступа ЖК-экран и клавиатуру. Так что большинство подобных устройств предоставляют удобный интерфейс для сетевого администрирования через http, а также SNMP. Действительно, интуитивно понятный web-интерфейс и красивый Wizard уже стали стандартом. Это, с одной стороны, плюс - удобно и дешево, а с другой - минус: редкой компании удается соблюсти все критерии информационной безопасности при проектировании таких интерфейсов. Все начинается с банальщины - со стандартных паролей к админ-зонам, ошибок в сценариях, багов в реализации SNMP, а заканчивается незащищенностью секретных данных. Нередко встречаются также более низкоуровневые ошибки - разнообразные переполнения при обработке сетевых пакетов, ошибки в работе DHCP и т.д. и т.п.

Практика позволяет познакомиться со всем этим и долго поддерживать знакомство, и порой не нужно прилагать никаких усилий, чтобы получить доступ к 802.11-устройству.

Доказательство - распространенность первой ошибки, о которой я расскажу.

СТАНДАРТНЫЕ ПАРОЛИ

■ Уязвимые устройства - все неадекватно настроенные. Чаще всего

случается с девайсами D-Link - любимчиками домашних пользователей.

■ Условия атаки - доступ к устройству через TCP/IP-сеть. Ты должен быть либо в одной кабельной сети, либо должен подключиться через Wi-Fi.

■ Цель атаки - административный http-интерфейс.

■ Описание.

Любое устройство с сетевым http-интерфейсом администрирования поставляется с минимальным набором предустановленных настроек, в том числе админские идентификаторы (логин/пароль). Некоторые пользователи по неизвестной мне причине не изменяют эти настройки, доверяясь стандартным заводским. Это

свойственно, прежде всего, домашним пользователям, которые всерьез считают, что во всей окрестности их дома только они такие прогрессивные и их 802.11-сети ничего не угрожает. Но мы-то с тобой знаем, что это не так. Исторически сложилось так, что самые дешевые и доступные беспроводные устройства производит фирма D-Link. Если ты обнаружил такую точку доступа, считай, что тебе уже везет! А если у нее еще и стандартный SSID и отсутствует всякое шифрование, можешь смело радоваться. Я недавно столкнулся именно с таким случаем, когда просканировал окрестности своего жилища. Без проблем подключился к точке «», получил по DHCP сетевой адрес и сразу попробовал прителне-

"Если хотите безопасности при использовании SNMP, не используйте этот протокол."



таться к 80-му порту точки доступа. Тут же выяснил, что там действительно висит некий web-сервер. Набрал в браузере <http://192.168.1.1>, я еще раз убедился, что передо мной роутер D-Link. Учитывая, что хозяева этого геймса не включили даже примитивного шифрования и не изменили SSID, я без раздумий ввел стандартную для D-LINK комбинацию "admin:admin" в форму аутентификации и получил доступ к админской панели. В итоге я стяжал доступ не только к халаявному интернету, но и ко всему устройству: при определенном желании можно было даже увести логин/пароль от СТРИМ-аккаунта, не говоря уже о том, чтобы подменить DNS-серверы.

Чтобы попробовать этот прием в действии для устройств от других производителей, будет полезно ознакомиться со списком стандартных паролей сетевых устройств, который легко найти на www.phenoelit.de/dpl/dpl.html.

ОШИБКА УПРАВЛЕНИЯ ЧЕРЕЗ SNMP

- Уязвимые устройства - Orinoco Residential Gateway и Compaq WL310.
- Условия атаки - доступ к 192/UDP-порту.
- Цель атаки - доступ к SNMP.
- Описание.

SNMP - Simple Network Manager Protocol, простой протокол сетевого управления. Этот довольно старый протокол используется для удаленного управления сетевыми устройствами, в том числе беспроводным оборудованием. Беда в том, что и сам протокол обладает целым рядом недостатков, так еще и производители часто допускают нелепые ошибки. Тут уместно вспомнить ставшую уже крылатой фразу: "Если хотите безопасности при использовании SNMP, не используйте этот протокол." Не вдаваясь в подробности, расскажу, что указанные в заголовке точки доступа подвержены следующей атаке. Если атакующий пошлет на 192 UDP-порт пакет хитроумного содержания, уязвимая точка ответит на него цепочкой байт, среди которых будет содержаться идентификатор Community name, используемый в этой реализации SNMP для нехитрой аутентификации. Захват этого ключа, а вернее имени, позволит получить доступ к SNMP-интерфейсу устройства. Для реализации атаки необходимо передать пакет следующего содержания:

```
"\x01\x00\x00\x00\x70\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
```



Работе с SNMP посвящена целая глава книги "Perl for system administration"



атака в работе

Довольно глупая затея - приспособить к точке доступа ЖК-экран и клавиатуру.

```
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
```

Уязвимое устройство должно ответить такой вот цепочкой байт:

```
01 01 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00 00 00 00 60 1d 20 2e 38 00 00 18 19 10 f8
4f 52 69 4e 4f 43 4f 20 52 47 2d 31 31 30 30 20
30 33 39 32 61 30 00 00 00 00 00 00 00 00 00
02 8f 24 02 52 47 2d 31 31 30 30 20 56 33 2e 38
33 20 53 4e 2d 30 32 55 54 30 38 32 33 32 33 34
32 20 56 00
```

Здесь параметр Community name, необходимый для дальнейшей аутентификации, равен 0392a0. Далее уже не составит особого труда написать несложный эксплоит для устройства, например на Perl. Для этого языка существует масса модулей, которые сделают работу с протоколом удобнее. За примером далеко ходить не нужно: Net::SNMP - идеальный вариант.

DOS И НЕАВТОРИЗОВАННЫЙ ДОСТУП

■ Уязвимые устройства - Siemens SANTIS 50, Ericsson HN294dp, Dynalink RTA300W.





(game)land



новый проект издательства (game)land

sync

SYNC - Новый мужской журнал

- SYNC является путеводителем по стилю жизни современного мужчины и охватывает все сферы его интересов
- SYNC отвечает интересам пользователей всех уровней, включая «экспертов», «пионеров» и «широкие массы»

О ЧЕМ?

Влияния современных технологий на жизнь людей. Новости из мира цифровых технологий: о чем говорят, чего ждут, что недавно появилось. Тесты/практика: использование оборудования и устройств в реальной жизни, оценка продукта конечными пользователями. Дом, автомобили, спорт, кино, музыка, видеоигры, интервью и красивые девушки.

Антон Карпов (toxa@real.hacker.ru)

ЗАЩИТА ВОЗДУХА

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

О способах обнаружения, взломе и уязвимостях беспроводных сетей разного рода уже сказано и написано много, но о том, как защититься от всех этих вещей, почему-то помалкивают. Все потому, что эта тема была отложена для отдельного материала, который ты читаешь прямо сейчас. Что ж, вперед! Обезопасим свое личное воздушное пространство от набегов вардрайверов.

Обеспечение безопасности Wi-Fi-соединений уже давно стало притчей во языцех. Отсутствие проводов окончательно развязало руки охочим до конфиденциальной информации злоумышленникам, среди которых может оказаться не только сосед по локальной сети, развлекающийся ARP-спуфингом, а любой человек с ноутбуком, находящийся в пределах досягаемости беспроводной сети. Призванный спасти несчастных пользователей, протокол авторизации, аутентификации и шифрования WEP совершенно не оправдал надежд, как и его вторая инкарнация WEP2 (в ней, по сути, декларировалось только увеличение длины ключа). Современные средства позволяют сломать 128-битный WEP-ключ за несколько часов присутствия в сети. Стандарт безопасности 802.11i и, в частности, стандарт WPA/WPA2, являющийся подмножеством 802.11i, по ряду причин все еще недостаточно распространены. И на данный момент ситуация складывается таким образом, что для обеспечения безопасности беспроводной сети администратор вынужден прибегать к полумерам и/или к старым проверенным технологиям, которые не разрабатывались специально для Wi-Fi. Именно о них я расскажу в первую очередь, а потом займусь 802.11i.

ОПАСНОСТЬ В ВОЗДУХЕ

Прежде чем начать строительство круговой обороны, выясним, от чего мы хотим защититься. Для беспроводных сетей основными проблемами безопасности являются:

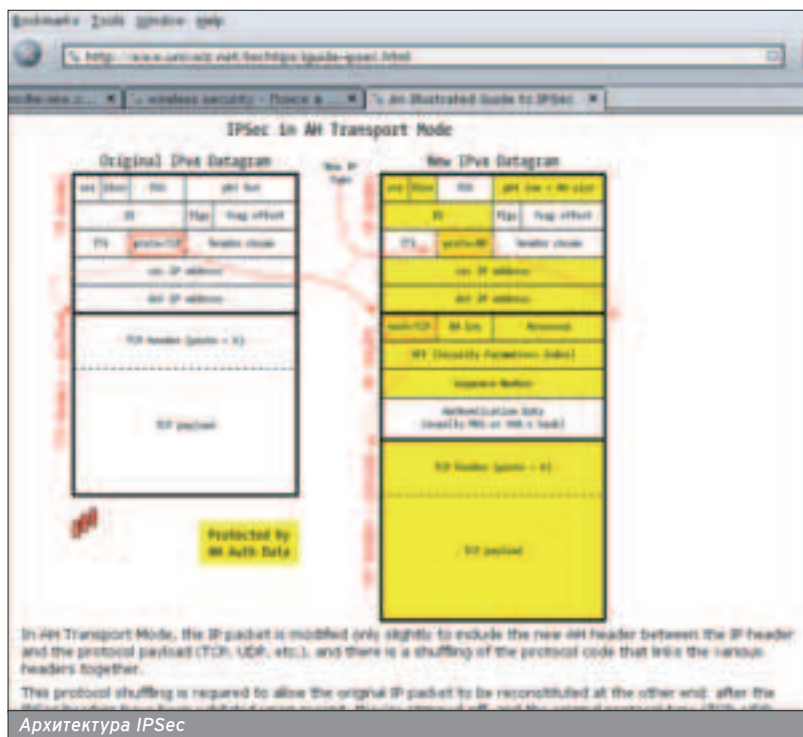
- Мониторинг и перехват трафика;
- Подключение к сети неавторизованных клиентов (внедрение подложных пакетов);
- DoS-атаки на беспроводную сеть;
- Атаки типа Evil Twin - внедрение подложного AP;
- Атаки на клиентские машины;

■ Атаки на AP (в том числе из-за уязвимостей в конфигурации точки доступа).

С последними двумя атаками все понятно: нужно своевременно патчить клиентские машины и грамотно настраивать AP, например отключить SNMP либо сменить на отличающуюся от SNMP community string по умолчанию, поставить сложный пароль на доступ к административному интерфейсу AP, своевременно обновлять прошивки и т.п. Многие AP умеют фильтровать доступ по MAC-адресу, и одной из полумер является как раз прописывание легитимных клиентов в ACL точки доступа. Огна-

ко такими способами не остановишь опытного взломщика, стремящегося проникнуть сеть, да и от перехвата конфиденциальной информации, летящей по воздуху, не защитишься. Для того чтобы пассивно sniffать весь трафик, совершенно не обязательно подключаться к какой-либо сети. Следовательно, нужно какое-то решение, осуществляющее, как минимум, шифрование трафика и авторизацию клиента в сети. И такое решение называется IPSec. Очень понятное и детальное описание этого протокола "в картинках" можно почитать тут: www.unixwiz.net/techtips/guide-ipsec.html.

Для использования IPSec необходимо настроить соответствующую политику на шлюз.





как это использовать (транспортный или туннельный режим; требовать использование ipsec или нет). Приведу конкретный пример, когда в качестве шлюза используется FreeBSD с включенной в ядро опцией IPSEC. Пусть для беспроводных клиентов выделена подсеть 192.168.1/24 и адрес шлюза - 192.168.1.1. Тогда для конкретного клиента 192.168.1.3 правила на шлюзе будут выглядеть следующим образом:

```
# flush previous SAD & SPD
flush;
spdflush;
# Security Association Database
# For ESP
add 192.168.1.1 192.168.1.3 esp 1011 -E 3des-cbc "secret-
passphrase";
add 192.168.1.3 192.168.1.1 esp 1012 -E 3des-cbc "secret-
passphrase";
# Security Policy Database
spdadd 192.168.1.3 0.0.0.0/0 any -P in ipsec esp/tun-
nel/192.168.1.3-192.168.1.1/require
spdadd 0.0.0.0/0 192.168.1.3 any -P out ipsec esp/tun-
nel/192.168.1.1-192.168.1.3/require
```

Это простейший случай, когда не используется никаких методов распределения ключа - парольная фраза вводится вручную. Стоит акцентировать внимание на выборе режима ipsec - туннельный. Этот режим используется для создания безопасного канала (secure hop) между клиентом и шлюзом, при нем шифруется весь IP-пакет, тогда как транспортный режим используется для создания защищенного канала "точка-точ" >>

Современные средства позволяют сломать 128-битный WEP-ключ за несколько часов присутствия в сети.

Нас же интересует практическая сторона вопроса.

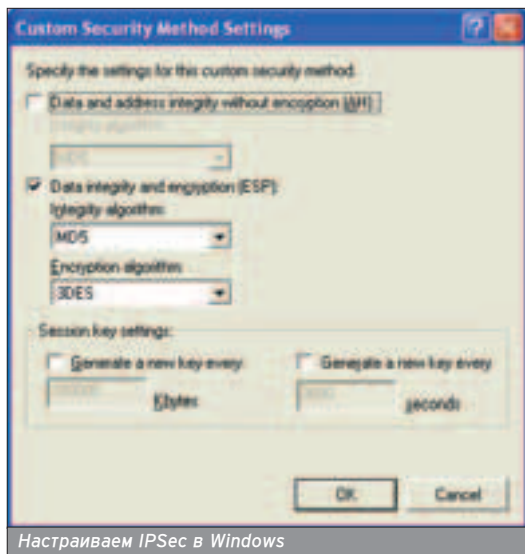
СТАРЫЙ ДОБРЫЙ IPSEC

■ Типичная схема подключения беспроводных клиентов в режиме Infrastructure (то есть с точкой доступа) выглядит следующим образом:

```
[client]-))) (((-[AP]-----[gateway]-----[wired network]
```

В такой схеме точка доступа играет роль моста между беспроводным и проводным сегментами сети (не путать с bridging mode!), а сама беспроводная сеть выделена в отдельный сегмент и роутится шлюзом в проводную LAN и/или интернет. Можно, конечно, подключить AP непосредственно к проводному сегменту сети, и тогда беспроводные клиенты будут в одной подсети с остальными. Но не рекомендую. Для использования IPsec необходимо настроить соответствующую политику на шлюзе, через который проходит трафик с AP. Если говорить в терминах IPsec, требуется указать правила ассоциации (Security Association), описывающие, что использовать (протокол AH или ESP), алгоритм шифрования (3DES, AES, и т.д.), тип ключа (IKE или прописать вручную) и политики ассоциации (Security Policy), описывающие,





Настраиваем IPSec в Windows

■ Добавляем второй список, назовем его in, повторяем описанное, за исключением того, что фильтр с Any IP Address выбираем как Source, а My IP Address как destination address.

Теперь нужно применить эти фильтры.

■ Два раза щелкаем мышью на созданной политике.

■ Нажимаем Add-> IP Security Rules.

■ Выбираем The tunnel endpoint is specified и вводим адрес шлюза. Жмем Next.

■ Выбираем Lan, жмем Next.

■ Выбираем Use this string to protect the key exchange, вводим секретную фразу, после чего... (правильно!) Next.

■ Выбираем созданный список фильтров out, клацаем по Next.

```
# setkey -DP
0.0.0.0/0[any] 192.168.1.3[any] any
in ipsec
esp/tunnel/192.168.1.1-192.168.1.3/require
ah/tunnel/192.168.1.1-192.168.1.3/use
created: Sep 15 03:30:21 2005 lastused: Sep 15
03:40:21 2005
lifetime: 0(s) validtime: 0(s)
spid=16390 seq=1 pid=5889
refcnt=2
192.168.1.3[any] 0.0.0.0/0[any] any
out ipsec
esp/tunnel/192.168.1.3-192.168.1.1/require
ah/tunnel/192.168.1.3-192.168.1.1/use
created: Sep 15 03:30:21 2005 lastused: Sep 15
03:40:22 2005
lifetime: 0(s) validtime: 0(s)
spid=16391 seq=0 pid=5889
refcnt=2
```

```
# setkey -D
192.168.1.3 192.168.1.1
ah mode=any spi=1235(0x000004d3)
reqid=0(0x00000000)
A: hmac-md5 6974736e 69636574 6f736d6f
6b656d61
seq=0x00000304 replay=0 flags=0x00000040
state=mature
created: Sep 15 03:30:21 2005 current: Sep 15
03:40:21 2005
diff: 600(s) hard: 0(s) soft: 0(s)
last: Sep 15 03:39:20 2005 hard: 0(s) soft: 0(s)
current: 135688(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 772 hard: 0 soft: 0
sadb_seq=3 pid=5878 refcnt=2
192.168.1.1 192.168.1.3
ah mode=any spi=1234(0x000004d2)
reqid=0(0x00000000)
A: hmac-md5 6974736e 69636574 6f736d6f
6b656d61
```

Удобно использовать цифровой X.509-сертификат клиента в качестве авторизационного документа.

ка", и в этом случае шифруется только тело IP-пакета.

Следует поместить указанный конфиг в файл /etc/ipsec.conf и перечитать настройки ipsec:

```
# setkey -f /etc/ipsec.conf
```

Если в качестве клиентской ОС используется также FreeBSD, то ее настройка будет точно такой же, только в SPD направления пакета - in и out - поменяются местами.

Если в качестве клиента используется Windows, настройка IPSec превратится в увлекательный процесс клацанья мышкой:

■ Start-> Run. Набираем mmc и жмем <ENTER>.

■ Console-> Add/Remove Snap In. Выбираем Add-> IP Security Policy Management и жмем Add, где выбираем Local Computer, затем Finish и Close.

■ Выбираем IP Security Policies в Local Machine, нажимаем правую кнопку мыши и выбираем Create IP Security Policy.

■ Вбиваем какое-нибудь название политики и жмем Next.

■ Снимаем галочку Activate и еще раз Next.

■ Снимаем выделение с Edit Properties. Finish.

Теперь у нас появилась новая политика. Аллилуйя! Но это еще не все.

■ Жмем правую кнопку мыши на вкладке IP Security Policies окна Console Root и выбираем Manage IP filter lists and filter actions, затем жмем Add.

■ Обзываем список фильтров out, затем снова Add.

■ Выбираем My IP Address как Source, Any IP Address как destination address. Убираем галочку mirrored.

■ Выбираем Require Security, не забывая давать англоязычный эквивалент нашего "Далее".

■ Затем повторяем то же самое, только вводим адрес клиентского компьютера и список фильтров - in.

Прорвавшись сквозь гебри диалогов и мастеров, наконец можно убедиться, что ipsec работает и клиент с сервером установили ассоциации с помощью все той же setkey:

Использование IPSec авторизует клиента в сети, однако никоим образом не авторизует точку доступа для клиента.

```
[[[...]]] wpa_supplicant
wpa_supplicant v0.9.9
Copyright (c) 2002-2005, Jouni Malinen <jmalinen@cc.hut.fi> and contributors

This program is free software. You can distribute it and/or modify it
under the terms of the GNU General Public License version 2.

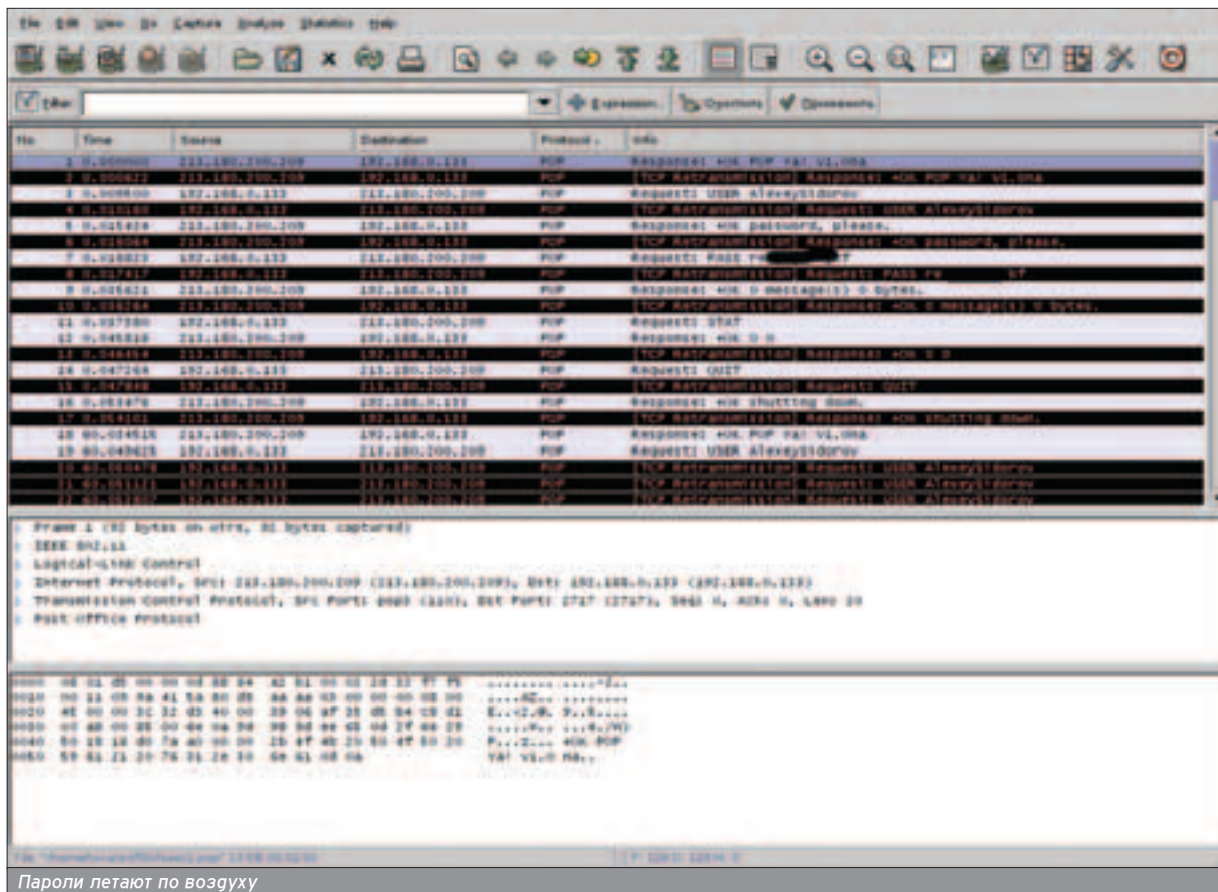
Alternatively, this software may be distributed under the terms of the
BSD license. See README and COPS for more details

usage:
wpa_supplicant [-Ebbnqqvw] [-i:iface] [-c:config file] [-D:driver] \
... [-P:pid file] [-N] [-s:name] [-s:conf: [-D:driver]] ...]

options:
-B = run daemon in the background
-d = increase debugging verbosity (-dd even more)
-K = include keys (passwords, etc.) in debug output
-t = include timestamp in debug messages
-h = show this help text
-L = show license (GPL and BSD)
-q = decrease debugging verbosity (-qq even less)
-v = show version
-w = wait for interface to be added, if needed
-N = start describing new interface

No networks (SSID) configured.
[[[...]]]
```

Поддержка WPA во FreeBSD 6



Если в качестве клиента используется Windows, настройка IPsec превратится в увлекательный процесс клацанья мышкой.

```
seq=0x00000350 replay=0 flags=0x00000040
state=mature
created: Sep 15 03:30:21 2005 current: Sep 15
03:40:21 2005
diff: 600(s) hard: 0(s) soft: 0(s)
last: Sep 15 03:39:25 2005 hard: 0(s) soft: 0(s)
current: 531216(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 848 hard: 0 soft: 0
sadb_seq=2 pid=5878 refcnt=1
```

Кроме того, запущенный tcpdump должен показывать исключительно наличие ESP-пакетов. Теперь весь трафик защищен.

Разумеется, данный способ построения IPsec довольно примитивен. Если клиентов много, возникнут задачи дублирования политик, к тому же трудно дергать админа каждый раз, когда новый легитимный клиент подключается к сети. В этом случае, по-моему, удобно использовать цифровой X.509-сертификат клиента в качестве авторизационного документа. Останется лишь выдать новому клиенту сертификат по запросу. Подробную статью с построением беспроводного шлюза с использованием OpenBSD и isakmpd на X.509-сертификатах написал Andrushock в одном из недавних номеров "Хакера".

IPsec - надежное, проверенное годами решение. С главной задачей, защитой трафика, он справляется на ура. Есть ли у него минусы? При всех плюсах - да, есть. Например, использование IPsec авторизует клиента в сети (но не на API), однако никоим образом не авторизует точку доступа для клиента, то есть не решает проблему ложного AP IPsec, но делает ее в известной мере бессмысленной: через AP злоумышленника все равно будут проходить зашифрованные пакеты либо не будут проходить вообще, в зависимости от того, потеряется ли виртуальный канал "клиент-шлюз".


802.11i и WPA

■ Новый стандарт (хотя разве можно назвать новым стандарт, принятый еще в 2004 году?) определяет не только меры по защите трафика в беспроводных сетях. Эта задача целиком отдается протоколу WPA, который, из-за полной несостоятельности WEP, пришлось даже выпустить раньше, отдельно от 802.11i. WPA предполагает использование протоколов авторизации семейства 802.1x, EAP, TKIP и RADIUS. TKIP здесь как бы приходит на смену WEP, выполняя

задачи по защите трафика, а EAP и RADIUS осуществляют авторизацию клиента в сети. Важно, что в стандарте 802.11i вместо TKIP используется алгоритм шифрования AES, но выпущенная отдельно версия WPA изначально предусматривала использование TKIP, так как для AES требовалась более мощное оборудование.

Если описывать коротко, совместная работа всех протоколов выглядит следующим образом: клиент авторизуется в RADIUS и затем, совместно с точкой доступа, генерирует сессионный ключ для шифрования трафика. Заметно, что разработчики стандарта серьезно подошли к вопросу обеспечения безопасности в корпоративных сетях. Но как быть SOHO-классу? Для пользователей домашних или малых офисных сетей разработан вариант WPA-PSK (Pre-Shared Key), при котором ключ не генерируется, а вводится пользователем, и необходимость использования сервера авторизации отпадает.

ЭПИЛОГ

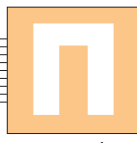
■ Как любил говорить профессор Преображенский, "Разруха - в головах, а не в клозетах". Сколько бы стандартов ни разрабатывали, какие бы протоколы ни придумывали, всегда найдутся люди, которым слово "безопасность" ни о чем не говорит. WPA? RADIUS? Вы о чем? 30% точек доступа во всем мире работают с заводскими настройками по умолчанию! 

Eto'o

УЗНАЕМ ПО ПОХОДКЕ

ОБНАРУЖЕНИЕ И FINGERPRINTING BLUETOOTH-УСТРОЙСТВ

Прежде чем начинать атаку на какой-либо Bluetooth-девайс, расположенный по соседству, необходимо собрать как можно больше информации о супостате: BT-адрес, наименование производителя, тип этого устройства, версию его прошивки, предоставляемые сервисы и т.д. Именно с обнаружения устройства и получения наиболее полной информации о нем начинается любая атака.



Получение информации о ломаемой системе - приоритетная задача для любого взломщика. Никто не компилирует наобум и не запускает сотни эксплойтов для ftp-сервиса, не зная достоверно его версию. То же в воздушных делах. Чтобы утащить через обехарр секретный номер из телефонной книги, почитать SMS-сообщения и заставить телефон позвонить по платному номеру, необходимо разузнать как можно больше об атакуемом девайсе. На практике это не всегда просто. Но мы разберемся.

ОПЫТНОЕ ЖЕЛЕЗО

Чтобы описанные мной манипуляции не казались слишком абстрактными, определимся с системой, в которой будем проводить свои опыты. Мне абсолютно все равно, какой ОС ты отдашь предпочтение, - я использовал FreeBSD 5.3 с дешевым (\$10) USB BT-адаптером. Для этой системы есть полноценный BT-стэк, написанный нашим соотечественником.

Я вполне допускаю, что ты будешь использовать Linux с Bluez или вовсе Windows. Это твое дело, и пока ты обдумываешь его, мы обсудим проблему обнаружения соседних BT-устройств.

ОБНАРУЖЕНИЕ

Даже если ты знаешь наверняка, что по соседству находится включенный BT-девайс, это еще не означает, что для тебя открыты все двери. Для начала атаки, как минимум, нужно знать BT-адрес ломаемого девайса. Довольно часто в этом нет ничего сложного: если девайс находится в discoverable-режиме, то он отвечает на специальные broadcast-пакеты, вы давая себя с потрохами и сообщая всем окружающим свой BT-адрес. Инициировать такое сканирование можно даже с мобильного телефона, правда, далеко не все аппараты позволяют пользователю ознакомиться с BT-адресами найденных устройств, большинство показывают только лишь символические имена девайсов. Нас это не устраивает, поэтому будем использовать более мощный инструмент - в моем случае им оказалась

софтина hccontrol, которая идет в поставке с BT-стэком для BSD.

Эта софтина занимается тем, что реализует все операции, связанные с интерфейсом HCI. Пользоваться этой программой чрезвычайно просто:

```
$ hccontrol -n имя_hci_узла команда
```

Тут слеует заметить, что имя узла - не то же самое, что имя интерфейса. Например, интерфейсу ubt0 соответствует имя ubt0hci. В качестве команды может быть указано несколько десятков допустимых HCI-операций. Я думаю, имеет смысл выделит лишь несколько из них.

Первая осуществляет поиск в окрестностях активных discoverable-устройств и называется Inquiry. Пользуются ей вот так:

```
$ hccontrol -n ubt0hci Inquiry
```

В качестве результата работы утилита выведет информацию о найденных устройствах - нас, прежде всего, интересуют их адреса.

Следующая команда, Remote_Name_Request, получает имя устройства по известному адресу и используется таким образом:

```
$ hccontrol -n ubt0hci Remote_Name_Request 00:0a:d9:7f:88:0d
```

После выполнения запроса на экране появится символическое имя устройства с указанным адресом. Полный список доступных команд можно получить набрав в консоли man hccontrol либо обратившись к документации на диске. А мы идем дальше.

BLUETOOTH ПИНГ-ПОНГ

В Bluetooth-стэке есть протокол L2CAP (Logical Link Control and Adaptation Protocol), позволяющий интерфейсам более высокого уровня передавать и получать пакеты данных длиной до 64 Кб.

L2CAP использует концепцию так называемых каналов, каждый канал представляет собой не что иное, как



Официальный сайт протокола: здесь можно найти тонны официальной документации

отдельное логическое соединение поверх радиопинка. Каждый канал привязан к некоторому протоколу (один протокол может занимать несколько каналов, но не наоборот), причем так, что каждый пакет L2CAP, получаемый каналом, перенаправляется к соответствующему протоколу более высокого уровня.

Есть две утилиты, предоставляющих доступ к этому протоколу. Первая имеет символическое название l2ping. Как несложно догадаться, эта тулза

предназначена для проверки связи между устройствами и с виду работает так же, как и icmp ping:

```
# l2ping -a 00:0a:d9:7f:88:0d
0 bytes from 00:0a:d9:7f:88:0d seq_no=0 time=37.823 ms
result=0
...
```

Но это только с виду! Обрати внимание на то, что многие устройства в ответ на L2CAP echo request возвраща-

ВНЕШНЯЯ АНТЕННА ДЛЯ BLUETOOTH-АДАПТЕРА

■ Организуя свирепые Bluetooth-атаки, ты рано или поздно столкнешься с ограничением, которое накладывает сама технология: абсолютное большинство устройств сейчас способны нормально работать на расстоянии до десяти метров. Если жертва ведет активный образ жизни, она создаст тебе определенные проблемы, поэтому крутые парни используют внешние антенны для Bluetooth-модулей. Разумеется, вполне можно купить культурное устройство с аккуратеньким выходом и подключить к нему готовую антенну.



Культурная внешняя ненаправленная антенна. Стоит дорого, работает плохо



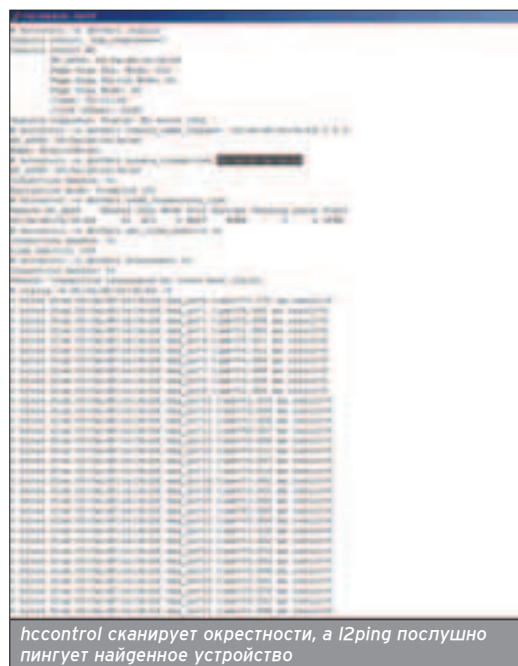
Эту антенну нужно отпаять

Настоящие киберпанки делают антенны самостоятельно, а не покупают их. Почитать об этом и кратко ознакомиться с теорией микроволновых антенн можно по адресу <http://oya.org.ua/wifi/wifi-helix-howto.html>.

Прежде всего, помни, что Bluetooth работает абсолютно на тех же частотах, что и стандарт 802.11a/b/g, поэтому все, что написано здесь об изготовлении антенн для Wi-Fi, применимо и к Bluetooth-модулям. Что же касается переделки самого адаптера, то необходимо лишь отпаять стандартную антенну, просверлить в корпусе дырочку 4 мм сверлом и установить в отверстии MMCX-разъем для подключения внешней антенны.



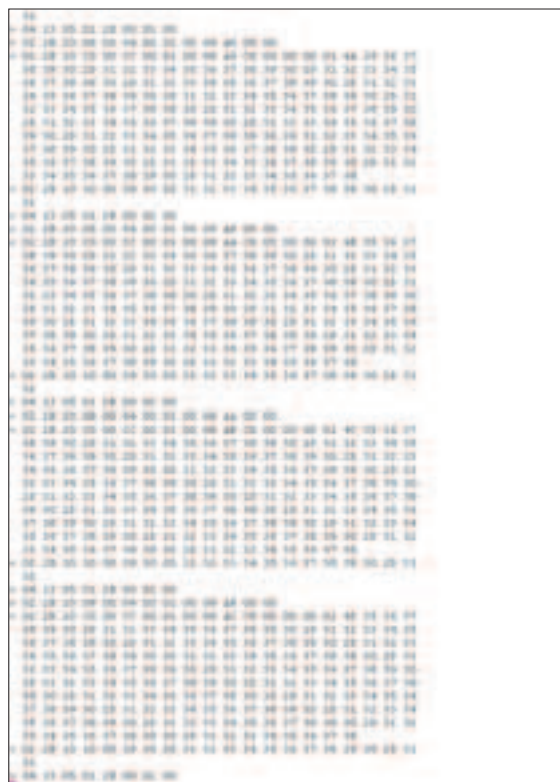
Киберпанковская направленная антенна



hcidump сканирует окрестности, а l2ping послушно пингует найденное устройство

ют пустые пакеты, поэтому 0 bytes - это в порядке вещей.

Помимо тестирования связи, у этой утилиты есть еще одно интересное применение - DoS-атаки на синезубые устройства. Подобно icmp-флуду, существует гипотетическая возможность завалить с головой любую Bluetooth-девайс L2CAP-пакетами, а тем самым прервать активные пользовательские соединения. Как я уже отмечал, максимальный размер пакета составляет 65 Кб, и, в общем-то, понятно, что для достижения цели необходимо использовать несколько устройств в режиме максимальной производительности. Также есть возможность вести "обстрел" в несколь-



Выход hcidump во время работы l2ping

ко потоков с каждого из доступных устройств. Плюс нужно экспериментально определить оптимальную глину пакетов и количество тредов - судя по моим опытам, оптимально работать в три-четыре потока, именно так достигается максимум используемой мощности канала.

ОБНАРУЖЕНИЕ НЕВИДИМОК

■ Все, о чем я говорил выше, применимо лишь к ломаемому устройству в "видимом" режиме. Если ты точно знаешь, что рядом с тобой находится активный девайс, но broadcast-сканирование не выявляет устройство, то знай: хозяин девайса перевел его в режим non-discoverable. Производители мобильных устройств, кажется, до сих пор считают, что невидимый режим - панацея от всех бед, взломщик просто не сможет выяснить BT-адрес устройства, и даже если стэк девайса дыряв как решето, злоумышленник не сможет воспользоваться этим. На многих телефонах невидимый режим стоит чуть ли не по умолчанию (или включается через несколько минут после активации BT), и производители советуют активно пользоваться этим. В самом деле, такой ход мысли кажется вполне разумным: пользователь всегда работает с ограниченным числом устройств (гарнитура, телефон девушки, ноутбук, PDA, телефоны трех друзей), и через неделю после начала использования этот список перестает расширяться. Соответственно, если телефону не нужно париться с новыми девайсами, он висит в невидимом режиме и все хакеры идут лесом. В этой ситуации добро действительно победило бы зло, если бы не несколько обстоятельств.

Находясь в невидимом режиме, устройство игнорирует широковещательные запросы, однако отвечает на пакеты, адресованные именно ему. Теоретически возможно просто угадать адрес соседнего устройства. А если угадать с первой попытки не получится, можно попробовать еще раз, а потом еще пару миллионов раз. Проблема лишь в том, что процесс угадывания затянется наолго: количество всех возможных адресов составляет 16^{12} , и, как легко понять, время полного сканирования будет просто неземным.

Второе обстоятельство заключается в административных вещах. Диапазоны для сетевых адресов выдаются производителям в специальной организации, которая осуществляет контроль над использованием адресных пространств. По стандарту, для идентификации производителя отводится целых три байта адреса. Кроме того, за крупными телекоммуникационными компаниями вроде Sony Ericsson, Nokia и Siemens зарезервировано несколько пространств емкостью по 16,7 миллионов адресов.

BT-СТЭК ВО FreeBSD

■ Bluetooth-стэк во FreeBSD реализован в виде модуля `ng_ubt` наш соотечественник Максим Евменкин. В пятой FreeBSD этот модуль присутствует по умолчанию, для более старых версий его необходимо собрать отдельно - сорцы можно взять на нашем диске или на сайте www.geocities.com/m_evmenkin. Чтобы поднять девайс, нужно подгрузить модуль следующей командой: `kldload ng_ubt`. Затем подключить адаптер к USB-порту и выполнить сценарий, активизирующий интерфейс: `/etc/rc.bluetooth start ubt0`. В консоли появится информация об устройстве, его адрес и т.д. Теперь уже можно начинать работу.



Установка BT-стэка под FreeBSD

Атаки на BT всегда проходят в тесной связи с социальной инженерией и в прямом взаимодействии с хозяином ломаемого девайса. Минимальное расстояние между жертвой и тобой - десять метров. По этой причине посмотреть производителя и даже конкретную модель устройства не составляет большого труда, более того, иногда приносит пользу: теперь мы можем значительно сократить количество вариантов для перебора. Если есть информация о производителе, то имеет смысл перебирать только адреса из соответствующих диапазонов - порядок 16^6 , что уже не так страшно. Однако даже сканирование половины этого диапазона на практике может занять значительное время - процесс должен быть ускорен.

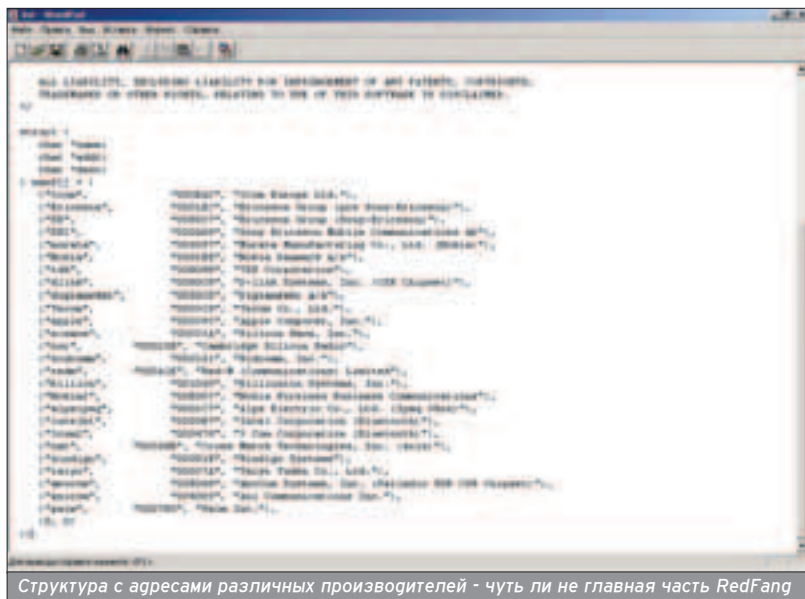
К сожалению, напрашивающаяся мысль, что для одинаковых моделей используются еще более узкие адресные пространства, не подтверждается. Nokia, насколько можно судить, раздает адреса девайсам абсолютно случайным образом. Однако иногда некоторые закономерности все же выявляются, и их используют для еще большего сужения перебираемого адресного пространства.

Как на практике возможно реализовать такой перебор адресов?

ПЕРЕБОР НА ПРАКТИКЕ

■ Давным-давно у меня была идея написать простенький скрипт, скажем, на Perl, который использовал бы стандартные утилиты вроде `l2ping` или `hccontrol`, сканировал адресные диапазоны, отыскивая устройства-невидимки. Самый быстрый вариант, который у меня получился, использовал именно `l2ping`. Причем я заметил, что скорость заметно увеличивается, если работать в несколько потоков.

Минимальный отклик от работающего устройства составляет примерно 0,02 с. В целом отклики мало отличаются друг от друга. Я даже пытался установить какую-то зависимость между числом потоков и временем проверки одного адреса. Разумеется, эта зависимость вряд ли носит линейный характер, но ее можно более-менее вменяемо приблизить квадратичной функцией. Экспериментально я остановился на чем-то вроде $0.05 + (n-1) * (0.005 * n)$ (конкретные коэффициенты примерные, могут сильно отличаться для разных систем), при этом производительность определяется следующим образом: $n / (0.05 + (n-1) * (0.005 * n))$. Если вычислить максимум этой функции, то окажется, что оптимально использовать три-четыре потока одновременно. При этом, увы, до приемлемой скорости работы еще далековато :(Для решения этой задачи



Структура с адресами различных производителей - чуть ли не главная часть RedFang

Стоит взять большой USB-хаб, наткнуть в него адаптеров и запустить параллельный перебор в redfang, как успех станет ближе к тебе в несколько десятков раз.

@stake разработала специальную утилиту с красочным названием RedFang. По неизвестной мне причине она больше не доступна на официальном сайте компании - на нашем диске ты можешь найти эксклюзивную копию :). К сожалению, собрать эту софтинку под FreeBSD мне не удалось, поскольку она создана для Linux'ового BT-стэка BlueZ. Пользоваться софтиной чрезвычайно просто:

```
./redfang -n 4 -r start-finish -t timeout
```

Здесь start - начальный адрес, finish - конечный, timeout - тайм-аут запросов, по истечении которого хост начинает считаться несуществующим. Авторы RedFang утверждают, что полный перебор диапазона для одного производителя занимает полтора часа. Врут, конечно :). Несложная арифметика: у нас имеется 16,7 млн адресов. Даже если проверка каждого из них будет занимать 0,01 с, общее время сканирования составит 167 000 с, то есть 46 часов. Такой перебор заинтересует лишь ученых, а на практике это время обнаружения никого не порадует. Разумеется, вести перебор адресов можно и с нескольких интерфейсов. Стоит взять большой USB-хаб, наткнуть в него адаптеров и запустить параллельный перебор в redfang, как успех станет ближе к тебе в несколько десятков раз. Прогрессивные BT-хантеры делают именно так!

КОЗЛЫ НЕ МЫ

■ Расскажу еще об одном приеме, в котором социальная инженерия занимает больше места, чем хак. Как легко

понять, когда два устройства хотят спариться, хотя бы одно из них должно быть видимым. Один телефон сканирует диапазон, находит интересное его устройство и начинает pairing-процесс. Поскольку человек X, работающий с клавиатурой, уверен на 100%, что под девайсом vasya висит его друг Васек и он очень хочет поскорее повыпендриваться перед приятелем, X не особо обратит внимание на тот факт, что устройств с именем vasya имеется в количестве двух штук (три, четыре, пять), и примет это за странный глюк. Разумеется, все остальные девайсы - совершенно отдельные устройства, принадлежащие третьему лицу и не имеющие никакого отношения к другу Васе. Если наш клиент выберет именно хакерский девайс для соединения (думаю, он не задумываясь кликнет по первому попавшемуся), то мигом запалит себя, выдав с потрохами свой BT-адрес и некоторую информацию, которая, при твоем определенном везении, поможет восстановить PIN будущей сессии. Далее взломщик быстро погасит свой троянский девайс, связь так и не установится, клиент крикнет Васе "Что-то глючит, сейчас еще раз попробую!" и уже без проблем установит соединение.

Вот такие методы обнаружения "невидимых" телефонов существуют в мире.

Возможно, тебе покажется, что часть этих вещей довольно надуманная. В самом деле, сканировать адреса четыре часа, если учесть, что все это время ты не должен отлучаться дальше десяти метров от атакуемого узла... Это малореально!

Но опыт показывает, что описанные приемы вполне жизненны и при наличии у тебя желания реализуются. Мы здесь говорим о глобальных недостатках, возможностях обойти механизмы защиты BT. А разве я говорил, что без всякой подготовки можно провести подобную атаку?

ГОЛУБАЯ ПЕЧАТЬ

■ Ты обнаружил в эфире активное устройство и узнал его BT-адрес. Неважно, находится этот девайс в discoverable-режиме или он невидим. Будем учиться удаленно определять некоторые свойства атакуемых узлов, такие как наименование производителя, модель, версия прошивки и т.д. В этом нам поможет технология blueprinting'a и соответствующий софт, который я с большим трудом отыскал на просторах Сети.

Прежде всего, нужно разобраться с тем, что такое blueprinting и как он работает. Довольно часто бывает нужно получить некоторую информацию об атакуемом устройстве. Прежде всего, выясняем, какой девайс обнаружен: искать бесплатный GPRS-интернет на беспроводной гарнитуре бесполезно, позвонить с видеокамеры тоже не получится. Негурно также получить информацию о производителе девайса и версии его прошивки, чтобы осмысленно использовать возможные баги в конкретных реализациях устройств. Оказывается, что все эти вещи возможно узнать просто располагая адресом BT-девайса как раз при помощи fingerprinting'a.

В случае с BT работа этой технологии не отличается ничем особенным. Используя специальную базу данных с "отпечатками" различных устройств, программа может легко отличать и на-



Выход утилиты spdtool



Файл с информацией о сигнатуре телефона Sony Ericsson k700

ходить уже знакомые ей девайсы. Тут дело в том, что разные версии устройств обладают различными параметрами, которые позволяют легко отличать даже версии прошивок. Исходя из этих параметров, вычисляются некую функцию, "отпечаток" устройства, который меняется от версии к версии, но одинаков для устройств с одной прошивкой.

Как это выглядит на практике? Для получения "отпечатков" BT-устройств, как правило, используются данные, получаемые из SDP-профилей устройств. SDP - Service Description Protocol, протокол описания сервисов, который предоставляет клиентам информацию о локальных сервисах устройства. Фактически, это просто стандарт описания предоставляемых ресурсов. Среди множества полей этих профилей особенный интерес для нас представляют Service RecHandle и Channel - именно из этих полей и формируется, как правило, "отпечаток" устройства: для различных устройств и даже версий прошивок наборы этих параметров различаются.

Для конкретной реализации этого процесса сорта написано мало. Я нашел простенький perl'овый скрипт с характерным названием br.pl, который прекрасно справляется со своей работой. Ищи его на нашем диске, а я пока расскажу, как его использовать. После распаковки архива с программой открывается множество файлов, самые главные из них - blueprint.db, br.pl и makedb.pl. Как несложно догадаться, первый файл - не что иное, как база данных с отпечатками устройств, br.pl - сам fingerprint, а makedb.pl - сценарий для пополнения базы с отпечатками девайсов.

Работать с софтиной чрезвычайно просто:

```
sdptool browse --tree XX:XX:XX:XX:XX | ./br.pl
XX:XX:XX:XX:XX
```

Как легко понять, первой командой получается содержимое SDP-профилей доступных сервисов, затем эти данные перенаправляются пайпом на вход сценарию br.pl, который вычисляет для них слепки и ищет в базе данных. Если такой отпечаток присутствует, для пользователя выводится описание устройства или предлагается добавить новую сигнатуру в базу данных для дальнейшего использования. К слову, это делается чрезвычайно просто. Чтобы добавить новое устройство в базу данных, создаем в папке devices новый текстовый файл, на его первой строке указываем диапазон производителя устройства, между "тэгами" ---info и /---info вводим описание устройства, а внутри ---sdp - вывод утилиты sdptool.

Пример файла с описанием BT-девайса

```
00:09:2D:XX:XX:XX
```

```
---info
Device: imate PDA2K
Version:
Bluetooth version: Broadcom BT-PPC/PE Version 1.0.0
Build 3500
Windows Mobile 2003 Second Edition
Version 4.21.1088 Build 14132
```

```
/---info
```

```
---sdp
Browsing 00:09:2D:XX:XX:XX
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10000
Attribute Identifier : 0x1 - ServiceClassDList
Data Sequence
...
Data Sequence
Data Sequence
UUID16 : 0x1101 - SerialPort
Version (Integer) : 0x100
Attribute Identifier : 0x100
Data : 42 6c 75 65 74 6f 6f 74 68 20 53 65 72 69 61 6c 20
50 6f 72 74 00
Attribute Identifier : 0x0 - ServiceRecordHandle
Integer : 0x10002
```

Файл создан, теперь необходимо воспользоваться сценарием makedb.pl, чтобы сгладить новую базу данных, с которой программа будет работать в дальнейшем.

Вот так легко обнаруживается и узнается куча разной информации о BT-девайсе, полезной для взлома, если в твоём распоряжении есть ноутбук, адаптер и несколько не самых редких утилит. Экспериментируй, и все получится.

Для получения "отпечатков" BT-устройств, как правило, используются данные, получаемые из SDP-профилей устройств.



"База данных" с сигнатурами - обычный текстовый файл

СПЕЦ ХАКЕР SMS СЕРВИС

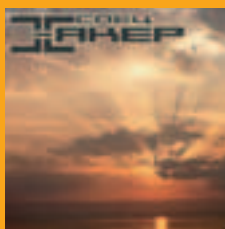
Хочешь фирменный лого на свой сотовый?

Пришли код логотипа (к примеру "1001") на номер **4446**.

Что нового ты хочешь увидеть в SMS-сервисе? Присылай идеи и критику на sms@real.xaker.ru



1049



1055



1076



1064



1045



1079



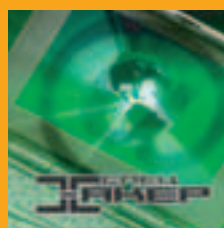
1007



1001



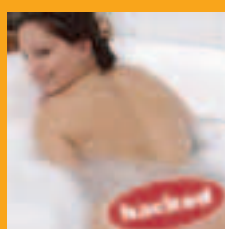
1010



1009



1020



1032



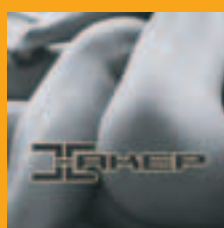
1075



1058



1077



1078

Пришли свой логотип! sms@real.xaker.ru

На диске к журналу есть новый СЮРПРИЗ, но он под паролем! Чтобы узнать пароль, пришли код **w0170** на номер **4445**.

Хочешь узнать, что значит термин?

Пришли код термина (к примеру "w0001") на номер **4444**.

идентификатор	(код w0008)	транслятор	(код w0092)
скрипт	(код w0009)	верификатор	(код w0093)
интерфейс	(код w0010)	спам	(код w0094)
терминал	(код w0011)	офшор	(код w0095)
библиотека	(код w0012)	крякер	(код w0096)
транзакция	(код w0013)	бета	(код w0097)
архитектура	(код w0014)	скин	(код w0098)
трассировка	(код w0015)	сертификация	(код w0099)
дистрибутив	(код w0016)	аутсорсинг	(код w0100)
утилита	(код w0017)	баннер	(код w0101)
брандмауэр	(код w0018)	локализация	(код w0102)
хост	(код w0019)	тестер	(код w0103)
подсеть	(код w0020)	гамп	(код w0104)
демон	(код w0021)	стек	(код w0105)
эксплоит	(код w0022)	исключение	(код w0106)
хостинг	(код w0023)	мидлет	(код w0107)
сервис-пак	(код w0023)	обфускатор	(код w0108)
файрвол	(код w0025)	документация	(код w0109)
брутфорсер	(код w0026)	поток	(код w0110)
тэг	(код w0027)	хэширование	(код w0111)
парсер	(код w0028)	браузер	(код w0113)
инициализация	(код w0029)	инсталлятор	(код w0114)
кодировка	(код w0030)	реестр	(код w0115)
визуализация	(код w0038)	аккаунт	(код w0116)
снифер	(код w0040)	домен	(код w0117)
кейлоггер	(код w0041)	девелопер	(код w0118)
троян	(код w0042)	флуг	(код w0119)
отладчик	(код w0043)	пиктограмма	(код w0120)
эмулятор	(код w0044)	архиватор	(код w0121)
хук	(код w0045)	экспозиция	(код w0128)
пиринг	(код w0047)	стробоскоп	(код w0129)
хаб	(код w0048)	бинарник	(код w0130)
фртп	(код w0049)	баг	(код w0131)
маппинг	(код w0050)	шлюз	(код w0132)
роутер	(код w0051)	шелл	(код w0133)
прокси	(код w0052)	блог	(код w0134)
редирект	(код w0053)	бэкап	(код w0135)
слот	(код w0054)	декодирование	(код w0136)
ник	(код w0055)	локалка	(код w0137)
биос	(код w0056)	бэкдор	(код w0138)
оболочка	(код w0057)	хомпага	(код w0139)
ядро	(код w0058)	сессия	(код w0140)
юстировка	(код w0059)	авторизация	(код w0141)
конвертер	(код w0060)	топик	(код w0142)
коаксиал	(код w0061)	профиль	(код w0143)
транспондер	(код w0062)	сегмент	(код w0144)
поляризация	(код w0063)	листинг	(код w0145)
патч	(код w0064)	алиас	(код w0146)
азимут	(код w0065)	свич	(код w0147)
кодек	(код w0066)	спуфинг	(код w0148)
граббинг	(код w0067)	фрикинг	(код w0149)
мультифид	(код w0068)	крэкинг	(код w0150)
бог	(код w0069)	сиквел	(код w0151)
пиксел	(код w0070)	ретранслятор	(код w0152)
модератор	(код w0071)	коммутатор	(код w0153)
фрейм	(код w0072)	аттач	(код w0154)
кряк	(код w0073)	плагин	(код w0155)
варез	(код w0074)	регистр	(код w0156)
сплиттер	(код w0075)	протокол	(код w0076)

Пришли свои термины на номер **4445** в виде **98 termini** (например "98 баг"). Не более 160 символов латиницей или 70 кириллицей.

Можно присылать свои термины

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступа в Интернет (оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно зайдя на wap-сайт <http://4446.ru>. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4444 – \$0,30 без учета налогов, на номер 4445 – \$0,60 без учета налогов, на номер 4446 – \$0,90 без учета налогов, на номер 4449 – \$3,00 без учета налогов. В случае ошибочного запроса услуга считается оказанной.

Content:

38 Мобильный ужас

Вирусы нашли новую среду для обитания - мобильные девайсы

44 Червивый КПК

Первые вирусы, трояны для мобильных устройств

48 SIM-SIM, откройся

Все, что ты хотел знать о SIM-карте, но боялся спросить

52 Секретов не будет

Все о прослушивании мобильных телефонов

56 Власть SMS

SMS может больше, чем тебе кажется

Дворецкий Дмитрий aka Burger_cdr (burgercdr@zelan.ru)

МОБИЛЬНЫЙ УЖАС

ВИРУСЫ НАШЛИ НОВУЮ СРЕДУ ДЛЯ ОБИТАНИЯ - МОБИЛЬНЫЕ ДЕВАЙСЫ

Вирусы семейства мобильных сегодня появляются с такой же завидной регулярностью, с какой ты пьешь свой горячий утренний кофе. Разговоры о каком-нибудь новом мобильном звере можно услышать буквально на каждом шагу. Взять, к примеру, лоток с телефонами б/у: один ничего не знающий эксперт рассказывает другому, как его милая ручная машинка со встроенным Bluetooth сначала без видимых причин перегружалась, а потом и вовсе отдавала концы. Бедолага сваливал все произошедшие несчастья, конечно, на предмет нашего будущего разговора.



HISTORIA EST MAGISTA VITA (ИСТОРИЯ - НАУКА О ЖИЗНИ)

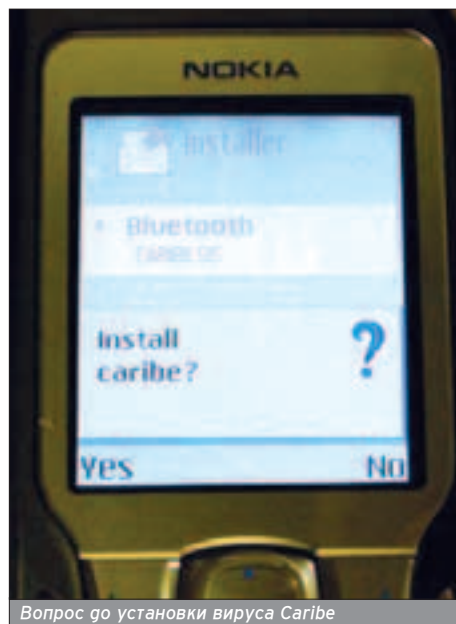
■ Перенесемся в 2004 год, июнь месяц, 14-е число. В этот день началась история вирусов для мобильных телефонов. На свет появился очередной ультрасовременный проект команды 29A, известной во всем мире своими смелыми экспериментами (а ныне наполовину посаженной в места не столь отдаленные). Возможно, кому-нибудь покажется, что проекту дали незамысловатое имя - Caribe, однако оно оставалось в умах вирусописателей долгие месяцы после знаменательной даты. Этот несмышленный малыш для телефонов под управлением Symbian OS (если быть точным, для телефонов Series 60 от Nokia) умел немного: инсталлировался, ОС при этом задавала кучу вопросов, а потом вовсю начинал рассылать себя любимого, используя интерфейс Bluetooth. Целью атаки могло стать любое устройство вплоть до кофеварки или принтера, если там был этот стандарт связи. Caribe не фальшивал устройству, посылая себя на все подряд, хотя работал только на телефонах от Nokia.

Этот малый проявил себя серьезнее несколько позже, показав небывалую живучесть по всему земному шару. Это чудо попало к нам где-то в середине января и вызвало неимоверный бум и появление сказок о страшных мобильных вирусах, поражающих все и вся. Все шло бы хорошо и замечательно и дальше: единичный всплеск не опасен сам по себе, а людей, которым интересны вирусы вообще, особо не заботили их мобильные собратья. Эта область, согласись, интересна только разве что энтузиастам. Но: однажды 29A опубликовала исходники известного вируса в своем журнале в декабре 2004 года в качестве новогоднего подарка для всех желающих. Только за последовавший за этим месяц появилось около 19-ти разновидностей вируса Caribe. Чуть ли не единственное, что могли сделать следующие "создатели" мобильных вирусов, - это поменять имя распространяемого файла, не забыв про сообщение, выводимое при заражении. Некоторые наглые особи угадали прародителя, если таковой имелся. И именно в одной из модификаций Caribe (то был червяк, окрещенный Symantec как SymbOS.Cabir.F) впервые мелькнуло назва-

ние Skulls, сыгравшее определенную роль в развитии мобильных вирусов. Skulls, по сути, был первым троянским конем для мобильных. Правда, он умел только портить установленные приложения, немного подставляя своего безобидного собрата Caribe. Наверное, так он выражал благодарность ;).

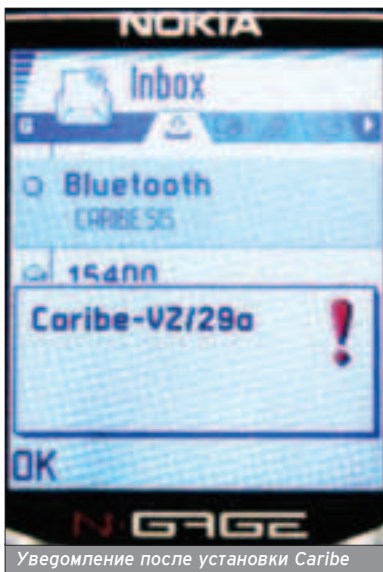
Первый серьезный вирус, с которого действительно следовало бы начать эру настоящих вирусов под мобильные платформы, появился в марте месяце 2005 года и был зарегистрирован в антивирусных компаниях под именем Commwarrior. Это чудо вирусописательской мысли могло распространяться не только через пресловутый Bluetooth! Commwarrior использовал принципиально новый способ распространения - через MMS. И, что приятно вдвойне, вирус был написан нашим соотечественником e10d0r'om и имел лозунг "ОТМОРОЗКАМ НЕТ!". В апреле месяце появился похожий экземпляр, но уже от иностранных коллег - Mibir. Как выразился сам e10d0r, это была "как попытка остаться на волне - неудавшаяся".

Ситуация с КПК или мобильниками под управлением WinCE на сегодняшний день более спокойная: обнаружено всего два вируса. Один из них - вирус в классическом понимании этого слова (заражает exe-файлы, подписывая себя в него), имя ему - Duts (обнару-



Вопрос до установки вируса Caribe

ВЗЛОМ УСТРОЙСТВ



Уведомление после установки Caribe

жен 17 июля). Второй - самый настоящий троян (Vradog, обнаружен 5 августа), открывающий порт 2989 и предоставляющий право сливать и заливать файлы, отображать сообщения и исполнять некоторые команды. По разговорам, оба творения принадлежат группе 29А, причем исходники Duts еще можно найти в Сети. Однако вирус написан на ассемблере, так что продвинутое знание в этой области, а также в области устройства ОС Windows Mobile будут просто необхо-

дими тебе, чтобы хоть что-нибудь понять.

COMMUNIS DOMUS (ОБЩИЙ ДОМ)

■ "Вирус - это программный код, способный самостоятельно размножаться и функционировать, имеющий механизмы защиты от обнаружения и уничтожения" (с) Jarod ("Что такое вирус", The Creatures Computer Virus Magazine #1, март 1999).

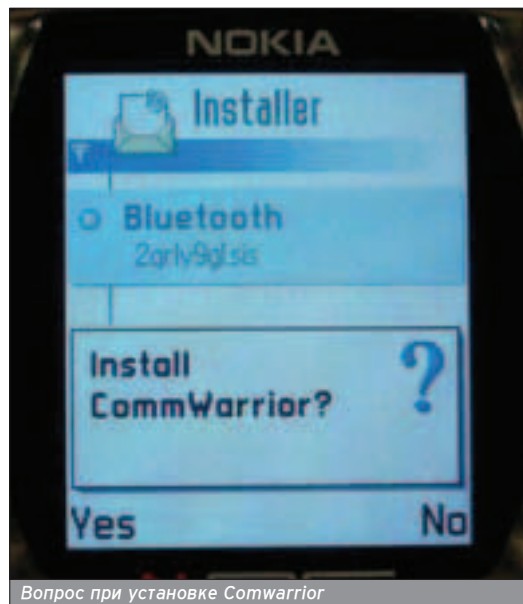
Из этого следует, что при написании любого вируса, в том числе мобильного, в дебрях сознания вирусописателя обязательно возникнут несколько вопросов: "Как вирус собирается распространяться? Что будущая зараза собирается делать с устройством? Как она собирается скрываться от рук преследователей? И для какой цели, собственно, пишется новое творение человеческих рук?"

КАК РАСПРОСТРАНЯТЬСЯ?

■ Способов распространения у выявленных и уже появившихся вирусов под мобильные телефоны не так много, а именно:

Bluetooth

■ Беспроводные технологии сегодня в моде, их можно встретить на каждом шагу: когда тебе дают такой ши-



Вопрос при установке Comwarrior

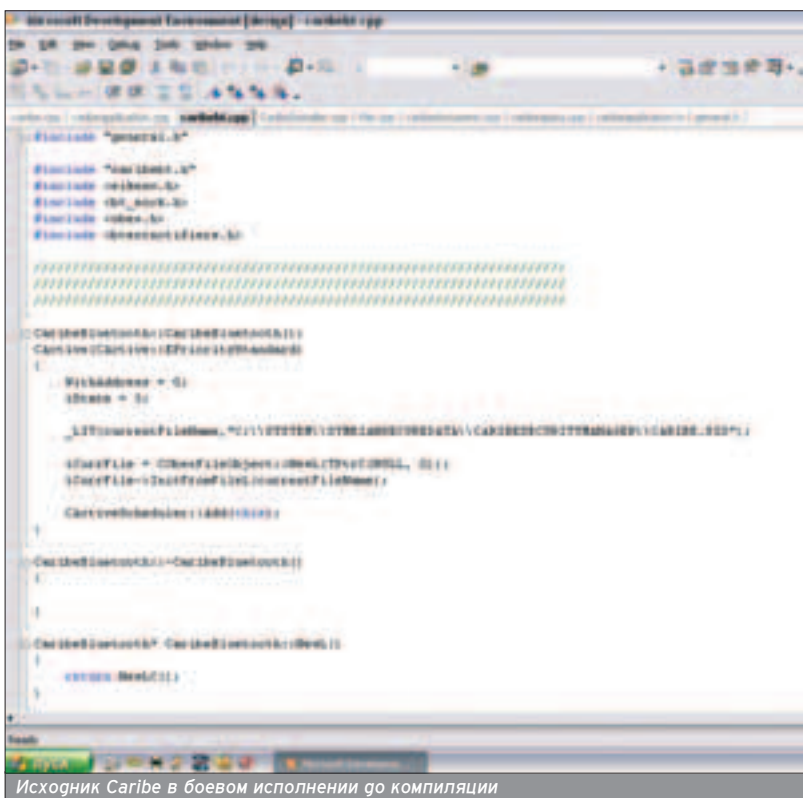
карный способ распространять вирус, сложно отказаться от него. Bluetooth - это, по сути, радио с ограниченным до десяти метров радиусом действия или несколько больше (в зависимости от оборудования). Итак, любое устройство, находящееся в режиме обнаружения, подвергается атаке: посылаются сообщения в виде установочного SIS-файла (для телефонов Nokia стандарт первоначально служил распространению игр, но по возможности он намного богаче), при получении файла пользователь вправе выбрать, принимать сообщение или нет. После принятия сообщения пользователь снова получит право выбирать, устанавливать ли приложение, и только после того, как и тут будет получено согласие, вирус наконец-то получит доступ к устройству. Как видишь, путь к сердцу машины в таком случае тернист и небезопасен для вируса на любом этапе, что, конечно, сказывается на его живучести. Но для него не все так плохо, как кажется на первый взгляд. Дело в том, что телефоны, поддерживающие Bluetooth, не орожены от ошибок в ОС так же, как и любая программа, поэтому рождаются такие досадные неприятности, как:

❶. SNARF-атака - с ее помощью возможен коннект на некоторые модели телефонов без какого-либо уведомления, последующая скачка всей телефонной книги, календаря и любых других данных.

❷. BACKDOOR-атака - позволяет не только скачивать всю информацию, но и использовать сервисы телефона, то есть интернет, WAP и GPRS, при этом сам пользователь телефона не будет знать о происходящем ничего.

❸. BLUEBUG-атака - на некоторых моделях телефонов позволяет получить доступ к AT-командам телефона, то есть отсылать сообщения и звонить на номера без ведома пользователя телефона (подробнее об этих атаках читай в других статьях номера).

"Вирус - это программный код, способный самостоятельно размножаться и функционировать, имеющий механизмы защиты от обнаружения и уничтожения" (с) Jarod



Исходник Caribe в боевом исполнении до компиляции



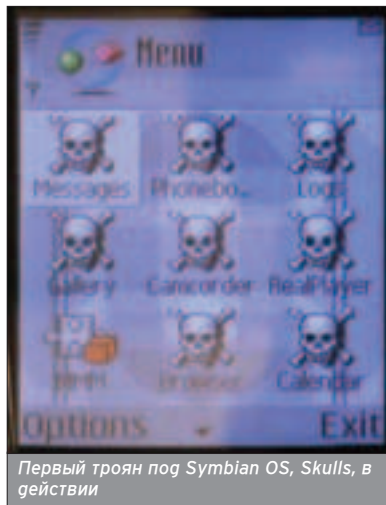
MMS от Comwarrior (скриншот эмулятора)

Любое из этих недоразумений и, потенциально, новые проблемы (например с самим стандартом Bluetooth) могут быть использованы вирусомисателями. Подчеркиваю, они МОГУТ быть использованы, так как на сегодняшний день не было выявлено использование вышеизложенных уязвимостей в телефонах. Причина здесь одна - резко ограниченное количество телефонов, имеющих подобные уязвимости.

Примерами вирусов, использующих Bluetooth для распространения, может стать классика вроде Caribe или CommWarrior, Mabir и MGDropper.

MMS

■ Усовершенствованная версия SMS сегодня достаточно плотно вошла в нашу повседневную жизнь. Вряд ли хоть кто-нибудь еще не пользовался услугами этого чудо-сообщения, не посылая всяческие открытки,



Первый троян под Symbian OS, Skulls, в действии

ИНТЕРВЬЮ С E10D0R'OM - СОЗДАТЕЛЕМ МОБИЛЬНОГО ВИРУСА COMMWARRIOR

Burger_cdr: Какие основные вопросы и задачи встают перед вирусомисателем при создании любого вируса под новую ОС?

e10d0r: Вирус - саморазмножающийся организм, прославляющий своего автора собственной жизнью. Поэтому техническая основа - функция репликации. Файловые вирусы умирают, наступила эра червей - именно на них стоит рассчитывать. Необходимо изучить, какие возможности дает ОС и на каком уровне, есть ли ограничения на их применение. Когда возможности выявлены и сделан выбор, следует задуматься: правильный ли он, возможно, что-то из списка тоже можно использовать, и это будет еще эффективнее. Неплохо изучить уязвимости выбранных технологий, в том числе на примере конкретной ОС, попробовать найти новые путем несложных тестов. Важный вопрос - размещение в памяти и собственная защита. И, конечно, основной вопрос - алгоритм. В частности, что должен делать вирус, пока он живет? Вирус не должен вредить - это удел ламеров. Обычно они вставляют деструктивную функцию в чужой код и компилят со своим копирайтом. Правильный вирус должен нести идеи своего создателя, претворять их в жизнь, по возможности не причиняя вреда.

Burger_cdr: Какие основные условия должны сложиться в новой ОС, чтобы под нее начали появляться вирусы?

e10d0r: Необходимо ограничить вид устройств - только мобильные устройства, у каждого класса своя специфика. Итак:

1. Достаточно открытый API.
2. Широкие возможности коммуникации, встроенные в ОС.
3. Популярность устройств с ОС, низкая стоимость устройств.
4. Высокая стоимость ПО, распространенность врезки.

Чтобы появлялось много интересных вирусов, еще пункт:

5. Сильная извращенность ОС и API - чтобы писать системный софт под нее мог только гурю. Известно, что если под ОС может писать любой дурак, то только дурак и будет писать.

Burger_cdr: Каким образом возможно избежать обнаружения мобильных вирусов и, как следствие, уничтожения вируса?

e10d0r: Технологии невидимости, основанные на перехвате функций API, не всегда реализуемы, а чаще всего просто не оправдывают себя. Очевидно, что для мобильных устройств лучший прием - модификация собственного кода, при котором маски и чек-суммы из вирусных баз не работают.

Полиморфные вирусы для Symbian OS еще не появились, но теоретически это возможно. Существует масса полиморфных генераторов для 80x86, необходимо оставить общую логику и переписать их под другой ассемблер, при этом учесть формат исполняемых файлов. Это непременно будет сделано каким-нибудь гурю. Эвристические анализаторы появятся еще не скоро, скорее всего, уже по факту. ARM-процессоры сегодня используются в значительной части мобильных устройств, их ассемблер достаточно необычен, но нельзя сказать, что он сложен. Он даже по-своему красив. Реализовать все это не так просто.

Есть еще один достаточно эффективный прием - прямое противодействие антивирусу. Есть ли смысл все время прятаться? Может, лучше сразу выйти и дать достойный отпор? Современные антивирусы умеют защищаться, но их защита не безупречна и всегда можно войти в противостояние с ними. Кто выйдет победителем - это вопрос. Я бы даже сказал, это вопрос чести и престижа.

Burger_cdr: Какие еще способы потенциально применимы для распространения вируса (кроме Bluetooth, MMS, в виде крэкнутой программы (и подобного)?

ИНТЕРВЬЮ С E10D0R'OM - СОЗДАТЕЛЕМ МОБИЛЬНОГО ВИРУСА COMMWARRIOR (ПРОДОЛЖЕНИЕ)

e10d0r: Глобальных открытий здесь, очевидно, уже не появится. Но всегда, как только будет возникать новая технология коммуникации, будет появляться и новый способ размножения для вирусов. Если говорить о том, что есть сейчас, то на телефоне вирусами не задействован только интернет. Учитывая создание новой мобильной зоны доменов, возможно, очень скоро начнется размножение вирусов для мобильных телефонов по e-mail. Также новые вирусы, очевидно, будут апдейтить себя по http – это достаточно актуально. Когда появляется багфикс или новая версия, нет необходимости повторно заражать устройство. В Symbian OS процесс включения GPRS имеет серьезные сложности из-за различия версий 6.1 и 7.0s (и последующих), но в целом все это решается.

Burger_cdr: Как мобильные вирусы можно использовать в коммерческих, рекламных или иных сферах (спам), ключом к которым являются деньги?

e10d0r: Хакер никогда не опускается до спамера, поскольку спамеры – это всегда каста изгоев. Под хакерами я подразумеваю увлеченных людей, посвятивших или готовых посвятить своему увлечению большую часть своей жизни, их больше привлекает исследование, а не его цель. Это не сетевые отморозки, которые, по сути, ламеры. Попытки заработать деньги на вирусах будут предприняты очень скоро. Возникновение спама в виде SMS, e-mail и MMS маловероятно, поскольку коммуникационные возможности мобильного устройства пока что сильно ограничены как пропускной способностью, так и кошельком его владельца. Однако попытки воплотить это в жизнь возможны. Вирус может каждый день скачивать обновление рассылок и спам-базу с сервера, в течение дня рассылать сообщения или, например, делать звонки и зачитывать поднявшему трубку какой-то wav-файл, также скачанный с сервера. Более реально опасность воровства и торговли конфиденциальной информацией. Будут попытки переслать с телефона номера кредитных карт и прочие данные вроде настроек клиентов платежных систем, которые уже всю портируются на мобильные устройства.

Burger_cdr: Возможно ли создание кросс-платформенных мобильных вирусов?

e10d0r: Возможно, скорее, теоретически. Возьмем, к примеру, технологию Bluetooth. Она позволяет переслать любой файл, например, через сервис OBEX Object Push. Конечно, потребуются подтверждение на прием и т.п., но тем не менее... Файл может быть дистрибутивом или исполняемым файлом. В большинстве случаев при поиске устройств можно определить производителя устройства и, с большой вероятностью, его тип. Определив это, можно "на лету" создать соответствующий файл уже под конкретную платформу и передать его.

Для Symbian OS UIQ и Series 60 это кросс-платформенность. Можно сделать уже сейчас внутри одного исполняемого файла, хотя и имеются сложности с MMS из-за разных реализаций. Сейчас актуальна кросс-платформенность Symbian OS и Windows Mobile. В случае нативных кросс-платформенных вирусов всегда важна связка "платформа плюс тип процессора". С этим есть существенные сложности: необходимо тащить за собой исполняемые файлы для обеих платформ, а это не всегда приемлемо из-за размера вируса.

Другой способ состоит в использовании кросс-платформенных языков, компилирующихся в байткод. Например java, python, .net и т.п. Такой код может выполняться на различных платформах и самостоятельно анализировать среду обитания, предпринимая те или иные действия. Сейчас эта возможность больше теоретическая. Вероятнее всего, первым кросс-платформенным вирусом для мобильных устройств станет все же вирус на нативном языке.



Вопрос при установке doomboot - одного из самых опасных вирусов

картинки и прочие разнообразные радости грузьям и подругам. Стандарт MMS – отличная штука, она позволяет присоединять всяческие файлы к сообщению, а умные вирусы получают дополнительный способ размножения. Так разве ты не откроешь присоединенный к сообщению файл, пришедший в сообщении от твоей подруги с темой что-то типа "Открой, милый. Это для тебя!?" Имея дело с интернет-вариантом, многие еще десять раз подумают, то тут затуманенные мозги пользователя разорвутся в клочья на месте, и он, радостный, начнет устанавливать все что угодно, открывая таким образом дорогу вирусу. Так делают на сегодняшний день два вируса Commwarrior и Mabr, выбирая телефон из списка жертвы и начиная слать копии себя любимого. Обе заразы обладают также продвинутым методом распространения через Bluetooth. Но, к счастью, оба вируса больше похожи на proof-of-concept, проделывают только всяческие фокусы, ну, сажают батарейку телефона из-за чрезмерного использования Bluetooth и т.п. То ли еще будет.

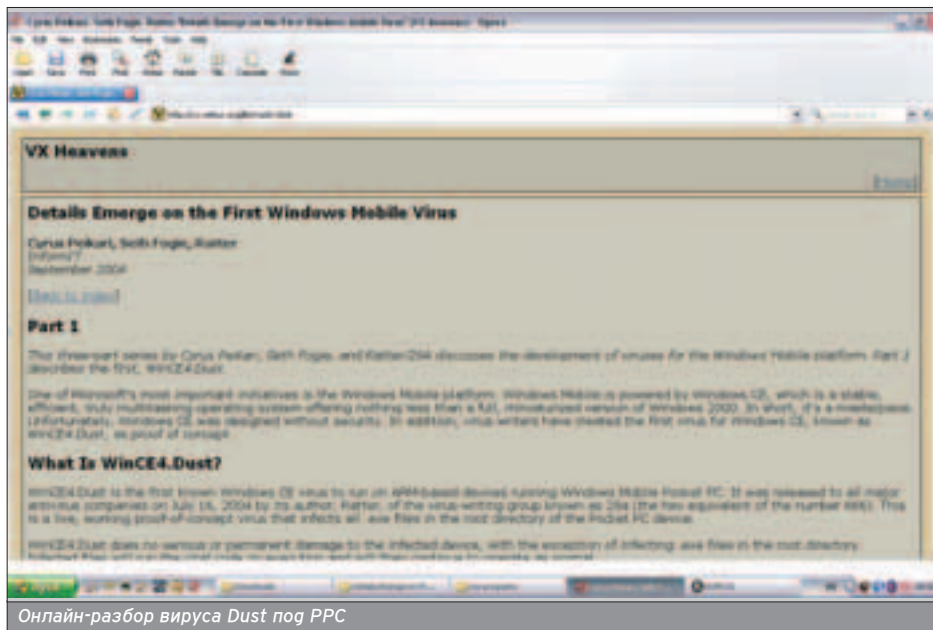
O-DAY soft

■ Подобным способом распространяли первые в мире вирусы. Используя лакомый кусочек типа последней версии игры или, например, популярной программы с крэком, вирус не забывает установить еще одну версию себя – в придачу к общему пакету. Так размножается Dampig (использует крэкнутую версию FSCaller) или Mos, который используется игрой Mosquitos, ну и, конечно, Doomboot, прикрывающийся якобы новой игрой Doom 2.

ЧТО ДЕЛАТЬ С УСТРОЙСТВОМ

■ Перспективы твоего телефона, зараженного очередным гагом, не такие уж и радостные, если ты обладаешь смартфоном от Nokia или другой фирмы – лишь бы с Symbian OS. Эта операция распространена довольно широко, развита с точки зрения





Онлайн-разбор вируса Dust под PPC

Реальная опасность возникнет только в том случае, если на сцену выйдут вовсе не одинокие энтузиасты, а действительно профессионалы, желающие получить прибыль от разработки вирусов для мобил.

функциональности и описана со всех сторон специально для будущих девелоперов. Конечно, в каком-то смысле этим разработчиком является и вирусолог.

Так что с телефоном можно сделать практически все: отключить Bluetooth, встроенный файломенеджер, телефонную книгу (вирус Dampig), попортить операционку, тем самым обеспечить поход владельца с телефоном в сервис-центр (Doomboot, который копирует несколько битых dll на C:\; Fontal,

который заменяет шрифты попорченными копиями; и Hobbes, проводящий вредительские операции с автозагрузкой), посылать SMS-сообщения на все четыре стороны, ударяя по кошельку владельца телефона (вирус Mos), или нечто издевательское вроде Onehor, который перезагружает сотовый, как только ты попытаешься воспользоваться системными приложениями. Так что проблем с воображением у создателей вирусов обычно не бывает, тем более что возможности техники позволяют воплотить любые фантазии в жизнь.

КАК ЗАЩИТИТЬСЯ ОТ АНТИВИРУСОВ

Механизмы защиты у современных вирусов не так уж разнообразны. Например, зараза под названием Drever предпочитает тупо затирать все антивирусные программы, какие найдет на просторах карты памяти мобильного телефона. Для вирусов пободных пакетов защит на сегодняшний день не так много и под PC, так что и такой способ годится. Вирус Doomboot предпочитает просто не показывать своего присутствия на телефоне, он потихому устанавливается вместе с игрой (похожий механизм у Dampig). CommWarrrior прикрывается в MMS фантастическими программами или обновлениями от www.symbian.com ("Dr.Web! New Dr.Web antivirus for Symbian OS. Try it!", "MS-DOS emulator

for SymbianOS. Nokia series 60 only. Try it!", "SymbianOS update").

Однако спешу тебя уверить: не все так страшно, как кажется на первый взгляд.

Все существующие вирусы под мобильные телефоны - это вирусы под Nokia с Symbian OS. Почему? Потому что в данном случае соблюдены все три золотых условия создания хорошего вируса:

1. Вирус изначально должен где-то распространяться и на чем-то паразитировать, нужна площадка - развитая ОС с множеством функций.

2. Эта ОС должна быть популярна, иначе по карманам или убеждениям пользователя много не поползаешь.

3. ОС должна быть хорошо документирована, практически до мельчайших подробностей, так как вирус сам по себе - достаточно сложная штука в реализации, и метод научного тыка тут вряд ли поможет.

К сожалению, все три пункта являются непрерывным спутником любого успешного проекта и, как только новая ОС набирает популярность, тут же появляются и вирусы под нее.

Во-вторых, реальная опасность возникнет только в том случае, когда на сцену выйдут вовсе не одинокие энтузиасты, а действительно профессионалы, желающие получить прибыль от этой затеи. Это произойдет в результате широкого распространения какой-либо одной операции, то есть в случае монополизации рынка (вспомни Microsoft и RPC-уязвимости), или в результате глобального развития кросс-платформенных языков типа Java, которые позволят полноценно управлять телефоном. Вот тогда в руках злоумышленников окажется поистине опасный инструмент.

"Какой прок, - скажешь ты, - от мобильников в плане денег?" А как же реклама? На сегодняшний день вполне можно создать вирус под мобильные телефоны, сложный для отлова, но полезный с точки зрения спама. И так легким движением захваченный телефон превращается в некое подобие, например, SMS-центра (га и с возможностью дополнения сообщений и номеров для рассылки, например через GPRS-технологии). Конечно, до тех пор, пока не кончатся деньги на счету у бедопаги-абонента.

CARITAS DEFENDERE (ЗНАЧЕНИЕ ЗАЩИТЫ)

Взглянем на проблему с другой стороны. Что же стоит сделать для предотвращения заражения?

1. Не открывать и не ставить программы, приходящие по Bluetooth или MMS с незнакомых номеров. Более того, в случае если программа пришла от знакомого, следует спросить его, не посылал ли он чего-нибудь. Последствия могут быть намного ужаснее, чем ты можешь представить.



Исходник Dust в боевом исполнении

❶. Не ставить программы, скачанные из ненадежных источников (p2p-сети, например), или хотя бы перед установкой проверять их антивирусом.

❷. Поставить антивирус и регулярно обновлять его базы (об этом чуть ниже).

❸. Шифровать особо важные данные: номера кредитных карт, пароли и т.д.

❹. По мере возможности следить за багтраком.

❺. Сделать своей новой обязанностью создание и обновление backup'a данных.

Я обещал поподробнее об антивирусах. Под современные телефоны на базе Symbian OS ныне их развелось очень много. Наиболее грамотный, на мой взгляд, сделала контора Касперского, хотя проект и находится на стадии бета-тестирования:

www.kaspersky.ru/beta?product=159317347.

Кроме того, удачный пакет для борьбы с вирусами предлагает SimWorks:

www.simworks.biz/sav/AntiVirus.php?id=home

Есть одно НО. В природе существуют вирусы, и их первое действие - это уничтожение обоих пакетов на твоём сотовом еще в процессе заражения. Так что для пушечки безопасности рекомендую также Mobile Disinfector от MpuLze, против которого еще не успели ополчиться существующие вирусы: www.mpulze.com/antivirus.php?part=3.

Ну а для шифрования данных под платформой Symbian тебе здорово поможет программа CodeGuard (www.hpc.ru/soft/software.phtml?id=10496) - она без проблем зашифрует все нужные тебе данные.

Для криптования SMS-сообщений советую воспользоваться программой Mum SMS6

<http://symbian.gtwar.com/#i517>.

Под другие платформы с поддержкой Java MIDP попробуй mWallet (<http://series60.ru/modules/mydownloads/showfile.php?id=964>) для хранения номеров кредитных карт, паролей и т.д.

Продвинутому пользователю могу предложить написать подобную программу самостоятельно. Для этого будут полезны исходники программы Cryptex, написанной на MIDP 2.0:

www.garret.ru/~knizhnik/cryptex-src.zip.

Для КПК на данный момент существует всего два вируса, но ты, как человек прогрессивный, обязан уже сегодня защитить все данные, в чем тебе поможет программа CryptoStorage: <http://forum.pocketz.ru/index.php?showtopic=5827&hl=%EA%F0%E8%EF%F2>.

Она создаст специальный шифрованный диск и не позволит злоумышленникам узнать всю правду о тебе.

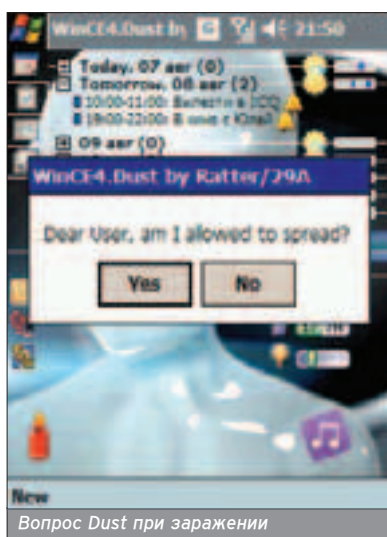
Также рекомендую использовать Resco Explorer 2003, который, по сути, является отличным файлменеджером, но к тому же умеет шифровать данные:

http://64.78.9.130/downloads/Explorer2003_p02.exe

TEXTUS FINITA (КОНЕЦ ЛИРИКИ)

■ Сегодня становится очевидным, что мир security вот-вот породит новую область деятельности - это безопасность мобильных устройств. Для них появляются вирусы, их становится все больше и больше. Это реальность, от которой никуда не деться. С дальнейшим развитием технологий и программных средств под мобильные устройства вирусы под них станут такими же достойными и развитыми, как их PC-варианты. Совсем скоро появятся первые полиморфные вирусы, новые методы маскировки и противодействия антивирусам, бесконечная

Впервые за всю историю VX-сцены возник смысл задуматься над перспективой появления первого кросс-платформенного вируса.



Вопрос Dust при заражении

гонка между лагерями вирусписателей и разработчиков антивирусов продолжится.

Кроме того, впервые за всю историю VX-сцены возник смысл задуматься над перспективой появления первого кросс-платформенного вируса. В случае с современными ОС под ПК эта задача казалась невыполнимой, мобильные устройства - совсем другое дело.

Нам с тобой, простым смертным, пора задуматься, как защитить себя от грядущей напасти, и быть на страже. Спектакль рождения и роста новой области обещает быть очень интересным и интригующим во всех смыслах.



ЧИТАЙ В СЕНТЯБРЕ:

Есть ли жизнь под DDoS-ом?
Методы защиты от масштабных нападений

Кликатель возвращается!
Продвинутый взлом сайта Clickatell.com

Есть контакт!
Теледильдоника - оргазм через интернет

Механика wм-процессинга
Организация приема интернет-платежей



НА НАШИХ ДИСКАХ ТЫ ВСЕГДА
НАЙДЕШЬ ТОННУ САМОГО СВЕЖЕГО
СОФТА, ДЕМКИ, МУЗЫКУ, А ТАКЖЕ
3 ВИДЕО ПО ВЗЛОМУ!

september
УЖЕ В ПРОДАЖЕ

www.xaker.ru

(game)

Hi-Tech (hi-tech@nsd.ru; http://nsd.ru)

«ЧЕРВИВЫЙ» КПК

ПЕРВЫЕ ВИРУСЫ, ТРОЯНЫ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Довольно долгое время трояны для карманных компьютеров и вирусы для сотовых телефонов оставались всего лишь мифом, но в последнее время для хакеров открылись новые горизонты, а именно - взлом портативных гевайсов.

Внашей жизни прочно укрепились портативные карманные устройства. Трудно найти человека, у которого не было бы, например, сотового телефона. Тем не менее, технический прогресс продвигается вперед семимильными шагами и на смену "обычным сотикам" пришли смартфоны, представляющие собой, по сути дела, "карманные компьютеры с функцией телефона". Параллельно телефонам, как бы в отдельном русле процесса необратимой глобальной компьютеризации развиваются карманные компьютеры (PDA), или, как их еще называют, "наладонники". Одним словом, жизнь продолжается, а основная задача хакера остается неизменной - заполучить информацию. Важную информацию, за которую заинтересованные люди готовы платить большие деньги - например телесфонная и записная книжка, компрометирующие SMS-сообщения и т.д. Мы поговорим

именно о взломе портативных гевайсов с помощью вредоносных программ.

НЕМНОГО О...

■ Для начала определимся с операционными системами, которых пока не очень много: Windows CE, Windows Mobile, Palm OS, ну и ось для смартфонов Symbian OS.

Впрочем, как ты уже заметил, Билл Гейтс не смог удержаться от того чтобы не приложить свою руку к новому устройству, что на этот раз у него неплохо получилось. Сложно сказать, связано ли это с тем, что КПК действительно трудно ломать, или с тем, что программисты мелкосерфта наконец-то взялись за ум.

И СОТВОРИЛ ОН АНТИВИРУС ДЛЯ КПК...

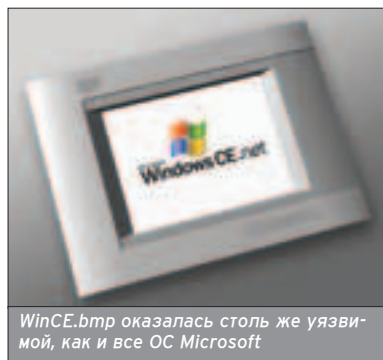
■ Как я уже говорил, очень долго считалось, что вирусы для карманных компьютеров - это миф. Но, тем не менее, даже в те времена Евгений Касперский (ну а кто же еще? - прим. автора) реализовал первый антивирус для карманных компьютеров, несмот-



КПК вошли в "зону риска" после появления мобильных вирусов



Мобильные телефоны могут хватать вирусы "на лету"



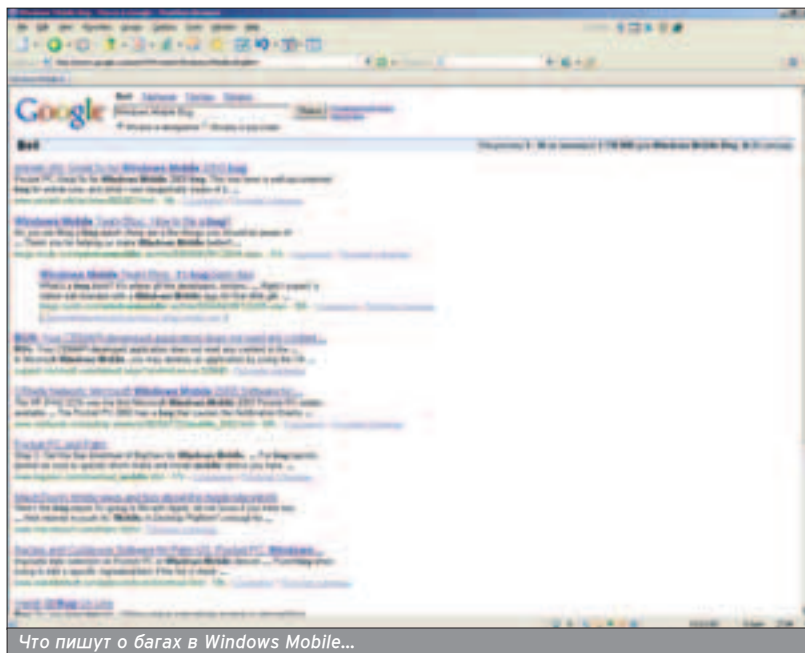
WinCE.bmp оказалась столь же уязвимой, как и все ОС Microsoft

ря на высказывания конкурентов о бесперспективности этого софта (высказывания можешь почитать на врезке).

Тебя наверняка озадачило то, что антивирус для карманных компьютеров был написан раньше, чем появился первый вирус для них. Вирусы для PDA существовали, но назвать их именно вирусами можно было только с натяжкой: они были больше похожи на безобидные программы-шутки. Помимо обыденной функции сканирования, в комплект Kaspersky Security for PDA 5.0 (именно так называлась первая версия) входили системы защиты

W W W

- <http://nsd.ru> - НеСанкционированный Доступ
- www.viruslist.com - энциклопедия вирусов
- <http://packetstormsecurity.nl> - багтрак
- www.kaspersky.ru - сайт лаборатории Евгения Касперского



Что пишут о багах в Windows Mobile...

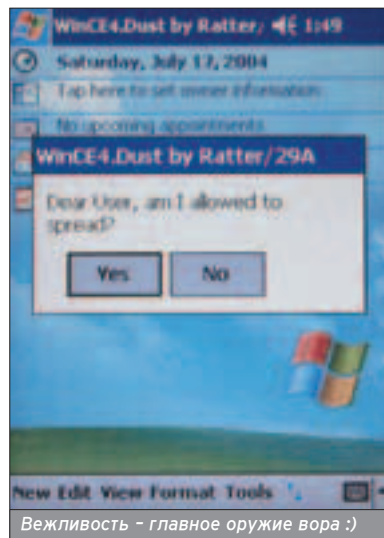
папок с помощью пароля и криптографическая функция. Еще одним немаловажным плюсом являлась поддержка сразу двух наиболее распространенных платформ: Palm и Pocket PC.

Следует отметить, что на данный момент антивирус для КПК получил широкое распространение среди пользователей, ведутся новые разработки, и вот уже недолго осталось

ждать до выхода Kaspersky Security for PDA 2006.

ПЕРВЫЙ ВИРУС ДЛЯ PDA

■ Первый реальный вирус для PDA был написан в июле 2004 года известной командой 29A, которая славились нововведениями в мир компьютерных вирусов. Имя этому вирусу – Dust. Он представлял собой приложение



Вежливость – главное оружие вора :)

ние, написанное под процессор ARM, был глиной 1520 байт, работал на PocketPC 2000, PocketPC 2002, PocketPC 2003. Вирус попадал на компьютеры через интернет или через компьютер при синхронизации под видом обычного приложения, например игрушки. Пользователь сам запускал его, на что вирус реагировал весьма неадекватно: спрашивал у пользователя разрешения на размножение :).

Если пользователь сам соглашался (а он почти всегда делал именно так, только непонятно почему), вирус искал в корне (my device) исполняемые файлы размером больше четырех килобайт и написанные под процессор ARM, затем дописывал себя в последнюю секцию каждого из найденных файлов, установив точку входа на свое начало. При этом в одно из неиспользуемых полей PE-заголовка вставлялась сигнатура "atar".

ПЕРВЫЙ ТРОЯН ДЛЯ КПК

■ В августе 2004 года появилась первая троянская программа под КПК, позволяющая злоумышленнику уга- »

Трояны для карманных компьютеров и вирусы для готовых телефонов долгое время оставались всего лишь миром, но в последнее время для хакеров открылись новые горизонты, а именно – взлом портативных девайсов.

Первый реальный вирус для PDA был написан в июле 2004 года известной командой 29A.

Первый реальный вирус для PDA был написан командой 29A.

ЕВГЕНИЙ КАСПЕРСКИЙ О BRADOR

■ Обнаружение первой троянской программы для карманных компьютеров подтверждает наши опасения, высказанные недавно в связи с появлением концептуальных вирусов для мобильных телефонов и для операционной системы Windows Mobile. WinCE.Brador.a – полноценная вредоносная программа, здесь уже не идет речи о демонстрации вирусписателями своих возможностей, мы можем наблюдать набор деструктивных функций, характерный для большинства backdoor'ов. Пользователи мобильных устройств находятся в реальной опасности, и можно только предполагать, что компьютерный андеграунд в ближайшее время еще больше активизируется в плане создания вредоносных программ для мобильных телефонов и карманных компьютеров. Ситуация с мобильными устройствами развивается так же, как когда-то было с настольными компьютерами. Вполне возможно, что нас ожидают крупные эпидемии КПК.



Евгений Касперский высоко оценивает опасность мобильных вирусов



Brador.a в списке процессов



Система защиты от вирусов для PDA

ленно контролировать мобильный девайс, когда он в онлайн.

В базах "Лаборатории Касперского" вирус обозначили как Backdoor.WinCE.Brador.a. При заражении в директории автозапуска WindowsCE (\Windows\StartUp\l) создается файл с именем svchost.exe размером 5632 байта. Когда PDA выходит в онлайн, вирусописателю по электронной почте отправляется письмо, содержащее IP-адрес. Затем для удаленного администрирования открывается порт 2989 или 44299.

Brador не умеет распространяться самостоятельно, поэтому он может попасть на налагодник только по вине самого пользователя и в виде любого "безобидного" приложения. Кстати, клиентская часть Brador.a коммерческая, и разработчиком мог быть наш соотечественник. Первые сведения об этом трояне пришли с российского адреса электронной почты, и письмо было составлено на русском языке. Евгений Касперский как в воду глядел, создавая свой антивирус для КПК. Его мнение о Трояне для КПК ты найдешь на врезке.

ПЕРВЫЙ ВИРУС ДЛЯ СМАРТФОНОВ

■ Вирус написан все той же командой вирусописателей 29A, которая выпустила "на волю" Dust - первый вирус для КПК, и вообще команда славится своими нововведениями в мир вирусов. В "Лаборатории Касперского" вирус назвали Worm.SymbOS.Cabir.a. Уже по названию вируса понятно, что он поражает только девайсы с операционной системой SymbianOS, на которой работают практически все современные смартфоны. Существует несколько версий этого вируса, но они практически ничем не отличаются, все версии передаются по Bluetooth. Червячок распространяется в виде файла

caribe.sys размером около 15 Кб. Внутри него несколько файлов: caribe.app, flo.mdl, caribe.rsc. При запуске червь выводит сообщение с текстом

КОМАНДЫ BACKDOOR'A BRADOR.A

D - вывод содержимого каталога
F - завершение работы backdoor'a
G - отправить файл
M - вывод сообщения на экран
P - принять файл
R - выполнить команду

"Caribe" или другим (зависит от модификации).

При включении телефона каждый раз запускается сканирование доступных телефонов по Bluetooth, на найденные устройства червяк отправляет свое "тепло". Есть маленький нюанс: чтобы заразиться, необходимо подтвердить прием сообщения по Bluetooth от неизвестного девайса, далее, в зависимости от устройства, автоматически предлагается установить Caribe.

МНЕНИЕ ЭКСПЕРТОВ ОБ ANTIВИРУСЕ ДЛЯ КПК В 2004 ГОДУ

■ Руководитель отдела антивирусных исследований Proantivirus Lab Андрей Каримов:

"Если серьезно, то, конечно, Security/Antivirus для PDA нужны. Security востребован уже сейчас. Что касается антивирусов для PDA, то сейчас они совершенно бесполезны, поскольку таких вирусов просто не существует. Есть несколько троянцев для Palm OS, да и те можно назвать троянцами с натяжкой. Безусловно, с появлением унифицированной операционной системы и удобных средств связи для этих устройств появятся и вирусы (99% вероятности, что это будут именно сетевые черви). Пока ситуация такова, что каждое третье устройство работает на своей ОС и вирусописатели пока просто не разобрались со всем.

Что касается оценки. Security для PDA (так уж получилось) от "Лаборатории Касперского" стоит на моем PDA еще с тех времен, когда это была непубличная бета-версия. Я бы оценил ее достаточно высоко - на четыре с плюсом по пятибалльной шкале. Оценивать антивирус, который не ловит вирусов, сами понимаете, проблематично. Мы пока не собираемся выпускать такой продукт, хоть и ведем разработки и исследования в этой области. Мы - небольшая компания, которая ориентируется в основном на домашнего пользователя, и для нас просто нерентабельно выпускать продукт, ориентированный в будущем на корпоративного пользователя, причем для альтернативной платформы".

■ Представители компании Panda Software Russia:

"На данный момент не существует антивирусов, разработанных компанией Panda Software для карманных компьютеров и налагодников. И можно сказать, что в ближайшем будущем подобной разработки не предвидится. Дело в том, что риск заражения карманных компьютеров вирусами не высок, поскольку операционная система никогда не допустит исполнения скриптов, полученных по электронной почте, так как для этого нет интерпретатора. Кроме того, программы Excel и Word в карманном компьютере не могут запускать макросы. Заражение осуществится тогда, когда карманный >>


СПИСОК ФАЙЛОВ CARIB

c:\system\apps\caribe\caribe.app
c:\system\apps\caribe\flo.mdl
c:\system\apps\caribe\caribe.rsc

Каталог SYMBIANSECUREDATA скрыт от глаз пользователя. При удалении "видимого вируса" его функциональность не нарушается.

C:\SYSTEM\SYMBIANSECUREDATA\CARIBESecurityMANAGER\CARIBE.SIS
C:\SYSTEM\SYMBIANSECUREDATA\CARIBESecurityMANAGER\CARIBE.APP
C:\SYSTEM\SYMBIANSECUREDATA\CARIBESecurityMANAGER\CARIBE.RSC
C:\SYSTEM\RECOGS\FLO.MDL

"Лаборатория Касперского" разработала бесплатную утилиту decabir.sis для удаления вируса, которая доступна с war-сайта лаборатории. Если вирус в телефоне не обнаружен, выскоит сообщение "Device is clean", если вирус был обнаружен и успешно удален, - сообщение "Carib has been removed. Please reboot".

Вот ты и ознакомился с историей хако-мобильного андеграунда. У тебя есть КПК? Если да, то ищи, пробуй, рискуй. Возможно, открытие новых горизонтов в области хака мобильных девайсов за тобой. 

МНЕНИЕ ЭКСПЕРТОВ ОБ АНТИВИРУСЕ ДЛЯ КПК В 2004 ГОДУ



На сайте Panda Software Russia ты найдешь интересную энциклопедию вирусов

компьютер подключится к стационарному ПК. В таком случае некоторые вирусы могут быть переданы с одного компьютера на другой, но тогда антивирус на ПК сможет обнаружить их, так как передача вирусов происходит через файлы. В случае задействования MS Outlook сложится другая ситуация. Карманный ПК обычно обменивается информацией с Outlook (календарь, контакты, заметки), при этом формат общих файлов не является стандартным. Но в этом случае Panda Antivirus для Outlook сгелает всю работу. Каждый раз, когда запускается какой-то раздел Outlook (в данном случае программа синхронизации), перед тем как установить какой-либо доступ, запускается антивирус и тем самым обеспечивается защита синхронизации. Вот почему установка антивируса в карманном компьютере на самом деле не так необходима, так как она лишь задействует ресурсы памяти и при этом все равно не будет осуществляться постоянная проверка. Следовательно, проверка не будет функционировать постоянно и нужно будет запускать антивирус каждый раз, когда Вы захотите проверить устройство..."

ЖУРНАЛ О КОМПЬЮТЕРНОМ ЖЕЛЕЗЕ



от создателей

ЖЕЛЕЗО

Тесты

- Тестирование бюджетных видеокарт
- Большой тест MP3-плееров на основе флеш-памяти
- DVD-проигрыватели для дома
- Память DDR для флуального использования
- Цифровые камеры полупрофессионального уровня
- Графические планшеты
- Versus-тест кулеров для видеокарт: GlacialTech Igloo NorthPole 1000 vs. Zalman VF700-Cu
- В сборе: ЭКСИМЕР Home Double Users

Инфо:

- Эволюция оптических носителей информации
- Технологии мультимедийной акустики
- Линейка: плееры Iriver
- Звездные железки: процессоры Intel
- Конструктор: комп-мечта

Практика:

- Разгон бюджетной системы
- Учим как вкляать ТВ
- Моддинг: Создаем Hard-Mobile
- Linux: Настройка поддержки UPS

ЖУРНАЛ КОМПЛЕКТУЕТСЯ
ДИСКОМ С ЛУЧШИМ СОФТОМ



Теперь 160 страниц!

Степан Ильин aka Step (step@gameland.ru)

SIM-SIM, ОТКРОЙСЯ

ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О SIM-КАРТЕ, НО БОЯЛСЯ СПРОСИТЬ

Я уже давно ухмыляюсь, когда наблюдаю за теми людьми, которые аккуратно хранят в своем кошельке две-три SIM-карты различных операторов и умело переставляют их в зависимости от времени суток, направления исходящего вызова и еще бог знает чего. При этом на мой резонный вопрос "Зачем так извращаться?" они обиженно отвечают: "Ведь так дешевле!" Пусть так, но уже давно существует способ быстрого переключения между операторами без акробатических трюков на ходу и рыгання на производителя, который сделал для симки "столь дико неудобное крепление".

ДВА В ОДНОЙ



■ Прогрессивные люди уже давным-давно в курсе, что вместо кучи SIM-карт можно сде-

лать одну универсальную, после чего легко переключаться между всеми необходимым операторами сотовой связи. Самый простой способ - купить адаптер на две SIM-карты. Технология проста как две копейки. Вспомни: основная часть SIM-карты - это обычный пластик, на котором красуется логотип оператора. А собственно чип занимает даже меньше половины всего пространства. Почему бы не воспользоваться этим и не сделать симку сразу с двумя чипами от разных операторов? Точно так же подумали наши китайские товарищи по несчастью и оперативно выпустили на рынок девайс, который внешне очень похож на обычную симку, с той лишь разницей, что имеет два "лотка" под чипы. Чтобы облегчить его использование, в комплект прилагаются специальные трафареты, с помощью которых даже ребенок сможет легко вырезать микросхемы из имеющихся SIM-карт. Когда этот этап будет завершен, микросхемы размещаются в адаптере, а адаптер в свою очередь вставляется в картоприемник телефона. Вот, собственно, и все. Переключение между номерами отныне будет осуществляться выключением/включением телефона или с помощью специального меню - это зависит от поколения адаптера. Все удовольствие обойдется тебе в 150-450 рублей, причем в

комплект включены специальные восстановительные контейнеры, на случай если потребуются восстановленные SIM-карты.

Использование подобного адаптера - это, пожалуй, самый дешевый, но вполне удобный способ наладить использование сразу двух SIM-карт. Но что делать, если симок будет больше? И не надо предлагать купить второй адаптер - это не наши методы!

МУЛЬТИ-SIM

■ Микрочип на SIM-карте - это своеобразный компьютер. Он может быть мощным и содержать массу данных, а может быть слабым и едва вмещать информацию, необходимую оператору сотовой связи. Фактически SIM - это смарт-карта со встроенным программным обеспечением, она может быть программируема или нет. Операторы сотовой связи, естественно, используют непрограммируемые SIM-карты, и единственное, что с ними можно сделать, - это использовать по назначению. Совсем другое дело с программируемой SIM-картой. С помощью программатора из нее можно сделать клон имеющейся SIM-карты или вообще записать на нее десяток номеров и тарифных планов, чтобы затем быстро переключаться с помощью специального меню. Думаешь, это сложно? Ошибаешься.

АУТЕНТИФИКАЦИЯ В GSM-СЕТЯХ

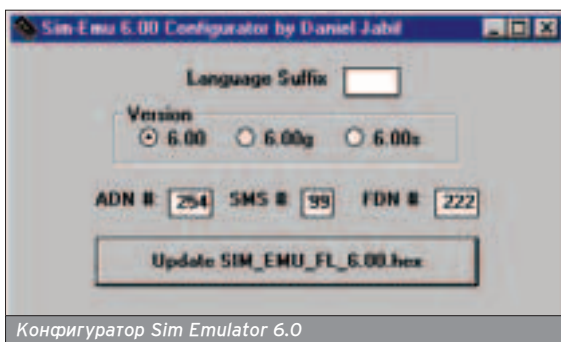
■ Многие считают, что на SIM-карте хранится номер абонента, но это далеко не так. На самом деле SIM-карта выполняет защитную роль, ограждающую GSM-сеть от несанкционированного доступа. Естественно, никакого номера, как и любой другой информации в открытом виде, на SIM-карте не содержится - напротив, все данные тщательно зашифрованы. При этом обмен данными по радиоканалу между мобильником и базовой станцией также осуществляется исключительно в зашифрованном виде (за исключением тех случаев, когда шифрование намеренно отключается оператором

связи, как это было во время терактов в Москве). Для того чтобы начать работу в сети, абоненту необходимо аутентифицироваться - глядя это и используется SIM-карта. Процесс начинается во время ввода PIN-кода пользователем и продолжается идентификацией в сети, этот механизм сейчас рассмотрим подробнее, разделив его на четыре этапа:

❶. В момент, когда абонент инициирует подключение, телефон устанавливает связь с ближайшей базовой станцией и передает по зашифрованному каналу специальный IMSI-код (International Mobile Subscriber Identity - международный идентификатор мобильного абонента), хранящийся на SIM-карте.

❷. Получив запрос на подключение, базовая станция сверяет полученный IMSI-код по своей базе данных и в случае совпадения отправляет мобильному устройству 128-разрядное случайное число (так называемое RAND), которое в свою очередь передается телефоном на SIM-карту. SIM-карта шифрует это число по алгоритму A3, используя при этом специальный Ki-ключ так же, как и IMSI, хранящийся на SIM-карте. В результате шифрования получается так называемый пописанный ответ (SRES), который сразу же отправляется на базовую станцию.

❸. В базе данных оператора имеется информация обо всех парах IMSI - Ki. Поэтому, получив ответ, система идентификации пробивает по IMSI-номеру его Ki-код и производит точно такие же вычисления, которые выполнялись на SIM-карте. Если SRES, полу-



Конфигуратор Sim Emulator 6.0



БУДЬ ОСТОРОЖЕН!

■ Покупая "чистую" карту, проверь ее на физическое повреждение контактной площадки: если таковые имеются, немедленно обращайся к продавцу и требуй замены. SIM-карты очень чувствительны к любым повреждениям. По этой же причине будь крайне осторожен, когда будешь выламывать карту из "коробочки". Лучше сделать это с помощью канцелярского ножика или другого режущего предмета.

ченный от абонента, с точностью совпадает со SRES'ом, сгенерированным системой идентификации, абонент считается аутентифицированным и ему разрешается доступ в сеть. При этом Ki-код, без которого нереальна идентификация, не передается - перехватить его таким образом невозможно!

❶ После этого SIM-карта на основе числа RAND, ключа карты Ki и алгоритма A8 генерирует временный ключ Kc, который используется во время шифрования данных при передаче.

Такой подход гарантирует, что звонки в сети могут осуществлять только законные абоненты, которые обладают SIM-картой, выданной оператором. Тем не менее, он не исключает использование краденых или клонированных симок. Для создания копии симки достаточно извлечь из нее уникальные IMSI- и Ki-коды и прописать их в другую карту. IMSI обычно слабо защищен и легко считывается специальными программами. В отличие от IMSI, "вытащить" Ki-код из SIM-карты существенно сложнее, так как для его защиты применяется специальный криптографический алгоритм COMP. Существует несколько версий этого алгоритма: COMP 128 v.1 (его используют большинство операторов сотовой связи), COMP 128 v.2 (уже пару лет его использует "Мегафон"), а также COMP 128 v.3, который не так дав-

но был ратифицирован, но пока не используется на территории России.

COMP 128 v.1 довольно долгое время считался защищенным, но, как это обычно бывает, его все-таки взломали. Это удалось инженерам из Калифорнийского университета: в 1998 году они считали Ki-ключ из SIM-карты. Это стало возможным за счет анализа большого количества триплетов Rand - SRES - Kc. После 5-25 тысяч попыток обращений к SIM-карте можно с большой достоверностью вычислить Ki-ключ, что сейчас успешно выполняется на практике. Что касается второй и третьей версий COMP 128, то с ними такой фокус не пройдет. Ошибки первой версии были устранены, алгоритмы были значительно усовершенствованы и практически исключают подбор Ki-кода. Впрочем, это не повод для отчаяния: большинство применяемых сегодня симок (за исключением "Мегафона" и некоторых региональных OpCoСов) по-прежнему используют COMP 128 v.1, так что их симки могут быть клонированы. Правда, здесь стоит упомянуть еще об одной защите, которая интегрирована в любую SIM-карту.

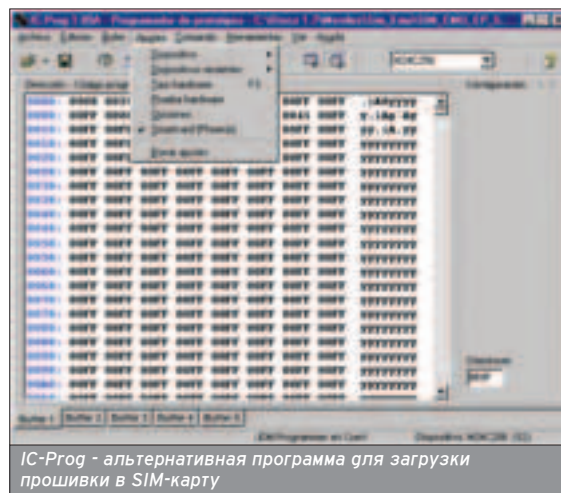
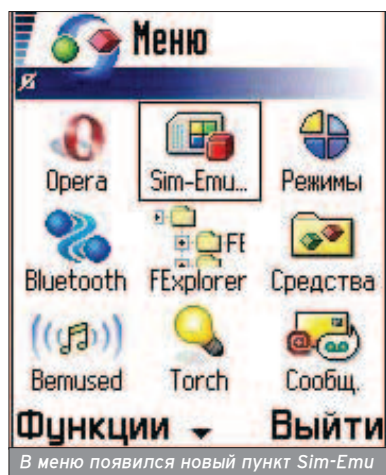
Для того чтобы ограничить возможности пользователя, многократно пытающегося авторизоваться, операторы задают для SIM-карт предел количества неудачных попыток. После каждой попытки счетчик авторизации (команда RUN GSM ALGORITHM) увеличивается на единицу и, как только он достигает значения верхней грани, SIM-карта блокируется и становится полностью неработоспособной. Понятно, что значение этого предела можно подобрать таким образом, чтобы оно было недостаточным для возможности перебора, но при этом вполне успешно обеспечивать работоспособность SIM-карты на протяжении всего срока эксплуатации. В самом деле, не все так печально: значение предела обычно довольно высоко, и его вполне хватает, чтобы единожды извлечь из него Ki-код. Удается ли сделать это второй раз - спорный вопрос. По этой же причине никогда не стоит браться за взлом уже клонированной SIM-карты, который, скорее всего, приведет к ее блокировке.

ПЫТКА SIM-КАРТЫ

■ Итак, задача ясна: нужно вытащить из симки IMSI- и Ki-коды, записать их на специально подготовленную "чистую" SIM-карту, дополненную специальным софтом для переключения между номерами, а также функцией задания их параметров. К счастью, все это давно уже сделали за нас. Народные умельцы сварили так называемые SIM-эмуляторы - специальные программы, которые прошиваются в SIM-карту, хранят значение IMSI- и Ki-кодов и предоставляют функцию удобного переключения между ними. Наиболее продвинутой и распространенной по праву считается программа SIM Emu (www.simemu.com) - с ее помощью можно хранить на одной карте до десяти других симок, номера центров SMS-сообщения, задавать для каждого номера PIN- и PUK-коды. Что касается переключением между ними, то оно осуществляется через удобное меню (SIM Menu) или же во время включения телефона. »



Silver Card идеально подходит почти всегда

**ВАЖНО!**

■ Бытует мнение, что PIN- и PUK-коды можно легко восстановить в сервис-центре. Помни: это не так! Если ты случайно забыл PIN-код, то тебе поможет только твой оператор сотовой связи. Никакой проffi даже с самым навороченным программатором и другими чудо-девайсами не сможет восстановить его. Это практически невозможно!



Sim-card reader/writer - US1 v2.0

Теперь нужно определиться с тем, каким образом можно считать идентификационные коды с SIM-карты. Понятно, что с помощью обычного телефона, каким бы навороженным он ни был, этого сделать нельзя. Понадобится, как минимум, специальный считыватель, предназначенный для сканирования SIM-карт. Это довольно примитивный девайс, который подключается к COM-, реже к USB-портам компьютера и имеет огромное количество реализаций. При желании все необходимые схемы можно найти на сайтах и форумах радиотематики. Но, как мне кажется, шутить с SIM-картами не стоит, поэтому рекомендую покупать все-таки готовые изделия, тем более что они стоят всего 500-600 рублей. Слово "считыватель" неслучайно: девайс умеет только считывать данные и не записывает их. В этом случае чистую SIM-карту нужно покупать с уже прошитой программой SIM Emu, а данные об IMSI- и Ki-кодах заносить уже через телефон.

Пустая симка - это та же самая SIM-карта в нашем привычном понимании, но с возможностью перезаписи. В настоящее время самое широкое распространение получили карты с процессором PIC16F877 и памятью EEPROM 24C64/256 (их цена варьируется от 250 до 350 рублей).



Комплект для спаривания двух симок

НАЙДЕТСЯ ВСЕ

■ Необходимое оборудование продается в специализированных салонах связи и радиорынках. Все те, у кого нет возможности попасть в подобные места, могут заказать "болванки", считыватели и программаторы в интернете (www.irda.ru, www.multisimcard.ru и т.д.).

❶. Gold Wafer Card - (PIC16F84+24C16) максимум 4 разных сотовых оператора, 31 номер в записной книжке, 1 SMS.

❷. Silver Card - (PIC16F877+24C64) максимум 8 разных сотовых операторов, 208 номеров в записной книжке, 10 SMS.

❸. Green Card - (PIC16F876+24C128) максимум 10 разных сотовых операторов, 250 номеров в записной книжке, 40 SMS.

❹. Black Card (Silver Card 4) - (PIC16F877+ 24C256) максимум 10 разных сотовых операторов, 254 номера в записной книжке, 99 SMS.

Если есть желание производить запись SIM Emu на смарт-карты самостоятельно, то придется раскошелиться на специальный программатор. Большинство из них является одновременно и считывателями, поэтому покупать два различных девайса, по сути, незачем. Цены на программаторы несколько выше: достойный вариант можно найти за 1100-1200 рублей.

БЛИЖЕ К ДЕЛУ!

■ Думаю, в теории теперь все более чем понятно. Предлагаю перейти к практике. Первый этап, считывание IMSI- и Ki-кодов, можно выполнить с помощью программы Sim Scan (<http://users.net.yu/-dejan>) или же Wogon Scan (www.satnavigator.ru/page-id-67.html). По опыту могу сказать, что последняя работает несколько быстрее, поэтому лучше будет использовать именно ее. Так или иначе, обе представляют собой вполне обычные программы, так что проблем возникнуть не должно. Просто вставьте считыватель/программатор (я использую US1 v2.0) в свободный порт компьютера и запустите Wogon Scan. После запуска необходимо провести кое-какую настройку, для которой в меню Card Reader выбери тип устройства для считывания Phoenix Card и переходи в меню Card Reader->Setting. После этого должно появиться окошко с настройками, в котором



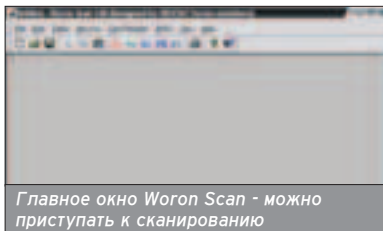
Размеры SIM-карты впечатляют!

пользователю предлагается обозначить номер COM-порта (COM Port Selection), а также частоту кварцевого генератора (Speed/Frequency). Любой программатор и любая симка совершенно точно будет читать на частоте 3,57 МГц, однако это самая маленькая скорость. Мы использовали программатор US1 v2.0, который способен опрашивать SIM'ку на частоте 3,57, 7,14 и даже 14,28 МГц. Тем не менее, это не значит, что с его помощью любая SIM'ка может считывать на высокой частоте. Нет! Например, в Москве SIM-карты "Билайна" сканируются исключительно на частоте 3,57 МГц, а симки "МТС" (кроме "Джинса") на 7,14 МГц.

Теперь, когда все готово, можно приступать к сканированию. Для этого в панели инструментов программы кликни по кнопке Ki и в появившемся окне, не изменяя опции и настройки, нажимай кнопку Start. В случае если выбранная частота и COM-порт были указаны верно, программа предложит ввести PIN-код, установленный на SIM'ке (если он, конечно, не отключен). После успешного ввода начнется процесс сканирования SIM-карты и поиск Ki-кода. Время окончания процесса сильно зависит от случая: бывает, конечно, ключ находится буквально за 10-15 минут, но чаще всего приходится ждать час или даже два. Как только процесс будет завершен, IMSI- и Ki-коды будут отображены в окне сканирования и главном окне программы. Главное - не забыть сохранить эти коды в отдельный файл. Если программе не удалось найти Ki-ключ (это если ты решишь поэкспериментировать и подсунуть ей "неклонировуемую" симку "Мегафона"), то Wogon Scan автоматически прекратит сканирование на 60 000-м обращении к SIM-карте. Только так можно гарантировать, что SIM-карта не будет заблокирована, ибо в противном случае ее останется разве что выбросить или повестить на брелок от ключей. Каждый оператор выставляет свой верхний предел по количеству обра-



Извлекаемая SIM-карту из такого крепления, будь крайней осторожен - не сломай ее



Главное окно Wagon Scan - можно приступить к сканированию

щений. Например, умельцы утверждают, что карты "Мегафона" блокируются после 90 000 обращений, так и не выдав свой Ki-код.

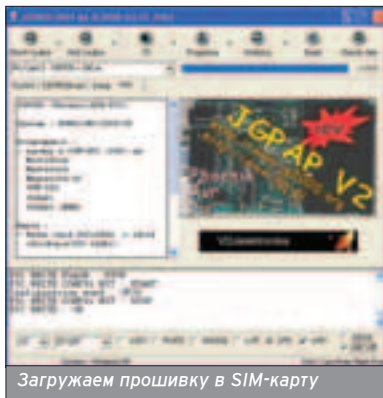
ПРОГРАММАТОР В ДЕЛО!

■ Как я уже говорил, можно приобрести либо уже прошитую чистую SIM-карту, либо непрошитую. В последнем случае ее придется прошивать самостоятельно - разберем этот процесс подробнее. Для каждого программатора существуют свои инструкции, свои режимы и свое программное обеспечение, однако в общих чертах все схоже. Я использую USI v2.0, поэтому буду описывать соответствующий процесс прошивки. При этом важно заметить, что в качестве "болванки" я использовал Silver Card - глядя других заготовок некоторые параметры могут отличаться.

Первое, что нужно сделать, - перевести программатор в нужное положение. Для этого на программаторе необходимо активировать режим JDM: SIM CLOCK - в положение PROGRAM PIC, SIM RESET - в положение PROGRAM PIC, SIM DATA - в положение PROGRAM PIC.

Далее пускаем в бой программу-прошивальщик. В принципе, можно использовать совершенно разные программы, однако производитель всегда рекомендует JGPROG (www.vgji.pl/index.php?pokaz=pap2&m=1). Указываем программе параметры Silver карты (Pic Card 2 - 16F876 + 24Cxx) и переходим к настройкам самого прошивальщика (меню Setup). Здесь всего два важных параметра: порт, к которому подключен программатор, и тип операционной системы. Помимо этого, нужно отключить опции WDT, PWRT, BODEN, LVP, CPD, WRT и поставить галку напротив 24C64. После этого программа будет полностью готова к работе.

Работа с картой начинается с программирования внешнего EEPROM, которое выполняется в два этапа. Пер-



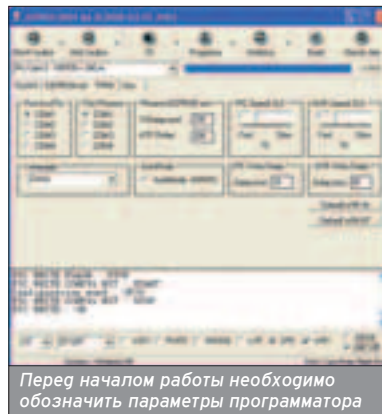
Загружаем прошивку в SIM-карту

вым делом записывается специальный загрузчик, а затем, уже с его помощью, загружается EEPROM. Загрузчик входит в состав JGPROG по умолчанию, поэтому достаточно открыть файл loader_PIC16F876.hex через меню (Load File-> Load Flash-> loader_PIC16F876.hex) и нажать на кнопку Write Flash/Eep_int/Cfg_bit. Программа выдает сообщение, что загрузчик был загружен в карту, и будет ожидать следующих инструкций. Для следующего действия программатор необходимо перевести в режим Phoenix: SIM CLOCK - в положение 3.579 MHz, SIM RESET - в положение HIGH RESET, SIM DATA - в положение SIM READER.

Теперь можно загружать непосредственно EEPROM: открой Load File-> Load Eeprom ext и выбери SIM_EMU_EP_6.00s_RUS.hex из комплекта прошивки SIM EMU 6.00. Внимательно проверь все и дави на кнопку Write Eeprom ext, через некоторое время загрузка будет завершена. Все! Теперь остается залить прошивку, и карточка будет полностью готова к работе. Прошивка выполняется в режиме JDM (параметры смотри выше) и аналогично загрузке EEPROM'a. Для этого нужно открыть файл SIM_EMU_FL_6.00s_RUS.hex из прошивки SIM EMU 6.00 (Load File-> Load Flash-> SIM_EMU_FL_6.00s_RUS.hex), затем кликнуть все по той же кнопке Write Flash/Eep_int/Cfg_bit. Даже если на карте уже была какая-то прошивка, JGPROG загрузит прошивку заново. Для того чтобы проверить правильность выполнения всех этих действий, существует специальная функция - нажми на кнопку Verify и смотри результат.

АТАКА КЛОНОВ!

■ После того как Sim Emu будет записана на карту, можно будет приступить непосредственно к ее настройке. Никакого дополнительного софта не требуется (хотя это и не возбраняется), все отлично выполняется на обычном сотовом телефоне с помощью по-



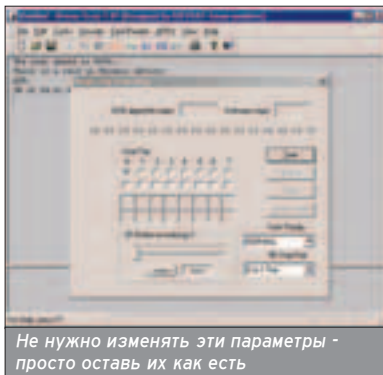
Перед началом работы необходимо обозначить параметры программатора

явившегося Sim Menu. Просто вставь полученную SIM-карту в телефон и включи его. Если телефон потребует PIN (а он должен!), то введи 1111 - прошивка устанавливает этот код по умолчанию. Далее в меню телефона ищи новый пункт SIM Emu, выбери его и переходи к настройке: Configure-> Config.Pos. На этом этапе необходимо ввести PIN2 (по умолчанию 1234) и указать параметры непосредственно клонируемой симки. А именно, позиция, на которую будет записан номер (от 0 до 9 - понятно, что она выбирается произвольно), IMSI- и Ki-коды, а также PUK- и PIN-коды, которые нужно придумать от балды и запомнить. Собственно, все. Остальные SIM-карты клонируются и заносятся в базу данных Sim Emu аналогично.

Переключение между номерами на большинстве телефонов осуществляется через меню. Но, к сожалению, есть модели телефонов, которые не поддерживают эту функцию. Если нарвался на такую неприятность, глядя каждого номера нужно прописать отдельный PIN-код (например, для первого - 1111, для второго - 2222 и т.д.). Теперь, глядя того чтобы переключиться между номерами, достаточно выключить-включить телефон и ввести нужный PIN-код нужной симки. SIM Emu самостоятельно определит, какие параметры соединения нужно использовать.

А ПОЧЕМУ БЫ НЕТ?

■ По-моему, довольно глупо не использовать возможность создать универсальную симку для каждого оператора сотовой связи. Затраты можно свести к минимуму, скинувшись на считыватель/программатор с друзьями. Пустые SIM-карты можно также прикупить оптом. И самое главное - все затраты в любом случае окупятся, когда все твои знакомые начнут взахлеб задавать вопрос: "А как ты это сделал?! А можешь и мне?"



Не нужно изменять эти параметры - просто оставь их как есть

Чистые SIM-карты можно купить оптом, все затраты окупятся.

S.A.N.

СЕКРЕТОВ НЕ БУДЕТ

ВСЕ О ПРОСЛУШИВАНИИ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Число пользователей мобильных телефонов стандарта GSM в мире превысило один миллиард. Каждый день они говорят обо всем, что только можно представить себе. Передается информация, которая стоит миллионы. Как можно прослушать ее? Слушает ли кто-то твои разговоры по телефону?

А возможно ли вообще прослушать чужой разговор в сетях GSM или все это слухи, запущенные "желтой" прессой и провокаторами? Разберемся с этим вопросом подробнее. Вот мнение "отцов" в лице Джеймса Морана - директора по подразделению, отвечающего в консорциуме GSM за безопасность и защиту системы от мошенничества: "Никто в мире не продемонстрировал возможность перехвата звонков в сети GSM. Это факт... Насколько нам известно, не существует никакой аппаратуры, способной осуществлять такой перехват". Есть ли смысл сомневаться в этих словах?

У сотовой связи (как и у любой радиосвязи) есть один огромный минус: передача данных идет "по воздуху", поэтому они могут быть перехвачены. Единственный способ предотвратить доступ к информации (в нашем случае прослушивание) - система безопасности на основе серьезного шифрования данных. Известно, что в создании системы безопасности протокола активное участие принимали спецслужбы стран НАТО. Основа системы безопасности GSM - три секретных алгоритма, которые сообщаются лишь поставщикам оборудования, операторам связи и т.д. A3 - алгоритм авторизации, защищающий телефон от клонирования, A8 - "сервисный" алгоритм, который генерирует криптоключ на основе выходных данных алгоритма A3, A5 - алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров. Больше всего нас интересует последний.

ОПЯТЬ A5

■ В сетях GSM используется две версии алгоритма A5: A5/1 и A5/2. Такое разделение произошло "благодаря" экспортным ограничениям на технологии шифрования. В итоге страны Западной Европы и несколько других наиболее цивилизованных мест получили право использовать алгоритм A5/1, а остальным странам (в том чис-

ле России) разрешили использовать "слабый" A5/2. Алгоритмы семейства A5 были засекречены, однако их основные детали стали известны уже к 1994 году. Сейчас об алгоритмах защиты GSM общественность знает практически все.

В A5 реализован поточный шифр на основе трех линейных регистров сдвига с неравномерным движением. Такой шифр зарекомендовал себя как довольно стойкий при большой величине регистров и некоторое время использовался в военной связи. В A5 используют регистры в 19, 22 и 23 бита, в совокупности дающие 64-битный ключ. При том, что глина шифра небольшая, вскрыть его "на лету" (а этого требует сама задача прослушки) не под силу даже довольно мощным компьютерам, то есть при должной реализации GSM-протокол может иметь неплохую практическую защиту. Но кое-кто имеет свое мнение насчет того, какая защита должна быть у сотовой связи. Например, свое мнение есть у спецслужб, которым фриеры должны сказать "спасибо".

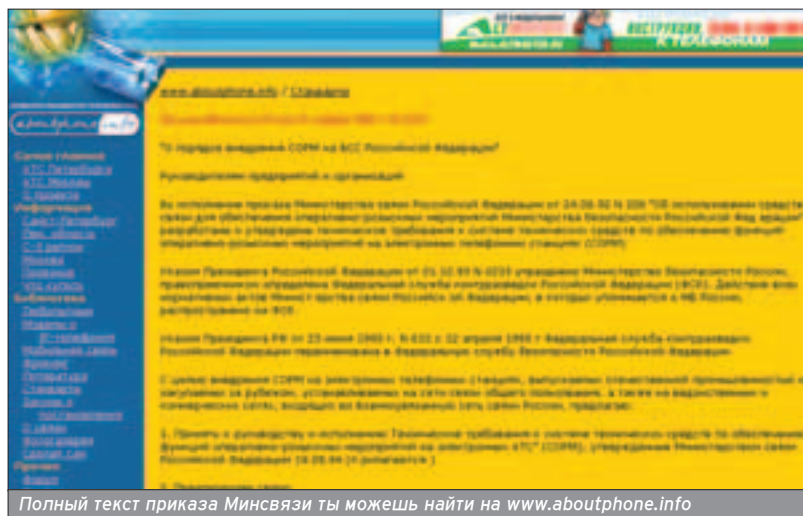
Вот выдержка из приказа Минсвязи "Об использовании средств связи для обеспечения оперативно-розыскных мероприятий Министерства безопасности Российской Федерации" (полный текст www.aboutphone.info/lib/sorm.html):

■ В состав оборудования сетей электросвязи должны быть включены аппаратные и программные средства, позволяющие проводить оперативно-розыскные мероприятия из удаленного пункта управления путем взаимодействия этого пункта и оборудования электросвязи.

■ Должна быть предусмотрена возможность по команде из пункта управления конспиративного подключения выделенных служб безопасности каналов и линии к любым абонентским линиям (каналам), в том числе находящимся в состоянии установленного соединения.

■ (Должен осуществляться)... контроль исходящих и входящих вызовов (местных, внутризональных, междугородных и международных) к/от определенных абонентов данной станции, а также контроль вызовов и заранее заданных номеров телефонной сети при исходящей связи абонентов этой станции.

Смысл документа таков: обеспечить полный контроль за абонентами любых средств связи (в том числе мобильной связи). Видимо, поэтому в 64-битном ключе 10 битов просто заменены нулями. Кроме того, из-за многочисленных конструктивных дефектов стойкость шифра находится на уровне 40-битного, который легко



Полный текст приказа Минсвязи ты можешь найти на www.aboutphone.info

может быть вскрыт любым современным компьютером за пару секунд.

Итак, возможность прослушивания любого абонента в сетях GSM - это не только реальность, но и норма, закон (кроме прослушивания, выписана "индальгенция" на определение местоположения, фриксацию номера и многие другие "услуги"). Что ж, ответ на вопрос "Есть ли прослушка в сетях GSM?" ты получил. Теперь разберемся с другим вопросом.

ТВАРЬ ЛИ Я ДРОЖАЩАЯ ИЛИ ПРАВО ИМЕЮ...

■ Как бы маркетологи ни убеждали нас в том, что защита GSM безупречна, это далеко не так.

Даже "сильный" А5/1 был вскрыт с помощью довольно обычного оборудования (хотя при этом использовались нетривиальные методики). Что уж говорить об А5/2? Кроме того, есть повод поблагодарить наши спецслужбы еще за одну вещь: при некоторых обстоятельствах операторы полностью отключают шифрование разговоров (так было на праздновании 300-летия Питера, при захвате заложников на Дубровке в Москве). Поэтому, используя средней мощности компьютер и "правильное" програм-

мное обеспечение, ты можешь расшифровывать сигнал с "вражеской" GSM-трубки за приемлемое время. В Сети выложено множество программ для взлома GSM-защиты, использующих разные методы (см. врезку).

Однако для расшифровки нужно сначала получить материал. Так ли это просто?

Аппаратура для перехвата и расшифровки GSM-сигнала появилась одновременно с принятием стандарта GSM. Сейчас в мире существует около 20-ти эффективных (и, если можно так сказать, популярных) видов оборудования по прослушке GSM-связи, стоимостью от \$12 000 до \$2. Более того, есть подобная аппаратура отечественного производства (разработка Военной академии связи имени С.М. Буденного), которая некоторое время назад использовалась во многих отделах управления "Р" МВД РФ.

Изделия для перехвата GSM-сигнала, независимо от их типа, быстродействия и цены, должны иметь следующие возможности:

- Контроль управляющего и/или голосового канала базовой станции;
- Контроль управляющего и/или голосового канала мобильного телефона;

■ Сканирование всех каналов и поиск активных (в данной точке);

■ Запись сигнала (или разговора) на жесткий диск (или другой носитель);

■ Фиксация номеров вызывающего и вызываемого абонента.

Это основные требования к аппарату, способному перехватить GSM-сигнал для последующей расшифровки. В подобных "средствах связи" среднего и верхнего ценового диапазона предусмотрена мгновенная расшифровка и возможность прослушивания сразу нескольких абонентов.

СНИФЕР ДЛЯ GSM

■ Использование разнообразных средств слежения за мирными гражданами всегда было прерогативой органов госбезопасности, поэтому в идеале наблюдаемые не должны даже догадываться о том, что за ними следят. Но "утечки" информации происходят даже из спецслужб, поэтому на рынке представлена разного рода спецтехника. Применение таких устройств - незаконное дело, поэтому они не продаются "в открытую". Как следствие, этот рынок оброс толпой "кигал" - если вдруг соберешься купить что-нибудь из спецтехники, не соглашайся на полную или даже частичную прегоплату.

ВОТ НЕКОЛЬКО ОБРАЗЦОВ ИЗДЕЛИЙ ДЛЯ МОНИТОРИНГА СИСТЕМ GSM-СВЯЗИ.

PostWin

■ PostWin - программно-аппаратный комплекс, имеющий в своем составе блок приема и обработки сигналов, две ПЭВМ класса P-III и комплект программ. Может использоваться для перехвата сигналов AMPS/DAMPS, NMT-450, GSM-900. Есть возможность вести запись на жесткий диск со сжатием (13 Кбит/с) и без сжатия (64 Кбит/с). »



Собственная базовая станция - лучшее средство для прослушивания чужих разговоров :)

КРИПТОАНАЛИЗ И ВЗЛОМ А5

■ Алгоритм основан на регистрах сдвига с линейной обратной связью определенной глины (19, 22, 23 бита). Начальные заполнения регистров определяются секретным и открытым ключами. Открытый ключ известен и отличается для каждого нового сеанса. При связи двух абонентов шифрование осуществляется дважды, так как А5 используется для безопасной связи между абонентом и базовой станцией. Вот основные методы атаки:

1. Лобовая атака

Самый простой тип атаки, однако достаточно эффективен при коротких регистрах. В случае с А5 (особенно А5/2) позволяет организовать вскрытие ключа с перебором максимум 2^{40} (2 в степени 40) вариантов. Делается предположение о содержимом первых двух регистров, а содержимое третьего регистра восстанавливается по шифрующей гамме.

2. Корреляционный анализ

Ходят слухи, что с помощью этого метода алгоритм А5/1 был вскрыт еще в 1994 году. О методе известно немного: "Для восстановления начальных заполнений используется техника разреженной матрицы (была опубликована в апреле 1993г. в издании Mobile Europe); для вскрытия используются приемы из криптоаналитических работ Андерсона, Доусона, Кларка".

3. Балансировка "время-память"

Если T - время, требуемое для вскрытия, M - память, то при произведении T и M, не меньшем 2^{63} , шифр может быть вскрыт. Чем больше памяти, тем меньше времени нужно для вскрытия :).

4. Цикловая структура А5

У.Дж. Чамберс пришел к выводу о том, что около 40% ключей алгоритма А5 приводят к циклу, длина которого $(2^{23}-1)/3$ бит, что поддается вскрытию с привлечением минимальных вычислительных ресурсов (по материалам книги "Поточные шифры. Результаты зарубежной открытой криптологии").



Компьютер + сканер диапазона 900 МГц - так выглядит большинство систем мониторинга связи

GSM Interceptor Pro

■ Более продвинутая система мониторинга GSM-связи. Из особенностей стоит отметить зону охвата станции: перехват прямого канала (от базовой станции) до 25-ти километров и до 800 метров - обратного канала (от трубки). Комплекс работает с алгоритмами A5/1 и A5/2.

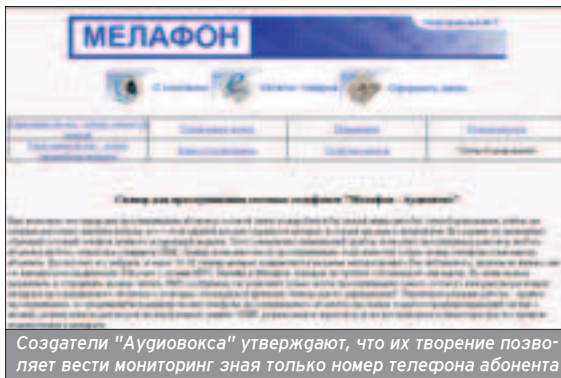
-SCL-5020

■ Данный аппарат разработали инженеры Индии. Кроме "джентльменского набора" опций, предлагается прослушивать до 16-ти GSM-каналов, определять расстояние до базовой станции, записывать речь на жесткий диск. Более подробную информацию по готовым решениям в области GSM-прослушки ты всегда можешь найти в Сети, однако, если будешь использовать простой сканер и заниматься расшифровкой на домашнем компьютере, сэкономишь свои кровные.

Интересное решение предлагает некая компания "Мелэфон" - сканер для прослушивания сотовых телефонов "Мелэфон-Аудиовокс".

Как утверждают производители, сканер позволяет вести мониторинг, если известен только номер телефона абонента (сомнительно, но имеет право на жизнь). Цена аппарата - 12700 рублей (www.melafon-bugs.ru/super_equipment.htm).

Мы пришли к тому, что комплекс для прослушивания чужих разговоров можно либо купить (цена ~15к - довольно дорого, но очень эффективно), либо собрать самому (~5-6к), но при этом надежность и качество работы такой системы - только твоя голов-



Создатели "Аудиовокса" утверждают, что их творение позволяет вести мониторинг зная только номер телефона абонента

ОБРАТНАЯ СТОРОНА МЕДАЛИ

■ Прослушивание GSM-телефонов становится все более распространенным явлением. Но что делать, если ты не хочешь, чтобы телефонные переговоры превратились в улики или компромат? К счастью, существует оборудование для защиты передачи данных и голоса. Принцип действия большинства из них - дополнительное шифрование данных на участке между двумя абонентами. В большинстве случаев устройства защиты от прослушивания разрабатываются для моделей телефонов определенной фирмы. Вот некоторые из них.

Референт-GSM

Предназначен для работы с телефонами SonyEricsson в сотовых сетях GSM, поддерживающих функцию передачи данных. Исходная речь сжимается до уровня 2,4 Кбит/с, после чего шифруется и передается модемом мобильного телефона по GPRS. Базовая версия использует 32-битный сеансовый ключ.

Альфа-С

Устройство выполнено в виде отдельного блока с гарнитурой hands-free для телефонов Siemens. Технические характеристики девайса следующие: уровень криптостойкости - 106, время работы - около 10 часов, размеры - 65x40x20 мм.

На современном рынке представлено довольно много подобных устройств, среди которых "Талисман-GSM", Mobi-GSM и др. Плюс некая организация под названием "Бюро научно-технической информации" ведет разработку смартфона, обеспечивающего шифрование на основе 256-битного ключа.

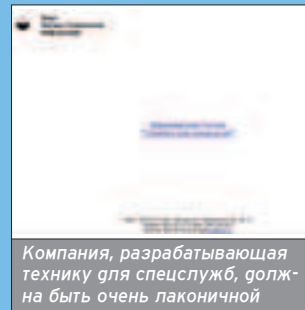
Крипосмартфон Cancort

Предполагается, что телефон сможет работать в двух режимах: "открытый" и режим шифрования. Криптозащита будет распространяться не только на голосовые данные, но и на SMS, GPRS, электронную почту, MMS. Пользователь может самостоятельно генерировать сеансовые ключи. Кроме того, технические характеристики смартфона находятся на уровне лучших аналогов, имеющих на рынке.

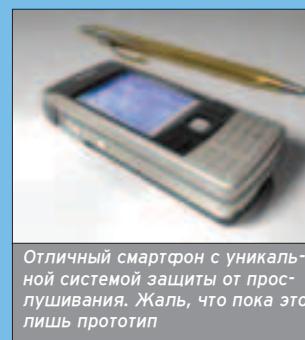
Если прототип будет доведен до массового пользователя (у российских разработчиков это редкость), продукт рискует стать очень востребованным, даже несмотря на его высокую цену.



Маленькое устройство - гарант серьезной защиты



Компания, разрабатывающая технику для спецслужб, должна быть очень лаконичной



Отличный смартфон с уникальной системой защиты от прослушивания. Жаль, что пока это лишь прототип



Все необходимое ты при желании найдешь на знаменитом Митинском радиорынке

ная боль. В любом случае, если есть задача получить как можно больше информации о человеке, GSM-прослушка - лишь один из множества инструментов, которые необходимо применять в комплексе. Если же ты просто хочешь узнать, о чем говорят люди по мобильнику, необходимый комплект оборудования можно при желании приобрести и на Митинском радиорынке.

Хочешь?

1-й номер
12 октября

- награть коллер в Counter-Strike или Quake 3?
- попасть на зарубежный турнир?
- замутить собственный чемпионат?
- выиграть навороченный автомобиль?
- стать крутым киберспортсменом?

ЧИТАЙ
ЖУРНАЛ **PRO** ГЕЙМЕРОВ



В первом номере:

На страницах:

- эксклюзивный репортаж с чемпионата России WCG 2005
- скандальная рубрика «Папарацци»
- как на 300 баксов съездить на турнир за бугор
- интервью: Cooler, Caravaggio, Flatra, Easy_Meg и Devil

На DVD:

- видеоуроки игры в Warcraft III, Quake III и Counter-Strike
- лучшие мувикли с ффарами и VODы StarCraft: Broodwar
- полная коллекция демов с WCG Россия 2005
- конфиги, необходимые для игры карты, патчи и моды

S.A.N.

ВЛАСТЬ SMS

SMS МОЖЕТ БОЛЬШЕ, ЧЕМ ТЕБЕ КАЖЕТСЯ

В 1992 году, когда инженер британской компании Vodafone отправил первое короткое сообщение, никто и представить себе не мог, насколько популярным станет сервис, тогда получивший название SMS (Short Message Service).

Впрочем, первые несколько лет после своего появления новый сервис не подавал никаких признаков жизни. Хотя возможность отправлять и получать текстовые сообщения была заложена в самом стандарте GSM, операторы не спешили продвигать новую технологию "в народ". Дело в том, что в начале 90-х рынок мобильной связи только формировался и даже подвижная голосовая связь была чем-то необычным. Постепенно сотовая связь, "элитный" способ коммуникации, превратилась в массовое явление. Почти параллельно с сотовой связью сервис SMS, находясь уже в семилетнем возрасте, стал обретать популярность, прежде всего среди молодежи. И в 2000 году, когда операторы позволили своим клиентам

посылать короткие сообщения пользователям других сетей, планету захлестнул поток сообщений глиной до 160-ти символов. Сегодня сервисом коротких сообщений активно пользуются около 80% абонентов мобильной связи в мире. В течение года отправляются миллиарды SMS'ок. Причины такой экспансии очевидны: небольшая стоимость, возможность отправить сообщения в ситуациях, когда телефонный разговор невозможен, возможность неограниченного количества просмотров принятого сообщения.

ЧТО В ОСНОВЕ

■ Основная функция технологии SMS - прием и передача текстовых сообщений. При этом процессы обмена голосовыми и текстовыми данными являются независимыми.

В самом простом случае, когда сообщение пересылается между двумя абонентами, технология обеспечивает следующие возможности:

■ Доставка сообщения без занятия речевого канала - так экономятся коммутационные ресурсы плюс сообщение может быть доставлено даже во время разговора.

■ Подтверждение доставки информации отправителю (либо оповещение о невозможности доставки).

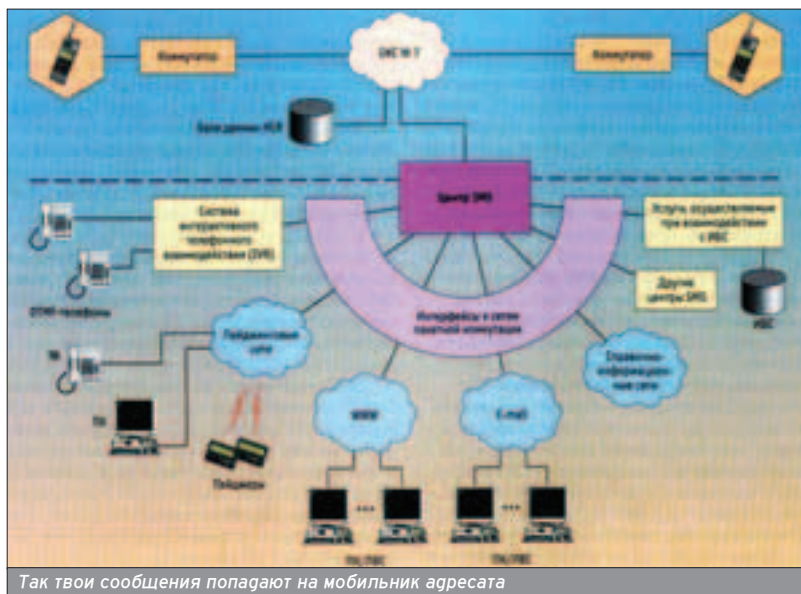
Благодаря этой опции ты без звонка узнаешь о нахождении абонента в зоне действия сети. Если абонент недоступен для базовых станций, сообщение придет к нему, как только он окажется online.

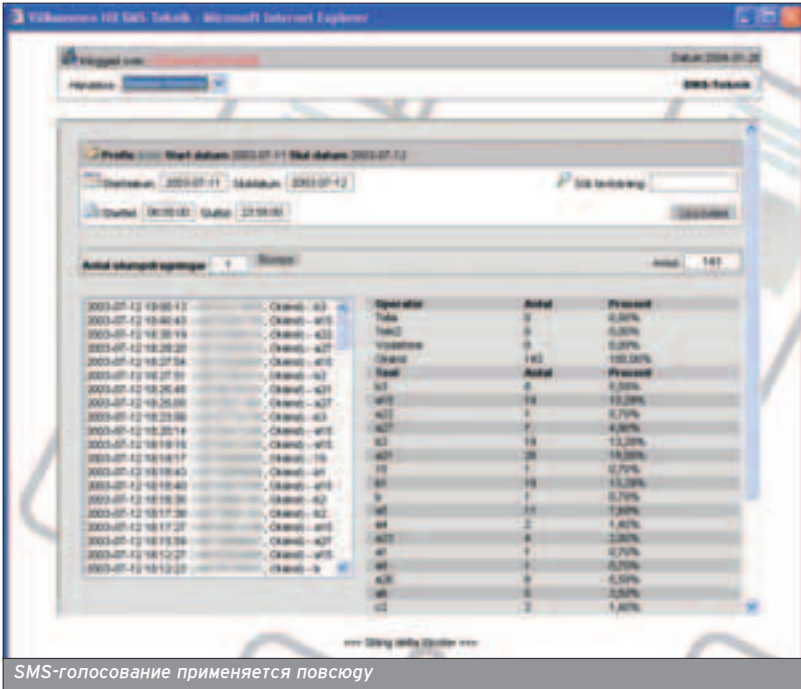
■ Независимость процесса обмена сообщениями от местонахождения абонента.

Факт независимости цены сообщения от того, где находится абонент, способствовал росту популярности SMS среди молодежи: если абоненты находятся в разных странах, цена голосовой связи между ними увеличивается многократно, а стоимость сообщения остается прежней.

При отправке сообщения снабжается служебной информацией, необходимой для правильной доставки адресату. Сообщения, поступающие в центр SMS, фиксируются в базе дан-

За один год отправляется несколько миллиардов SMS!





SMS-голосование применяется повсюду

ных системы и отправляются агрегаторам в соответствии с прописанной схемой доставки. При этом SMS-центр взаимодействует с базой данных HLR, в которой находится информация о клиентах оператора сотовой связи. В общем случае сообщение передается по обычным сигнальным каналам и достигает выбранного абонента, после чего текст сохраняется в его SIM-карте. Если доставить сообщение в данный момент времени невозможно, система периодически возобновляет попытки передачи. Доставленное сообщение удаляется из базы данных SMS-центра (хотя удаление после доставки, как и хранение в процессе, - настраиваемая функция).

Несмотря на перечисленные заслуги технологии, ее главный плюс - способность интегрироваться с другими сетями пакетной коммутации. Именно факт "связи с внешним миром" делает сервис SMS интересным как для инвесторов, так и для пользователей. Благодаря возможности взаимодействовать со многими информационными сетями, сегодня работают многочисленные информационные сервисы, организована продажа медиаконтента и контроль лицевого счета в реальном времени.

Итак, на сегодняшний день налажено взаимодействие с:

- Биллинговой системой;
- Справочно-информационными сетями;
- Электронной почтой;
- Службой Web.

БИЛЛИНГ И УПРАВЛЕНИЕ УСЛУГАМИ

■ Операторы сотовой связи - не альтруисты, поэтому их услуги стоят денег. Тарифы на услуги и статистику по их использованию отслеживает биллинговая система. Технология

SMS предоставляет широкие возможности по работе с биллинговой системой оператора. Вот стандартные примеры взаимодействия абонента с БС:

- Запрос об остатке средств на лицевом счете.

Абонент сети может получить данные о состоянии своего счета в реальном времени. В зависимости от оператора (и тарифного плана) может быть выдана вот такая информация: средняя скорость расходования средств (и, соответственно, прогнозируемая дата отключения), факт приближения к по-

рогу отключения определенных услуг (или самой связи) и т.д.

- Прием платежей по картам. Отправив определенное сообщение (вида *101*(номер карты)#), абонент получит от оператора уведомление о пополнении счета или узнает об ошибке.
- Подключение и отключение услуг.

Возможность клиентов взаимодействовать со своими системами выгодно оператору: упрощается введение новых сервисов, оповещение абонентов и т.д.

СПРАВОЧНО-ИНФОРМАЦИОННЫЕ СЕТИ

■ Взаимодействие с информационными сетями позволяет абоненту получать любую информацию на экран своего мобильного телефона. Долгое время продажа информации была прерогативой операторов связи. Эти сервисы не рекламировались, и узнать о них можно было разве что прочитав "Справочник абонента". Плюс скудность инфо-меню: прогноз погоды, гороскоп и прочее. Со временем ситуация резко изменилась и основной продаваемой информацией стал медиаконтент. За последние три года российский рынок мобильного контента пережил бурный рост, и по состоянию на 2004 год его объем составил \$310 млн. Наибольшей популярностью пользуются мелодии, логотипы, Java-игры. К "медиаконтенту" относятся и интерактивные услуги: чаты, SMS-игры, потери и др.

Главное достоинство технологии SMS - возможность интеграции.



"SMS как пульс жизни", - гласит иностранная реклама сервиса

Несмотря на фантастическое разнообразие информации, получаемой с помощью справочно-информационных сетей, существует всего два режима ее поступления абонентам связи:

1. Пассивный.

Чаще всего это периодически рассылаемая информация, на которую (как правило) подписан абонент, - в основном новости, курсы валют, расписание определенных мероприятий, анекдоты и т.д.

2. Интерактивное взаимодействие.

"Общение" с инфо-базами с помощью коротких сообщений. При таком режиме можно обеспечить гибкое перемещение по базе данных для получения нужной информации. Таким образом могут быть организованы: расписание движения транспорта, биржевые котировки, мобильный банк.

ЭЛЕКТРОННАЯ ПОЧТА

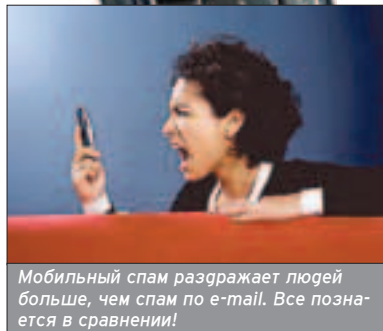
■ Хотя многие современные мобильные терминалы способны отправлять и принимать e-mail стандартными средствами SMTP, обмен электронной почтой посредством SMS-сервиса стал довольно популярным (самая развитая услуга - именно получение почты на мобильник). Технология обеспечивает следующие варианты обмена:

■ Отправка сообщения.

Абонент набирает адрес и текст сообщения и отправляет его так же, как и обычное SMS-сообщение. Доставка сообщения обеспечивается SMS-центром.

■ Получение сообщения.

Каждому абоненту сотовой сети ставится в соответствие некий электронный адрес. Поступающая на этот адрес почта направляется SMS-центром на "трубку" абонента. В зависимости от объема письма информация может приниматься полностью или частично. Сервис, как правило, можно настроить так, чтобы просто получать сообщения о новых письмах или краткую информацию (отправитель, дата, тема и др.).



Мобильный спам раздражает людей больше, чем спам по e-mail. Все познается в сравнении!

ИНТЕРНЕТ

■ Связка "SMS+интернет" позволяет любому пользователю, имеющему доступ к Сети, отправить сообщение/много сообщений любому абоненту сотовой сети абсолютно бесплатно и анонимно. Более того, есть возможность отправить сообщение от имени любого абонента. Также не проблема получать сообщения от абонентов на компьютер. Удобно? Да, особенно в ситуациях, когда нет доступа к мобильной связи (находишься ты вне зоны действия сети, например), но есть доступ к Сети.

Любая развившаяся технология рано или поздно привлечет внимание коммерсантов и будет эксплуатироваться ими. Если технология предполагает получение (обмен) информации, то она станет одним из инструментов получения прибыли и, соответственно, распространения рекламы. Когда-то такое превращение произошло с e-mail, и в итоге мы получили тонны спама, за который расплачива-

SMS-СПАМ

■ Возможность рассылать спам посредством SMS - "золотая жила" для рекламодателей и одновременно головная боль для многих (в перспективе всех) абонентов сотовых сетей. Число абонентов мобильной связи - более миллиарда. Это крупнейшая база данных, содержащая почти все возможные целевые аудитории, так что рекламировать можно что угодно. Еще один принципиальный плюс SMS-спама перед e-mail: не нужно собирать спам-листы. В отличие от агрессивной электронной почты, номера телефонов легко генерировать с большим "выходом годных".

Задачи SMS-спамера - максимальная эффективность рекламы, максимальный охват аудитории и максимально обеспеченная собственная анонимность. Посмотрим, как это реализуется.

Большинство операторов мобильной связи предоставляют возможность отправлять короткие сообщения со своего сайта. SMS-спамеры первой волны использовала этот факт, так как ни один оператор не следил за количеством отправленных сообщений. Позже появились ограничения на количество сообщений, отправленных с одного компьютера. Но что такое компьютер с точки зрения Сети? Правильно, это IP-адрес. Меняя IP-адрес, мы можем получить "индугульгенцию" на отправку еще некоторого количества сообщений. На этом основано большинство программ для массовой рассылки сообщений, в том числе SMSreklama.

Софтина позиционируется как "инструмент для интернет-маркетинга" и позволяет:

■ Массово рассылать SMS-сообщения на телефоны абонентов большинства сотовых сетей России и ближнего зарубежья.

■ Отправлять сообщения анонимно.

■ Генерировать базы данных телефонов целевой аудитории (в программе есть встроенный генератор номеров).

В будущем обещается поддержка многопоточности, поддержка SOCKS PROXY, расширение списка операторов. Кардинальный минус, как это чаще всего бывает, - цена в \$300.

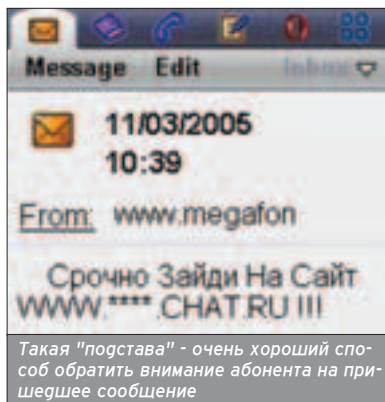
Более рациональный вариант - использование SMS-шлюзов (sms-gate). Количество сообщений здесь, как правило, не лимитируется, поэтому такие шлюзы живут недолго (однако свежие, то есть еще не убитые, всегда можно найти в Сети).

Для того чтобы использовать любой из двух обозначенных рецептов (не включая smsreklama), понадобится простая утилита, умеющая выбирать номер из базы, вставлять его в форму и отправлять сообщение. Кроме того, необходима софтина, умеющая перебирать проху-серверы (из списка) и направлять запросы через

Связка "SMS-интернет" способна на многое.



емся собственным трафиком, потерей времени в поисках нужного письма и собственными нервами. Для справедливости стоит сказать, что кое-кто из нас использует это явление себе во благо - за размещение рекламы люди готовы платить (аудитории спамеров могли бы позавидовать некоторые телевизионные каналы). И теперь, "благодаря" потенциалу взаимодействия SMS с другими сетями, обороты набирает...



них (например SocksChain). Из этого можно сделать главный вывод: SMS-спам - это просто!!!

Если сама техника рассылки сообщений не так уж сложна, то повышение эффективности разосланной рекламы - дело творческое, требующее креативности и плодovitости на идеи. Один из "классических" рецептов - подмена отправителя.

Давно существуют программы, которые позволяют в поле "номер отправителя" писать все что угодно - вплоть до набора букв, а не цифр. И этим пользуются! Как не воспользоваться шансом послать сообщения от имени известной фирмы? Кто не обратит внимание на такое? Судя по всему, в ближайшее время появится другая, прямо противоположная SMS-спаму возможность, - блокировка входящих SMS на выбранном номере телефона. Совсем недавно безызвестная компания Samsung запатентовала интересную технологию, которая позволяет удалить отосланное сообщение с телефона адресата. Для того чтобы это сделать, нужно отправить еще одно сообщение с командой на удаление (применимо только к непочитанным SMS'кам). Совершение таких деструктивных действий - дело будущего (пусть очень недалекого). Ог-

нако злоумышленники уже довольно давно пытаются "найти" мобильные аналоги компьютерных вирусов, которые можно было бы отправлять через короткие сообщения.

SMS-УБИЙЦЫ

■ В 2001 году в ПО некоторых телефонов была найдена одна довольно интересная уязвимость: при получении SMS-сообщения определенного содержания телефон выключался и не работал до тех пор, пока владелец не произвел удаление/установку аккумулятора. Возможность временно "убивать" телефон дистанционно стала широкоизвестной, в результате расплодилось слухи о том, что с помощью текстовых сообщений можно полностью вывести телефон из строя.

На самом деле все более прозаично. Доподлинно известно, что телефоны Nokia 3310/3330/6210 были "неравнодушны" к сообщению вида "0x04 0x05 0x015 0x8A". "Убийственным" для телефонов Siemens стало сообщение вида "%English" (кавычки - часть сообщения). Этой напасти оказались подвержены многие телефоны вплоть до 55-ой серии. Некоторые мудрецы приводят также другие тексты для "писем счастья" (в их числе "%Deutsch", "%Magyar" и др.), правда, их работоспособность не выяснена. Если не хочешь возиться с набором сообщений, можно использовать соответствующий софт, например Sms Attacker. Достаточно выбрать производителя аппарата, и программа пошлет по нужному номеру "убийствен-



Даже "телефон всех времен и народов" оказался уязвим к SMS-атакам

ную SMS'ку". Кроме того, есть приятная опция: рассылка SMS по списку и по диапазону адресов. Ничего не мешает провести акт массового убийства телефонов.

Как бы то ни было, SMS-убийцы уходят в прошлое и через некоторое время о них будет помнить только история. Однако найденные уязвимости показали всем, что, кроме очевидных перспектив развития, технология SMS таит в себе коварные "подводные камни".

SMS-спам -
это очень просто!



- НУ И ГДЕ МОЙ КРЯКЕР ИНТЕРНЕТА?



- А ТЫ ЗАПУСТИ .EXE-ШНИК ИЗ АТТАЧА!

НЕ ВЕДИСЬ НА ВСЕ ПОДРЯД, ЧИТАЙ **WWW.XAKER.RU**

Content:

60 Арсенал для охоты

Вооружись до зубов для вардрайвинга

66 Завоевание интернета

Атака на Cisco IOS

72 Взлом Пентагона

Как взломать закрытую сеть

78 Утилизирую мобильного друга

Обзор хакерских утилит для мобильных платформ

84 Трубки-сканеры

Все о взломе беспроводных телефонов

88 Вам звонят из милиции

Обзор софта для телефонных розыгрышей

90 За связь денег не берем

Все о бесплатных сервисах связи

94 Фрикинг по-жесткому

Фрикинг изнутри

Евгений Ермолаев aka Saturn (saturn@linkin-park.ru)

АРСЕНАЛ ДЛЯ ОХОТЫ

ВООРУЖИСЬ ДО ЗУБОВ ДЛЯ ВАРДРАЙВИНГА

Тяга к халяве всегда была одной из главных особенностей русского национального характера! Методы добычи чего-нибудь "просто так" совершенствуются день ото дня. Наиболее популярным объектом добычи у жителей "виртуальных миров" является интернет. Однако для удачной охоты во всемирной паутине тебе понадобится целый арсенал спецсредств. О них и поговорим.

ОСОБЕННОСТИ НАЦИОНАЛЬНОГО ВАРДРАЙВИНГА

У рядовых пользователей всегда было желание сделать свою жизнь как можно удобнее. Когда-то таким удобством стала незабвенная ОС Windows, и хакеры до сих пор пользуются этим обстоятельством. Примерно в это же время пользователю показали пряник под названием dial-up, который тоже не остался без внимания "заинтересованной общественности". Сейчас популярность завоевывают мобильность и свобода от проводов. Рядовые пользователи и крупные фирмы отдают все больше предпочтения беспроводным средствам для передачи данных. Как известно, "информация должна быть свободной", поэтому ничто не мешает пользоваться чьей-нибудь выделенкой бесплатно. При этом в качестве внутренних ресурсов хакер получает документы, пароли к почте и много другой полезной информации той сети, к которой подключился. Существует масса материалов, описывающих методы взлома защиты различных сетей (в том числе беспроводных), написано много тематического софта, однако я расскажу об основе любого взлома - оборудовании. Когда речь идет о "стационарной" работе хакера, все просто. В этом случае подойдет компьютер средней мощности, сетевая карта или, в крайнем случае, модем. Все остальное - дело софта и головы хакера. В случае с вардрайвингом существует несколько обстоятельств и условий, которые являются определяющими факторами при выборе оборудования. Часть из них объективны (дождь, снег, жадность милиции), часть - зависит только от расположения конкретного вардрайвера.

Итак, выделим три главных правила, которые желательно соблюдать при выборе оборудования:

●. Мобильность

Вардрайвер почти обречен на скитания по городу и поиск беспроводных сетей, кото-

рые могут оказаться полезными для него. Чтобы эти скитания доставляли как можно меньше неудобств, необходимо позаботиться о комфортном перемещении и максимальном удобстве используемой вычислительной техники. По вопросам перемещения в пространстве обращайся в автомобильные издания. А по поводу вычислительной техники важно соблюсти следующее: это должны быть устройства с минимальным весом и работающие автономно.

●. Незаметность

Любой человек, совершающий противозаконные действия (статью 272 УК РФ еще никто не отменял), должен позаботиться о своей безопасности. В данном случае - привлечь как можно меньше внимания, поэтому попросишься с параболическими антеннами (хотя их использование дало бы просто уникальные возможности), стационарными компьютерами, костюмами Микки-Мауса и прочими вещами, которые выделяют человека из толпы. Из этого правила (как впрочем, из любого) есть одно довольно интересное исключение, но о нем ниже.

●. Контроль местоположения

Контроль возможности определения своих координат в пространстве. Это правило может пригодиться в двух случаях: жадна



С помощью подобной антенны можно значительно расширить географию поиска сетей

Если хочешь остаться незамеченным - попросишься с параболическими антеннами :).

вернуться на "места боевой славы" и желание как можно скорее освободиться от опеки соответствующих органов. Это основные правила, которые рекомендуется использовать вардрайверу. Однако каждый может (а значит, должен?) подкорректировать и дополнить все вышесказанное исходя из своих внешних обстоятельств. Например, можно носить с собой удостоверение работника ЖЭКа, чтобы в любой нужный момент попасть на крышу жилого дома и тем самым добиться лучшего приема сигнала. Пользуясь простыми правилами и соображениями здравого смысла, попробуем подобрать оптимальный набор инструментов для занятий вардрайвингом.

РУЖЬЕ, БРЕЗЕНТОВЫЙ ПЛАЩ...

■ Для продуктивной охоты за беспроводными сетями можно подобрать несколько разных комплектов оборудования, но в большинстве из них будет входить:

Ноутбук

■ Наверное, не стоит лишний раз расписывать роль ноутбука во взломе сети :). Если же у тебя остались сомнения по поводу его необходимости в данной затее, почитай www.thg.ru/network/20050806/print.html. В данном обзоре больше всего внимания уделено моделям с самым продолжительным временем автономной работы, а также ноутбу-



Фирменный дизайн от IBM (модель X40) - классика жанра

кам с наилучшим соотношением "вес-возможности". Итак, какой же ноутбук нужен вардрайверу? Вот несколько вариантов: IBM ThinkPad X40, Fujitsu-Siemens LifeBook S7010 и Asus M3700N.

Ноутбуки от IBM являются образцом легендарной надежности, почти идеального баланса производительности и мобильности. В этом смысле ThinkPad X40 - не исключение. Только вдумайся: 7,5 часов автономной работы от стандартной батареи позволит работать почти полный день, а ночью ставить компьютер на зарядку (время зарядки - 3,5 часа). Благодаря удивительной легкости и компактности (вес 1,23 кг, габариты 268x211x21 мм), а также довольно высокой производительности (Intel Pentium M 1,2 ГГц, 512 Мб DDR SDRAM, видео Intel Extreme Graphics 2 и жесткий диск на 40 Гб) данный ноутбук, возможно, станет идеальным вариантом для вардрайвера. Однако если будет постоянно нужен оптический дисковод или большое количество портов, то данный ноутбук (и все машинки такого класса) уже не является хорошим решением, поскольку с док-станцией компьютер сильно прибавляет в весе. И тут возникает смысл присмотреться к Fujitsu-Siemens LifeBook S7010.

Данная модель также претендует на звание ноутбука с идеальным балансом производительности и мобильности. При весе 1,77 кг LifeBook S7010 »



Приятный дизайн плюс отличная эргономика - Fujitsu-Siemens LifeBook S7010

Ноутбуки IBM - практически идеальный баланс производительности и мобильности.

РАСЧЕТ ДАЛЬНОСТИ СВЯЗИ ДЛЯ БЕСПРОВОДНЫХ УСТРОЙСТВ

■ У любого вардрайвера рано или поздно возникает вопрос: как узнать максимальное расстояние, на котором может быть расположена ломаемая точка доступа. И главное: как увеличить это расстояние? Для этого нам нужно обратиться к физическим законам распространения радиоволн, которые, кстати, еще никто не отменял. Для определения дальности связи рассчитывается суммарное усиление тракта и по графику определяется максимальное расстояние.

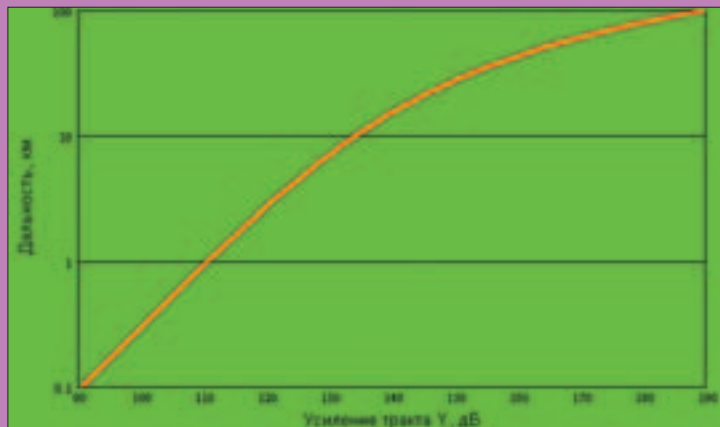


График для расчета дальности по суммарному усилению тракта

Для определения суммарного усиления тракта необходимо знать следующее: мощность передатчика (P), коэффициент усиления передающей и приемной антенны (Gt и Gr соответственно), чувствительность приемника (Pmin), потери в коаксиальном кабеле с обеих сторон (в нашем случае ими можно пренебречь). Тогда формула имеет вид: $Y = P + Gt + Gr - Pmin$. Стоит заметить, что все эти значения должны быть выражены в децибелах (дБ). Для того чтобы перевести милливатты (мВт) в децибелы, нужно взять десятичный логарифм числа и умножить его на 10. Для тех, кому лень считать, хороший калькулятор для расчета радиолинков - www.tayle.com/calc.php.



Asus M3700N - идеальный помощник для бизнес-пользователя. А как насчет вардрайвера?

обладает 14-дюймовой матрицей, оптическим приводом и большим количеством разъемов: 4x USB, PS/2, LPT, D-Sub, DVI, COM, RJ11. Модульный отсек, в который может быть установлен оптический привод (по умолчанию), жесткий диск или второй аккумулятор - очень существенные плюсы данной машинки. Время автономной работы несколько меньше, чем у предыдущего объекта тестирования, - пять часов. Похоже, в своем классе данный ноутбук является одним из лучших. Недостатков немного: матрица и цена. По поводу первой, было бы более правильным установить матрицу с разрешением 1400x1050 (SXGA+). Цена - \$2200 - без комментариев. Стоит ли таких денег данный девайс? Это можно понять, посмотрев на 14-дюймовые ноутбуки в ценовой категории "до \$1500".

Asus M3700N относится к серии M3, которая позиционируется производителем как "Идеальный помощник для бизнес-пользователя: высокопроизводительный процессор, матрица с высоким разрешением, возможность установки второй батареи, небольшой вес и стильный дизайн". Сразу стоит обратить внимание на матрицу: 14,1" с разрешением

НЕ ТОЧКОЙ ДОСТУПА ЕДИНОЙ

■ По большому счету, вместо точки доступа можно использовать PCI-адаптер стандарта 802.11b/g и усилитель. Более того, существуют переходники со встроенным усилителем до 200 мВт. Однако при использовании точки доступа выигрыш не столько в мощности, сколько в разнообразии используемых средств. Почти все точки доступа ценовой категории "от \$100" могут работать в нескольких режимах, имеют DHCP-сервер, а также имеют режим hide, что очень важно для личной безопасности.

Для полноценного поиска нужен внешний Wi-Fi-клиент с выходом на внешнюю антенну.

SXGA+(1400x1050), что нечасто встретишь в ноутбуках данной категории. Дизайн действительно стильный, однако качество сборки несколько хуже двух вышеназванных моделей (Asus, конечно, уважаемая марка, однако до IBM ей далеко). Вес довольно небольшой - 2,3 кг, то есть на 500 грамм больше, чем Fujitsu-Siemens LifeBook S7010. Что касается портов вывода (это один из "козырей" Asus), четыре порта USB 2.0, один слот PCMCIA type II, порт LPT и выход на внешний монитор, разъем i-Link (IEEE-1394), инфракрасный порт. А вот беспроводная связь подкачала: всего лишь 802.11b. Обозначенное время работы от батареи - четыре часа, однако это не соответствует действительности. При "офисном режиме" работы ноутбук выдерживает примерно три часа, что является довольно средним показателем.

Вердикт: качественный, довольно легкий ноутбук за небольшие деньги.

Подводя итоги, можно сказать, что все три представленные здесь модели ноутбуков имеют право называться "лучшим выбором для вардрайвера". Какой больше подходит тебе, решай сам! Стоит, однако, сказать, что чего-то в данном обзоре не хватает. Время поправить это недоразумение, представив еще одну модель. В этот раз для любителей Apple - PowerBook G4.

Данный девайс несколько не вписывается в правило №2 ("Незаметность") - он слишком сильно отличается от ноутбуков intel. Однако если для тебя "Think Different" - не пустые слова, это то, что нужно. Посмотрим, что предлагает "яблоко" для нужд рядового взломщика беспроводных сетей. Начнем с того, что процессора PowerPC хватит для решения большинства задач. У PowerBook отличная матрица, яркая и с приличными углами обзора. Вес ноутбука несколько великоват - 2,1 кг (против 1,23 у IBM), зато здесь "отдельная" видеокарта и винчестер на 60 Гб. С точки



Пожалуй, по части дизайна ноутбуки Apple (модель PowerBook G4) не имеют конкурентов



Навигатор Garmin E-Trex Legend C имеет большой цветной дисплей и подключается по USB

зрения аппаратной части - очень хорошая машинка для вардрайвера. Однако своеобразный софт делает решение такой задачи нетривиальным. В общем, пусть этот вопрос останется на совести любителей Apple. Остается добавить, что цена на сие чудо компьютерной техники - около \$2000.

ВНЕШНИЕ "НАСАДКИ"

■ Какой бы замечательной вычислительной машиной ты ни обзавелся, глядя того чтобы взломать беспроводную сеть, нужно... найти ее. Эффективный радиус охвата у встроенных Wi-Fi-адаптеров - 100 метров. Этого вполне достаточно для работы в офисе, однако для полноценного поиска и поддержки нормального радиопинка - едва ли. Это значит, что нам понадобится внешний Wi-Fi-клиент, причем с выходом на внешнюю антенну. Таким клиентом может быть либо сетевая карта, либо точка доступа с режимом Wireless Client.

Подходящие сетевые карты бывают двух форм-факторов: PCMC и подключаемые по USB. Первые удобны с точки зрения их компактности, однако к ним неудобно подключать внешнюю антенну. Переходник, в народе именуемый pig-tail, с довольно большим усилием отключается от сетевушки. С другой стороны, если планируется использовать мощную антенну, использование PCMC-карт - единственный выход. Таких карт на сегодняшний день очень много, вот самые яркие представители:

Lucent ORINOCO WaveLAN Turbo 11

■ Данная карточка совместима со стандартом 802.11b, однако при этом мощность передатчика 15 дБм - один из лучших показателей в своем классе. При работе на скорости 1 Мбит/с производитель обещает дальность связи до 540 метров. Интерфейс карты - PC Card Type II Extended. Цена карты составит около 60-ти вечноезеленых, что довольно дорого.

Cisco AIR-LMC340

■ Cisco - крупнейший в мире производитель сетевого оборудования. Однако, судя по всему, он отличается здоровым консерватизмом, что проявляется, прежде всего, в небольшом ассортименте беспроводной продукции. Представленная PCMC-карта уникальна. Она не имеет выхода на внешнюю антенну. Встроенная антенна имеет коэффициент усиления 2,2 дБ. Но здесь есть что усиливать: мощность передатчика составляет 100 мВт (20 дБ), а в PCMC-картах почти невозможно встретить это. Более того, такая мощность редко встречается в точках доступа. К сожалению, карта работает в стандарте 802.11b. Цена гейса кусается - ~\$200.

Кроме PCMC-карт, выход на внешнюю антенну имеют некоторые особи сетевых карт, подключаемых по USB.



КПК начального уровня для выполнения стандартных задач (HP iPAQ hx2110)



Pretec CompactGPS - один из многих GPS-модулей формата CF

Нередко цена решения КПК+GPS получается примерно такой же, как у отдельного GPS-приемника.

Рассмотрение этих устройств выходит за рамки данной статьи, но их можно легко найти в Сети.

КОМПАС, ЗВЕЗДЫ...

■ Настоящий охотник за беспроводными сетями должен озаботиться определением координат, причем не столько своих, сколько объектов наблюдения. В любом крупном городе нашей необъятной Родины на сегодняшний день существует масса Wi-Fi-сетей. Запомнить их местоположение без соответствующего устройства нереально. Это насущное устройство имеет название - GPS-приемник.

Нас интересует устройство, которое можно подключить к компьютеру. COM-порт (большинство приемников подключаются именно по этому порту) не устроит: он встречается в сов-

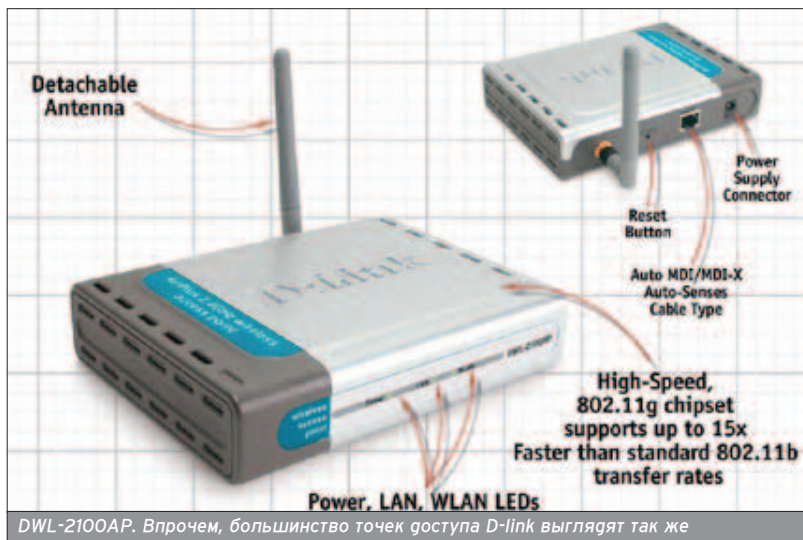
ременных ноутбуках слишком редко. Достойный пример - Garmin E-Trex Legend C.

При карманном размере (5,6x10,7x3,1 см) навигатор имеет большой цветной дисплей (176x200 пикселей; 3,3x4,3 см) и массу возможностей. Навигатор способен сохранять до 1000 путевых точек, 20 маршрутов по 125 точек, число точек в траектории - до 10 000. eTrex Legend содержит встроенный электронный компас, функцию выхода в заданную точку, функцию поиска обратного пути (TrackBack). Имеется возможность загрузки карт. Приемник неприхотлив и экономичен: для автономной работы в течение 36-ти часов ему требуется всего две AA батарейки, а в автомобиле - питание от штатного "прикуривателя" 12 В. В комплект входит интерфейсный USB-кабель, поэтому подключение к компьютеру не составит проблемы. Цена навигатора - \$425.

Существует еще множество GPS-приемников с разными возможностями, но все это отдельные специализированные устройства. Однако существует реальная альтернатива в виде КПК плюс GPS-модуль формата CompactFlash (есть GPS-модули под SD, однако разумнее оставить этот слот под память). Для такой связи подойдет любой современный КПК с разъемами под CompactFlash и SD/MMC. В случае когда "подходит все", принято акцентировать внимание на ценовых категориях low-end и hi-end, предоставив право выбора "золотой середины" читателю. Что ж, так и сделаем. »



Pocket Loox 718 - "голгоиграющий" КПК с широкими возможностями



Некоторые точки могут быть использованы в качестве беспроводных сетевых карт.

HP iPaq hx2110

■ iPaq hx 2110 - младшая модель в обновленной линейке HP, состоящей из трех моделей: HP iPaq hx2110, hx2410 и hx2750. Машинка комплектуется процессором Intel XScale PXA270 с частотой 312 МГц, набором памяти 64+64 (ОЗУ+ПЗУ). Этого должно быть достаточно для выполнения основных задач, однако про ресурсоемкие задачи придется забыть. Трансфлективный экран имеет разрешение 320x240 точек, что гораздо больше, чем у большинства GPS-приемников. HP iPaq hx 2110 имеет встроенный модуль Bluetooth, который может быть очень удобен при обмене информацией с ПК. Цена устройства - \$300.

Вердикт: если планируешь использовать КПК как GPS-навигатор, MP3-плеер и электронную записную книжку - трудно найти лучшее решение.

Fujitsu-Siemens Pocket Loox 718

■ Данный "карманный помощник класса люкс" является одним из самых дорогих КПК на платформе Pocket PC. Посмотрим, что же может предложить производитель за 530 американских президентов. Первое, что хочется отметить, - сенсорный экран с VGA-разрешением (640x480), это один из главных козырей современных КПК класса hi-end. Такой экран будет удобен не только при использовании GPS, но и практически во всех задачах, решаемых с помощью КПК. А расширить круг таких задач призван Intel XScale PXA272 - процессор, работающий на частоте 520 МГц, и набор памяти 128+64 (ОЗУ+ПЗУ). Pocket Loox 718 поддер-

живает полный набор коммуникаций: Wi-Fi, Bluetooth, IrDA, USB-хост. К последнему можно напрямую подключать USB-накопители и другие устройства. Причем покупать дополнительный кабель не придется - он поставляется в комплекте. Отдельно стоит сказать о времени автономной работы (очень важный показатель для варрайвера): на Pocket Loox 718 установлена батарея очень внушительной емкости (1640 мАч), которой хватает на 12 часов активной работы (при прослушивании музыки батарея "живет" 16 часов).

Вердикт: отличный девайс, сочетающий в себе самые последние достижения в области конструирования КПК.

Что касается GPS-модулей, их на сегодняшний день довольно много на рынке. Цена колеблется в районе \$80-150 в зависимости от таких параметров, как точность определения координат, наличие коннектора для внешней антенны и прочее. В общем, при использовании КПК начального уровня цена решения КПК+GPS получается примерно такой же, как у отдельного GPS-приемника.

СТАЦИОНАРНЫЙ ВАРДРАЙВИНГ


■ Какие бы устройства ты ни использовал, "классический" вардрайвинг предполагает перемещение по городу в поисках беспроводных сетей. Но кто сказал, что это единственный способ получить доступ к "вражеской" сети? Есть другое решение. Как говорится, если вардрайвер не идет к сети, сеть идет к вардрайверу. Описываемый ниже способ подойдет самым от-

чаянным охотникам за чужой информацией. Итак, суть способа состоит в том, чтобы из дома (офиса, конспиративной квартиры) вести поиск беспроводных сетей и заниматься их взломом (а впоследствии пользоваться интернетом на халяву). Для этого понадобятся: стационарный компьютер или ноутбук, точка доступа, антенна.

ТОЧКИ ДОСТУПА

■ Задача - увидеть как можно больше беспроводных сетей из одной точки. Для того чтобы решить эту задачу, требуется создать как можно более широкую зону охвата собственной точки. Поэтому нам пригодится мощная точка доступа с возможностью подключения внешней антенны. Отличное решение - D-link DWL-2100AP. Это самая мощная двухдиапазонная точка в модельном ряду D-link в ценовой категории до \$150. В модельном ряду D-link есть более мощные точки доступа, которые, к тому же, не сильно отличаются по цене от выбранной (например DWL-3200AP). Однако только DWL-2100AP и DWL-2210AP имеют режим работы Wireless-client, то есть эти точки могут быть использованы в качестве беспроводных сетевых карт. Выбор пал на первую по причине ее низкой стоимости. Более того, данная точка доступа может работать в режиме "точка - много точек", поэтому ты получишь шанс обеспечить халявным интернетом не только себя, но и своих грузей, живущих неподалеку. В комплекте с DWL-2100AP поставляется всенаправленная антенна с коэффициентом усиления 3dbi, однако ее нужно заменить на что-нибудь более стоящее. И здесь есть два совершенных разных решения: всенаправленная или направленная антенна. Первая дает охват по всем направлениям (360 градусов по горизонтали), однако радиус действия при этом довольно небольшой - до 1,5 км на прямой видимости. Направленные антенны дают больший охват, но при этом только в ограниченном сегменте. Такую антенну придется направлять несколько раз, до тех пор пока не будет достигнут желаемый результат.

УДАЧНОЙ ОХОТЫ!

■ Вардрайвинг - новое и довольно модное явление, которое может стать национальным видом спорта. Благодаря очень слабой защите беспроводных сетей это занятие стало уделом многих. Тем не менее, в любом деле есть специалисты и дилетанты. Специалиста видно сразу по набору инструментария. Кроме того, это занятие в России является незаконным, поэтому нелишней будет забота о собственной безопасности. В общем, выбирай свой "набор вардрайвера" и занимайся. 

СОДЕРЖАНИЕ CD

- Спец 07(56), Мобильные деньги
- Хакер 07(79)
- Железо 07(17)
- Мобильные компьютеры 07(58)
- Обновления для Windows за месяц

Кто-то удаленно воспользовался уязвимостью в твоём ПО? Не поможет firewall? Возвести настоящую "огненную стену" тебе поможет софт с диска - станешь настоящим секьюрити-гуром, узнай о безопасности клиентских приложений все!



НА ДИСКЕ:

Extras:

- Весь софт из номера:
- NetStumbler 0.4.0
- Resco Explorer 2005
- WarLinux 0.5 ISO
- Woron Scan 1.09
- ...и все-все, чтобы стать wardriver'om!

+ ко всему:

- War.Linux
- Windows без проводов
- On\$Mobile
- Свежий софт на каждый день
- Обновления Windows (9x/XP/NT/2000/2003)
- Спец 08(57), (anti)cracking
- Августовские номера: Хакер, Железо, MC

И ЕЩЕ: весь софт из номера!

В АТАКУ!

- Atelier Web Firewall Tester
- CRACKL@B Protected Storage Viewer 1.0 (+src)
- DNSTest 1.0
- FireHole 1.01
- Ghost 1.1
- LeakTest 1.2
- mbtest 0.2
- Nessus 2.2.5
- Nmap 3.81
- Outbound
- pcAudit 3.0.0.9
- pcAudit Leak Test
- Rainbow Crack 1.2 (src/scripts)
- Shadow Security Scanner 7.61
- Showtraf 1.5.0
- Surfer 1.1
- Thermite
- TooLeaky
- Wallbreaker 4.0
- winsock sniffer 1.76
- YALTA

РОЕМ ОКОПЫ

- AFICK 2.8-1
- 3proxy 1.5
- bstring-05302005
- DrWeb 4.32b (win/linux)
- Ethereal 0.10.12 (win/src)
- fwmon v1.1.0
- Kaspersky Anti-Hacker 1.7
- Kaspersky Anti-Virus Personal Pro 5.0
- Kaspersky Personal Security Suite 1.0
- Netstatp v2.0
- NetTime 2b7 (+src)
- Norton Antivirus 2005
- Norton Internet Security 2005
- pclnternet Patrol
- Proxomitron 4.5
- RKDetect (by Offtopic)
- Safe Run As
- SpyBot Search&Destroy 1.4
- Symantec AntiVirus for Handhelds

- Symantec AntiVirus for Series60/80
- TCPView v2.40
- WinPcap 3.0/3.1beta4

ИНСТРУМЕНТЫ

- MINGW 4.1.1
- putty 0.58 (+src +sftp-GUI)
- SecureCRT 5.0

СОФТ ОТ NONAME

- AutoPatcher XP Jul2005
- AWicons 9.2.0
- CrackDownloader 2.2
- DrWeb Browser plugin
- FeedReader 2.9.0
- NetView 2.92
- NINJAM 0.06
- Saver 1.2
- TaskSwitch XP 2.0.6
- TrueCrypt 3.1.a
- WAPT 3.0

Все это на
МУЛЬТИЗАГРУЗОЧНОМ CD!

Крис Касперски ака мышьяк

ЗАВОЕВАНИЕ ИНТЕРНЕТА

АТАКА НА CISCO IOS

Дыра, обнаруженная в маршрутизаторах Cisco и обнародованная на хакерской конференции Black Hat 2005 USA, наделала столько шума, что попала на страницы некомпьютерных газет. О ней много пишут, но все как-то в общих словах - никакой конкретики. Говорят о скором конце интернета, пугают захватом управления магистральных каналов связи, но исходных кодов эксплойта не показывают...



"Я считаю, что должен сделать то, что необходимо, - для страны в целом и национальной инфраструктуры в частности. У меня есть информация, что подрывные элементы уже активно занимаются диверсионной деятельностью против IOS. Я считаю необходимым рассказать всем, что да, IOS уязвима"

Майкл Линн

НЕМНОГО ПРЕДЫСТОРИИ

■ Все началось с того, что 26 января 2005 года телекоммуникационный гигант Cisco Systems обнародовал сообщение о дыре в своей новой операционной системе Cisco IOS, установленной на миллионах маршрутизаторов ("Cisco Security Advisory: Multiple Crafted IPv6 Packets Cause Reload" www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.pdf). Однако информация была неполной. Технические детали отсутствовали, и добыть их легальным путем не удавалось. Cisco явно что-то скрывала, пряча за туманными фразами, которые можно было трактовать и так, и эдак. Компания ISS (Internet Security Systems), специализирующаяся на информационной безопасности, решила на собственное расследование. Провести его поручили молодому (всего 24 года), но довольно продвинутому хакеру Майклу Линну (Michael Lynn). Шеф вызвал его к себе на ковер и спросил: "Можешь ли ты дизассемблировать ISO и разобраться с этой уязвимостью?" Ну, какой хакер ответил бы "нет"?



Cisco в боевой стойке



Могучий Cisco пошатнулся

Всю ночь Майкл пил кофре и пытался Cisco, но все-таки нашел... совсем грубую дыру, намного более коварную и могучую. К в общем-то безобидной перезагрузке (reload) добавился захват управления, а это уже серьезно. Представитель ISS немедленно позвонил в Cisco и сказал: "Хорошо, мы на 100% не уверены, что нашли тот же самый баг, о котором вы говорили, но наш баг гораздо более серьезен. Вы говорили, что возможен только отказ в обслуживании, но баг, найденный нами, допускает захват управления". Но там не поверили: "Ваш парень лжет. Невозможно выполнить shell-код на Cisco IOS". Майкла снова вызвали на ковер, приказав написать эксплойт: "Майкл, твой новый исследовательский проект есть Cisco IOS. Вынь да положи рабочий эксплойт для Cisco IOS, чтобы мы могли доказать, что те ретиски неправы".

Весь следующий месяц Майкл провел в ожесточенных расследованиях. Но даже имея работоспособный эксплойт на руках, ISS так и не смогла убедить телекоммуникационного гиганта, что его маршрутизаторы дырявы, как старый галош. Только 14 июня (то есть спустя три месяца!) они выслали инженера, который охарактеризовал себя как "архитектора IOS", чтобы закрыть этот вопрос раз и навсег-

да. Майкл в присутствии адвоката продемонстрировал работу эксплойта, натянув маршрутизатор по самые помидоры. Это повергло инженера в глубокий шок, но вместе с тем и развеселило: "Вау! Это круто!" Инженер ознакомился с черновой версией презентации, которую Майкл планировал продемонстрировать на конференции Black Hat, и укатил назад в свою компанию...

Руководство ISS отнеслось к презентации с большим одобрением: "Эй, ты хочешь выступить на Black Hat'e? Это нам нравится!" И порекомендовало распространить эксплойт среди всех тестеров компании: "Раздай его всем инженерам по продажам и всем бумажным тестерам". Но Майкл опасался за последствия: "Неужели вы не понимаете, что если вы сделаете это, то произойдет утечка?" Руководство, недоуменно пожав плечами, возразило: "Это проблема Cisco". Короче, все шло своим чередом. Презентация готовилась, а конференция приближалась. Неожиданно Майкла вызвали на ковер и под угрозой увольнения запретили упоминать факт дизассемблирования IOS. Затем его пригласил на пиво большой босс из Cisco и предложил отложить презентацию... на год - до тех пор, пока не будет выпущена новая версия операционной системы. Телекоммуникационный гигант осознавал угрозу, но отчаянно не хотел, чтобы ее осознали другие. Сошлись на том, что вместе с Майклом на сцену поднимется парень из Cisco, который скажет "пару слов", очевидно, обозвав докладчика лжецом, но Майкла это не беспокоило. Чтобы развязать себе руки, он уволился из ISS, решив прочитать доклад во чтобы то ни стало. Кто-то же должен предупредить народ об опасности!

Cisco осознавал угрозу, но отчаянно не хотел, чтобы ее осознали другие.



Cisco – самые мощные объекты хакерских атак

И доклад "The Holy Grail: Cisco IOS Shellcode and Remote Execution" был действительно прочитан! Эффект разорвал аудиторию взрывом атомной бомбы. Майклом заинтересовались Военно-воздушные силы, Агентство национальной безопасности и, конечно же, небезызвестный CERT. Они предложили ему подключиться к проекту по разработке антихакерской стратегии выхода из ситуации, но это уже совсем другая история. Вернемся к Cisco, чья реакция оказалась весьма неоднозначной. Во-первых, при содействии организаторов Black Hat она изъехала текст презентации из материалов конференции и конфисковала сопроводительные компакт-диски, заменив их точно такими же, но без доклада. Во-вторых, она обвинила Майкла во всех смертных грехах, в том числе в краже интеллектуальной собственности.

Сейчас Майкла ожидает куча судебных исков и разбирательств, а Cisco ведет охоту на всех тех, кто осмелился выложить копию доклада в интернет. К счастью, всемирная сеть живет по своим законам и любые попытки взять ее под контроль имеют обратный результат. Копии плодятся как кролики. Оригинальную презентацию

можно скачать, например, здесь: www.security.nnov.ru/files/lynn-cisco.pdf. А здесь лежит видеоролик, запечатлевший конфискацию дисков в самой "демократической" стране мира: downloads.oreilly.com/make/cisco.mov.

ДЫРА ДЫРЕ РОЗнь

■ Ошибочно считать, что go презентации оборудование Cisco считалось неуязвимым. Так думать мог либо некомпетентный специалист, либо маркетолог. Это не первая и не последняя уязвимость в IOS. Дыры в маршрутизаторах обнаруживались и раньше. За последние пять лет их накопилось около двухсот (!), в чем легко убедиться, посетив сайт CISO:

www.cisco.com/en/US/products/products_security_advisories_listing.html. А это только официально подтвержденные уязвимости! Неопроверженных, естественно, больше.

Существует множество эксплоитов, в том числе и с переполнением буфера, через которые засыпается shell-код, берущий маршрутизатор под свой контроль. Их можно найти практически на любом хакерском сайте. Например:

www.secureteam.com/exploits/50POLIFCAE.html, www.antiserver.it/Cisco-Exploit/ и т.д. В частности, еще три года назад в Cisco IOS обнаружилось переполнение буфера, приводящее к захвату управления, и был написан демонстрационный эксплоит, выставленный на конференции Black Hat 2002 Asia ("Attacking Networked Embedded Systems" - www.blackhat.com/presentations/bh-asia-02/bh-asia-02-fx.pdf), детально описанный в 60-м номере журнала Phrack ("Burning the bridge: Cisco IOS exploits"). Так что заслуги Майкла и масштабы угрозы сильно преувеличены. Линн не был первопроходцем. Обнаруженная им уязвимость примени-

Security Advisory	First Published	Last Updated
Cisco Security Advisory: IOS: Confusable Characters in CDP Messages	22-Aug-2006 17:00 GMT	24-Aug-2006 16:00 GMT
Cisco Security Advisory: Cisco IOS: Privilege Escalation Vulnerability in Protocol Stack	22-Aug-2006 17:00 GMT	
Cisco Security Advisory: Cisco: Cisco-Access: Authentication and API Access	17-Aug-2006 16:00 GMT	
Cisco Security Advisory: IOS: Config-Exec: Configuration	29-Jul-2006 16:00 GMT	11-Aug-2006 16:25 GMT
Cisco Security Advisory: Cisco: IOS: IPv6: Neighbor Handling Vulnerability	12-Jul-2006 16:00 GMT	16-Jul-2006 22:00 GMT
Cisco Security Advisory: Cisco: IOS: IPv6: Neighbor Handling Vulnerability	13-Jul-2006 16:00 GMT	
Cisco Security Advisory: Cisco: IOS: IPv6: ICMP: First Level of Service	13-Jul-2006 16:00 GMT	
Cisco Security Advisory: IOS: IOS: Authentication: Users	29-Jun-2006 15:40 GMT	01-Jul-2006 16:00 GMT
Cisco Security Advisory: IOS: IOS: IPsec: Tunnel: L2L3: Cisco: Vulnerability	11-May-2006 16:00 GMT	
Cisco Security Advisory: Vulnerabilities in Cisco: IOS: Source: Shell: Denial	06-Apr-2006 16:00 GMT	03-May-2006 16:00 GMT
Cisco Security Advisory: Confusable CDP Messages	12-Apr-2006 12:00 GMT	22-Apr-2006 22:30 GMT
Cisco Security Advisory: IOS: Vulnerability in Network IOS: Cisco: IOS: IPv6: Neighbor Handling	20-Apr-2006 21:00 GMT	13-Apr-2006 22:00 GMT
Cisco Security Advisory: Vulnerability in the Shared File Exchange: Shell Implementation	06-Apr-2006 16:00 GMT	
Cisco Security Advisory: Cisco: IOS: Malformed: L2L3: Denial of Service	06-Apr-2006 16:00 GMT	30-May-2006 16:00 GMT
Cisco Security Advisory: Cisco: IOS: IPv6: Neighbor Handling	03-May-2006	

Страничка официального сайта Cisco с описанием подтвержденных дыр

ма только к IPv6 (он же "интернет 2") и только к IP-пакетам, пришедшим с локального интерфейса. То есть хакнуть свой собственный маршрутизатор можно, а чей-то чужой, взятый наугад, уже нет. Вот тебе и власть над магистральными каналами, вот тебе и интернет, поставленный на колени.

Вопреки распространенному мнению, рабочий код эксплойта ни на конференции, ни в сопроводительных материалах так и не был продемонстрирован. Майкл не оставил никаких намеков, в каком направлении рыть, но это не помешало остальным хакерам повторить его подвиг, и дыра была переоткрыта, однако слишком рано говорить о каком бы то ни было практическом использовании. IPv6 войдет в нашу жизнь не через год и не через два, а к тому времени IOS будет повсеместно или практически повсеместно обновлена. Впрочем, кое-где IPv6 все-таки используется (особенно у апплинков), так что всегда можно найти подходящую "дырку".

СВЕТ И ТЬМА В КОНЦЕ ТОННЕЛЯ

■ Дыры в маршрутизаторах - вполне закономерное явление, которого следовало ожидать. Еще ни одному



Хакер, повторивший подвиг Майкла

Хакеры всколыхнулись и бросились штурмовать IOS.

МАЙКЛ ЛИНН СОБСТВЕННОЙ ПЕРСОНОЙ

■ Майкл Линн - известный хакер, специализирующийся на встраиваемых (embedded) системах, хачиньи ядра, обработке сигналов, криптографии, голосовой телефонии, дизассемблировании и сетевых протоколах. В последнее время сосредоточился на безопасности инфраструктуры критических каналов маршрутизации (securing critical routing infrastructures).



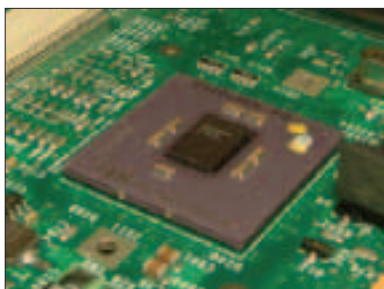
Майкл Линн, выполняя поручение ISS, обнаружил в Cisco гораздо более опасную "дыру"

разработчику не удалось реализовать TCP/IP без ошибок. Обнаруженные уязвимости - симптом тяжелой болезни. До сих пор маршрутизаторы работали лишь потому, что выпадали из поля зрения хакеров, которым намного более выгодно ковырять Windows/LINUX/BSD, а не возиться с Cisco. Оно и понятно. Традиционные операционные системы у каждого стоят на столе, а до маршрутизатора еще дотянуться нужно! Завладеть такой штукой может далеко не каждый, к тому же дизассемблирование IOS требует высокой квалификации и специальной подготовки. Нет никакой готовой информации, и каждый шаг требует кучи исследований. Вместо наезженной дорожки перед нами расстилается сумеречная тьма непроходимой местности, усеянной множеством ловушек. Впрочем, не все так сложно. Как говорится, что сделано одним человеком, может быть понято другим. Главное - даже не знания. Главное - это желание и настойчивость.

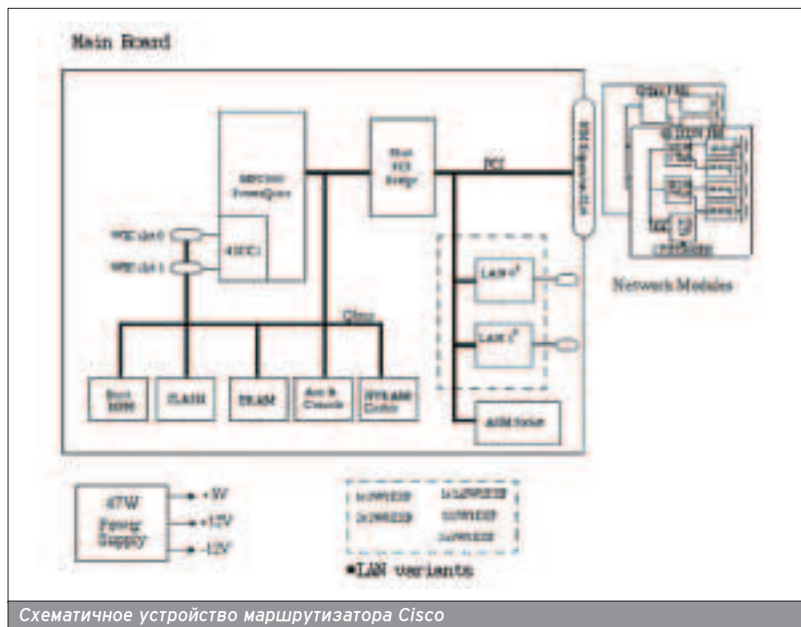
Cisco наступила на грабли. И скоро получит в лоб. Она выиграла тактическое сражение, но проиграла стратегическую войну. Попытка удержать информацию под спудом породила скандал, а скандал породил интерес. Хакеры всколыхнулись и бросились штурмовать IOS. "Причина, по которой мы это делаем, заключается в том, что кто-то сказал: «Вы не делаете этого», - заявил один из них. "Глинн не ограничился только идеями, хотя и не сообщил всех деталей. Но он сказал достаточно, чтобы люди могли понять, как им действовать, и они сделали это", - добавил другой. Всплеск интереса к IOS обещает принести множество новых дыр, так

Модель	Процессор
700	x86 (Intel)
100x, 160x	MC68360 (Motorola)
2500	MC68030 (Motorola)
2600	PowerPC MPC860 (Motorola)
3810	PowerPC MPC860 (Motorola)
3600	MIPS R4700 (IDT)
4000	MC68040 (Motorola)
4500,4700	MIPS R4700 (IDT)
7200	MIPS R4700 (IDT)
7200 NPE 200 и выше	MIPS R5000 (IDT и QED)

Таблица 1. Процессоры, использующиеся в маршрутизаторах Cisco



Процессор PowerPC, установленный в Cisco



Схематичное устройство маршрутизатора Cisco

что следующий год должен быть весьма "урожайным". Но как подступиться к маршрутизатору? Монитора нет, клавиатуры нет... Какие инструменты нам понадобятся? Какие машинные языки следует изучить? Короче, для начала исследований нам нужен хороший стартовый толчок.

ВНУТРИ МАРШРУТИЗАТОРА

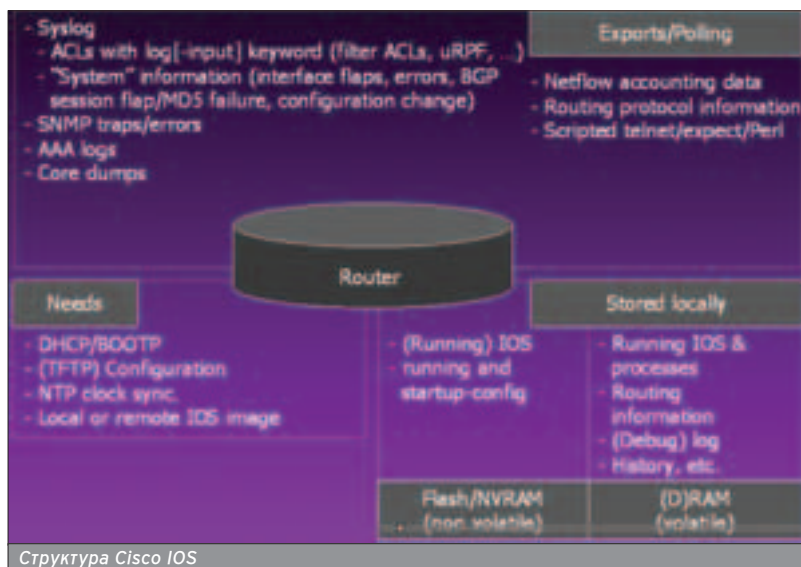
Архитектурно Cisco состоит из материнской платы, процессора, памяти, шины и интерфейса ввода/вывода. Процессоры довольно разнообразны. В зависимости от модели маршрутизатора, в них может быть установлен и традиционный Intel, и Мотороллер, и MIPS. В частности, на дизассемблированных фрагментах, приведенных в пре-

зентации Майкла, легко узнаются PowerPC, так что поклонники x86 отдыхают или в срочном порядке изучают ассемблеры для остальных платформ. Перечень используемых процессоров приведен в таблице 1.

Полностью укомплектованный Cisco несет на своем борту четыре вида памяти:

- 1. Энергонезависимую перезаписываемую FLASH, содержащую сжатый образ операционной системы (для сжатия используется библиотека zlib);
- 2. Энергонезависимую перезаписываемую NVRAM со стартовой конфигурацией (startup-config);

До сих пор маршрутизаторы работали лишь потому, что выпадали из поля зрения взломщиков.



Структура Cisco IOS

①. Энергозависимую перезаписываемую DRAM/SRAM (обычная оперативная память);

①. Энергонезависимую неперезаписываемую постоянную память типа BootROM, содержащую ROMMON-код, включающий себя процедуру начального тестирования POST, первичный загрузчик IOS - короче говоря, ПЗУ в его обычном понимании.

В усеченных конфигурациях NVRAM может отсутствовать. Подробности можно найти в материале "Cisco Router Forensics"

(<http://cansecwest.com/core03/CSWcore03-RouterForensics-DDoS-v101.ppt>).

Если процессор - сердце маршрутизатора, то операционная система - его душа. В оборудовании Cisco главным образом используются две операционные системы: CatOS и IOS (Internet Operation System), причем последняя намного более популярна, это операционная система реального времени, скомпилированная gcc и поозрительно похожая на BSD. Она основана на монолитной архитектуре ядра, то есть загружаемых модулей нет, во всяком случае, пока. По соображениям быстродействия в ранних версиях оси все процессы работали с одним и тем же образом (image) и разделяли единое адресное пространство (share memory space). Никакой защиты от воздействий со стороны одного процесса на код/данные, обрабатываемые другим процессом, не предусматривалось, что существенно облегчало написание shell-кода. Также имелся псевдомногозадачный планировщик невытесняющего типа "run to completion" (выполнение до завершения). Другими словами, если в NT операционная система сама переключает потоки без участия со стороны программиста, то в IOS поток должен явно вызвать системную функцию для передачи управления. А это значит, что shell-код может легко захватить власть над системой и не давать удалять себя, впрочем, радоваться по этому поводу слишком рано. Начиная с IOS-XR поддерживается и защита памяти между процессами, и вытесняющая многозадачность. (Подробности о структуре IOS можно почерпнуть из книжки "Inside Cisco IOS software architecture" издательства Cisco Press, которую легко найти в любом парнокопытном.)

Поверх ядра накинано множество программного обеспечения, занимающегося самыми разнообразными задачами, - от маршрутизации до "чистки" конюшен, причем в различных "железках" это программное обеспечение сильно неодинаково. И приложения, и ядро работают с одинаковым уровнем привилегий и имеют доступ ко всем системным ресурсам. Программные файлы представляют собой обыкновенные 32-битные статически линкованные ELF'ы с покоцанной отладочной информацией (ELF 32-bit

MSB executable, statically linked, stripped).

Управление маршрутизатором осуществляется через любой внешний порт - от COM-шнурка до telnet-терминала, работающего на TCP/IP. Интерфейс - командная строка. Среди команд есть как документированные, так и недокументированные (подробнее о недокументированных командах можно узнать у старика Гугла: запрос "undocumented IOS command" выдает тысячи ссылок, среди которых встречается немало полезных, в том числе www.xfocus.net/tools/200307/DOTU.pdf).

Вот, например, результат команды "show proc":

```
scep#show proc
CPU utilization for five seconds: 10%/4%; one minute:
14%; five minutes: 14%
PID QTY PC Runtime (ms) Invoked uSecs Stacks
TTY Process
 1 M* 0 1248 107 11663 2204/4000 1
Virtual Exec
 2 Lst 802DF16 34668 313 110760 1760/2000
0 Check heaps
 3 Cwe 801D5DE 0 1 0 1736/2000 0
Pool Manager
 4 Mst 8058B20 0 2 0 1708/2000 0
Timers
 5 Lwe 80BF04A 24 46 521 1448/2000
0 ARP Input
 6 Mwe 81F78F0 4 1 4000 1744/2000 0
SERIAL A'detect
 7 Lwe 80D935A 4 1 4000 1656/2000
0 Probe Input
 8 Mwe 80D8CD6 0 1 0 1744/2000 0
RARP Input
 9 Hwe 80CA966 80 89 898 3116/4000
0 IP Input
10 Mwe 80F41BA 16 322 49 1348/2000
0 TCP Timer
11 Lwe 80F5EB8 8 3 2666 3244/4000
0 TCP Protocols
12 Mwe 813785E 80 177 451 1588/2000
0 CDP Protocol
13 Mwe 80D5770 0 1 0 1620/2000 0
BOOTP Server
14 Mwe 8112C0 1356 1522 890 1592/2000
0 IP Background
15 Lsi 8121298 0 25 0 1792/2000 0 IP
Cache Ager
16 Cwe 80237BE 0 1 0 1748/2000 0
Critical Bkgnd
17 Mwe 802365A 12 5 2400 1476/2000
0 Net Background
```

```
18 Lwe 804E82E 16 4 4000 1192/2000 0
Logger
19 Msp 80456DE 80 1493 53 1728/2000
0 TTY Background
20 Msp 802345C 20 1494 13 1800/2000
0 Per-Second Jobs
21 Msp 80233F2 68 1494 45 1488/2000
0 Net Periodic
22 Hwe 80234DC 4 1 4000 1724/2000
0 Net Input
23 Msp 8023482 772 25 30880 1800/2000
0 Per-minute Jobs
24 Lwe 8109834 4 2 2000 3620/4000
0 IP SNMP
25 Mwe 815CE08 0 1 0 1712/2000 0
SNMP Traps
26 ME 811805A 0 26 0 1892/2000 0
IP-RT Background
27 ME 803B0F8 32 11 2909 2760/4000
2 Virtual Exec
```

Настоящим подарком для хакеров стала команда "gdb", вызывающая встроенный отладчик и поддерживающая следующие подкоманды:

```
gdb
debug PID /* не реализовано */
examine PID /* отладка процесса с указанным PID */
kernel /* отладка ядра, работает только с консоли */
```

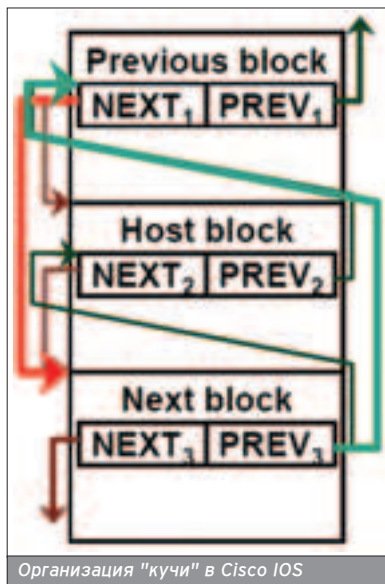
Однако, прежде чем использовать отладчик, его необходимо скомпилировать. Идем на www.gnu.org/software/gdb/download, берем копию свежее или, наоборот, постарее (предпочтительно использовать gdb-4.18, как наиболее протестированную) и говорим:

```
mkdir m68k-cisco
./configure --target m68k-cisco
make
```

В результате мы получим двоичный файл для платформы m68k. Для остальных платформ компиляция осуществляется аналогичным образом. Теперь можно начинать отладку! Консоль в это время будет нефункциональна, а весь обмен с отладчиком пойдет через его собственный отладочный протокол, описанный в исходном файле remote.c. На маршрутизаторе устанавливается серверная часть отладчика, а на терминале - кли-»

Команда	Назначение
g	вывести содержимое регистров процессора на терминал
GXX..XX	запись регистров, каждый байт регистров описывается двумя hex-цифрами. Регистры следуют во внутреннем формате gdb, а байты в регистры - в порядке, диктуемом процессором данного типа
mAA.AA,LLLL	чтение памяти, где AA..AA - адрес ячейки, а LLLL - глина блока
MAA.AA,LLLL:XX..XX	запись памяти, где A..AA - адрес ячейки, LLLL - глина блока, а XX..XX записываемые данные
c	продолжить выполнение программы
cAA..AA	продолжить выполнение программы с указанного адреса
s	выполнить следующую машинную команду и остановиться
sAA...AA	выполнить машинную команду с указанного адреса и остановиться
?	вывести last signal на терминал

Таблица 1. Процессоры, использующиеся в маршрутизаторах Cisco



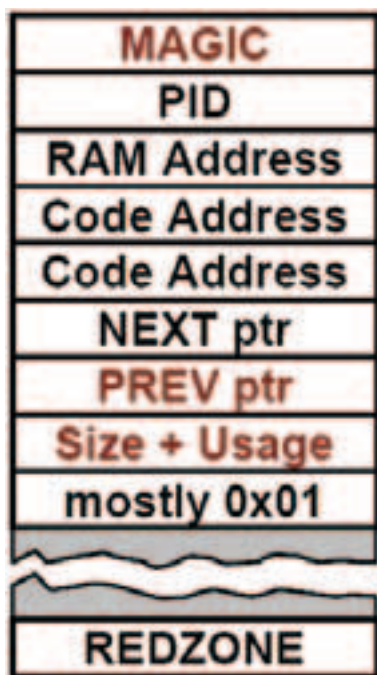
Организация "кучи" в Cisco IOS

ентская. Причем отладка ядра (подкоманда kernel) возможна только с консоли.

Дадим команду "gdb examine 18", где "18" - идентификатор отлаживаемого процесса (в данном случае "logger"). Подробнее обо всем этом можно прочитать на сайте команды XFocuz: www.xfocuz.net/articles/200307/583.html). Основные отладочные команды перечислены в таблице 2.

Для отладки желательно иметь символическую информацию, однако IOS - это закрытая система с закрытыми спецификациями (ну, не такими уж и закрытыми, если учесть, что это порт BSD, унаследовавший родимые пятна багов в zlib, ssh и SNMP), и символической информации не достать (во всяком случае, через легальные каналы), тем не менее, корпеть над дизассемблированием дампа не придется.

В мае 2004 года корпоративная сеть Cisco Systems была взломана и



Структура "кучи" в Cisco IOS

ПРОГРАММА ДЛЯ РАСЧЕТА КОНТРОЛЬНЫХ СУММ

■ Ни одна из версий IOS, работающих на платформе M68K, не использует аппаратные механизмы контроля памяти, предоставляемые MMU (Memory Management Unit - блок управления памятью), поэтому запись в кодовый сегмент проходит вполне беспрепятственно. Для защиты от непреднамеренного разрушения используются контрольные суммы. Каждые 30 или 60 секунд специальный процесс сканирует кодовый сегмент на предмет проверки его валидности и перезагружает маршрутизатор, если контрольные суммы не совпадают с расчетными. Однако против преднамеренной модификации эта "защита" уже не срабатывает, поскольку контрольные суммы легко пересчитать и поправить. Это можно сделать, например, так:

```
// (c) freedemon
#include <stdio.h>
unsigned char const hexchars[] = "0123456789abcdef";
char tohexchar (unsigned char c)
{
    c &= 0x0f; return(hexchars[c]);
}

int main(int argc, char **argv)
{
    unsigned char checksum; int count; char *command; char ch;
    if (argc <= 1) exit(1); printf("gdb protocol command: ");
    command = argv[1]; putchar('$'); checksum = count = 0;
    while ((ch = command[count]))
    {
        putchar(ch); checksum += ch; count++;
    }
    putchar('#'); putchar(tohexchar(checksum >> 4));
    putchar(tohexchar(checksum)); putchar('\n');
}
```

Разрушение "кучи" - наиболее распространенный баг маршрутизаторов Cisco.

исходные тексты системы IOS 12.3, 12.3t попали в руки хакера по кличке franz, который распространил через IRC небольшую часть сорцов (~2,5 Мб) в качестве доказательства. Самое интересное, что Майкл обнаружил бага именно в этом месте. Позднее усиливается тем фактом, что дизассемблировать IOS за ночь современно невозможно, а именно столько потребовалось franz'у для анализа.

К настоящему времени исходные тексты просочились в Сеть, и теперь их можно найти в любом парнокопытном. Полный объем архива составляет 800 Мб, и его перекачка на Dial-Up'e может занять несколько месяцев, однако она стоит того! Впрочем, отсутствие исходных текстов - это еще не преграда. IDA Pro в руки - и поехали.

ГДЕ И КАК ИСКАТЬ ДЫРЫ

■ Приемы поиска переполняющихся буферов в Cisco IOS мало чем отличаются от приемов для других осей, но в ней есть и свои особенности. Стек используется крайне редко, в основном она налегает на "кучу". По сообщениям Cisco, разрушение "кучи" - наиболее распространенный баг ее маршрутизаторов. Но вот о том, что причиной разрушения являются переполнения динамических буферов, она предпочла умолчать. Так что дыры есть! Методика переполнения "кучи" подробно описана в моей книге "Hacker shell-coding uncovered" и в статье "Once upon a free()" из 57-го номера Phrack'a. В IOS все блоки памяти объединены в двунаправленный список следующего типа:

ИСТОЧНИКИ

■ Вот три основных источника данных для поиска переполняющихся буферов: исходные тексты, обновления firmware и дампы памяти. Исходные тексты хороши тем, что их легко читать, но они не дают никакой информации о реализации системы на конкретном маршрутизаторе, к тому же их добыча, вообще говоря, не совсем законна. Firmware, как правило, упакован, и перед дизассемблированием необходимо распаковать его, причем сделать это не так-то просто, потому как Cisco слегка покалечила заголовки. Майкл использовал WinRAR, другие хакеры используют zlib и пишут свой распаковщик самостоятельно. Дампы памяти, создаваемый либо по команде, либо в результате краха системы, часто бывает сильно поврежден, и дизассемблировать его непросто. С другой стороны, он содержит реальный образ рабочей системы, поэтому наиболее точно отображает текущее положение дел.



Cisco IOS можно взломать и с ноутбука.

```
foo->prev->next = foo->next;
foo->next->prev = foo->prev;
```

При освобождении памяти выполняется следующий код, исключая текущий блок из цепочки занятых блоков:

```
*prev=*next;
*(next+20) = *prev;
```

Результатом этой операции становится запись в ячейки *prev и *(next+20) значений *next и *prev. Если в результате переполнения нам удастся подменить поля prev и next, мы сорвем банк, получив возможность писать произвольные данные/код в любое выбранное место. Эта техника (кстати, она разработана хакерами FX и KIMO) получила название "Uncontrolled pointer exchange", но, прежде чем воспользоваться ей, необходимо познакомиться со структурой кучи. Она довольно проста.

Вначале идет так называемый магический номер (MAGIC), равный AB1234BCh, а в самом конце - Красная Зона (REDZONE), равная FD1001DFh. Обе выполняют охранную функцию, и нельзя затирать их. Значение указателя prev проверяется перед освобождением, и потому должно быть валидно. В упрощенном виде проверка выглядит так:

```
if (next_block->prev!=this_block+20) abort();
```

Еще проверяется значение поля Size + Usage, старший бит которого определяет занятость блока (0 - свободен, 1 - занят), что создает проблемы при строковом переполнении, поскольку мы не можем располагать здесь нули, а минимальное значение,

которое мы можем получить, получается слишком большим (7F010101h). Однако тут есть обходной путь. Поскольку переполнение разрядной сетки никем не контролируется, использование значений типа 7FFFFFFh даст ожидаемый результат.

Остальные поля никак не контролируются и могут содержать любые значения. Короче говоря, написание shell-кода вполне возможно. Операционная система IOS использует статические адреса (а это хорошо!), но они меняются от одного билда к другому - вот это плохо. Поэтому, прежде чем атаковать жертву, необходимо тем или иным способом определить версию IOS (иначе червь сдохнет еще в зародыше), что можно сделать через CDP или SNMP.


Еще хуже, что IOS контролирует целостность кучи и автоматически перезагружает маршрутизатор, если цепочка ссылок (chunk linkage) оказывается разрушенной. За это отвечает специальный фоновый процесс, в зависимости от загрузки маршрутизатора пробуждающийся каждые 30 или 60 секунд. Именно он проверяет магический номер и красную зону. Так что shell-коду отпущено совсем немного времени. Конечно, 30 секунд - это целая вечность для процессора, за это время можно не только внедриться в целевое железо, но и заразить множество соседних маршрутизаторов. FX с KIMO предложили несколько решений этой проблемы, но все они оказались нежизнеспособными. Майкл был первым, кому удалось нащупать правильный путь, простой, как и все гениальное.

Оказалось, что процедура abort(), выполняющая перезагрузку, использует специальный флаг-семафор, предотвращающий повторное вхождение (по такому же принципу устройства защита от многократного нажатия <Alt><Ctrl> в NT). Если мы установим его в единицу, функция abort() тут же выполнит return без всякой перезагрузки. Ниже приведен ее ключевой фрагмент. (Впрочем, маршрутизатор все равно будет перезагружен через некоторое время, так как куча разрушена, так что shell-коду надо спешить.)

```
stwu    sp, var_18(sp)
mflr   r0
stmw   r29, 0x18+var_C(sp)
stw    r0, 0x18+arg_4(sp)
lis    r9, (crashing_already_ >> 16)
lwz    r0, (crashing_already_ & 0xFFFF)(r9)
cmpwi  r0, 0
bne    loc_80493D18 # return
```

На платформе MIPS операционная система IOS ведет себя иначе. На стадии инициализации она перепрограммирует MMU, запрещая модификацию кодового сегмента. Любая попытка записи в эту область вызывает крах системы и последующую перезагрузку маршрутизатора. Против непреднамеренной модификации этот механизм действует очень хорошо, но здравомыслящий хакер после пятого пива сможет легко обойти его. Идея заключается в отбоковании одной из физических кодовых страниц на область данных в записываемый регион. Аналогичный трюк, кстати говоря, используется и для модификации ядра NT. В частности, он применяется во многих брандмауэрах и утилитах Марка Руссиновича.

НАДОЛГО И ВСЕРЬЕЗ

■ Операционная система IOS распространена чрезвычайно широко: она встречается и в коммутаторах, и в маршрутизаторах, и в точках доступа, однако не стоит думать, что, обнаружив новую дыру, мы сможем взять все эти устройства под свой контроль: в них используются различные процессоры и различные версии IOS, так что с каждой железкой приходится воевать индивидуально. А вот хорошая новость. В отличие от серверов и персональных компьютеров, далеко не весь парк IOS-оборудования позволяет обновлять прошивку, а даже если и позволяет, далеко не каждый администратор об этом задумывается всерьез. И самое главное. Ты спросишь: "Взлом Cisco - это хорошо, но причем тут «мобильный взлом»?" Все очень просто: Cisco IOS можно взломать и с ноутбука :-). 

Крис Касперски ака мышцх

ВЗЛОМ ПЕНТАГОНА

КАК ВЗЛОМАТЬ ЗАКРЫТУЮ СЕТЬ

Настоящие хакеры не знают границ и проникают в закрытые сети различных могущественных организаций. Как они это делают? Продемонстрируем технику взлома на примере серверов милитаристского Пентагона, который вовсе не такой защищенный, как кажется.



ЗДЕСЬ НЕ ШУТЯТ

■ Информационная война - это действительно война, а не игра в салочки. Если хакера поймают, бритоголовые дяди будут долго и нудно надругаться над ним во все дырки в далекой американской тюрьме. Не секрет, что наша страна предпочитает не ссориться с Америкой и выдает информационных преступников по первому требованию. А даже если не выдает, сажает сама, так что, как ни крути, все равно геморрой. Первая задача хакера - обеспечение собственной безопасности. В статье "Безопасный взлом через GPRS", опубликованной в одном из последних номеров "Хакера", описываются основные идеи, позволяющие взять верное направление. Тем не менее, угроза раскрытия все равно есть, поэтому до приобретения боевого опыта лучше практиковаться на виртуальных сетях, которые можно протянуть в любом эмуляторе, например в VM Ware. Также недопустимо оставлять на взломанном сервере инициалы, любую компрометирующую информацию и т.п. И уж тем более недопустимо делиться подобными фактами с друзьями или оставлять записи в рабочем журнале или дневнике. Даже у стен есть уши. Впрочем, все это лирика. Перейдем к делу.

ПОЧЕМУ СТРАТЕГИЧЕСКИЕ СЕТИ УЯЗВИМЫ?

■ Протянуть защищенную сеть очень легко. Обычная витая пара или коксиал, отрезанный от интернета, - и хакеры сосут лапу. Но это в теории. На практике такая схема непрактична и нежизнеспособна. Пентагон не сосредоточен в одном-единственном здании, а представляет собой разветвленную организацию, сотрудники которой работают в различных странах и не могут мотаться за каждым документом к черту на рога. То же самое относится к коммерческим фирмам и корпорациям. Например, к концерну BMW или FORD. Развертывание собственной проводной сети было бы

идеальным решением с точки зрения безопасности, однако это не по силам даже такому могущественному государству, как США, поэтому приходится использовать уже существующие каналы связи, к которым относятся, в первую очередь, X.25-сети, спутниковая связь и, конечно же, интернет. X.25-сети - весьма популярные и надежные каналы передачи данных, владельцами которых, как правило, выступают крупные телефонные компании (например AT&T), опутавшие своими проводами весь мир. В основном они используются для связи между отдельными сегментами закрытой сети, расположенными в различных городах и странах. В Сети можно найти множество FAQ'ов по устройству и взлому X.25-сетей. Практически все нашумевшие взломы так или иначе связаны с X.25-се-

тями. Именно так был хакнут CityBank и множество других компаний. При наличии прямого выхода в Сеть достаточно иметь обыкновенную терминальную программу, однако в этом случае хакера смогут легко вычислить, поэтому приходится искать шлюзы из интернета в X.25. Чаще всего таким "шлюзом" становится слабо защищенная жертва, подключенная к X.25. Впрочем, при желании можно воспользоваться и более традиционными методами взлома.

Никакая организация не обходится без представительства в интернете. Для полноценной работы требуется, как минимум, web-сайт, электронная почта, реке ftp-сервер и прочие второстепенные сервисы (по вкусу). Опять-таки, с точки зрения безопасности, компьютеры, "смотрящие" в интернет, должны быть физически

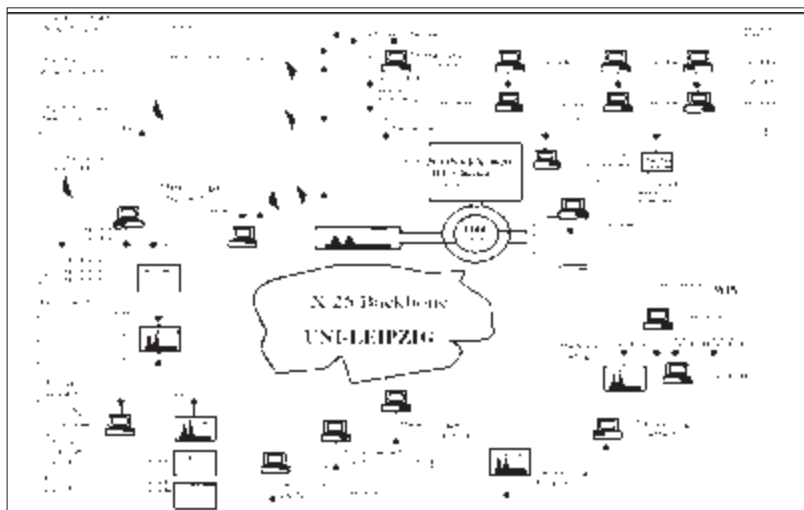
Практически все нашумевшие взломы связаны с X.25-сетями.



Пентагон - объект нашей атаки

ХИЩЕНИЕ ПАРОЛЯ

■ Как похитить пароль из закрытой сети? Это самое простое! Достаточно иметь e-mail человека, окопавшегося по ту сторону баррикады. Очень многие из нас имеют гурную привычку назначать одинаковые пароли на все ресурсы, хотя "в приличных домах" по соображениям секретности это ни в коем случае не рекомендуется! Но... запоминать множество различных паролей тоже нереально. Один мой товарищ стянул из закрытой сети интересный архив с жизненно важной информацией. Естественно, запароленный, причем запароленный не абы чем, а RAR'ом последней версии. Парольные переборщики отдыхают. Словарный поиск тоже не дал ничего интересного. После мытарств и терзаний решили обратиться за помощью к самой жертве. Грозить ей паяльником не стали, но пару интересных ресурсов посунули. Весь фокус в том, что эти ресурсы требовали аутентификации, то есть, проще говоря, ввода пароля. Очень часто жертва вводит свой любимый универсальный пароль. В крайнем случае, становятся известны привычки жертвы: выбирает ли она в качестве паролей словарные слова, и если выбирает, то по какому принципу. В данном случае паролями оказались женские имена с четырьмя цифрами на конце, представляющими, судя по всему, знакомых девушек с датами их рождения. Был составлен специальный переборщик, и меньше чем за день секретный архив удалось открыть.



Пример развертывания X.25-сети

Даже военные обычно огораживают закрытую сеть лишь брандмауэрами и парольными системами защиты.

отключены от "закрытой" сети, а весь обмен данными должен осуществляться только через съемные носители типа CD-R, причем перенос информации с интернет-компьютеров во внутреннюю сеть допустим только после тщательной проверки на наличие вредоносных программ, которые, как известно, могут внедряться не только в исполняемые файлы, но и в документы. Однако соображения удобства берут верх над разумом и даже военные организации обычно

ограниваются тем, что огораживают закрытую сеть брандмауэрами и парольными системами защиты. Физический доступ к ней из интернета все-таки остается, а интернет, как известно, представляет собой совокупность узлов, объединенных маршрутизаторами. Маршрутизатор - это обычный или специализированный компьютер, который может быть взломан, как и все остальное. Во-первых, многие маршрутизаторы поддерживают возможность удаленного управле-

ния через telnet и имеют вполне предсказуемые пароли словарного типа. Во-вторых, в них время от времени обнаруживаются ошибки переполнения буфера, приводящие к возможности захвата управления.

Взяв маршрутизатор под свой контроль, хакер может легко перехватывать трафик и даже модифицировать его! В частности, недавно в CISCO IOS уже обнаружилось две критические уязвимости (см. статью "Завоевание интернета" в этом номере), а сколько их там есть еще, никто не знает. Доступ ко многим секретным сетям открывается в результате контролирования трафика, причем это удается даже тем, кто не имеет представительства в интернете, но использует интернет-каналы для своих нужд. В частности, трансатлантический оптоволоконный кабель обслуживает уйму закрытых учреждений и потому представляет собой весьма лакомый кусок. У некоторых сотрудников (особенно внештатных) могут быть установлены модемы, принимающие входящие звонки, или уязвимое клиентское обеспечение. Не стоит забывать и о беспроводном оборудовании. Bluetooth, инфракрасные порты, Wi-Fi - все это может использоваться для проникновения.

ОСНОВНЫЕ СПОСОБЫ АТАКИ

■ Начнем с самого простого - с сотовых телефонов и ноутбуков.

Подобраться к зданию атакуемой организации на расстоянии прямой видимости (с небоскребов оно будет видно за несколько километров, а то и дальше). При этом быть вооруженным снайперской антенной (см. статью "Охота за голубым зубом", опубликованную в одном из последних номеров "Хакера"). В итоге получаем вот такие возможности: а) обнаружить уязвимые устройства; б) посмотреть содержимое записной книжки сотового телефона; в) осуществить звонок с сотового телефона жертвы или передать SMS от ее имени на любой номер; г) посмотреть содержимое файлов ноутбука и записать на него собственный shell-код. Разумеется, не всегда удастся осуществить задуманное в полном объеме. Однако количе- »



Развитие беспроводных технологий расширяет возможности для взломщика

ство успешных взломов этого типа стремительно растет, а окружающие нас устройства становятся все дырявее и опаснее.

Достоверно известно, что американские генералы активно используют ноутбуки от Compaq с Windows XP, в которой беспроводной стек реализован с грубыми ошибками, допускающими засыпку shell-кода, - со всеми вытекающими отсюда последствиями. Так же достоверно известно, что ряд американских крейсеров управляют Windows NT, дыры которой хорошо известны. Таким образом, взлом военных объектов - это не миф, а суровая реальность.

По опыту общения с отечественными военными могу сказать, что им категорически запрещено хранить какую бы то ни было мало-мальски значимую информацию на ноутбуке, но... они ее хранят, потому что так удобно. Что же говорить про американцев и всяких прочих банкиров. Они вообще с карманными компьютерами не расстаются. Знакомые автора не раз и не два вытаскивали через дырявый Голубой Зуб секретные файлы, просто направляя антенну в окна офисов или проезжающих мимо автомашин.

Основной недостаток такой атаки - необходимость прямого физического контакта с жертвой. Скажем, атаковать Пентагон из Урюписка уже не получится. А лететь в Америку чревато далеко идущими последствиями. В случае провала операции оттуда мож-



Хакерская параболическая антенна для ее перехвата



Передвижная станция спутниковой связи, используемая военными

АТАКА НА АДМИНИСТРАТОРА

■ Один из популярных способов проникновения в хорошо защищенную сеть выглядит приблизительно так: звоним администратору и сообщаем, что из абсолютно достоверных источников нам стало известно о готовящейся атаке, после чего раскрываем несколько туманных "деталей" в обтекаемых словах, вешаем трубку. Существует вполне твердая вероятность того, что администратор, пытаясь повысить безопасность своей системы, только добавит дыр (чем сильнее волнуется администратор, тем выше эта вероятность). Для того чтобы отвлечь внимание, можно прибегнуть к имитации атаки, выполняя различные бессмысленные, но целенаправленные действия. Известен случай, когда в ответ на мусор, направленный в 80-й порт, администратор одного интернет-магазина просто отключил web-сервисы, чтобы "спокойно" проанализировать ситуацию, поскольку считал так: лучше на время остаться без web'a, чем позволить хакерам проникнуть в локальную сеть и похитить конфиденциальную информацию. Естественно, простой web-серверов обернулся внушительными убытками, хотя никакой опасности на самом деле и не было.

но и не вернуться. Или вернуться уже седым стариком с широко разработанной задницей, что, очевидно, не входит в наши хакерские планы.

Спутниковая связь - другое дело. Вопреки расхожему мнению, спутник вешает не таким уж и узконаправленным пучком, покрывающим огромные территории. Кое-что можно ловить даже на ширпотребовскую тарелку, однако для серьезной работы потребуется специальное оборудование на несколько тысяч долларов или... куча свободного времени, чтобы сконструировать его самостоятельно. Перехватом чужих передач сегодня увлечены

многие. Конечно, в большинстве своем данные зашифрованы, так как наверху сидят не дураки, однако военный комплекс чрезвычайно инертен по своей природе и во многих местах использует морально устаревшие алгоритмы шифрования, которые вскрываются на современных процессорах за срок от нескольких дней до года, а ряд оперативных данных передается "открытым тестом" без (!) какой-либо шифровки. Не так давно мы с товарищем (его имя называть не буду: все равно ты его не знаешь) откопали очень интересный канал, передающий... прогноз погоды. Между



Коротковолновый трансивер, используемый для радиоперехвата



Еще один трансивер - попроще и подешевле



прочим, очень точный и хороший прогноз, намного более полный, чем можно найти в интернете.

В коммерческих же корпорациях процент незашифрованной информации очень велик, и он ловится на обычную спутниковую тарелку - нужно только перевести ее в "неразборчивый" режим. В основном попадают рекламные ролики и другая медиainформация, но иногда в хакерском ключе удается унести документы, касающиеся структуры внутренней сети или установленного на ней оборудования. Все это существенно облегчает дальнейший взлом...

Еще стоит упомянуть коротковолновый диапазон, используемый как любителями, так и профессионалами. Простой КВ-трасивер стоимостью в пару сотен долларов (особенно если это подержанный отечественный девайс военного образца) позволит перехватывать многие секретные передачи. Обычно "говорят" морзянкой, но также используют и человеческий голос, а в последнее время много информации передают в "компьютерном" варианте. Конечно, радиоперехват не имеет никакого отношения к локальным сетям, но от этого его популярность не уменьшается. В эфире можно услышать много такого, что не найдешь ни на одном из серверов Пентагона. Эфир - это настоящий Клондайк, тем более что он неподвластен традиционным средствам контроля и в нем можно найти множество грузей, в том числе хакеров. Например, проинструктировать своих союзников, как взломать уже упомянутые ноутбуки американских генералов.

Впрочем, все это слишком экзотичные способы атаки, большинство читателей вряд ли воспримет их всерьез, мало кто будет пользоваться ими на практике за неимением весьма дорогостоящего оборудования.

ПРОНИКНОВЕНИЕ ЧЕРЕЗ ИНТЕРНЕТ

■ Глотнув холодного пива (колы/кваса) и поплевав на лапки глян храбрости, подсымкнем трусы и наберем в браузере заветную строку www.pentagon.gov. Конечно, это только публичный сайт, но, во-первых, он связан с закрытой сетью, а во-вторых, даже сам по себе он представляет собой весьма нехилую мишень для атаки. Можно ли взломать его? Мы сейчас попробуем и тогда все узнаем!

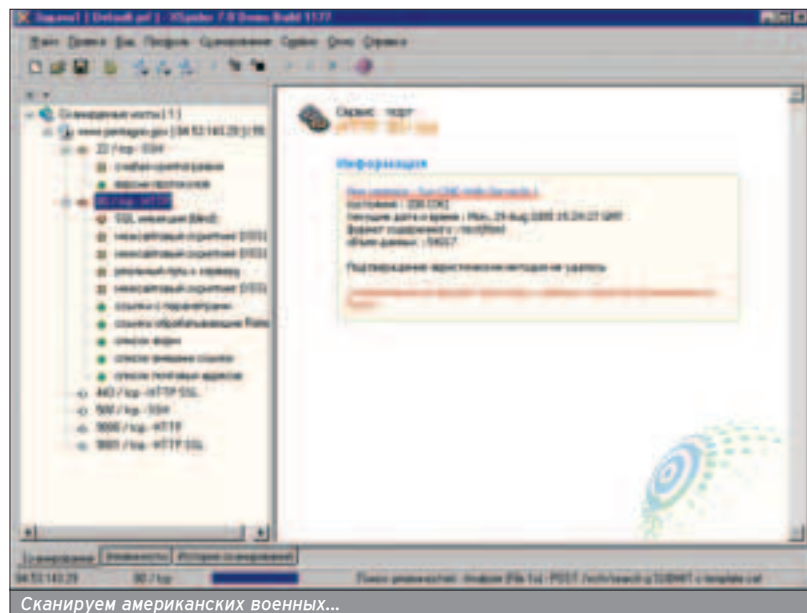
Для быстрого анализа обстановки лучше всего воспользоваться одним из многочисленных сканеров безо-

пасности. Я предпочитаю отечественный XSpider - постоянно обновляемый, мощный, удобный в работе и... бесплатный. Ну, практически бесплатный. Демонстрационная версия находит все известные ей уязвимости, но сообщает минимум информации о дыре. К тому же имеются следующие ограничения: отсутствуют потенциально опасные проверки на DoS-уязвимости, проверки содержимого web-серверов на предмет SQL-инъекций, инъекций кода, получения файлов, не содержат детали, отсутствует целый ряд проверок, использующих оригинальные эвристические механизмы, отсутствуют проверки, связанные с использованием различных словарей, и т.д. и т.п.

Тем не менее, для большинства задач этого вполне достаточно. Главное - определить направление, в котором следует рыть, выявляя все явно уязвимые сервисы, а остальное можно сделать и самостоятельно. Свежая версия лежит на сайте www.ptsecurity.ru. В zip-архиве она займет чуть больше 4 Мб (www.ptsecurity.ru/download/xs7demo.zip). Полноценную версию можно либо заказать на сайте, либо найти в любом парнокопытном.

К слову говоря, в военных организациях работают далеко не самые лучшие специалисты, поскольку по условиям труда это, скорее, похоже на тюремное заключение, а не на убежище души. Именно поэтому вероятность успешного взлома весьма высока. Коротче говоря, запускаем сканер, в меню "Правка" выбираем "Добавить хост" (или просто наживаем <Ins>), вводим имя атакуемого сервера (в данном случае www.pentagon.gov) или его IP- >>

Простой КВ-трасивер за \$200 позволит перехватывать многие секретные передачи.



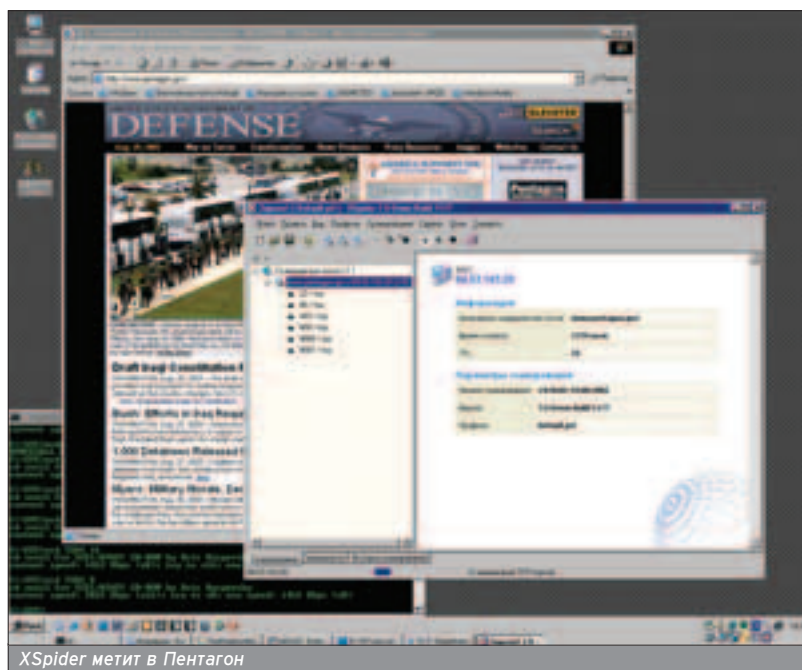
адрес (в данном случае 84.53.143.29). Ждем, что нам скажет XSSpider. Придется ждать довольно долго. Даже на шустрых DSL-каналах полный цикл сканирования занимает более трех часов, в течение которых нам придется пить кофе и открывенно скучать, тупо созерцая строку статуса, комментирующую происходящее...

Первым делом XSSpider определяет открытые порты. Их целых шесть: 22/TCP (SSH), 80/TCP (HTTP), 443/TCP (SSL), 500/TCP (SSH), 9000/TCP (HTTP) и 9001/TCP (HTTP SSL). Ради эксперимента можно подключиться к серверу по 9001-му порту, набрав в строке браузера `www.pentagon.gov:9001`. И это сработает! Правда, мы попадем на ту же самую страницу сайта, что и вначале, поэтому от такого взлома немного пользы. Но лиха беда начало! XSSpider определил тип SSL-сервера, в качестве которого используется SSH-1.99-Server-VI, основанный на OpenSSH Server, - его исходные тексты свободно лежат в Сети. Если повезет, то, основательно изучив их, найдешь одну или несколько ошибок переполнения буфера, впрочем, быстрый успех маловероятен. Можно угробить кучу времени - и все впустую. Лучше подождать, пока их не найдут другие, а затем быстро атаковать сервер, пока его не успели запатчить. Но мы же не хотим провести всю оставшуюся жизнь в ожидании? ОК, тогда идем дальше!

SSL-сервер поддерживает устаревшие версии протоколов 1.33 и 1.5, которые недостаточно безопасны и могут быть взломаны за разумное время. Однако для этого нам, во-первых, необходимо тем или иным образом перехватить трафик, а во-вторых, дождаться, пока на сервер не поступит клиент, использующий протокол устаревших версий. Довольно малоперспективное занятие... Лагну, ос-

ШАНТАЖ

■ Если попытки проникнуть в сеть, несмотря на все усилия, так и не возымели успеха, хакер может отвлечься на прямой шантаж сотрудников фирмы. Статистика показывает, что угроза физической расправы встречается довольно редко, а если и встречается, то в подавляющем большинстве случаев и остается лишь угрозой. Лигируют обещания рассказать ревнивому мужу (жене) о супружеской измене - неважно, имела ли она место в действительности. Для этого вовсе не обязательно устанавливать скрытые камеры или заниматься фотомонтажом - достаточно быть хорошим рассказчиком, умеющим убедить собеседника. Опасаясь распада семьи, многие из нас идут на мелкие (с нашей точки зрения) должностные преступления, оборачивающиеся, тем не менее, значительными убытками для фирмы. Второе место занимают угрозы убедить сына (дочь) жертвы XX/XY в том, что XX и XY - не его (ее) настоящие родители. В подростковом возрасте между детьми и родителями часто возникают серьезные конфликты, поэтому вероятность того, что ребенок поверит постороннему яде, а значит, нанесет себе тяжелую душевную травму, отнюдь не нулевая!



тавим SSL в стороне и возьмемся за web, который, как всегда, выглядит довольно многообещающим скоплением багов. Сайт Пентагона вращается под: Sun-ONE-Web-Server/6.1, а SunOS, по сути, является клоном UNIX'a. В ней намного меньше дыр, чем в LINUX'e, но намного больше, чем, например, в BSD. К слову сказать, использование рабочих станций от компании Sun - вполне типичное явление для любой крупной организации, и вполне реально получить доступ к ним (достаточно напоить пивом любого банковского администратора).

Сканирование web-сервера занимает львиную долю общего времени взлома, зато обнаруживает уйму любопытных подробностей. XSSpider обнаруживает шесть ошибок SQL-инъекций. Что такое SQL-инъекция? Это весьма коварная дыра, позволяющая формировать свои собственные запросы к базе и просматривать секретные данные. К сожалению, в демон-



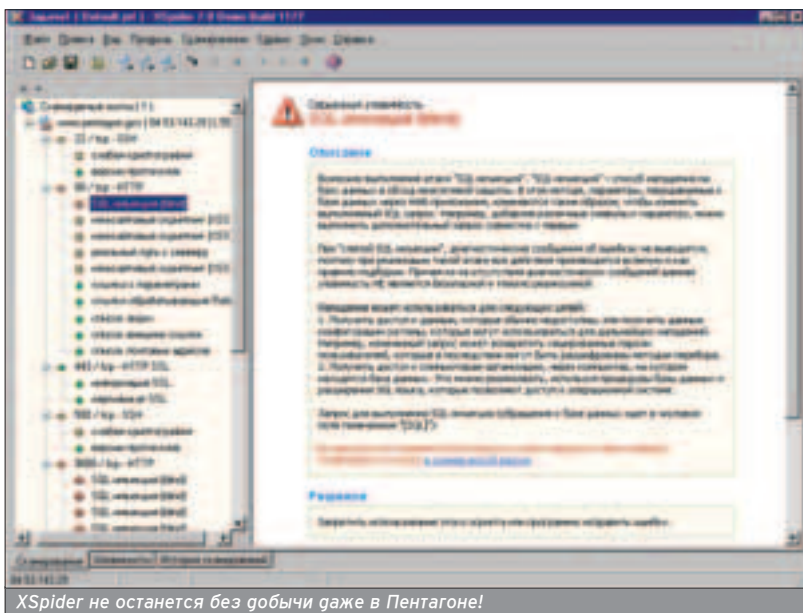
Свежую версию XSpider можно скачать с сайта www.ptesecurity.ru

XSpider обнаруживает шесть ошибок SQL-инъекций!

страционной версии отсутствует подробная техническая информация, и нам остается лишь гадать, как должен выглядеть хакерский запрос. Для удобства XSpider дает ссылку на коммерческую версию, а ниже - несколько ссылок со статьями по теме SQL-инъектига. Очень удобно! Щелкаешь и читаешь! Кстати говоря, если понять прошлогодний "Хакер", то в одном из номеров можно найти статью "База данных под прицелом", где все расписано.

Еще пентагоновский сервер подвержен межсайтовому скриптингу или, как его называют профессионалы, XSS (Cross site scripting). Проще говоря, это возможность вставить HTML-код в уязвимую страницу. Вряд ли получится добраться до секретных данных с его помощью, зато можно пе-

рехватывать пользовательские сессии или навязывать всем посетителям сайта поглужные данные, то есть производить дедфейс. Учитывая, что сайт Пентагона - это информационно-политическое лицо Америки, к которому обращаются новостные агентства всего мира, целостность его содержания очень важна. Хорошо продуманная геза может иметь далеко идущие последствия. Как всегда, XSpider приводит ссылки на статьи по теме кросскриптинга, которые будут полезны для анализа, но для определения формы уязвимого запроса потребуются приобрести коммерческую версию. Но мы же не террористы и не вандалы, правда? Вот и не будем пакостить! Тем более откуда у нищих студентов деньги?



XSpider не останется без добычи даже в Пентагоне!

Остальные дыры не так интересны. Из них можно упомянуть разве что успешно определенную версию и тип SSH-сервера, в качестве которого используется AkamaiGHost. Дополнительную информацию и исходные тексты можно найти в интернете, только вряд ли поиск переполняющихся буферов быстро увенчается успехом. Судя по всему, сеть Пентагона не защищена брандмауэром. Пинг и трассировка проходят легко. Следующий листинг приводится в качестве подтверждения:

Трассировка маршрута к 84.53.143.29 с максимальным числом прыжков 30

```
1 1650 ms 22 ms 22 ms 83.239.33.45
2 27 ms 31 ms 79 ms 192.168.15.220
3 34 ms 57 ms 27 ms 83.239.0.17
4 28 ms 27 ms 27 ms 195.161.158.25
5 149 ms 104 ms 144 ms Ind-bgw0-ge0-3-0-0-rt-comm.ru
[217.106.6.45]
6 111 ms 202 ms 111 ms 195.66.224.202
7 108 ms 107 ms 108 ms 84.53.143.254
8 159 ms 128 ms 155 ms 84.53.143.29
```

Трассировка завершена.

По современным меркам корпоративная сеть без брандмауэра (или с демократически настроенным брандмауэром) - это вопиющий факт и исклечение из правил. Впрочем, брандмауэр еще не помеха. Достаточно открыть "Хакер" со статьей "Преодоление firewall'ов снаружи и изнутри" и сломать защитную стену в пух и прах. То же самое относится к сканированию IP-адресов. Пентагон от этого никак не защищен. Можно просканировать подсеть целиком. Впрочем, она довольно однообразна, и ничего интересного в ней нет. В частности, узлы 84.53.143.27 и 84.53.143.28 держат открытыми следующие порты: 22/TCP (SSH), 80/TCP (HTTP), 123/UDP (NTP), 500/TCP (SSH) и 1935/TCP (TINCAN). Правда, при попытке подключиться к 80-му порту нас ждет глубокий облом. Вот и помись после этого туда, куда не просят. Как говорится, незванный гость хуже татарина.

ПРОСТО ПОСМОТРЕЛИ...

■ Конечно. Было бы наивно ждать от этой статьи полной демонстрации взлома военных серверов или закрытых сетей. Во-первых, к моменту публикации информация неизбежно устарела бы (админы же не только пьют кофе). Во-вторых, кто захочет подписывать приговор самому себе, расписавшись в совершении преступления? Фактически, мы ничего не сделали - только запустили готовую программу, явно не относящуюся к числу вредоносных. Никакого злого умысла у нас тоже не было. Просто хотелось посмотреть...

Иван Касатенко aka SkyWriter (sky@real.xakep.ru)

УТИЛИЗИРУЙ МОБИЛЬНОГО ДРУГА

ОБЗОР ХАКЕРСКИХ УТИЛИТ ДЛЯ МОБИЛЬНЫХ ПЛАТФОРМ

Как часто я сидел где-нибудь в кафе и буквально чувствовал, как волны в 2,4 ГГц пронизывают меня, как байты проникают прямо в мозг... Как я жалел тогда, что под рукой нет моего старенького десктопа, чтобы взять эти волны под контроль. Однако теперь его с легкостью заменит и мой мобильный гаджет! Вникай же в обзор софта, необходимого хакеру для взлома с помощью своего маленького друга!



SERIES 60

PuTTY для SERIES60

- Классический

PuTTY теперь доступен для твоих извращенных игр и на Series60. В общем-то, практическая ценность данного приобретения находится под достаточно большим вопросом, но как proof-of-concept - очень ничего. Так что если вдруг захочется поругать огромный мощный сервер с помощью твоего смартфона, то теперь у тебя есть такая возможность!



Все как и в настольном варианте: SSH v1/v2, Telnet и т.п. плюс небольшое количество глюков, видимо, вызванных портированием.

МОЩНА TELNET FOR NOKIA 3650/6600

■ Честно говоря, я бы постеснялся называть программу так. Остается надеяться, что ударение нужно ставить все-таки не на том слогое ;).

Это чудо может подключаться к *nix-серверу по Telnet/SSH и эмулировать VT220, используя при этом для ввода клавиатуру телефона. Что по-



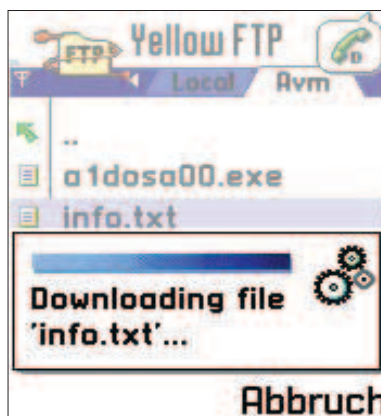
ХАКЕРСПЕЦ 10(59) 2005

казалось приятным, так это поддержка "ландшафтного" режима: экран 80*24 логично располагать именно в таком положении. Еще один плюс - небольшие размеры программы.

Обнаружен только один минус - \$25 за использование программы.

YFTP 1.35 S60

■ В названии четко прослеживается знакомая комбинация из трех букв. Нет, не та ;).



Я говорю об FTP. Да, действительно, это FTP-клиент для твоего смартфона. С этой штуковиной открывается целая куча возможностей по исследованию сетей: от безобидного скачивания софта, до... ммм... изменения HTML-кода страничек сайтов. Поддерживает активный и пассивный режим работы, FXP (протокол передачи файлов с сервера на сервер без участия клиента). Естественно, программа сохраняет параметры серверов, к которым ты подключаешься, так что тебе не придется каждый раз с лицом мученика набирать IP'шники с клавиатуры смартфона (благо IPv6 пока не вошел в моду).

Бонус этой программы в том, что она выполняет и роль простенького локального файл-менеджера - мелочь, а приятно!

NETTOOLS 0.2

■ Софтина представляет собой миглет SSHv1-клиента. В общем, простое ПО, позволяющее быстро и легко уп-



равлять угаленным сервером по зашифрованному каналу. В качестве бонуса содержит в одном флаконе утилиты ping, whois и traceroute - очень и очень неплохо для начала, верно?

NETFRONT 3.2 S60

■ При помощи этого приложения ты получаешь быстрый и относительно удобный доступ к обычным HTML-страничкам со своей мобилы. Для этого используется какая-то фирменная технология рендеринга HTML, позволяющая без проблем отображать крупные страницы на маленьких экранчиках обычных смартфонов. Но основной плюс браузера состоит даже не в этом - показывать HTML-странички должны уметь все. Основной плюс netfront в том, что он позволяет отображать страницу в упрощенном формате, то есть получить представление об ее структуре еще до того, как загруз-



ХАКЕРСПЕЦ 10(59) 2005

зятся "тяжелые" элементы (графика, анимация, любимые MID-файлы, веселые наигрывающие на фоне).

Браузер поддерживает все основные стандарты, принятые в сообществе WWW: HTML 4.01, CSS, sHTML, XHTML 1.1, SSL и ECMA Script (JavaScript 1.5).

OPERA 8.0 S60

■ Нужно ли представлять приложение с таким именем? В борьбе с IE оно стоит в одном эшелоне, прямо совсем рязышком с Mozilla.

Для тех, кто водит тяжелую бронетехнику, говорю, что это известный, быстрый и продвинутый HTML-браузер. Только теперь (и вновь) для Series 60.



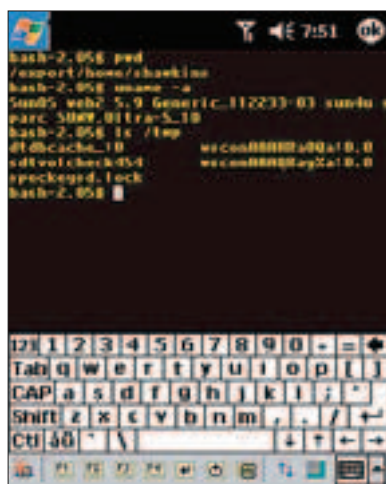
Основная фишка Opera - это уникальная система SSR (Small Screen Rendering), позволяющая по-настоящему просматривать странички на мобиле без дополнительного масштабирования и горизонтальной прокрутки.

Браузер поддерживает новый CSS2, поэтому позволяет просматривать web-странички, которые оптимально используют цветные экраны смартфонов.

POCKETPC

MToken 3.2.1

■ Программа представляет собой классический терминальный/Telnet-клиент. Естественно, специально заточена под КПК, даже мышь поддерживает в Midnight Commander'e, что



является приятной неожиданностью для подобных софтин. Помимо обычного Telnet, мы можем: устанавливать прямые подключения по последовательному порту, передавать и принимать файлы через XModem с контролем целостности, вести лог обмена данными, осуществлять автоматический логин и т.п. mToken умеет эмулировать терминалы VT100/VT102/VT52/ANSI. В общем, если ты фанат хаксорских BBS или просто влюбился в mToken как в Telnet-клиент, то это 100% MustHave.

WI-FI COMPANION 2.5.1

■ Настоящий компаньон настоящего wardriver'a. Все просто и наглядно: все свойства подключения и набор дополнительных утилит как на лагони!



Wi-Fi Companion, по утверждению разработчиков и по моей проверке, порадует тебя целой кучей разных фишек, в число которых входят:

- Wi-Fi Finder - поиск точек доступа;
- Утилита для подключения в один клик;
- Система энергосбережения - автоматическое управление для экономии питания;
- Работа со всеми протоколами защиты Windows Mobile (WPA, WPA-PSK, 802.1x, 40/128-bit WEP, Open);
- Быстрое подключение к Wi-Fi-сетям и поддержка соединения в определенной сети;
- Ping-утилита - для проверки подключения и исследования сети;
- Trace Route утилита - для отображения маршрута пакетов.

MOBILE MYIP 1.1.2

■ В основном, конечно, утилита для рядовых пользователей, но в повседневной сетевой жизни практически незаменима и для нормального человека ;).

- Позволяет:
- Отображать текущее имя устройства и IP-адрес;
 - Обновлять эту информацию в реальном времени;
 - Делать классический PING;
 - Резолвить DNS-имена.



MOCHA REMOTE CLIENT 1.2 PPC

■ Клиент удаленного рабочего стола от все той же смешной фирмы. Желательно использовать ее же сервер. В общем-то, ничего выдающегося не вытворяет, но то, что должна делать, делает хорошо. Удобна для управления удаленным компом, эээ, скажем, без ведома управляемого. При небольшой модификации сервера, конечно.

Так как софтина кушает довольно много трафика, рекомендуется к использованию только в сетях с широким каналом.

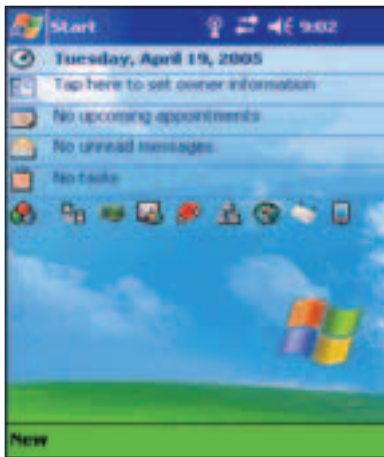


К недостаткам урологического клиента можно отнести наличие всего трех типов клавиатур: US, US International и Danish, а к достоинствам - SSL-шифрование, три разных вида просмотра экрана, горизонтальный режим работы и возможность удобной прокрутки изображения стилусом.

NETBOX 1.50

■ С появлением вирусов и троянов для КПК актуальной стала проблема просмотра текущих соединений, статистики TCP и UDP. Все это умеет NetBox. Помимо этого он показывает MAC-адрес, IP-адрес, информацию DHCP, WINS, мониторит трафик, пингует hosts, отображает окружение локальной сети и, естественно, поддерживает элементарные функции работы с DNS (резолвинг имен, адресов и получение MX). В качестве приятного бонуса - индикаторы батарей и сво-

»

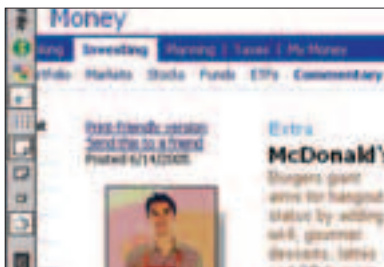


бодной памяти, возможность скачивания web-страниц и сохранения их на КПК (то, чего так не хватает штатному Pocket IE!).

Это инструмент настоящего профессионала - очень рекомендую!

МОCHA VNC 1.1 PPC

■ Mocha VNC - программа для полного защищенного SSH2-гоступа с Pocket PC КПК к твоему настольному компьютеру через интернет или локальную сеть.



Возможности вкратце:

- Протокол VNC с поддержкой: Raw, CopyRect, Hextile, ZRLE и Zlib;
- SSH2-туннелирование;
- Прокрутка стилусом.

И все в том же духе.

NET MONITOR 2.10

■ Приблуд для КПК, представляющий собой программу для анализа локальной сети. Незаменима при настройке сетевых параметров и тестировании работы ЛВС.



Основные возможности:

- Детальная информация обо всех сетевых адаптерах;

■ Поддержка VGA/QVGA-экранов и режимов Portrait/Landscape;

■ Анализатор входящего и исходящего трафика;

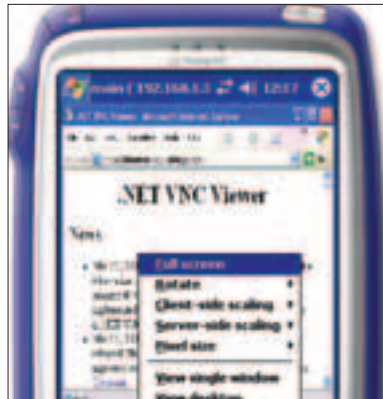
■ Импорт и экспорт сетевых профайлов;

■ Утилита Ping;

■ Сканер WLAN.

.NET VNC VIEWER 1.0.1.16

■ Клиент VNC на .NET. Скачав программу, ты можешь стать свидетелем легендарной кросс-платформенности .NET, так как этот шедевр работает и на Pocket PC, и на настольном компьютере под управлением ОС Windows. В отличие от подобных программ, умеет поворачивать изображение на 90 градусов и работать в полноэкранный режиме, что неосцимемо отрадно.



Возможности:

- Все основные функции VNC-клиента;
- Полноэкранный режим;
- Поворот экрана;
- История сессий;
- Возможность установки скрытого VNC-сервера на удаленном ПК и его контролирование с КПК.;

VXSNMP 0.9.1

■ У тебя возникала необходимость поуправлять каким-нибудь SNMP-совместимым устройством? Если честно, нечасто пользовался такими возможностями, но, по утверждениям производителей устройств, очень многие сетевые компоненты поддерживают этот протокол. Так почему бы не воспользоваться этим приятным фактом ;)?



POCKETPUTTY 0.2 ALPHA 0.53B

■ Экспериментальная версия любимого PuTTY теперь и на PocketPC. С новыми багами и фичами. Если честно, мне очень понравилось ощущение чего-то старого доброго.

Если ты фанат Пути (не путать с Президентом РФ!), то очень советую попробовать это чудо.



RETINA WIFI SCANNER

■ Софтина представляет собой бесплатный сканер, предназначенный для обнаружения беспроводных устройств или проверки наличия беспроводного сетевого соединения.



Помогает обнаружить все мобильные (и не очень) устройства, подключенные к сети, и выяснить их характеристики. Неосцимемо для служб безопасности и IT-профессионалов, так как позволяет отслеживать состояние сети в режиме реального времени. Может работать как на КПК, так и на обычном настольном компьютере.

Что самое удивительное, при всех возможностях сканер предоставляется компанией Retina совершенно бесплатно! Халява, сээр-р!

Z2 POCKETLAN FOR POCKET PC 2002/2003 3.11

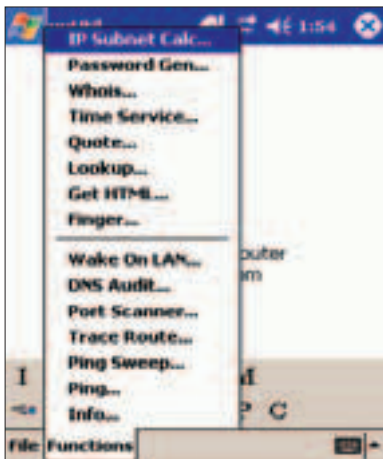
■ Эта софтина подойдет для фанатов SMB (протокол обмена файлами в среде ОС Windows). Ты только посмотри на ее достоинства:



- Wake on LAN: включает настольный ПК, находящийся в режиме StandBy.
- IP Report: создает отчет по всем настройкам IP, TCP/IP-статистике, IP-маршрутизации и ARP-кешу.
- Выводит папку NETWORK в Pocket File Explorer.
- Автоматически сканирует удаленные компьютеры и определяет их имена, открывает файлы с удаленных ПК в Pocket File Explorer, проигрывает MP3 и фильмы через Windows Media Player.
- Умеет добавлять, удалять и изменять alias'ы (maps) сетевых ресурсов.
- Автоматически определяет, что произошло подключение к сети, переключает все ресурсы.
- Плагин в File Explorer позволяет работать с сетью без ввода текстовых адресов.
- Печатает простой текст на сетевых принтерах.
- Проверяет IP- и MAC-адреса, обновляет IP-адрес через IP Config.
- Улучшенный Ping умеет выяснять имя удаленного ПК и его MAC-адрес.
- IP Scan ищет IP, MAC и NIC компьютеров, Wi-Fi-точки и маршрутизаторы сети.

VXUTIL 1.6.2

- Ты еще не определился со своим сетевым "швейцарским раскладным ножом"? Тогда вот новый кандидат. Многофункциональная программа включает в себя: DNS Lookup, Finger, IP Subnet Calculator, Password



Generator, Ping Sweep, Ping, Port Scanner, Quote, Time Service, Trace Route, Wake On LAN, Whois и т.д. Впечатляет, правда?

NETWORK BROWSER 1.2

- Еще один инструмент, точнее, даже не инструмент, а ящик с инструментами - и все они для работы с сетями.

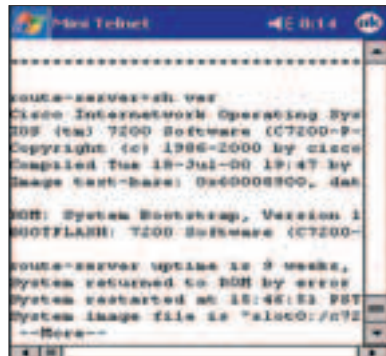


Итак, в Network Browser можно обнаружить:

- Просмотр сетевых ресурсов, все как на настольном компьютере.
- Доступ к расшаренным файлам без подключения сетевых дисков (mapping drives).
- Самый настоящий Terminal Server Client. Если ты вдруг нарыл реквизиты для доступа к серверу, то сможешь посмотреть их в деле на месте.
- Подключение и отключение сетевых дисков.
- Отображение статуса сетевого Wi-Fi-подключения и доступных сетей.
- Печать текстовых файлов на сетевом принтере.
- Инструменты конфигурирования сети.
- Редактор списка известных хостов.
- Поддержка горизонтального режима (правда, лишь на Windows Mobile 2003).
- Классические Ping и Trace route - куда же без них?

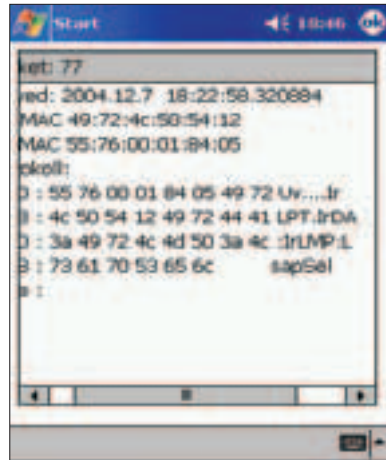
MINI TELNET 1.0A PPC

Самый простой Telnet-клиент для Pocket PC КПК. Поддержка протокола RFC854. Ничем особо не удивил, кроме размера, скорости работы и обилия глюков на каждый байт кода :).



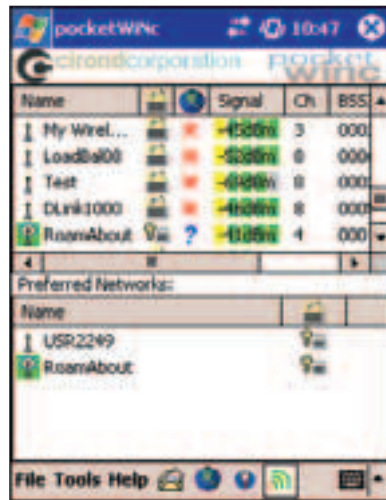
CENETDUMP REALTIME NETWORK SNIFFER 1.1

Самый настоящий sniffер для твоего КПК! Тех, кто в танке, информирую, что это программа для перехвата сетевых пакетов в реальном времени. Работает со всеми вариантами подключения. Поддерживает фильтры по портам и протоколам, поэтому заметно облегчает ориентирование в потоке данных, а также содержит в себе утилиту ping.



POCKETWINC 2.0

- Софт для подключения КПК к Wi-Fi-сетям. Помнишь, насколько геморройно было подключиться к беспроводной сети с КПК раньше? А если сеть не твоя, так это вообще целая история... Но теперь процедура подключения сильно упрощается! Ставь и варрайв!



Приятного в pocketWinc встретись:

- Детектор сетей 802.11;
- Анализатор Wi-Fi-сетей (предоставляет действительно много информации о сети);
- Быстрое подключение к сети плюс анализатор подключения Wi-Fi-сети к интернету;
- Много справочной информации: точки доступа, их SSID, BSSID, сила сигнала, статус;
- Управление WEP-ключами;
- Диагностика Wi-Fi-сети, есть trace. >>

AIRSCANNER MOBILE FIREWALL 1.0B

■ Самый настоящий сетевой брандмауэр для Windows Mobile/Pocket PC КПК. Выполнен качественно, работает на уровне NDIS, в двух направлениях. Работа программы основывается на правилах доступа, которые могут определяться пользователем.

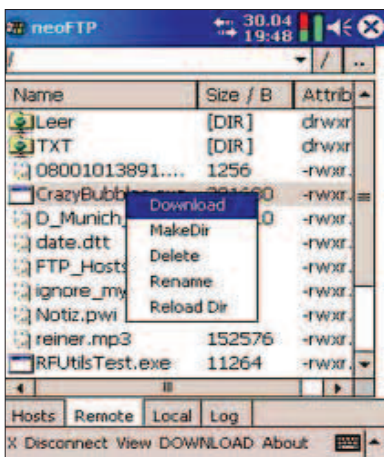


AirScanner Mobile Firewall анализирует пакеты по определенным критериям: порту, IP-адресу, адресу URL и т.п. Программа представляет собой именно файрвол, а не программу для блокирования приложений.

Сортина бесплатна для персонального использования.

NEOFTP 0.9

■ Бесплатный FTP-клиент для Pocket PC КПК. Поддерживает докачку файлов и имеет адресную книгу FTP-серверов, так что тебе не придется по много раз набирать IP-адреса и имена пользователей. Бесшовно интегрируется с neoTools - neoScan.

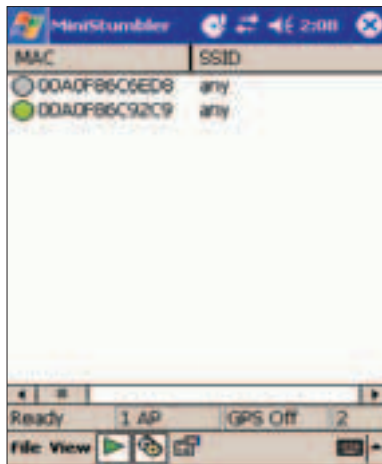
**NEOTOOLS - NEOSCAN 0.9**

■ Да-да, это то самое, с чем интегрируется вышеупомянутый субъект по имени neoFTP :). Представляет собой быстрый и достаточно удобный сканер сети. Помимо основных возможностей сканирования, включает в себя: Ping, Ping Range, traceroute, GetHTTP, WhoIS и поддержку SMTP.

MINISTUMBLER

■ Для тех, кто знаком с NetStumbler'ом: это порт твоей люби-

мой сортины, только для КПК. Порт довольно удачный, обладает вполне интуитивно понятным интерфейсом. Приятным сюрпризом было то, что NetStumbler и MiniStumbler имеют общий формат сохраняемых файлов.



Для тех, кто не знаком с NetStumbler'ом: эта тулза позволяет обнаруживать 802.11 b/g сети, анализировать их зону покрытия и хорошо помогает в настройке соединений с применением направленных антенн. Для чего это можно использовать, гети? Правильно, Сигоров, для варграйвинга! Это ПО считается чуть ли не классическим сортом в этом плане, так что, если ты фанат данного вида госура, MiniStumbler плюс КПК - совет да любовь.

WIFIFOFUM 0.3.3

■ Специально для варграйверов! Бесплатный сканер сетей 802.11 (Wi-Fi), предназначенный для работы на Pocket PC 2003. Сканирует все точки доступа 802.11 и выводит их список. Если у тебя есть GPS-приемник, то возрадуйся: программа запишет еще и местоположение точек доступа! Все это, естественно, легко сохраняется в файл. Этаким настоящим пленгатор!

Отличия этой версии от предыдущей доступной - 0.3.1:

- Увеличено число форматов log-файлов.
- Для каждой Wi-Fi-точки сохраняется значение GPS-координат, где ее сигнал был наиболее мощным.



■ Прописана возможность автоматического создания лога при каждом сканировании.

■ Добавлена поддержка ряда iPAQ'ов.

SNMPUTILS 1.0

■ Продолжаем работать с SNMP. На этот раз интерфейс еще более грузеженный: пакет состоит из двух запускаемых файлов snmpget и snmpset для получения значений из MIB и их сохранения соответственно. Честно говоря, на любителя. На любителя командной строки под КПК :).


POCKETPCPROXY

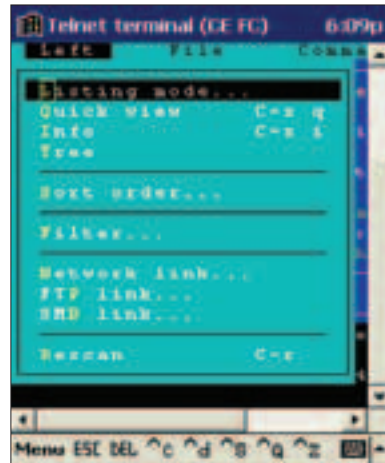
■ Прокси для КПК. Хотя PocketPCProxy находится на стадии разработки и глюки в нем, как понимаешь, неизбежны, во многом он вы-



полняет свои функции. Связь между КПК осуществляется при помощи Bluetooth PAN. На данный момент поддерживает только протокол HTTP GET. Смотрим, наслаждаемся и ждем новых версий?

CE FILECOMMANDER 1.1

■ Очень приятный файл-менеджер с поддержкой ftp- и telnet-протоколов - бальзам и кондиционер в одном флаконе. Но это еще не все! Совершенно бесплатно ты получаешь еще и HEX-редактор - незаменимый для любого хакера инструмент теперь и на КПК. 



НЕ ОГРАНИЧИВАЙ
СЕБЯ

Играй
просто!
GamePost

**ПОЛУЧИ
МАКСИМУМ
УДОВОЛЬСТВИЯ**

ИСПОЛЬЗУЯ ДОПОЛНИТЕЛЬНЫЕ АКСЕССУАРЫ



Монитор
Shuttle XP17SG

\$675.99



Наушники
AKG K406 AFC

\$162.99



Колонки
M-Audio Studiophile
LX4 2.1 System

\$339.99



Шлем
I-O Display Systems
i-Scape II

\$269.99



Корпус
Shuttle SB83G5C

\$485.99



Pinnacle Systems
ShowCenter 1000g

\$285.99

* В нашем магазине
вас ждет более
1000 игр
на ваш выбор

* Постоянно
обновляемый
ассортимент

* Товары от
самых лучших
производителей



Тел.: (095) 780-8825
Факс.: (095) 780-8824

www.gamepost.ru



Roman aka Docent (roman@docent.msk.ru)

ТРУБКИ-СКАНЕРЫ

ВСЕ О ВЗЛОМЕ БЕСШНУРОВЫХ ТЕЛЕФОНОВ

Несколько лет назад, примерно во второй половине 90-х, владельцев бесшнуровых телефонов вдруг охватила паника. Домой и в офисы ко многим людям стали приходить колоссальные счета за международные переговоры с такими дальними странами, о которых они знали разве что по школьному учебнику географии. Конечно же, никого, кому они могли звонить в те страны, у этих людей не было. В местных узлах МГТС выстраивались очереди недовольных, пытающихся доказать, что по номерам, обозначенным в счете, они никому не звонили. Кто-то добивался правды через суд, кто-то умудрялся разжалобить сотрудников МГТС, а кому-то не оставалось ничего, кроме как подсчитать количество ноликов в сумме, изображенной в счете, и под страхом отключения телефона отправиться оплачивать.



оначалу мало кто из рядовых абонентов гадался, что причиной несчастья был их привычный и столь милый сердцу бесшнуровый телефон, с которым они могли дефилировать по квартире или офису, как герои американского кино. Они полагали, что либо МГТС ошиблась, либо злостные пираты подключились к их линии где-нибудь в подъезде или в коллекторе телефонной сети и поговорили за их счет с далекой Австралией. Пострадавшие стали блокировать автоматический выход на междугород через "8", чтобы осложнить пиратам дозвон за границу. Позднее в желтой прессе начали появляться статьи о том, что вся проблема заключается в бесшнуровых телефонах, в основном тех, которые имеют дальний радиус действия, - например Panasonic 900MHz, Sanyo, Senao и Harvest. Радиус действия этих телефонов, как правило, был намного больше площади квартиры, и с ним запросто можно было ходить и разговаривать на расстоянии до одного километра и более от базового блока в условиях города. А навороченный Harvest, так активно продававшийся на Митинском радиорынке, мог добивать на десятки километров, если применить к нему продававшиеся там же усилители и антенны.

Нужно напомнить, что сотовая связь в то время была еще не такой дешевой, как сейчас, поэтому бесшнуровые телефоны пользовались неплохой популярностью. Чего стоило одно только их дизайнерское решение: трубка, напоминающая сотовую (по тем временам), придавала им дополнительную привлекательность. Конечно же, наш любимый Госсвязьнадзор не очень-то одобрял такие технические средства и не сертифицировал их. Некоторые модели вообще вообще работали на запрещенных для гражданского диапазона частотах. Но возможность быть пойманным не сильно пугала потребителя, да, собственно, и случаев поимки за ис-

пользование таких трубок история не напоминает. Все эти телефоны работали в обычном аналоговом диапазоне и имели примитивную "защиту", сводящаяся, в основном, к тому, чтобы находящиеся рядом телефоны одного диапазона не мешали друг другу, а также чтобы трубка с помощью нехитрого открытого кода опознавала только свой базовый блок (это и было слабое место системы). В то время разработчики, скорее всего, еще не знали о грозящей опасности. Все это, конечно же, создавало очень благоприятную почву для развития нового направления в радио- и телефонном пиратстве.

ТРУБКИ-СКАНЕРЫ

■ Сейчас трудно сказать, где и когда впервые появились трубки-сканеры,

но, скорее всего, изобрести их могли именно у нас в странах бывшего СССР. Эти трубки изготавливались на основе обычных трубок от бесшнуровых телефонов и умели "вешаться" в качестве дополнительной трубки на любой базовый блок, аналогичный этой трубке. Дальностью этих телефонов позволяла "отловить" базы в пределах городского квартала, а если применить Harvest с различными примочками, то, как уже было сказано, радиус действия мог достигать десятков километров.

Принцип работы трубок-сканеров был достаточно простой. В схему трубки впаивали перепрограммируемый микроконтроллер на основе PIC (или его аналог с защитой в него специальной программой) и микросхему ППЗУ

Harvest мог добивать на десятки километров!

Антенна наружная для радиотелефонов 900 МГц "С" - 900"



Основные технические характеристики

- Наружная антенна направленного действия для радиотелефона в составе телефона (ориентированные АЧТВ 900 предназначены для подключения к радиотелефонам диапазонов 900 МГц (РЧ-каналы - 9000, 9200 и др.)
- Антенна рассчитана для работы в интервале температур от -40 С до +50 С и сохраняет рабочие эксплуатационные характеристики в течение 100% при температуре 25 С.
- Антенна устанавливается в количестве 1 шт. (для исключения создания помех и радиопомех для радиотелефона в составе) и не требует дополнительной защиты.
- Диапазон рабочих частот 150 - 1000 МГц.
- Получила сертификат соответствия.
- Создана в соответствии с требованиями стандарта G.S.P.
- Классификация: сотовый, не более 1.8.

Использование наружных антенн для радиотелефонов позволяет существенно улучшить их характеристики



Трубки-сканеры открыто продаются в интернете



На сайте www.prodect.ru ты найдешь всю информацию о стандарте DECT

(EEPROM). После такого апгрейда включенная трубка начинала сканировать весь свой диапазон, и в ее память записывались коды совместимых базовых блоков, если таковые попадались в радиусе действия трубки. Сканирование осуществлялось методом перехвата кода: захотел законный хозяин базового блока совершить звонок - его трубка перед набором номера передала свой код базовому блоку, блок сравнил его с записанным в своей памяти и разрешил сделать звонок; этот же код перехватила трубка-сканер в руках пирата и занесла его в память - в следующий раз при попытке сделать звонок пиратская трубка будет посылать в эфир любой из записанных кодов, и на него ответит базовый блок, которому подходит этот код.

После таких манипуляций с этой трубки можно было позвонить через любой записанный в память базовый блок, который определял такую трубку как "свою". При этом владелец блока даже не подозревал, что его телефоном кто-то пользуется. Далее

все ограничивалось только тем, кто звонит и зачем, - можно было и международный звонок совершить, и взрывное устройство активировать. Иногда, подняв трубку на параллель-

ном телефоне, через твой собственный базовый блок можно было послушать разговор пиратов и вмешаться в него :).

Многочисленные банки памяти позволяли сохранять коды от базовых блоков таким образом, что для каждого района города выделялся отдельный банк памяти и время поиска базового блока при переездах по городу сокращалось. Имелась возможность выбрать предпочтительные базовые блоки, связь на которых лучше, а "базы" с не очень качественной - занести в черный список и исключить из повторного сканирования. Поначалу трубки были рассчитаны на то, чтобы только совершать звонки, - собственно, от них, как правило, это и требовалось. Но позднее в них начали добавлять возможность принимать звонки - оставалось только узнать, какому коду соответствует чужой телефонный номер. Фактически, получался некий аналог сотового телефона, позволяющий звонить по всему миру на халяву. За чужое удовольствие платили несчастные абоненты - владельцы бесшнуровых телефонов. В то время, когда еще не начался сотовый бум, мобильники были дорогим удовольствием, а IP-телефония находилась в зачаточном состоянии, такая халява не могла не привлекать любителей поговорить за чужой счет или позвонить бесплатно из любой точки своего города.

В первую очередь этим благом стали пользоваться, конечно же, гости столицы: иностранные студенты, гастарбайтеры, челноки и прочие эмигранты - для осуществления бесплатных звонков на родину. Пиратские очаги нелегальных абонентов сосредотачивались, как правило, вокруг гостиниц, общежитий и рынков. Некоторые даже умудрялись зарабатывать с помощью трубки-сканера, открывая подпольные переговорные пункты с дешевой международной связью, например, в общежитиях. Позднее удобство такой связи оценили и гру-



"Ростелеком" не "огорчает" использование трубок-сканеров.



DECT/GSM телефон Sagem



Трубка-сканер в действии

гие не очень чистые на руку граждане, желающие обзавестись бесплатной мобильной связью.

В интернете появилось множество сайтов умельцев, которые предлагали переделать обычную трубку от беспроводного телефона в сканер или продавали готовые трубки-сканеры и наборы для самостоятельной переделки с полной документацией. Цены на девайс колебались в пределах \$250-350 в зависимости от модели переделанной трубки. А набор для самостоятельной переделки можно было купить всего за \$30-60. Некоторые сайты существуют и по сей день - достаточно ввести в поисковой системе что-нибудь вроде "сканирующие трубки". Ты увидишь большой список,

вывозящий как на страницы умельцев, так и на всякие схемы по переделке. Не факт, конечно, что все эти сайты еще живы. Некоторые такие умельцы уже получили свой срок. Как ни крути, но эпидемия, разгар которой пришелся на 1997-2000 годы, сильно поутихла, и чуть ниже я расскажу, что способствовало этому.

Пиратский прогресс быстро привел к тому, что трубки-сканеры обросли кучей полезных свойств.



Знаменитые радиотелефоны Panasonic - "родители" трубок-сканеров

Многие абоненты стали блокировать выход на межгород через "8".

КОНТРМЕРЫ

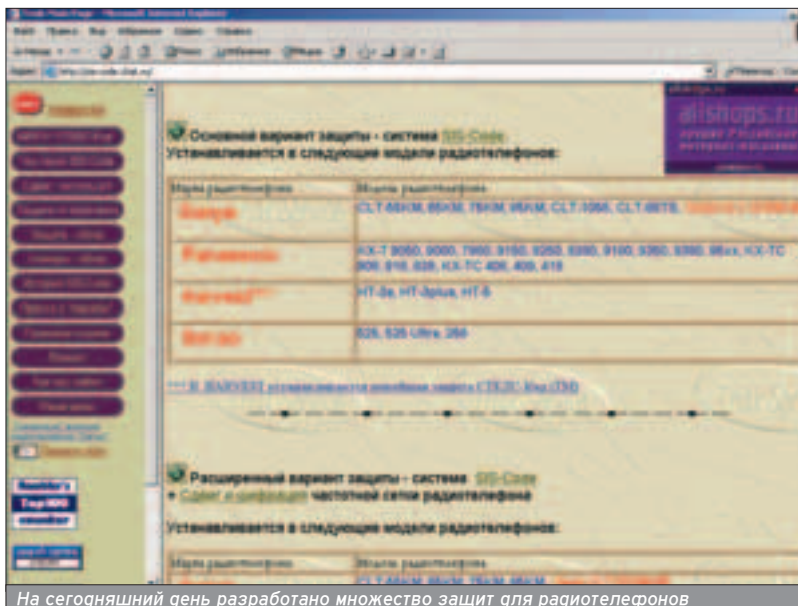
■ Когда в прессе стали появляться первые статьи о пиратах, атакующих базовые блоки законопослушных граждан, журналимеры предлагали в качестве защиты всегда класть свою трубку на базовый блок - разумеется, это полнейший бред, а не спасение. Многие абоненты просто шли на телефонный узел МГТС и писали заявление о блокировании автоматического выхода на межгород через "8". Такой выход был самым простым и горился только на первое время: звонок в другой город при блокировке "восьмерки" становился возможным только после специального заказа оператору, который позже перезванивал и уточнял заказ. Но и это не спасало от любителей секса по телефону, желающих пользоваться бесплатной "мобильной" связью по городу, потенциальных террористов и просто хулиганов.

Для решения проблемы умельцы придумали всяческие абонентские блокираторы - коробочки, которые вставлялись в разрыв телефонной линии и следовали настройкам абонента, то есть не позволяли набирать номера, начинавшиеся с "8", и перед каждым звонком требовали вводить установленный заранее код. Очень неудобно! В ответ разработчики сканирующих трубок стали встраивать в свои изделия функции перебора этих самых кодов и прочие обманные примочки. Еще одним способом простейшей защиты было отвинчивание антенны от базового блока - так сокра-

щали радиус действия беспроводного телефона. Но при такой защите и сам владелец трубки мог пользоваться ей только в своей квартире и только в паре десятков метров от "базы".

На смену блокираторам стали приходиться другие решения. Вполне возможно, что они были разработаны теми же умельцами, которые придумали трубки-сканеры. Один из таких девайсов, например, представлял собой схему, собранную на том же самом PIC-процессоре. Одна часть этого устройства встраивалась в трубку, другая - в базу. Код, отправляемый такой трубкой, кодировался специальным ключом, который изменялся каждый раз при совершении звонка. Примочка уже более серьезно усложнила жизнь владельцам сканеров. Подобрать постоянно меняющийся ключ шифрования и получить код - может быть, теоретически выполнимая задача, но на практике в данных условиях она нереализуема.

Для защиты попроще можно было заменить задающую частоту кварца в трубке и базовом блоке, благодаря чему частотная сетка каналов, в которой работал телефон, смещалась и становилась недоступной для сканера, сделанного по данную модель телефона. Если очень захотеть, то эту защиту, в общем, тоже можно было обойти, хотя вряд ли кто-то стал бы возиться с этим, особенно когда в ра-



На сегодняшний день разработано множество защит для радиотелефонов

За чужое удовольствие платили абоненты - владельцы беспроводных телефонов.

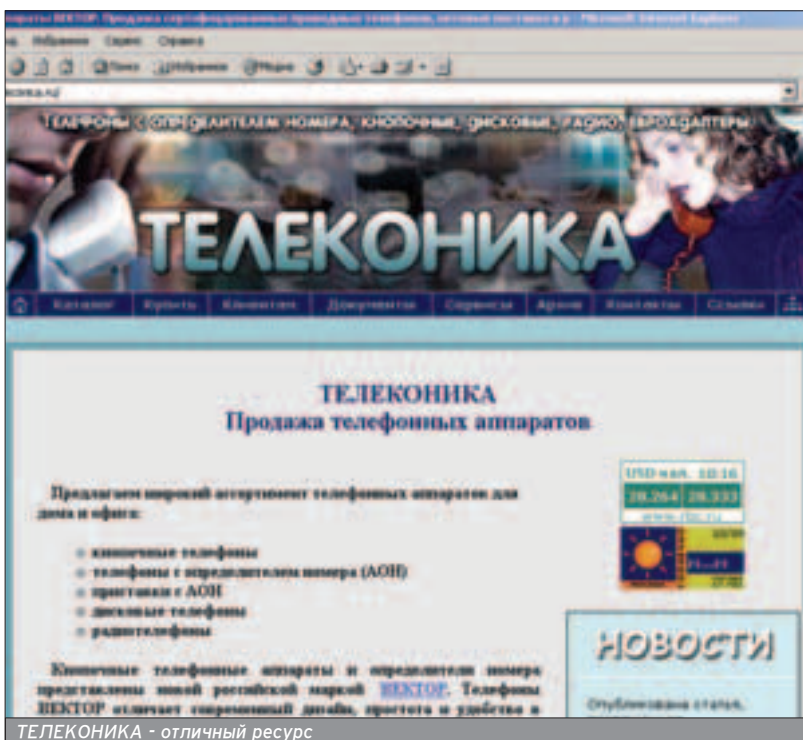
диусе действия сканера еще много аналогичных базовых блоков.

КОНТРОЛЬНЫЙ ВЫСТРЕЛ

Такой кавардак не мог продолжаться бесконечно, и он прекратился, конечно же, не только из-за описанных контрмер. Разработчики беспроводных телефонов тоже стали задумываться о защите. Кроме того, со временем рынок стал все больше наполняться беспроводными телефонами DECT-стандарта, защищенного намного серьезнее, а его небольшой радиус действия вряд ли мог заинтересовать пиратов-умельцев. Свое веское слово сказал и Госсвязьнадзор: была введена обязательная сертификация всех средств связи, ввозимых в страну. Напомню, что все упомянутые мной телефоны, ставшие столь популярными среди пиратов (Panasonic 900MHz, Sanyo, Senao и Harvest), работали на не предназначенных для гражданских целей диапазонах - со временем эти девайсы исчезли с прилавков.

Контрольным выстрелом стал сотовый бум - обвал цен на мобильную связь и распространение IP-телефонии. Разработка и продажа сканеров стала невыгодной. Конечно же, на барахолках все еще можно найти старые дальнбойные Harvest и Senao, также осталось и немалое число их приверженцев, которые просто позаботились об установке всевозможных защит на свои аппараты. Новые сертифицированные модели этих телефонов также можно найти в продаже, но они оснащены более серьезными средствами безопасности. Трубки-сканеры, так или иначе, покидают сцену и остаются только в истории радио- и телефонного пиратства.

Контрольным выстрелом стал сотовый бум.



ТЕЛЕКОНИКА - отличный ресурс

S.A.N

ВАМ ЗВОНЯТ ИЗ МИЛИЦИИ...

ОБЗОР СОФТА ДЛЯ ТЕЛЕФОННЫХ РОЗЫГРЫШЕЙ

Хочешь разыграть своих друзей, изменив голос? И ты уже придумал отличную шутку? Полдела сделано, но для его полной реализации тебе потребуется несколько занятных программ, которые помогут устроить розыгрыш по полной. О них и пойдет речь в этой статье.

Хочется добавить несколько радостных минут в свою жизнь - разыграть соседа или позвонить в милицию от имени заклятого врага? В этом тебе поможет данная статья.

Как тебе такая идея: звонишь по любому телефонному номеру (старому доброму преподавателю, например) и говоришь: "Здравствуйте, вас беспокоит АТС, вы не могли бы нам помочь? Скажите, сколько метров кабеля идет от телефона к розетке? ... Теперь отмерьте пять метров и засуньте его подальше..." Ответ жертвы в этом случае - уже хороший повод повеселиться, но мы пойдем дальше.

Через некоторое время звонишь по тому же номеру и говоришь примерно следующее: "Извините, вас беспокоят из милиции. Мы хотели сказать, что поймали тех хулиганов, которые звонили вам, поэтому можете вытащить провод из ...". После этого либо жертву увозят в психушку, либо тебя - в травматологическое отделение. Если перспектива пребывать в больнице не греет твою душу, а расшатать кому-нибудь нервы - насущная необходимость, читай дальше.

Посмотрим, что нужно сделать, чтобы очередной прикол не дал "гробовщикам заработать по червонцу". Первое, что может избавить врачей от лишнего пациента, - Анти-АОН. Эта замечательная услуга предоставляется всеми операторами сотовой связи. Следующая проблема - подозрительно похожий голос работника АТС и доблестного сотрудника милиции. Да и знакомые будут прерывать твои телефонные шутки ненужными словами типа "Вася, это ты?". А во избежание недоразумений...

МЕНЯЕМ ГОЛОС

К счастью, теперь не нужно быть мастером пародийного жанра, чтобы суметь временно изменить свой голос до неузнаваемости. В этом деле поможет любая программа для редактирования звука (например SoundForge). Кроме того, счастливые обладатели

звуковой карты Sound Blaster Live! могут поставить APS-грайверы и в реальном времени менять любые звуки на входе. Но никогда не знаешь, где и при каких обстоятельствах вдруг захочется кого-нибудь разыграть. Можно, конечно, таскать с собой ноутбук, но есть идея получше - использовать КПК или смартфон. Посмотрим, какой софт сделает тебя профессионалом пранка.

SSEYO MINIMIXA++



Маленький смартфон + SSEYO miniMIXA++ = веселье

MiniMIXA - одна из очень немногих программ для редактирования музыки на КПК и смартфонах, продукт компании Tao Group. С выходом этой замечательной утилиты многочисленные пользователи мобильных устройств получили многоканальный микшер и полноценную студию звукозаписи. Софтина поддерживает множество звуковых эффектов, технику микширования и позволяет сводить до ге-

вяти звуковых каналов. miniMIXA поддерживает многие аудиоформаты, поэтому созданные треки можно будет отправлять на телефон. Большие любители качественного звука записи (насколько это возможно в данном случае) со встроенного микрофона вряд ли останутся довольными (об аппаратном решении для повышения качества записи читай ниже). Микшер работает на смартфонах под управлением Windows Mobile 2002/2003 и на Pocket PC. Главный минус в том, что китайцы из Tao Group хотят денег и поэтому сделали утилиту платной.

STRANGE VOICE

Впрочем, существуют и чисто аппаратные решения. Контора под звучным названием Mobile Dream выпустила устройство, которое, несомненно, станет хитом среди любителей телефонного пранка. Итак, данный девайс - hands free с функцией изменения голоса, поддерживающий семь различных типов голосов. Девайс прост в применении, как молоток, однако для любителя розыгрышей полагает в разряд must have. Кроме средств для изменения голоса, скорее всего, понадобятся софт для записи голоса. Представь себе человека, находящегося в депрессивном состоянии и доведенного до сумасшествия ежедневными звонками. Это и есть твоя жертва, и то, что она скажет, когда в очередной раз услышит очередной прикол, навсегда пополнит историю ми-

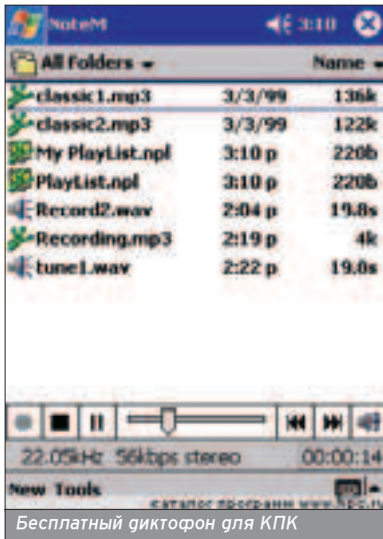
ПРАНК

Скачать
Мой телефон
Настройка
Софт
Мобильные
Смартфон
Планшет

Дать название программе и установить для смартфона.
В архиве с программой есть инструкции для быстрой регистрации программы

Название	Версия	Для чего нужен
WbAAR	v1.0.0	Эта программа сканирует все файлы и программы на устройстве
CellCode	v2.1	Программа для поиска и идентификации различных типов и форматов записей
Voice	Voice File & Voice 3.3	Программа предназначена, чтобы вы могли редактировать все что угодно, чтобы изменить, то звучание в WAV файле или что-либо. Поддерживает любой формат wav 20, и также это же предназначено - вы можете использовать файлы для генерации
MiniMIXA	MiniMIXA v1.1	Программа для создания телефонных розыгрышей, может записывать все с помощью микрофона

На <http://swide.narod.ru/soft> ты сможешь скачать занятные программы для пранка



рового пранка (может быть, добавит несколько матерных слов в твой словарный запас).

NOTEM 1.21

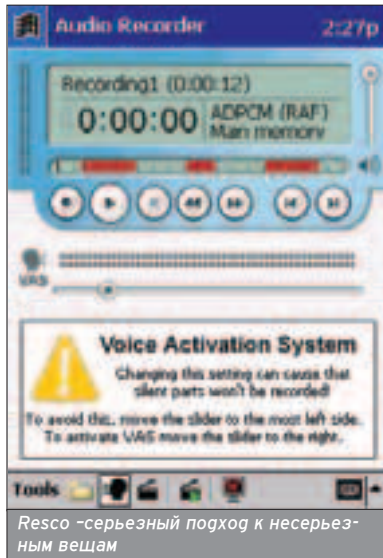
■ Если речь идет о необходимости записать голос, первое, что приходит в голову, - "научить" КПК выполнять функцию диктофона. Такая же мысль, скорее всего, пришла в головы наших мелкомягким друзьям из Регмонга, когда они писали Windows for Pocket PC. Однако то, что называется стандартным диктофоном, имеет несколько недостатков, главный из которых - расточительный wav-формат, "съедающий" любое количество памяти. Бесплатная утилита NoteM таких недостатков не имеет и пишет звук с GSM-компрессией (при записи голоса обрезаются верхние частоты) или в формате MP3. Есть возможность конвертировать файлы из wav в MP3 и наоборот. NoteM позволяет также выбирать качество записи: поддерживаются несколько битрейтов (16, 56, 128 kbps). Для увеличения времени работы есть функция записи с выключенным экраном.

RESCO AUDIO RECORDER FOR POCKET PC

■ NoteM будет вполне достаточно для записи криков взбесившейся бабки, однако, если ты хочешь использовать "диктофон" для решения серьезных задач (например записать лекции, на которых отсутствуешь), больше подойдет Resco Audio Recorder for Pocket PC.

Рекордер от Resco имеет более солидные возможности, чем NoteM, однако при этом требует денежной компенсации за праведные труды программистов. Чтобы понять, стоит ли игра свеч (а результат - труда), обратимся к основным функциям:

- Встроенная система активации голосом;
- Возможность выключать дисплей во время записи;
- Запись по расписанию;
- Поддержка карт памяти CF, SD, MMC;



- Индикатор силы сигнала в реальном времени;
- Запись файлов в форматы MP3, raf, wav.

PDAUDIO-CF

■ Как уже было сказано, если есть необходимость максимально улучшить качество записи, стоит присмотреться к аппаратным решениям. PDAudio-CF - одно из них.

Карта формата Compact Flash от Core Sound представляет собой внешний цифровой диктофон. В отличие от встроенных в КПК микрофонов, PDAudio пишет звук с более высокими битрейтами. Устройство позволяет хранить данные на flash-карте, которая входит в комплект и помещается в дополнительный жакет. Если верить разработчикам, с помощью PDAudio



Небольшой микрофон в формате CF с небольшим жакетом для карты того же формата

можно записать до трех часов качественного звука без подзарядки КПК.

ПРАВИЛА ХОРОШЕГО ТОНА

- Чтобы телефонные розыгрыши доставляли максимальное удовольствие тебе и минимальную головную боль "клиентам", нужно соблюдать несколько правил:
 - Веди свою телефонную базу во избежание встреч с вечно занятыми номерами, организациями и просто неинтересными собеседниками. Заодно можно вести учет самых безбашенных (веселых, злых, разговорчивых и т.д.) собеседников, чтобы звонить им по несколько раз :);
 - Какие бы подробности ты ни узнал о себе после очередного прикола, не стоит наезжать на жертву или говорить лишнее. ☹

Strange Voice - hands free с функцией изменения голоса, поддерживающий семь различных типов голосов.



По адресу www.core-sound.com ты сможешь найти много информации о PDAudio

Евгений Ермолаев aka Saturn (saturn@linkin-park.ru)

ЗА СВЯЗЬ ДЕНЕГ НЕ БЕРЕМ

ВСЕ О БЕСПЛАТНЫХ СЕРВИСАХ СВЯЗИ

В начале 70-х годов прошлого века появились фриеры - сообщество людей, которое можно назвать ответвлением классического хакерского движения. "Мы пользуемся бесплатно тем, на чем вы хотели нажиться", - вот их девиз. Фрикинг зародился 30 лет назад, но возможность бесплатно пользоваться некоторыми сервисами до сих пор существует.



КАК ЭТО БЫЛО

■ Все началось с того, что John Draper (известен и как Cap'n Crunch) обнаружил, что свисток, который в качестве подарка кладут в каждую коробку с быстрым завтраком "Капитан Кранч", издает звук с частотой 2600 Гц.

Звук этой частоты использовался (используется в вашей АТС?) оборо-



Не все завтраки одинаково полезны! Завтрак "Капитан Кранч" оказался самым полезным для роста и развития фрикинга



Вот он - легендарный создатель blue-box!

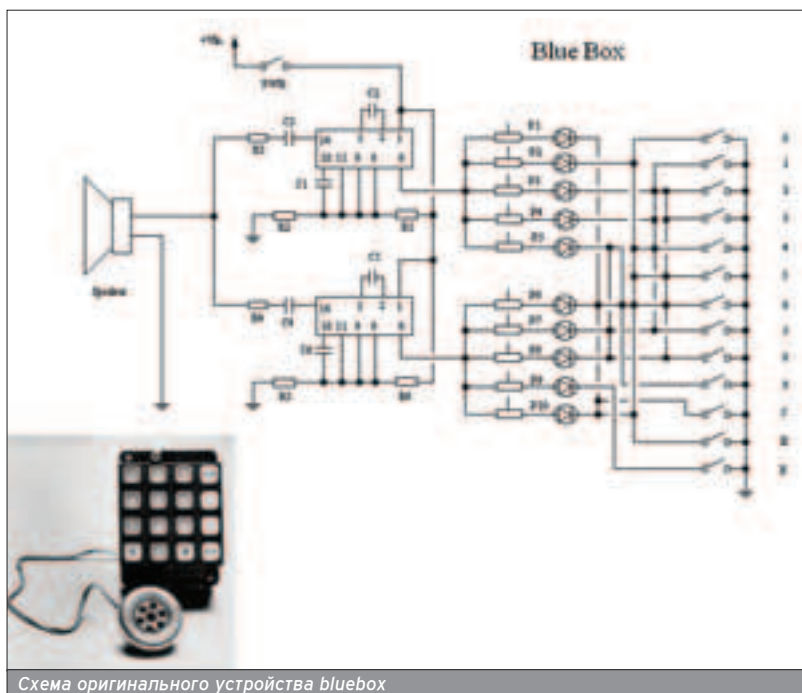
ванием переключения для освобождения линии абонента. Тот самый свисток из коробки завтрака Cap'n Crunch моделировал ситуацию, при которой телефонный абонент вешает трубку, чтобы владелец телефона смог бесплатно воспользоваться связью: абонент не вешает трубку, а с помощью свистка "имитирует" это действие, в результате введенная в заблуждение АТС за связь денег не берет. Джон Дрейпер создал легендарное устройство bluebox, споры о котором до сих пор не прекращаются.

Многие слышали об этом устройстве и знают, что оно создано для ведения бесплатных междугородних разговоров. Однако любой связист

скажет, что такое устройство невозможно создать в принципе, при этом он не приведет четких аргументов, а скорее всего, отошлет к "популярной литературе по устройству АТС". Что это? Связисты говорят об объективных данных или отрицают факты, чтобы сохранить свою репутацию? Чтобы понять это, нужно разобраться, в каких условиях был создан bluebox и с какими устройствами планировалось применять его по прямому назначению.

В 1954 году корпорация Bell Telephone System перешла на новую систему управления АТС, в которой команды отправлялись на АТС в виде сигналов определенной частоты. Один из сигналов ("отбой") был реа-

Bluebox дал серьезный толчок для развития бесплатного доступа к средствам связи.



лизован в виде сигнала с частотой 2600 Гц. Всем ясно, что эта информация не разглашалась и что "лазейка" была обнаружена Джоном Дрэйпером случайно, но сомневаться в работоспособности лазейки не приходится. Более того, классический bluebox работает на всех междугородних каналах, за исключением тех, на которых требуется сигнализация ОКС-7 (это относится и к России, где еще осталось много аналоговых АТС).

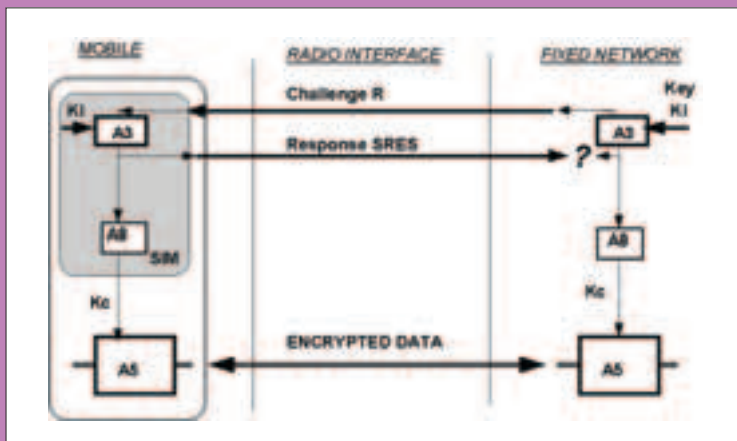
Сейчас bluebox теряет свою актуальность, но его концепция останет-

ся в истории как культовая ("концепция", потому что определенный сигнал можно моделировать чем угодно), так как она породила целое направление, позже названное фрикингом. История с частотой 2600 Гц подтолкнула идею бесплатного доступа к средствам связи к серьезному развитию, и даже сейчас время от времени обнаруживаются "дыры" в системах связи, позволяющие пользоваться некоторыми сервисами бесплатно. Таким сервисам и посвящен этот материал.

БЕЗОПАСНОСТЬ В ПРОТОКОЛЕ GSM

■ Для обеспечения безопасности в протоколе GSM используются три закрытых алгоритма:

A3 - алгоритм аутентификации, A8 - алгоритм генерации криптоключа, A5 - алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров. Существует две версии алгоритма A5 - A5/1 - основная версия, A5/2 - ослабленная версия алгоритма (используется и в России).



Основные алгоритмы, используемые для обеспечения безопасности протокола GSM

Три элемента системы обеспечивают секретность идентификатора абонента, служебных и пользовательских данных: модуль идентификации абонента (SIM-карта), мобильный терминал (сотовая трубка), базовая станция. SIM-карта содержит Международный Идентификатор Мобильного Абонента (IMSI), ключ авторизации, алгоритмы A3 и A8, PIN-код. Сотовый телефон занимается шифрованием оцифрованной речи по алгоритму A5. Базовая станция использует все три алгоритма.

В теории GSM обеспечивает мобильным телефонам надежную защиту от "клонирования" и гарантирует конфиденциальность переговоров.

Однако в любой аппаратуре сотовой связи на этапе разработки закладываются следующие возможности:

- Определение точного местонахождения абонента;
- Прослушивание разговоров;
- Фиксация реквизитов сторон, вызывающих и принимающих вызов, и многое другое.

Именно из-за существования этих возможностей в частных реализациях протокола GSM используются ослабленные версии алгоритмов (например A5/2) либо шифрование не используется вообще (к примеру в Ираке).

Совокупность этих фактов делает возможным взлом защиты GSM-сетей.



Видимо, с этого таксофона говорили бесплатно не один раз...

БЕСПЛАТНЫЙ "МЕЖГОРОД" - ЭТО ПРОСТО

■ Идея превращения платной междугородней телефонии в бесплатную стара как мир, в разное время она имела разные реализации, но и сегодня не потеряла своей актуальности. Конечно же, самый простой способ поболтать на халяву - это позвонить за счет "дяги Васи".

"Дядя Вася" - лучший друг халявщика

Использование "ресурсов" третьего лица - древнейший способ получения чего-нибудь на халяву. В данном случае нас интересует электросвязь. Существует несколько "рецептов", позволяющих обмануть ближнего своего. Некоторые из этих способов используют несовершенство технологий и техники, некоторые - доверчивость людей.

Social Engineering, или обмани ближнего своего

Не так давно был введен в действие оригинальный способ сэкономить на междугородних переговорах по таксофону. После того как "жертва" заканчивает общаться по таксофону, некий персонаж подходит к ней (в идеале это симпатичная девушка) и просит воспользоваться карточкой в обмен на символическую плату. После окончания "разговора" карточка возвращается "жертве". С первого взгляда - все нормально.

Все карточки (одного номинала) выглядят совершенно одинаково и отличаются лишь серийными номерами. Так вот: "клиенту" возвращается "пустая" карта, в то время как злоумышленник забирает себе кар- »

точку "жертвы" и пользуется ей по своему усмотрению. Данный способ при всей своей простоте имеет несколько недостатков. Во-первых, довольно велик риск оказаться пойманным "за руку". Во-вторых, эффективность затеи не очень высокая: никогда не знаешь, ради чего рискуешь. Гораздо более привлекательным выглядит использование чужого стационарного номера. Поскольку счета за телефон приходят по факту, то, один раз получив доступ к номеру, можно использовать его без ограничений (по крайней мере, несколько дней). На сегодняшний день есть два довольно эффективных и в то же время сравнительно безопасных способа говорить по телефону за чужой счет.

Бесплатный сыр бывает ... на частоте 900 МГц

Последнее время все больше россиян пользуются беспроводными аппаратами, в которых для связи с "базой" вместо провода используется радиоканал. Наиболее интересны для фрикера трубки, работающие на частоте 900 МГц. Дело в том, что у всех этих телефонов есть одна приятная особенность: если линия абонента свободна (он ни с кем не говорит) и при этом трубка не лежит на "базе", радиоканал остается свободным. Появляется возможность подключить другую трубку к этой "базе", то есть получить доступ к телефонному номеру "жертвы" и вести переговоры от ее имени.

Это выглядит примерно так: фрикер ходит по подъезду многоэтажного дома с радиотрубкой частоты 900 МГц и ищет сигнал от какой-нибудь "базы". Поскольку радиус действия

таких телефонов довольно велик (в здании до 50-ти метров), необходимость подходить под дверь каждой квартиры ликвидируется. У этого решения есть огромный минус: поскольку фрикер ходит с трубкой определенной модели, то и сигнал он увидит только от соответствующей "базы", что сильно ограничивает круг потенциальных "клиентов". Для того чтобы избежать подобного рода проблем, злоумышленники используют сканирующие устройства (чаще всего самодельные), специально предназначенные для перехвата сигнала определенной частоты. Важно, что абсолютное большинство беспроводных телефонов подвержено таким перехватам сигнала. Однако наиболее ценными для фрикера являются телефонные аппараты с двумя трубками. В этом случае радиоканал



Такое объявление операторам не помешало бы повесить - чтобы фриеры увидели

За телефонное "пиратство" в России предусмотрена лишь административная ответственность.

нал открыт всегда, независимо от положения трубок. При правильном подходе этот способ очень и очень эффективен, однако есть небольшой минус - необходимость находиться рядом с квартирой (офисом, домом) "жертвы" при переговорах. Итак, самое время усложнить задачу: необходим рецепт получения доступа к бесплатной междугородней (и, как следствие, международной) связи, который обладает преимуществами описанного выше способа и лишен его недостатков. Фантастика? Реальность!

ПОДМЕНА АБОНЕНТСКОГО НОМЕРА

■ Данный способ основан на той же идее, что и предыдущий, - разговор за счет случайного абонента, однако реализация несколько отличается. Благодаря использованию оборудования для подмены абонентского номера (например анти-АОН), фрикер может находиться где угодно (но необходимо оставаться в пределах городской сети). Это большой плюс, поскольку, во-первых, так фрикер усложняет работу органов правопорядка, а во-вторых, получает возможность заработать. Никто не мешает снять квартиру, поставить нужную аппаратуру и организовать пункт междугородней/международной связи. Кстати, в Сети полно предложений по продаже оборудования для подмены абонентских номеров. Заканчивая разговор о междугородних переговорах, замечу, что этот вид фрикинга противозаконен. Однако и здесь можно найти для себя благо: за телефонное "пиратство"

в России предусмотрена лишь административная ответственность.

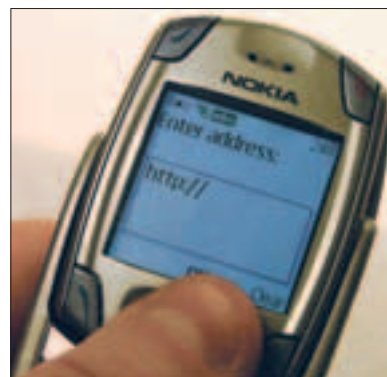
Итак, теперь ты знаешь, как сэкономить на телефонных переговорах (и даже заработать на них) некоторую сумму денег за счет "гяня Васи". Как видишь, есть вполне реальная возможность использовать ТФОП совершенно бесплатно, но фиксированная связь уходит в прошлое, мобильность становится нормой жизни для миллионов людей во всем мире. Самое время обзавестись бесплатной сотовой связью.

СОТОВАЯ СВЯЗЬ - ЗА СЧЕТ ОПЕРАТОРА

■ Мобильная связь имеет неоспоримые преимущества по сравнению со стационарной. И дело здесь не только (и не столько) в отсутствии привязки расположения телефонного аппарата к определенному месту, но и в целом ряде сервисов сотовой связи, самым интересным из которых является мобильный интернет



Многие пользуются подобными трубками. Но почти все забывают ставить их на "базу"



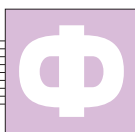
Истинные фриеры не могли оставить без внимания мобильный интернет

Евгений Ермолаев aka Saturn (saturn@linkin-park.ru)

ФРИКИНГ ПО-ЖЕСТКОМУ

ФРИКИНГ ИЗНУТРИ

О самых различных способах фрикинга написано немало, однако эти материалы редко затрагивают его основы. В этой статье мы расскажем тебе, как выглядит фрикинг изнутри.



фрикинг (англ. phreaking) - сленговое выражение, означающее взлом телефонных автоматов и сетей, обычно с целью осуществления бесплатных звонков. В начале 70-х годов фрикинг был делом высококлассных специалистов в области систем связи (в частности в области телефонных сетей). Со временем аудитория этого рода деятельности очень сильно расширилась, а в результате любой старшеклассник мог заниматься "взломом" телефонных аппаратов по разработанному кем-нибудь сценарию. Такое положение дел быстро изменило значение слов "фрикинг" и "фрикер". Сегодня под последним понимают скорее хулигана, поймающего таксофон, а не специалиста в области связи. "Что же плохого в том, что любой может пользоваться некоторыми услугами бесплатно?" - скажешь ты и будешь неправ. Во-первых, уязвимости в системах связи, найденные фрикерами "старой школы", все больше теряют свою актуальность, а искать новые некому. Во-вторых, массовое занятие взломом сетей связи привлекло внимание Большого Брата, поэтому с каждым днем фрикинг становится все более опасным занятием. Итак, что же делать, если гуша просит халавы, а разум не хочет в тюрьму? Оптимальный вариант - изучать предмет посягательства как можно глубже. В нашем случае предметом посягательства станут телефонные сети общего пользования.

ИСТОРИЯ ТЕЛЕФОННЫХ СЕТЕЙ

Итак, самое время рассказать занимательную историю про гядюшку Белла, его изобретение и автоматические телефонные станции. 10 марта 1876 году некто Александр Грехам Белл сказал следующее: "Mr. Watson - Come here - I want to see you" ("Мистер Уатсон, зайдите. Я хочу вас видеть"). Неудивительно, правда? Все-таки люди иногда говорят. Однако это были первые слова, сказанные по телефону. На тот момент "телефонная

сеть" состояла из двух аппаратов, соединенных напрямую проволокой. Такой способ соединения применяли еще некоторое время - до тех пор, пока телефонными аппаратами стали пользоваться далеко не единицы.

Через некоторое время абонентов стало довольно много и появились городские телефонные сети. Каждому аппарату присвоили номер. Соединением абонентов занимались телефонистки, работавшие на телефонных станциях круглосуточно. В то время еще не существовало понятия аутсорсинга, поэтому для экономии на рабочей силе стали искать способы автоматизации процесса установления и обслуживания соединений. Так появились автоматические телефонные станции (АТС).

АТС декадно-шагового типа

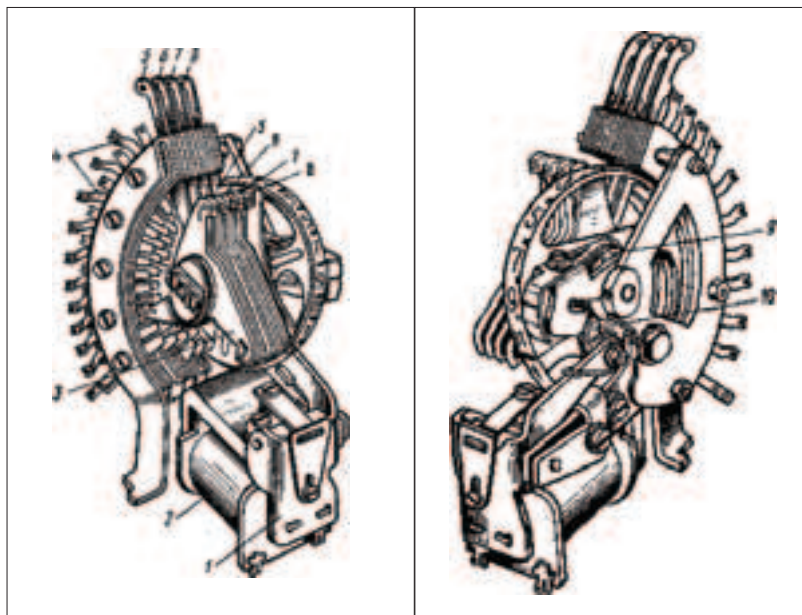
Годом рождения этого типа АТС считается 1889 год, когда Алмону Строугеру пришла в голову идея шагового искателя (ШИ).

Электромеханический шаговый искатель состоит из трех основных частей:

1. Контактное поле - неподвижная часть, состоящая из ламелей;
2. Подвижная часть с контактными щетками (используется для создания электрического контакта с нужными ламелями);
3. Движущий механизм, перемещающий подвижную часть в нужное положение. Осуществляется только вращательное движение.

Емкость таких искателей определяется количеством ламелей. Самые популярные шаговые искатели ШИ-11 и ШИ-17 имеют емкость 11 и 17 номеров соответственно.

Для АТС большей емкости был разработан декадно-шаговый искатель, щетки которого совершают два вида движений: вращательное и поступательное. Такой искатель имеет несколько групп ламелей, расположенных в горизонтальном и вертикальном направлениях, благодаря чему в



Шаговый вращательный искатель ШИ-11:

1 - якорь, 2 - электромагнит, 3 - трехлучевые контактные щетки, 4 - контактные ламели, 5-8 - входы щеток, 9 - движущая собачка, 10 - храповик

контактное поле можно включить до 100 абонентских линий.

Благодаря своей простоте АТС декадно-шагового типа завоевали огромную популярность. До сих пор значительная часть парка городских телефонных сетей в России построена на таких АТС (в Москве 25% АТС - декадно-шагового типа). Минусы АТС ДШ очевидны. Шаговый искатель имеет механические контакты, которые изнашиваются из-за постоянного движения. В результате износа и окисления контактов в процессе разговора появляются посторонние шумы. Кроме того, такие линии практически непригодны для использования модемов. С точки зрения фрикинга такие АТС почти безнадежны, поскольку в них отсутствуют "органы управления".

Многократный координатный соединитель (МКС)

Прогресс никогда не стоял на месте, и начало XX века не было исключением. В 1914 году в Швеции товарищ Бетлаундер изобрел предмет головной боли многих студентов - многократный координатный соединитель (МКС).

МКС - коммутационное устройство релейного типа, используемое в основном на городских, сельских, междугородных координатных автоматических телефонных станциях и автоматических телеграфных станциях. Соединитель называют а) многократным, потому что в нем может быть одновременно осуществлено несколько (до 20-ти) соединений; и б) координатным, потому что место каждого соединения определяется точкой пересечения подвижных вертикальных и горизонтальных реек.

Для подробного описания принципа действия МКС обычно отводят целый раздел учебника, поэтому интересующихся отсылаю к книге "Автоматическая коммутация и телефония" под редакцией Г.Б. Метельского.

АТС координатного типа (АТСК)

Через 25 лет после изобретения МКС была построена первая АТС координатного типа.

В таких АТС реализована сигнальная система, благодаря которой фрикеры получили доступ к бесплатным междугородним звонкам с помощью устройства под названием Bluebox.



Координатная АТС

Информация о сигнальной системе АТС становится еще важнее, если учесть распространенность координатных АТС в России.

СИГНАЛЬНАЯ СИСТЕМА

■ В результате развития автоматической гальневой связи (междугородней и международной) возникла потребность в удаленном управлении коммутирующим оборудованием. Теоретически такое управление можно построить одним из трех способов:

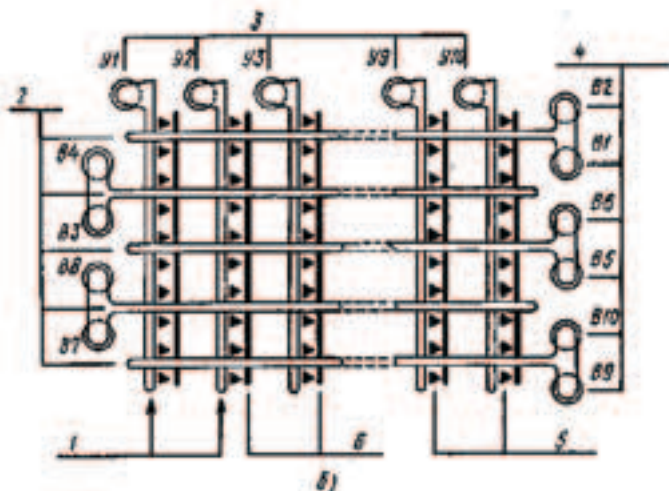
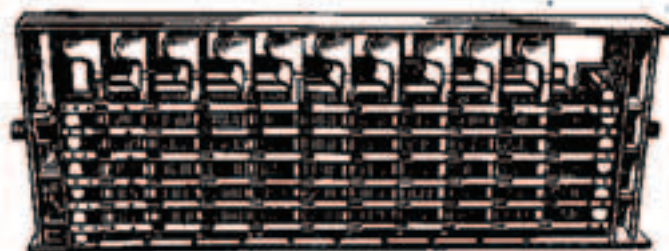
1. Управление импульсами (каждая команда подается с помощью набора импульсов определенной длины);
2. Использование специальных управляющих каналов (управление с помощью каналов связи, созданных исключительно для передачи команд);
3. Управление тонами (команда подается с помощью тоновых сигналов внутри полосы пропускания телефонной сети (3100 Гц).

На практике первые два способа никогда не применялись. Дело в том, что импульс не может пройти непосредственно через каналы гальневой связи, имеющие множество усилителей и преобразователей сигнала. Использование же отдельных управляющих каналов экономически невыгодно прежде всего потому, что их нужно строить. Остается последний вариант, который с успехом применяется во всем мире (теперь ты понимаешь, почему все телефонные службы просят переключиться в тоновый режим перед выбором опций?). Тоновая сигнальная система является двусторонней, то есть абонент и принимает, и посылает сигналы на АТС.

СИГНАЛЫ, ПЕРЕДАВАЕМЫЕ АБОНЕНТУ ОТ АТС

■ Если ты хоть раз пользовался телефоном, то знаешь несколько простых фактов. Первое: при поднятии трубки телефона (либо нажатии клавиши "вызов" на радиотрубке) можно услышать непрерывный гудок. Этот гудок извещает тебя о том, что твое абонентское устройство (в народе его называют телефоном) подключилось к свободному каналу. Теоретически возможна такая ситуация: снимаешь трубку и слышишь короткие гудки. Чтобы в результате не выкинуть телефон, тебе нужно знать следующее: прерывистый сигнал "говорит" о пе- ➤

Сигналы, передаваемые на АТС, - реальное средство контроля АТС и экономии денег.



Многократный координатный соединитель: а - внешний вид, б - схема; 1,2 - удерживающие и выбирающие планки, 3,4 - удерживающие У1-У10 и выбирающие В1-В10 электромагниты, 5 - контактные пружины, 6 - контактные струны

Наименование сигнала	Длительность, с		Уровень или напряжение	Частота, Гц
	Импульс	Пауза		
	Непрерывная передача		от -6 до -30 дБ	425 ± 25
Ответ станции				
Посылка вызова	0,8 ± 0,1 или 1,0 ± 0,1	3,2 ± 0,1 или 4,0 ± 0,1	16...110 В	16...50
Контроль посылки вызова	0,8 ± 0,1 или 1,0 ± 0,1	3,2 ± 0,1 или 4,0 ± 0,1	от -6 до -30 дБ	425 ± 25
Занято	от 0,3 до 0,4	от 0,3 до 0,4	от -6 до -30 дБ	425 ± 25
Занято - перегрузка	от 0,16 до 0,2	от 0,16 до 0,2	от -5 до -30 дБ	425 ± 25

Характеристики сигналов, передаваемых от АТС абоненту

регрузке сети (то есть свободных каналов для подключения нет). В момент, когда номер уже набран, тебя могут ожидать еще два сигнала: посылка вызова или "занято". Если получаемые от АТС сигналы представляют для фрикера чисто теоретический интерес, то сигналы, передаваемые на АТС, - это реальное средство контроля АТС и экономии денег.

СИГНАЛЫ, ПОЛУЧАЕМЫЕ АТС ОТ АБОНЕНТА

При использовании локальной связи (в пределах одной АТС) абонент передает на АТС только номер, с которым желает связаться. Передача номера в рамках координатных АТС осуществляется импульсами переменного тока. Существует шесть передаваемых на АТС частот: f0-700 Гц, f1-900, f2-1100, f4-1300, f7-1500 и f11-1700 Гц. Каждому номеру присвоена комбинация двух частот.

Цифра номера	Комбинация частот
1	f0.f1
2	f0f2
3	f1f2
4	f0f4
5	f1f4
6	f2f4
7	f0f7
8	f1f7
9	f2f7
0	f4f7

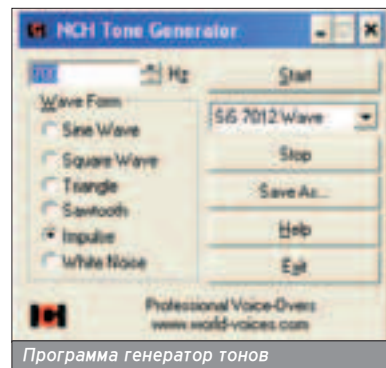
Самым интересным моментом в передаче данных на АТС для нас является передача служебных сигналов - будем рассматривать междугородную связь.

На каждой АТС существуют каналы передачи набора на удаленные станции. В случае междугородней связи набор кода региона указывает станции выбрать маршрут по стране. На станции дальней связи включается расчетное оборудование, которое определяет номер вызывающего абонента и в соответствии с ним начисляет деньги за минуту разговора. Как уже говорилось выше, импульсная передача на станцию дальней связи исключена, поэтому управляющие сигналы находятся в полосе частот 300-3100 Гц. Функции управления и частоты не разглашаются, однако о некоторых стало известно еще в 70-х годах прошлого века.

BLUEBOX - ШАМАНСКИЕ ПЛЯСКИ С ЦИФРОЙ 2600


Одна из таких частот - 2600 Гц. Тон данной частоты "говорит" АТС о том, что канал свободен. Когда вызываемый абонент вешает трубку, дальняя станция отключает линию от его шлейфа и подает в нее сигнал 2600 Гц. Вызывающая сторона, приняв этот сигнал, отключает вызывающего абонента и заканчивает начисление счета. Кроме того, поскольку изначально автоматические станции умеют принимать тоновые сигналы от абонента, при некоторых обстоятельствах сигнал 2600 Гц может быть воспринят и выполнен АТС. Bluebox'ы работают благодаря этому факту.

Основная задача Bluebox'ов состоит в том, чтобы после установки соединения послать в линию с вызывающей стороны сигнал частотой 2600 Гц. Оборудование на обеих станциях интерпретирует это как команду "разорвать соединение", что и произойдет. Оба абонента услышат короткие гудки. Однако оборудование производит сброс не сразу, а спустя примерно две секунды. Если прервать сигнал 2600 до истечения этого вре-



Программа генератор тонов

мени (0,8 с), транк будет отключен, но вызываемый абонент останется подключенным к своей АТС дальней связи. Кроме передачи частоты 2600 Гц, некоторые Bluebox'ы умеют передавать телефонный номер (как сумму комбинаций двух частот). Такой "ящик" должен также иметь клавишу, сообщающую на АТС о том, что номер набран и оборудование должно начать вызов. На сегодняшний день существует несколько вариантов построения "синей коробочки" - от аналоговых до компьютерных. Если твой любимый инструмент - паяльник, можешь обратиться к Сети, где найдешь массу схем аналоговых Bluebox'ов. Мы же посмотрим, как можно реализовать компьютерный вариант "коробочки".

Понадобится компьютер, имеющий звуковую карту для посылки сигналов в телефонную линию. Звуковую карту нужно подключить к линии через адаптер, включающий в себя трансформатор и поразумевающий прием обратных сигналов. Кроме того, понадобится программа генерации тонов. Такие программы можно скачать в Сети в большом количестве или написать самостоятельно. 

При некоторых обстоятельствах сигнал 2600 Гц может быть воспринят и выполнен АТС.

БАРХАТНАЯ РЕВОЛЮЦИЯ
МУЖСКОЙ СЕЗОН

ПОДРОБНОСТИ В КИНОТЕАТРАХ СТРАНЫ



@mail.ru®

НАМ ДОВЕРЯЮТ ДАЖЕ СПЕЦАГЕНТЫ

Content:

98 Мобильная оборона

Как защитить себя от мобильного взлома

102 Обзор сайтов и софта

Что посмотреть о мобильном взломе на бескрайних просторах Сети

Рахал Лу Кум

МОБИЛЬНАЯ ОБОРОНА

КАК ЗАЩИТИТЬ СЕБЯ ОТ МОБИЛЬНОГО ВЗЛОМА

Тебе никогда не приходилось оплачивать счета за звонки, которых ты не совершал? Данные с налагодника или ноутбука внезапно не исчезали? Считай, что тебе крупно повезло. Электронное мошенничество процветает, и взломы совершаются постоянно. Параллельно с развитием беспроводных технологий их количество стало стремительно возрастать. В этой статье мы дадим несколько советов по защите от мобильного взлома.



КОВАРНОЕ ВРЕМЯ

■ В далеком прошлом, когда

Землей владели динозавры, а в ходу были дискеты с MS-DOS, вирусные эпидемии сводились к проблемам личной гигиены: не копируй программы у тех, кому не доверяешь, вот и все. Вскоре появился интернет, и все изменилось. Стоит только подключить компьютер к Сети, как в нем тут же заводятся черви, шпионы и трояны, лезущие изо всех дыр. Их ловят антивирусы, брандмауэры и другой софт, однако вся индустрия находится в состоянии неустойчивой истерии. С мобильными устройствами стало еще хуже. Без средств беспроводной связи они смешны (сотовый телефон, подключаемый к ноутбуку через шнурок, выглядит не по-детски), а беспроводная связь по своей природе чрезвычайно уязвима перед атаками, особенно если она проектировалась кое-как.

Производители предлагают нам 128-битное шифрование и прочие прелести прогресса, вызывающие геморрой при настойке, но стреляющие мимо хакеров. Помните Пуха? "Не то чтобы ты совсем не попал, но ты попал не в шар!" Верить рекламе и цветастым буклетам может питекантроп, да и тот ископаемый, и чтобы не остаться без штанов, отганных на покрытие чужих разговоров, приходится самостоятельно разбираться во всех аспектах беспроводной безопасности. Хакер может осуществлять несан-

кционированное подключение к устройству, перехватывать трафик, отслеживать перемещение жертвы в пространстве или устраивать полный DoS. Уже зафиксировано несколько случаев взлома влиятельных лиц, и с каждым днем активность хакеров все возрастает. Разработчики беспроводных протоколов делают хвост пистолетом и сваливают всю ответственность на производителей оборудования, которые где-то что-то криво реализовали. Производители в свою очередь наезжают на пользователей, выбирающих предсказуемые пароли, неправильно конфигурирующих устройства и вообще отродясь виноватых (хотя пользователь еще не подписывался быть экспертом, и вообще непонятно, за что он платит деньги). В общем, виноватых не найдешь, а между тем количество беспроводных устройств уже исчисляется сотнями миллионов, эту цифру, если учесть прецеденты атак, в корзину не выбросишь. Это уже целый кворум!

Какое устройство выбрать из всего многообразия? Какое ломается легко, а какое обеспечивает наивысшую безопасность? Популярные издания дают довольно противоречивые ответы, а технические специалисты изъясняются заковыренным языком, наводящим на мысль, что плановый отдел давно переименовали в марихуановый.

ЗОНА РИСКА

■ Радиус действия большинства беспроводных устройств ограничен дистанци-



Девушка и не подозревает, что ее атакуют

ей в 10-500 метров (точная цифра зависит от класса и конструктивных особенностей конкретного оборудования), поэтому атакующий должен находиться в непосредственной близости от жертвы, что очень непорочно с физиологической точки зрения. Могут поймать и кое-что оторвать. По этой причине атаки с налагодников и ноутбуков осуществляются достаточно редко. Большинство пред-



С виду пистолет, а на самом деле - направленная антенна, отстреливающая беспроводные устройства с приличного расстояния

почитает дистанцироваться на безопасное расстояние, подключив к своему десктопу WLAN-карту и воспользовавшись внешней антенной. Добротная антенна направленного типа, снабженная усилителем мощности, уверенно держит связь на расстояниях до 1,5-2 км, а в некоторых случаях и больше того, так что простой бдительности для обнаружения атакующего уже недостаточно!

Такую антенну вместе с усилителем можно купить и легально. Их выпускает Hyper Technology, Broadcast Warehouse, "Ра-

диал" и многие другие компании. Среди хакеров большой популярностью пользуется направленная антенна HG2415Y типа Radome Enclosed от компании HyperLink Technology, которую можно заказать по интернету. Рассчитанная на стационарный монтаж, она, тем не менее, неплохо чувствует себя на фотографическом штативе или даже на обыкновенном ружейном прикладе, который превращает ее в мобильный инструмент для слежения за подвижными жертвами. Завидев парня с этой штукой, действуй хладнокровно и адекватно. Говорят, в этих случаях хорошо помогает рессора от трактора



Беспроводной взлом, осуществляемый из дома

"Беларусь". Бесшумно и безотказно!

Параболические антенны работают на расстояниях, ограниченных, фактически, лишь горизонтом видимости, однако они катастрофически немобильны, а для хакера самое главное - вовремя смотаться с места преступления. Как правило, они стационарно устанавливаются на балконе или на крыше многоэтажного дома и нацеливаются на неподвижную жертву, например на офис компании, в которой работаешь ты.

Защититься от этого можно применением специальных "шумелок-пыхтелок", загружающих весь радиодиапазон в области 2,4 ГГц, которыми окружается весь

периметр здания. Их может собрать любой радиолюбитель за чисто символическую плату, например за бутылку пива. Правильно подобранная мощность "шумелки" никак не влияет на работу беспроводных устройств внутри офиса, но препятствует антенной охоте, вынуждая атакующего применять дорогостоящие фильтры. Правда, шумелки не совсем законны и службы радионадзора (не путать с рыбнадзором) могут с этого кое-что поиметь. В смысле, могут выписать штраф.

Как вариант, можно обернуть стены офиса металлическим экраном, заземлить жалюзи, предприняв целый комплекс шпионских мер. Это законно, но внутри такого офиса не будут работать сотовые телефоны. Так что надо исходить из того, что сигнал всегда может быть перехвачен, и выбирать беспроводное устройство, которое просто так не взломаешь. Теперь понятно, для чего было придумано шифрование? Правда, оно не всегда спасает.

ШИФРОВАНИЕ

■ На рынке доминирует два типа устройств: одни поддерживают шифрование до 64 бит, другие - до 128. Что это значит для нас в практическом плане? Ма- >>



Охотник за беспроводными устройствами в полном боевом снаряжении



Направленная антенна на стационарной установке

128-битное шифрование вызывает мучения при настройке, но стреляет мимо хакеров.

ЧТО В ИМЕНЕ ТВОЕМ?

■ Общепринятая практика перевода Bluetooth как "Голубой Зуб" выглядит довольно странной, если не сказать "погозрительной". В качестве оправдания вспоминают короля викингов Harald Blatend, якобы получившего свое прозвище из-за потемневшего переднего зуба и воссоединившего Данию с Норвегией. Произношение его имени созвучно с Bluetooth'ом, в честь которого он и был назван.

Легендарный хакер Юрий Харон предлагает свою версию перевода, которая мне кажется наиболее близкой к истине (если, конечно, допустить, что истина вообще существует). "Blue" на жаргоне электронщиков означает "легкий", "простой", а tooth - "сцепка", "зацепление". Соединив все вместе, получаем "Легкая сцепка", "Простая Связь". Логично?



PCI-карта с Bluetooth - это настоящая дыра, с помощью которой можно проникнуть на компьютер



Беспроводные устройства и микроволновые печи работают на одной и той же частоте - 2,4 ГГц

тематика говорит, что для вскрытия ключа методом brute force (он же метод грубой силы, также называемый "каменным топором") в среднем требуется совершить $2n/2$ операций, где n - длина ключа в битах. Персональные компьютеры наших дней свободно перебирают до миллиона ключей в секунду, следовательно, 64-битный ключ будет гдето через 584 942 лет. Может быть, и раньше, но ненамного. Даже если взломщик сумеет оптимизировать алгоритм перебора и объединит в сеть несколько сотен мощнейших машин, он все равно останется в дураках. Это как в том американском анекдоте. Дали одному мужику триста лет, а он говорит: "Я же столько не отсижу!" Судья: "Ну мы же не бюрократы, отсидите сколько сможете". А сломать 128-битный ключ вообще нереально, даже если подойти к этому вопросу с головой. Но это - в теории.

На практике же заявленная "битность" шифрования практически никогда не достигается. Возьмем, например, Bluetooth, 128-битный ключ которого генерируется на основе 4-значного PIN-кода. В худшем случае хакеру придется перебрать 1000 комбинаций, а в среднем взлом заканчивается через 500. Даже калькулятор потребует меньше секунды времени! Хорошее же шифрование нам предлагают, нечего сказать! А если вспомнить, что большинство из нас оставляет PIN в "0000" по умолчанию или выбирает легко предсказуемые комбинации (например год своего рождения), то взломщику даже не потребуется осваивать криптографию и искать хакерский софт - достаточно просто методично перебирать PIN-номера один за другим. Обычно на подобные манипуляции уходит час-полтора. Некоторые устройства поддерживают 6-значный PIN. Перебрать его "вручную" уже нереально, но автоматическим переборщиком он ломается без проблем.

А многие устройства вообще позволяют обмениваться AT-командами, не зная никакого пароля! AT-команды - это служебные комму-

ОШИБКА ПЕРЕПОЛНЕНИЯ В WIDCOMM

■ Создатели Bluetooth предлагают готовое программное обеспечение для его поддержки, распространяемое под торговой маркой WIDCOMM (Wireless Internet and Data/Voice Communications - Беспроводной Интернет и Коммуникации для передачи Голоса и Данных), которое избавляет производителей оборудования от необходимости реализовывать весь стек протоколов самостоятельно. Программисты старой школы хорошо знают истинную цену решений "из пробырки". Обжегшись на чужих ошибках пару раз, они не доверяют никакому коду, кроме своего собственного. И не зря!

В августе 2004 года в WIDCOMM'е было обнаружено тривиальное переполнение буфера, позволяющее захватывать управление устройством простой посылкой специально подготовленного пакета. Никакой PIN для этого подбирать не нужно!

Уязвимость затрагивает BTStackServer версии 1.3.2.7, 1.4.1.03 и 1.4.2.10, используемые в Windows 98, Windows XP, Windows CE и других. Кроме этого, WIDCOMM используется многими компаниями: Logitech, Samsung, Sony, Texas Instruments, Compaq, Dell... Полный перечень включает в себя более трех десятков наименований. Все Bluetooth-устройства, производимые этими компаниями, находятся под угрозой и в любой момент могут быть атакованы. Для популярного налагодника HP IPAQ 5450 даже написан специальный эксплойт! В некоторых случаях проблема решается установкой всех заплаток или сменой прошивки, некоторые же устройства остаются открытыми до сих пор. Подробности можно найти здесь: www.pentest.co.uk/documents/pti-2004-03.html.

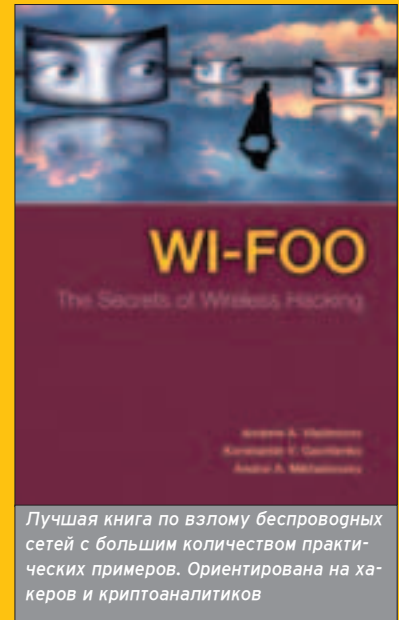
Но все-таки лучше держать Bluetooth выключенным и использовать красный глаз.

Так все-таки безопасны беспроводные сети или нет? Голубой Зуб небезопасен однозначно (и это мы только что доказали!), взломать Wi-Fi-устройства, поддерживающие стандарт IEEE 802.11i (WPA2), еще никому не удалось и, судя по всему, в обозримом будущем и не удастся. Все остальное оборудование (WEP и WPA1) вскрывается без труда. Ни частая смена секретных ключей, ни SSID, ни привязка к MAC-адресам, ни даже так называемое 128-битное шифрование от настоящих хакеров не спасает и годится разве что на роль пугала, воздействующего на новичков и просто любопытствующих пользователей, читающих хакерские журналы.

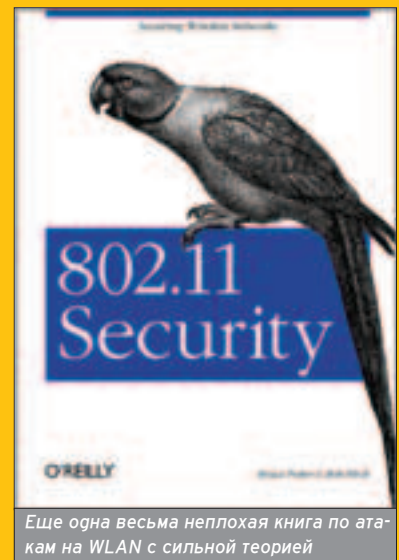
никационные команды, с помощью которых с устройством можно вытворять что угодно: звонить войсом, просматривать содержимое адресной книги, уничтожать файлы и т.д. Вот неполный

список моделей сотовых телефонов, страдающих этой "болезнью": Nokia 6310, 6310i, 8910 и 8910i; Ericsson/Sony Ericsson T68, T68i, R520m, T610 и Z1010; Motorola V80, V5xx, V6xx и

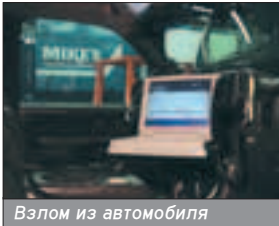
E398. У Siemens'a в этом плане дела обстоят намного лучше, и без знания PIN'a к нему не подключишься. Однако, как мы уже говорили, PIN легко подобрать. Гарантированно защититься от



Лучшая книга по взлому беспроводных сетей с большим количеством практических примеров. Ориентирована на хакеров и криптоаналитиков



Еще одна весьма неплохая книга по атакам на WLAN с сильной теорией



Взлом из автомобиля

атак на Bluetooth нельзя! Поэтому никогда не держи его включенным без необходимости!

Перейдем к Wi-Fi-устройствам, также известным под именем WLAN. Они используют то же самое 64/128-битное шифрование. Во всяком случае, внешне. В действительности ключ состоит из двух частей: 24-битного вектора инициализации, который передается открытым текстом, и 40/104-битного секретного ключа. Фактическая "битность" шифрования намного меньше заявленной! Но реклама предпочитает молчать об этом, делая из нас жертв уже второй раз. Нет, определенно надо топтать в общество защиты прав потребителей и качать свои права. Как легко показать, 40-битный ключ взламывается за несколько часов, поэтому с ним далеко не уйдешь. Тут же нагрянут и взломают. А потом снова нагрянут и снова взломают!

104-битный ключ выглядит намного более надежным. Простой математический расчет показывает, что до окончания нефти и других природных ресурсов его никто не взломает, а после - сотовые телефоны станут неактуальными и человечество будут заботиться совсем другие проблемы. Тут энергетический кризис назрел, понимаешь, а вы со своими паролями.

Математика, конечно, - точная наука. Споры нет. Но в военное время значение синуса может достигать четырех! Защита похожа на столб. Ее трудно перепрыгнуть, но легко обойти. Механизм шифрования, используемый беспроводными устройствами первого поколения, настолько кривой, что вскрывается мотком проволоки и отверткой. Опознать это чудо можно по логотипу WEP (Wired Equivalent Privacy - Эквивалент Проводной Безопасности), напечатанному на этикетке или содержаще-


мус в конфигурационных настройках устройства. За все время своего существования этот самый WEP латался столько раз, что на нем уже живого места нет, но ломать его не перестали. В Сети лежит огромное количество атакующих утилит, с которыми управится даже ребенок! В прессе постоянно появляются сообщения о взломе ноутбуков и ноутбуков различных актеров и певиц, и хотя технические подробности, как правило, не разглашаются, косвенный анализ позволяет установить, что в большинстве случаев в деле фигурируют устройства, поддерживающие шифрование WEP, то есть никакое не шифрование, а его полную профанацию! Мой тебе совет: держись от него подальше!

Достаточно многие устройства поддерживают технологию ACL (технология Access Control List - Список Управления Доступом), блокирующую несанкционированное подключение всех "левых" устройств, которую "эксперты по безопасности" настоятельно рекомендуют держать во взведенном состоянии. Только это как мертвому припарка, и ее очень легко обойти. Все работает приблизительно так. У каждого сетевого устройства имеется уникальный MAC-адрес, назначаемый производителем. В настройках карты хранится список MAC-адресов, заполняемый потребителем и перечисляющий адреса всех устройств, подключения с которых разрешены. Вроде бы все правильно, но разработчики не учли, что MAC передается по Сети открытым текстом и может быть легко перехвачен. Подавляющее большинство беспроводных карт позволяют перепрограммировать свой MAC, что называется, "на лету". Словом, ACL обеспечивает лишь видимость защищенности по типу "в Baggage все спокойно". В общем, ситуация ласты и потребители пролетают, в смысле ругаются матом, дергают производителей и требуют: "Ну сделайте же хоть что-нибудь!"

Производители подумали и сделали. Несколько лет назад на рынке появились

устройства, поддерживающие WPA (Wireless Protected Access - Беспроводной Защищенный Доступ). Что это такое? Вообще типичную инженерную контуру. Трещат клавиатуры, гудят жесткие диски, озонирует лазерный принтер и вдруг раздается страдальческий голос: "Господи, как у меня устала задница!" И тут же следует ответ: "А ты попробуй думать головой".

Грубо говоря, WPA - это навороченный WEP, реализованный на той же самой аппаратной базе с сохранением всего технологического цикла. В общем, не головой, а... Производители довели прошивку - и все! И хотя в открытом доступе готовых атакующих программ до сих пор не наблюдается, безопасность WPA находится под большим сомнением, то есть под прицелом. И чьи-то хакерские руки уже держат спусковой курок. Со дня на день WPA все непременно будет взломан - теоретический фундамент уже есть, осталось только сесть и накопить. Кто-то, возможно, уже и накопил, теперь сидит радуется, а другим не дает. Потому что редиска!

Тем не менее, до сих пор не зафиксировано ни одного достоверного взлома устройств с WPA, и для домашнего использования они вполне пригодны. Но лучше не хвататься за хвост умирающего мамонта и обратить внимание на новый стандарт шифрования IEEE 802.11i, по маркетинговым соображениям переименованный в WPA2. Да какой это, к черту, WPA? Он устроен совсем по-другому, требует совсем других микросхем, и вообще в нем все не так. Смена отлаженного технологического цикла индустрии невыгодна, и с его внедрением пока не спешат, однако устройства на его основе уже начинают появляться и их ассортимент с каждым днем будет неуклонно расширяться. Как говорится, выбирай - не хочу. Как не хочу?! Это как раз то, что нам нужно! 

Тестирование мобильных устройств PDA, ноутбуков и сотовых телефонов

Лучшие аксессуары для PDA и ноутбуков

Легкая выбор

Таблица совместимости устройств в

выборе устройств

100% гарантия

Доставка по всей территории России

Клиентский центр в Москве

Бесплатно с доставкой на дом

Мобильные компьютеры

- Upgrade CD-ROM
- Высокоскоростной модем
- Сетевые адаптеры
- Текст как файл
- CD-R RW 2x
- Поддержка AOD
- Телетекст и интернет
- Синхронизация с Microsoft
- Передача файлов через интернет
- Бесплатный ИС



Мобильные компьютеры



Андрей Каролик (andrusha@real.hacker.ru)

ОБЗОР САЙТОВ И СОФТА

ЧТО ПОСМОТРЕТЬ О МОБИЛЬНОМ ВЗЛОМЕ НА БЕСКРАЙНИХ ПРОСТОРАХ СЕТИ

Всем ясно, что журнал не резиновый и многое в него не помещается чисто физически. То, что не влезло, мы даем в виде ссылок. Отдельно хорошие ресурсы, статьи и утилитки - кому что нужно.



WWW.WARDRIVING.COM

Зная, что вардрайвинг пишется как wardriving, несложно найти соответствующий сайт в Сети методом гугления. Сайт без лишнего графического изыска и, что называется, по теме. Все на английском, зато обновляется часто. Новостная лента введет тебя в курс дела, а разделы экипи-



ровки

(www.wardriving.com/setup.php) и безопасности (www.wardriving.com/security.php) пригодятся на практике. В экипировке описаны нужные утилитки, есть ссылки на производителей антенн, сетевых карт и GPS-приемников. И еще много полезных ссылок на другие аналогичные ресурсы. Очень хороший ресурс! Если планируешь заняться вардрайвингом, обязательно посети его.

WWW.HYPERLINKTECH.COM

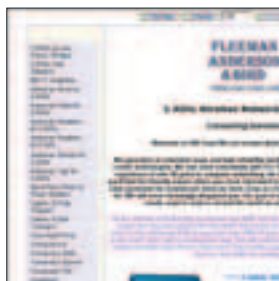
Уж что-то, а антенны продаются совершенно легально, купить их гораздо проще, чем холодное или огнестрельное оружие. Не забудь прикупить вместе с антенной и усилитель. Хорошие антенны выпускают Hyper Technology, Broadcast Warehouse, "Па-



диал" и многие другие компании - в интернете их масса. Но среди хакеров наибольшей популярностью пользуются антенны типа HG2415Y (Radome-Enclosed) от компании HyperLink Technology. На сайте www.hyperlinktech.com можно заказать любую антенну через интернет на дом. Тут же приведены все спецификации выбираемых антенн, наглядные картинка и параметры. Доставка не бесплатная, но ехать в Штаты еще накладнее.

HTTP://INTERFACES.BY.RU/INTERFACES.HTM

Здесь можешь найти информацию об интерфейсах, в том числе о IEEE 802.11g. По-русски, с картинками и достаточно подробно. Кто выпускает железки, как они работают, в чем разница между модификациями стандарта, как можно повысить пропускную способность, совмести-



мость оборудования и дополнительная литература. Можно посетить и родной сайт со спецификациями - <http://grouper.ieee.org/groups/802/11>, но, естественно, там все уже на английском.

WWW.FAB-CORP.COM

А здесь можно посмотреть (и купить) различные железки, работающие на частоте 2,4 ГГц (Wi-Fi) и использующие стандарты Wi-Fi 802.11b и Wi-Fi 802.11g. Тут точки, адаптеры, усилители, всевозможные антенны, фильтры, сплиттеры, кабели, коннекторы, и все это в большом количестве. Так что, если есть банковская карточка и желание заняться мобильным взломом в его самом прикольном проявлении, беги сюда: здесь закупишься инструментами без проблем.

WWW.WI-FIPLANET.COM

Еще один хороший ресурс, посвященный Wi-Fi. Стандартный набор рубрик: новости, статьи, обзоры, технологии, хот-споты, форум, глоссарий и железки. Здесь можно поискать хот-споты и по России, только непонятно, кто пополняет базу, так как список состоит всего из восьми адресов. Плюс я был приятно удивлен, когда попытался зайти на форум и был про-



информирован, что мой IP-адрес забанен :).

WWW.ISS.NET/WIRELESS/WIRELESSLAN802_11BSECURITYFAQ.HTM

Онлайн-FAQ (ЧАВО) по безопасности беспроводной сети 802.11b. В довесок стоит посмотреть неофициальную страничку www.drizzle.com/~aboba/IEEE, также посвященную проблеме безопасности сетей, построенных по стандарту IEEE 802.11. На втором сайте просто обилие ссылок по теме, так что недостаток в информации быть не должно :).

HTTP://AIRSNORT.SHMOO.COM ИЛИ HTTP://AIRSNORT.SOURCEFORGE.NET

AirSnort - как ты, наверное, уже знаешь, утилита, реализующая атаку Fluhrer-Mantin-Shamir (FMS), то есть взлом за счет "слабых" ключей. Если не можешь реализовать такую атаку сам, достаточно скачать AirSnort, запустить ее и наслаждаться. Но для успешной атаки нужно будет немало подождать, чтобы перехватить достаточное количество пакетов. Обычно это порядка пяти-десяти миллионов, в зависимости от интенсивности обмена данными с жертвой. Сбор информации идет в пассивном режиме, поэтому потенциальная жертва не сможет засечь атаку.

WWW.KISMETWIRELESS.NET

Kismet - любимый сетевой сниффер Wi-Fi для LINUX-хакеров. Как это часто бывает, изначально ориентированная на исследо-



вательские цели программа стала основным оружием для перехвата трафика.

Поддерживает большинство железок и беспроводных протоколов, удобна в использовании и к тому же абсолютно бесплатна. Перехватывает сетевой трафик, показывает SSID- и MAC-адреса, подсчитывает количество пакетов со слабыми векторами инициализации и т.д.

WWW.E.KTH.SE/~PVZ/WIFI

■ dwergrack - утилита от хакеров из лаборатории Hikari of DasbOden Lab, была выпущена еще в начале 2002 года. Это усиленный FMS-алгоритм, сокращающий количество необходимых пакетов с шести миллионов (как для AirSnort) до 500 тысяч. Знающие люди говорят, что иногда 40/104-битный ключ взламывается всего с тремя тысячами пакетов, что позволяет атаковать домашние точки доступа, которые более чувствительны к избыточному трафику. Но, несмотря на все эти улучшения практической реализации, суть атаки полностью аналогична FMS-алгоритму.

WWW.CRO.NET:8040/CODE/NETWORK

■ Aircrack - снифер для беспроводных сетей стандарта 802.11 с возможностью расшифровки 40-



битных и 104-битных WEP-ключей.

WWW.NETSTUMBLER.COM

■ Network Stumbler - лучший сканер беспроводных сетей под Windows. Позволяет обнаруживать беспроводные сети и получать массу полезной информации о них. К примеру, можно определить имя и название сканируемой сети, производителя оборудования, наличие шифрования для передачи данных и т.д. В спарке с GPS-приемником Network Stumbler может записывать в log-файл не только различные характеристики точки вроде уровня сигнала или типа шифрования, но и ее координаты! А это позволит в дальнейшем наложить всю информацию о найденных AP на карту. Невероятно удобно. Кроме того, Network Stumbler поддерживает почти все существующие сетевые адаптеры и абсолютно бесплатен!

На www.netstumbler.com также имеется вариант и для Pocket PC - MiniStumbler, который обнаруживает сеть, измеряет интенсивность сигнала, отображает SSID/MAC-адреса, определяет наличие WEP-шифрования. Обычно в связке с MiniStumbler еще использу-

ют Sniffer Portable и Aircracker Mobile, которые грабят все пролетающие мимо пакеты и записывают их в файл. Полученные пакеты через взломщик паролей пропускаются чаще всего уже на обычном ПК -



ресурсов процессора КПК тут уже не хватит.

HTTP://WEPLAB.SOURCE-FORGE.NET

■ WepLab - Альтернатива Aircrack, умеющая перебирать возможные значения по словарю, что иногда очень эффективно.

WWW.SONAR-SECURITY.COM

■ Stumbverter - удобная программка для обработки логов сканеров и нанесения обнаруженных точек доступа на растровые изображения карт местности. Напечатать небольшой тираж и пойдешь продавать в электричках :). Кстати, интересная идея.

HTTP://BINAERVARIENZ.DE/PROJEKTE/PROGRAMMIEREN/KISMAC

■ Утилита KisMAC - весь хакерский инструментарий для MAC'a в одном флаконе. Все интуитивно понятно. Есть сетевой сканер, снифер, парольный пере-

борщик (brute force) и криптоанализатор слабых векторов инициализации. Для извращенцев есть планировщик, позволяющий осуществлять атаки по расписанию :).

WWW.XAKEP.RU

■ Не могу не упомянуть всеми горячо любимый сайт журнала. Он живет совершенно своей жизнью и с журналом почти не пересекается. Тем не менее, на нем регулярно выставляются хорошие свежие статьи и ссылки на другие ресурсы. Там можно узнать последние новости из мира взлома, почерпнуть новое о софте и даже написать собственную статью, если хорошо разбираешься в теме.

HTTP://FORUM.CXEM.NET

■ Форум паяльника - хорошая идейная кладовая по фрикингу и пересекающимся темам: жучки, сотовая связь, спутниковое ТВ, микроконтроллеры, электроника и все в таком духе. Если ты представляешь, как выглядит паяльник, то уже есть повод зайти на сайт :). Тут тебе и взлом домофонов, и АТС, и аппаратов DECT, и клонирование симок, и са-



Отдых, который вам нужен

ИГИДА АЭРО
Т. 945 3003
945 4579

Лиц. ТД № 0025315

АВЦ
Т. 508 7962
504 6508

модельный сотовый сканер, и два телефона на одну линию, и bluebox - в общем, куча невероятно интересных штук. У форума есть и свой сайт - <http://cxem.net>, с залежами различных схем и программ, которые могут понадобиться в процессе.

WWW.HACKERSRUSSIA.RU

■ Рай для фрикера: радио, сотовая связь, мобильки, телефоны, АТС, моббинг, пейджинг, транкинг, фрикинг, жучки. Гигабайты полезной информации, программ и ссылок на другие ресурсы. К примеру, ты интересуешься карточками - тут есть описание белорусских, украинских, питерских карточек, еврочипов, эмуляторов, различных прошивок и программ для перезаписи. По каждому направлению есть своя ветка в форуме - www.hackersrussia.ru/Forum/forum.php. Не найдешь - так спросишь :).

WWW.ABOUTPHONE.INFO/JS/PHREAK.HTML

■ Много полезного по телефонии и фрикингу. Как они сами пишут, "материалы по всем аспектам несанкционированного доступа к аппаратуре АТС (бесплатный межгород, обман таксофонов, обман АОН, подслушивание разговоров) и о том, что бывает с теми, кто пытается этим заниматься" :).

HTTP://DOSKA.POLIGON.INFO

■ Доска объявлений для тех, кто хочет продать или купить электронные компоненты, радиодетали, расходные материалы и оборудование. Можно предложить услуги или бартер. При этом сообщения не хранятся более 30-ти дней, так что информация особо

не устареет. Хватает и спама, но в целом тот, кому нужны детали, оценит.

WWW.TEXTFILES.COM/PHREAK

■ Если от фрикинга ты в восторге, но про сам фрикинг ничего не знаешь (очень часто бывает именно так), то стоит заглянуть в эту виртуальную библиотеку. Тут просто тонны различной информации по фрикингу. В основном статьи написаны в 80-х и 90-х годах, то есть в те времена, когда фрикинг только появился, встал на ноги и заявил о себе. Проще понять историю развития фрикинга, тенденции и смену приоритетов вслед за изменением технологий. Часть материалов уже устарела, но ностальгия же жива. При желании можно выкачать все разом, но придется тянуть более десятка гигабайт :).

HTTP://PRANKI.INFO/FILES

■ Море пранков и приколов. Пранк - от английского prank ("выходка", "проделка"). Не стоит путать пранки с любовным телефонным хулиганством. Ребята гораздо умнее, избегают номеров с АОНами и просто глупых или, наоборот, очень умных людей. Зато любят заводных и с подвешенным языком :). Более подробно о самом пранке можно почитать в статьях: http://pranki.info/files/modules.php?name=Articles&pa=list_pag&articles_categories_id=1. А скачать пранк-перлы можно тут: <http://pranki.info/files/modules.php?name=Files>.

HTTP://BENPRANKS.NAROD.RU

■ Еще один сборник прикольных пранков. На самом деле их полно, но этот понравился частотой обновления и приличным количе-

ством уже имеющихся пранков, причем авторских. В интернете, как правило, встречаешь просто копии одного и того же, авторские пранки в цене :). Тут же можно найти программы, которые помогут самому сделать подобное: Modem Spy v 2.3 (небольшая и удобная, для голосовых модемов) и Ascrecord (для записи телефонных разговоров). Только будь осторожен, за это могут и по голове "погладить".

HTTP://FTN.PP.RU/FIDOT7.RU.PHREAKS

■ Зеркало фидошного форума RU.PHREAKS. Если просто в интернете ты вряд ли встретишь живого фрикера, то здесь это более чем возможно. Домашнего адреса, конечно, тебе никто не даст и в гости на чай не позовет. Но поделиться знаниями и что-то посоветовать здесь могут. Главное - не надоедать :), не спрашивать по сто раз то, что уже спрашивали другие. Придерживайся правила: сначала прочитай имеющиеся сообщения, и только если там нет того, что интересно, смело спрашивать. А в остальном - смотри, читай, пиши туда свои эпосы.

HTTP://FORUM.WEBHACK.RU

■ Один из форумов по взлому и безопасности, в котором есть отдельная ветка "Радиолобительство и фрикинг". Почему выбрали именно это? Наиболее живой (посты не датируются прошлым годом, как на других форумах) и достаточно активный (более 300 тем). В целом не ограничи-

вайся, конечно, только им, открывай поисковик и по запросу "форум по фрикингу" черпай ресурсы. Вряд ли понадобится еще один форум - на многие вопросы ты получишь ответы уже в этом :).

ОТДЕЛЬНЫЕ СТАТЬИ

■ www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf - та самая нашумевшая статья от Scott Fluhrer, Itsik Mantin и Adi Shamir "Слабые места алгоритма распределения ключей RC4" ("Weaknesses in the Key Scheduling Algorithm of RC4"). Именно эти ребята раскопали существование классов слабых (weak) ключей, в которых несколько битов ключа оказывают значительное влияние на зашифрованные данные, что способствует ускорению взлома благодаря избавлению от перебора миллионов (если не миллиардов) комбинаций.

<http://bugtraq.ru/library/security/zaurus.html> - вардрайвинг с Zaurus.

www.turnpoint.net/wireless/cantennahowto.html - как сделать антенну своими руками, используя консервную банку.

www.oreillynet.com/cs/weblog/view/wlg/448 - еще один эпос про самодельную антенну, только на этот раз используется упаковка от чипсов :).

www.turnpoint.net/wireless/has.html - сравнительные тесты антенны-самопала из упаковки от чипсов, с промышленным образцом, который продается в интернет-магазинах.

www.computery.ru/upgrade/faq/oft/2005/sfaq_214.htm - о Wi-Fi-сниферах.

www.securitylab.ru/analitics/216384.php - атаки на WEP.

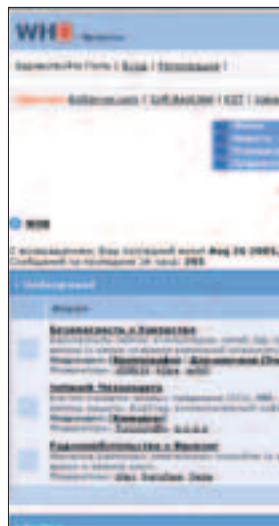
www.cyberinfo.ru/3/87_1.htm - проникновение в беспроводную сеть.

www.aboutphone.info/js/lib/phreak/history.html - фрикинг сотовых телефонов в России.

www.aboutphone.info/js/lib/phreak/taxphone.html - бесплатные звонки с таксофонов.

www.aboutphone.info/js/lib/phreak/blackbox.html - BLACK BOX - бесплатные звонки с обычного телефона.

www.xaker.ru/magazine/xa/063/090/1.asp - фрикинг по-русски. 



Если ты хочешь помочь нам делать журнал, вступи в фокус-группу Спеца! Участники фокус-группы смогут первыми оценить предстоящие нововведения, высказывать свое мнение о каждом номере напрямую редакции. От тебя требуется немного: быть в онлайне, периодически отвечать на вопросы редакции и, самое главное, желание. Чтобы попасть в фокус-группу, нужно всего лишь заполнить эту анкету и прислать ее нам. Если ты не хочешь быть в тест-группе, все равно пришли анкету - нам это очень важно!

Давно ли ты читаешь "Хакер Спец"?

- С первых номеров
- Около года
- Несколько последних номеров
- Первый раз

Как ты считаешь, изменился ли "Хакер Спец" за последнее время?

- Да, улучшился
- Да, ухудшился
- Нет, по-моему, не изменился

Какой из последних номеров тебе понравился больше всего?

- 07.05(56) - Мобильные деньги
- 08.05(57) - (anti)cracking
- 09.05(58) - Security-фокусы
- 10.05(59) - Мобильный взлом

Хотелось бы тебе новых рубрик в ОФФТОПИКе?

- Да
- Нет

Достаточно ли объемна ТЕМА НОМЕРА?

- Вполне
- Ее надо увеличить
- Слишком большая

Было бы тебе интересно читать новости в Спеце?

- Да
- Нет

Интересна ли тебе СТОРИ?

- Да
- Нет
- А что это?

Какие компьютерные журналы ты еще читаешь?

- Хакер
- CHIP
- CHIP Special
- Компьютерра
- Upgrade
- Мир ПК
- Upgrade Special
- Другой _____

Какой оптический привод в твоём компьютере?

- CD-ROM/CD-RW
- Combi CD-RW/DVD-ROM
- DVD-ROM/DVD-RW

Предложи тему для очередного номера:

О себе

ФИО

Где ты живешь?

E-mail

Сколько тебе лет?

- Меньше 17
- 18-20
- 21-23
- 24-27
- 28-30
- 30-33
- Больше 33

Твое семейное положение?

- Холост
- Женат

В каком вузе ты учишься?

- Техническом
- Гуманитарном
- Я не учусь в вузе

Связана ли твоя работа с информационными технологиями?

- Да
- Да - планирую работать в ИТ
- Нет
- Я не работаю

Твой средний месячный доход?

- Меньше \$100
- \$100-300
- \$300-700
- Больше \$700

Сможешь ли ты сам собрать компьютер?

- С закрытыми глазами
- По книжке
- Сомневаюсь

Какой у тебя канал в интернет?

- Выгеленка
- Dial-up
- Нет интернета

Чем ты пользуешься для общения в Сети?

- E-mail
- Чаты
- ICQ и другие мессенджеры
- Другое _____

На каком языке ты пишешь?

- Assembler
- C/C++
- Pascal/Delphi
- Basic/VB
- Perl
- Другое _____
- Я не программер

С какими платформами у тебя есть опыт работы?

- PC (Windows)
- *nix (Unix, Linux, BSD)
- Macintosh
- Palm OS
- Pocket PC (Windows CE)
- EPOC/Symbian
- Другое _____

Какие из перечисленных вещей у тебя есть?

- DVD-плеер
- DVD-ROM
- MP3-плеер
- Ноутбук
- Домашний кинотеатр
- Мобильный телефон
- КПК (коммуникатор)
- Цифровой фотоаппарат
- Цифровая видеокамера
- GPS-навигатор

- Да, я хочу в фокус-группу!

Заполненную анкету присылай по адресу: 101000, Москва, Главпочтамт, а/я 654, Хакер Спец с пометкой «Анкета» или на vote@real.hacker.ru.



АНОНС

Читай в следующем номере Спеца

СКРЫТАЯ УГРОЗА

- Кунсткамера шпиона
- Военный шпионаж
- Зарубежные разведки
- Слежка в реальной жизни
- Шпионское оборудование
- Изменение внешности
- Жучок своими руками
- Скрытое видеонаблюдение
- Правовые аспекты
- Противодействие шпионажу
- Компьютерная слежка
- PGP: история и мифы

+
Весь софт
на CD

А также:

- СКРЫТЫЕ СИСТЕМНЫЕ СЛУЖБЫ СЕТЕВОГО УРОВНЯ IP В ЗАКРЫТЫХ ОС И ДРУГИЕ РАСКРЫТЫЕ ТАЙНЫ!

СКОРО В СПЕЦЕ:

ИНТЕРНЕТ-ДЕНЬГИ

Обменники валюты, казино и другие web-сервисы, связанные с интернет-валютой. Различные платежные системы: WebMoney, e-gold, GoldMoney, PayPal и др. Заработок, процессинг: что и как реализовать. Как делают пирамиды. Виртуальные банки. Мошенничество, «кидалово» в e-commerce.

ПАПЕ ЛЕНЬ ИДТИ В МАГАЗИН?

НЕ ГРУСТИ!

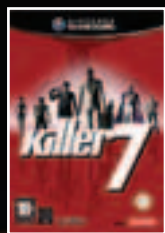
РАССКАЖИ ЕМУ ЧТО

в интернет магазине GamePost



Juiced

\$55.99



Killer 7

\$83.99



Grand Theft Auto:
San Andreas

\$79.99

* Не нужно выходить из дома, чтобы сделать заказ

* Покупку можно оплатить кредитной картой

* Игру доставят в день заказа

PlayStation 2 (Slim)

\$175.99



GameCube

\$139.99



Xbox

\$279.99

Играй просто!

GamePost



Тел.: (095) 780-8825
Факс.: (095) 780-8824

www.gamepost.ru



Content:

108 Видеоатака!

Тестирование современных видеокарт

113 Матплата для железного экстремала ECS PF5 Extreme

114 Паяльник

Стань PHREAK'ом: те самые коробочки

HARD

Дмитрий Окунев, test_lab (test_lab@gameland.ru)

ВИДЕОАТАКА!

ТЕСТИРОВАНИЕ СОВРЕМЕННЫХ ВИДЕОКАРТ

Последние месяцы очень положительно отразились на состоянии рынка видеокарт: все больше моделей Hi-End-сектора переходят в более низкую ценовую категорию, становясь общедоступным мейнстримом. Кроме того, появляется все больше чипсетов, позволяющих при адекватной стоимости получить достойную производительность даже в самых современных играх. Мы решили провести небольшой экскурс в эту область и протестировали несколько моделей видеокарт из разных ценовых категорий. Отметим, что практически все устройства из материала имеют одну особенность - улучшенную в сравнении с референсной системой охлаждение, поэтому эти девайсы можно отнести и к оверклокерским моделям.

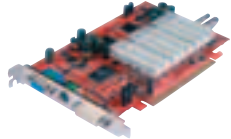

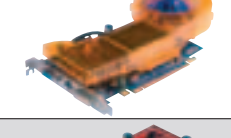
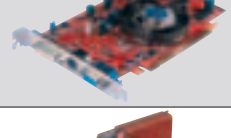
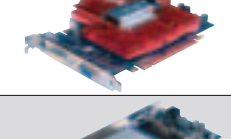
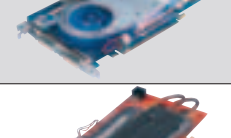
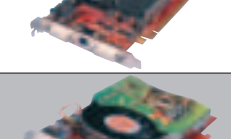
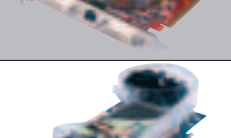

ТЕХНОЛОГИИ

■ Современная видеокарта - это не только мощный чипсет, но и такие важные компоненты, как память и система охлаждения. С первым все понятно: стоит обратить внимание на рабочие частоты, которые часто завышаются производителями, а также на количество пиксельных конвейеров, которое на некоторых "урезанных" моделях плат легко увеличивается, повышая производительность девайса на порядок. С памятью сложнее. Во-первых, следует обратить внимание на ширину шины обмена с процессором: чем она больше, тем лучше. Во-вторых, большое значение имеет латентность модулей. Здесь отсчет идет в обратную сторону: чем меньше значение, тем больше шанс безболезненно повысить их частоту. Ну и, наконец, последний, но немаловажный фактор - тип упаковки: это TSOP (устаревший способ исполнения корпуса с планарными выводами, который ограничивает частоту памяти) или BGA (микросхемы с выводами в виде шариков на пузе - гораздо более привлекательный форм-фактор с лучшими частотными характеристиками).

Выбор системы охлаждения зависит только от твоих предпочтений: для разгона следует

test_lab выражает благодарность за предоставленное на тестирование оборудование российским представителям компаний nVidia, ATI, Sapphire, Asus.

СПИСОК УСТРОЙСТВ

	GeCube Radeon X600XT Extreme
	GeCube Radeon X700 Pro
	Sapphire Radeon X700 Pro Toxic
	Sapphire Radeon X550
	Asus EN6600 GT Silencer
	Asus EN7800 GT
	PowerColor X800XL
	PowerColor X800GT
	Chaintech Apogee AE6800

Тестовый стенд

Процессор: Intel Pentium 4 670 3,8 ГГц

Материнская плата: ECS PF5 (Intel i945P, LGA775)

Память: 2x512 Мб DDR2 XMS2-4300 Corsair

Жесткий диск: Seagate Barracuda 80 Гб

Блок питания: 350 Вт PowerMan Pro

брать плату с мощным кулером, охлаждающим не только чип, но и память. Если же над платой не планируется проводить никаких оверклокерских манипуляций, вполне достаточно несложной и даже пассив-

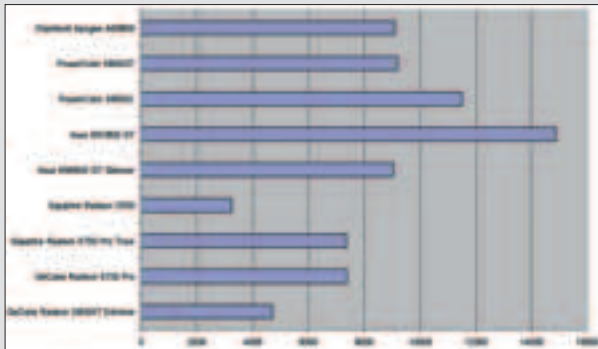
ной (без вентилятора) системы.

МЕТОДИКА ТЕСТИРОВАНИЯ

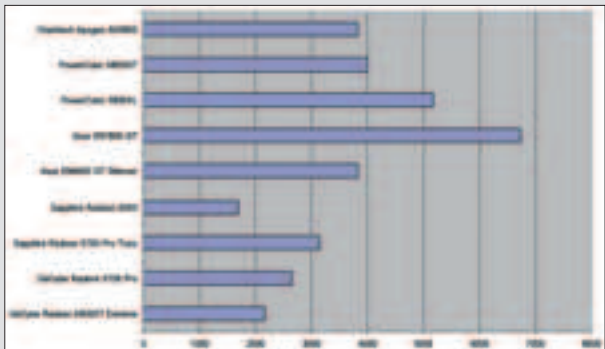
■ Был использован следующий набор приложений: 3DMark'03, 3DMark'05, а так-

же игры Unreal Tournament 2004, Doom 3, Far Cry. Помимо основного теста, в котором бенчмарки прогонялись на стандартных настройках, а игры - в разрешениях 1024x768 и 1600x1200, для высокопроизводитель-

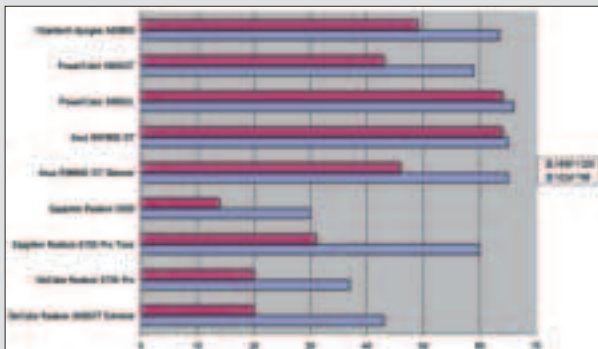
ных плат были проведены дополнительные испытания, в которых участвовали только игровые приложения, причем в драйвере форсировалась анизотропия 16x и полноэкранное сглаживание уровня 4x.



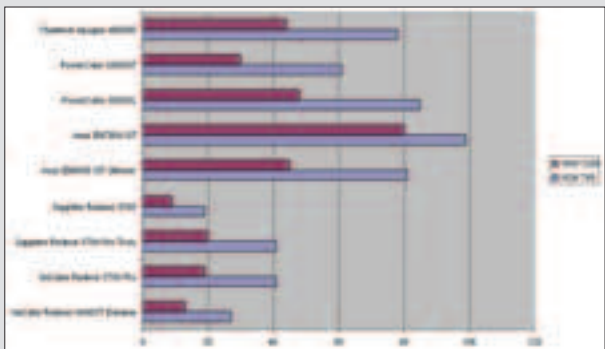
3DMark'03: более 14 000 "попугаев" в 3DMark'03 - реальность не только для экстремальных оверклокеров



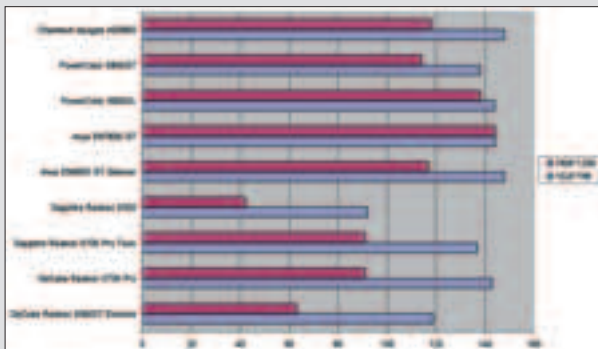
3DMark'05: если бы не топовый Asus EN7800GT, платы от ATI стали бы победителями...



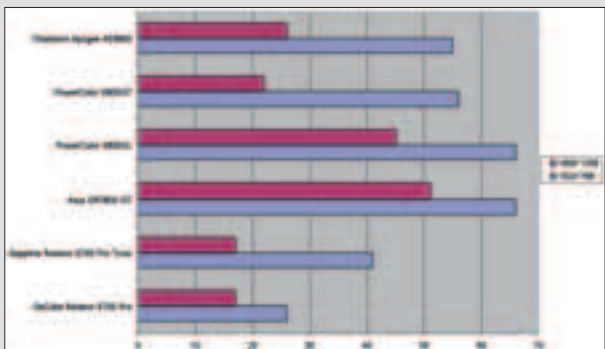
Far Cry: GeForce Radeon X700 Pro показала неожиданно слабый результат в Far Cry



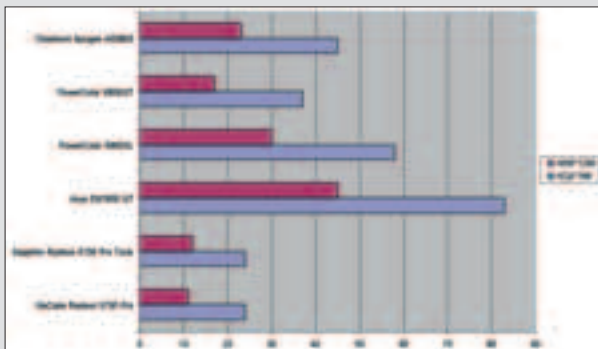
Doom 3: Middle-End от NVIDIA идет на равных с лучшими решениями от ATI. На то он и Doom :)...



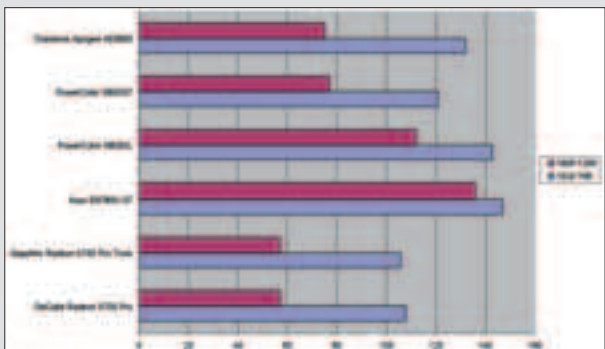
UT2004: плата на NVIDIA GeForce 7800GT, кажется, подобралась к "потолку" возможностей UT2004



Far Cry AA+AF: новый GeForce 7800GT или уже не новый Radeon X800XL - кто кого?



Doom3 AA+AF: NVIDIA, как всегда, вне конкуренции. Это особенно заметно при дополнительной нагрузке



UT2004 AA+AF: с большинством современных карт играбельность в UT2004 сохраняется даже при "утяжеленных" графических настройках...

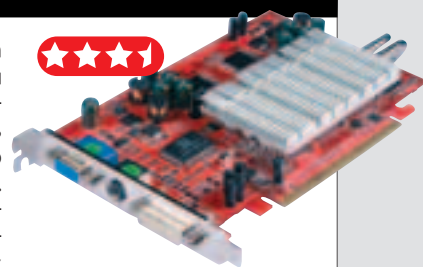
GECUBE RADEON X600XT EXTREME

» Плата поставляется в небольшой картонной коробке и комплектуется не очень богато по сравнению с другими моделями. С другой стороны, для конечного пользователя комплект поставки девайса - далеко не камень преткновения, тем более что эта видеокарта относится к бюджетной ценовой категории. Но продукту GeCube и без того есть чем похвастаться: он обладает повышенными рабочими частотами как по чипу, так и по памяти (525/400 МГц против штатных 500/380

Технические характеристики:
Интерфейс: PCI Express
Ядро: ATI RV380
Количество пиксельных конвейеров, шт: 4
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 525
Частота памяти, МГц: 398 (796)
Тип памяти: DDR-1
Выходы: DVI, D-Sub, S-Video
Цена: \$169

МГц). А если учесть, что в модели используются модули памяти BGA с задержкой 2,2 нс, то можно с уверенностью сказать, что и эти значения - далеко не предел. Система охлажде-

ния GeCube Radeon X600XT Extreme целиком пассивная, так что о лишнем шуме можно забыть раз и навсегда (ну или до следующего апгрейда :)). Она состоит из двух небольших алюминиевых радиаторов, соединенных тепловыми трубками, и на ощупь греется не очень сильно. Тем не менее, если такой девайс покупается с учетом будущего сурового разгона, мы все же посоветовали бы использовать полноценную активную систему, желательно с возможностью охлаждения



памяти. И напоследок упомянем наличие VIVO, что наверняка придется по вкусу начинающим кинолюбителям.

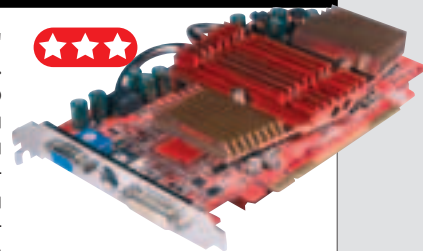
GECUBE RADEON X700 PRO

» Еще одна плата от GeCube, на этот раз основанная на чипсете ATI Radeon X700PRO - недавнем фаворите в линейке канадской компании, но сейчас это лишь неплохое Middle-End-решение. Тем не менее, GeCube Radeon снабжен всем, что нужно добротной домашней системе: 128 Мб памяти типа GDDR-3, работающей на 128-битной шине, восемь пиксельных и четыре вершинных конвейера, а также фирменная система охлаждения SilenCool. О пос-

Технические характеристики:
Интерфейс: PCI Express
Ядро: ATI RV410
Количество пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 128
Частота ядра, МГц: 425
Частота памяти, МГц: 432 (864)
Тип памяти: GDDR-3
Выходы: DVI, D-Sub, S-Video
Цена: \$151

ледней расскажем подробнее: как и предыдущая модель, эта плата легко обходится без вентилятора, который успешно заменен громоздкой медной конструкцией с тепловыми

трубками, "обнимающей" устройство с обеих сторон. Несмотря на то, что "крылья" этой конструкции накрывают собой модули памяти, говорить об их эффективном охлаждении нельзя, так как между ними отсутствует контакт. Эти ответвления, скорее, служат для более эффективного отвода тепла от чипа. К сожалению, все перечисленное не помогло плате в процессе тестирования, например Far Cry показал слабый результат для такого чипсета.



Мы можем порекомендовать данный девайс только любителям абсолютной тишины и откровенным фанатам GeCube, впрочем, на базе ATI Radeon X700Pro это далеко не худшее решение...

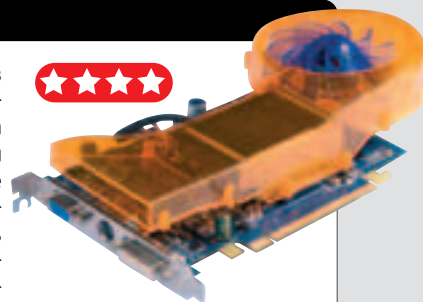
SAPPHIRE RADEON X700 PRO TOXIC

» Это решение от Sapphire - гораздо более удачный, по сравнению с предыдущей моделью, пример платы на базе чипсета ATI Radeon X700PRO. Сразу видно, что компания хотела представить пользователям всех категорий нечто неординарное, привлекательное и впечатляющее: на плате реализована собственная двухслотовая система охлаждения турбинного типа (что, впрочем, повредит доступности близлежащего PCI-разъема). Супер до-

Технические характеристики:
Интерфейс: PCI Express
Ядро: ATI RV410
Количество пиксельных конвейеров, шт: 8
Шина памяти, бит: 256
Объем памяти, Мб: 256
Частота ядра, МГц: 425
Частота памяти, МГц: 432 (864)
Тип памяти: GDDR-3
Выходы: DVI, D-Sub, S-Video
Цена: \$184

вольно тихий и прекрасно смотрится в действии благодаря наличию ультрафиолетовой подсветки вентилятора (в комплекте поставляется специальная

лампа, устанавливаемая в корпус). Память также охлаждается достойно: на модулях располагаются небольшие алюминиевые радиаторы. Но самое главное в этой плате - легкость ее работы на частотах, которые гораздо выше базовых благодаря фирменному драйверу APE (Automated Performance Enhancer). Тебе даже не нужно разбираться в тонкостях разгона - достаточно установить программное обеспечение, и плата все сделает за тебя! Как



показывают графики, производительность платы превосходная, поэтому вывод однозначен: из всех решений на этом чипсете Sapphire Radeon X700Pro Toxic - далеко не худший экземпляр.

SAPPHIRE RADEON X550

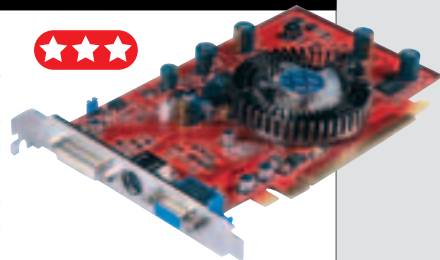
Эта плата, на первый взгляд, являет собой пример самого обыкновенного бюджетного устройства: простенькая система охлаждения, небогатая комплектация (драйверы, плеер DVD, мануал и S-Video-переходник), отсутствие VIVO. Но не стоит обманываться. Девайс, конечно, бюджетный и едва ли рассчитан на топовые игры и высокую детализацию, в своем классе он стоит на ранг выше аналогов. Все потому, что в этой плате применена высокопро-

Технические характеристики:

Интерфейс: PCI Express
Ядро: ATI RV370
Количество пиксельных конвейеров, шт: 4
Шина памяти, бит: 128
Объем памяти, Мб: 256
Частота ядра, МГц: 400
Частота памяти, МГц: 250 (500)
Тип памяти: DDR-2
Выходы: DVI, D-Sub, S-Video
Цена: \$70

изводительная память DDR-2, работающая на 128-битной шине и установленная в количестве 256 Мб, а VGA-упаковка модулей позволяет рассчитывать на высокий разгонный по-

тенциал. А дальше ты и сам знаешь, что делать. Остается лишь повысить рабочие частоты до максимума (кстати, будет полезно еще немного поработать над охлаждением, скажем, установить радиаторы на модули памяти и сместить кулер на более мощный). Заводские значения карты таковы: 450 МГц по чипу и 250(500) по памяти. Если учесть время выборки модулей 2,8 нс, что соответствует частоте 350 МГц, то перед платой открываются самые радужные



перспективы. Итого, в любом случае мы имеем неплохой результат за относительно небольшие деньги. Хороший выбор для не слишком хардкорных геймеров и рядовых пользователей.

ASUS EN6600 GT SILENCER

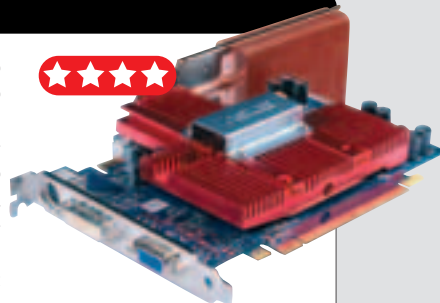
Даже если бы мы не заметили на упаковке логотип компании, мы с уверенностью сказали бы, что эта видеокарта - продукция Asus. Кто же еще, как не эта компания, станет снабжать свой далеко не топовый девайс такой красивой удобной коробкой и богатой комплектацией? Вместе с платой в огромном картонном боксе можно обнаружить не только шнур для подключения к HDTV и переходник D-Sub/DVI, но и богатейший набор софта, пять популярных игр и два мануала -

Технические характеристики:

Интерфейс: PCI Express
Ядро: NVIDIA NV43
Количество пиксельных конвейеров, шт: 8
Шина памяти, бит: 128
Объем памяти, Мб: 256
Частота ядра, МГц: 300
Частота памяти, МГц: 500 (1000)
Тип памяти: GDDR-3
Выходы: DVI, D-Sub, S-Video
Цена: \$175

краткий и подробный. Сама же плата заставила нас впасть в коленопреклоненный трепет: мы давно не видели такой оригинальной конструкции системы охлаждения! Она состоит из закрепленного на чип-

сете массивного медного радиатора, накрывающего также модули памяти, и теплоотвода - второго радиатора, закрепленного сверху, прямо над платой. Теплоотвод в свою очередь состоит из множества медных пластин и связан с основной частью тепловой трубкой. Как ты уже понял, система полностью пассивна, а значит, бесшумна. Правда, как мы установили, она довольно сильно греется. На плате установлено 256 Мб памяти GDDR-3 со 128-битной шиной, работающей на частоте



500(1000) МГц, частота чипсета - 300 МГц. Что до результатов теста, то они не слишком неожиданные. Производительность на уровне, особенно это видно в тесте с Doom 3, в котором обогнать продукцию NVIDIA крайне сложно.

ASUS EN7800 GT

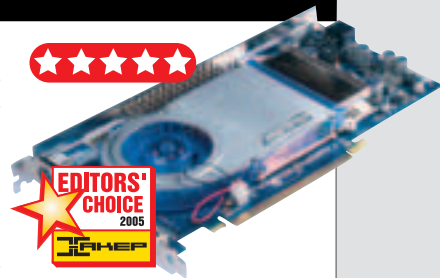
Чипсет NVIDIA GeForce 7800GT уже сам по себе заслуживает отдельной оценки. Еще бы! Топовое решение, одно из мощнейших на сегодняшний день. А если плату на этом чипсете выпускает компания Asus, то и вовсе стоит ждать чего-то экстраординарного. В принципе, так и есть: в коробке вместе с платой можно обнаружить два мануала, огромное количество софта и игр, а также фирменный пластиковый CD-бокс, довольно удобный и стиль-

Технические характеристики:

Интерфейс: PCI Express
Ядро: NVIDIA NV47
Количество пиксельных конвейеров, шт: 20
Шина памяти, бит: 256
Объем памяти, Мб: 256
Частота ядра, МГц: 275
Частота памяти, МГц: 500 (1000)
Тип памяти: GDDR-3
Выходы: 2xDVI, VIVO
Цена: \$650

ный. Плата, помимо высочайшей производительности, может похвастаться неплохой функциональностью. В частности, здесь есть мечта всех режиссеров-любителей - функция

VIVO :). Девайс снабжен 256 Мб памяти типа GDDR-3 с 256-битной шиной, работающей на частоте 500(1000) МГц (частота ядра - 275 МГц). Система охлаждения состоит из массивного радиатора, накрытого сверху алюминиевым кожухом, и вентилятора, смещенного влево относительно центра, - это позволяет прогонять воздух по всей площади устройства. Модерам и просто эстетам наверняка понравится приятная синяя подсветка этого вентилято-



ра, ну а оверклокерам - его мощь (правда, шума от него достаточно). Результаты тестов говорят сами за себя: плата показывает высочайший результат как в Doom 3, коньке NVIDIA, так и в прочих приложениях.

POWERCOLOR X800XL

» Эта плата от компании PowerColor собрана на базе чипсета ATI Radeon X800XL - мощный и в то же время не самом дорогом геймерском решении. Характеристики девайса довольно привлекательные: чип имеет 16 пиксельных конвейеров и работает в паре с высокопроизводительной памятью GDDR-3, установленной в количестве целых 512 Мб! Функциональность также не подкачала: видеокарта легко подключается к HDTV, поддерживает вывод изображения на два

Технические характеристики:
Интерфейс: PCI Express
Ядро: ATI R430
Количество пиксельных конвейеров, шт: 16
Шина памяти, бит: 256
Объем памяти, Мб: 512
Частота ядра, МГц: 400
Частота памяти, МГц: 490 (980)
Тип памяти: GDDR-3
Выходы: 2xDVI, VIVO
Цена: \$346

монитора и имеет функцию VIVO.

Система охлаждения, используемая в PowerColor X800XL, построена довольно интересно: на чипсете расположен только один ра-

диатор, а он, в свою очередь, соединен почти традиционными тепловыми трубками со своей "второй половиной", расположенной на обратной стороне платы. И эта половина - не что иное, как полноценный кулер с вентилятором, служащий здесь банальным теплоотводом! Кстати, именно этот вентилятор немного смутил нас. Его крепление, пожалуй, слишком свободное и позволяет ему "болтаться", что уже говорит о невысокой надежности девайса...

Плата требует дополнительного питания в обязатель-



★★★★★

ном порядке, хотя вряд ли это можно отнести к недостаткам. В конце концов, не составляет труда найти свободный разъем Molex, а видеокарта потребляет гораздо меньше драгоценных ватт, чем многие топовые модели на чипсетах Nvidia...

POWERCOLOR X800GT

» Видеокарта, основанная на одном из новейших чипсетов ATI, ориентированных на мейнстрим-сектор рынка. Это решение позиционируется как основной конкурент сверхучастному nVidia GeForce 6600GT, и, надо сказать, ему есть что показать зарвавшемуся сопернику! Девайс оборудован 256 Мб памяти типа GDDR-3 с шиной обмена 256 бит и временем выборки 2 нс, это позволяет надеяться на отличный разгонный потенциал! Рабочие же частоты девайса таковы: 475 МГц по ядру и

Технические характеристики:
Интерфейс: PCI Express
Ядро: ATI R480
Количество пиксельных конвейеров, шт: 8
Шина памяти, бит: 256
Объем памяти, Мб: 256
Частота ядра, МГц: 475
Частота памяти, МГц: 490 (980)
Тип памяти: GDDR-3
Выходы: 2xDVI, VIVO
Цена: \$175

490(980) МГц по памяти. Комплектация платы не представляет собой ничего выдающегося: мануал, небольшой набор софта, в который входит игра Hitman:

Contracts, ну и, разумеется, всяческие переходники и кабели для HDTV и TV-Out. В качестве системы охлаждения здесь представлена стандартная наработка (это, наверное, единственный кулер в обзоре без претензий на оригинальность) - широкий алюминиевый радиатор с вентилятором, смещенным относительно центра. В принципе, ничего плохого о ней сказать нельзя, кроме того, что она не охлаждает память. Если же учесть неплохой потенциал этих модулей, то мы посоветовали бы снабдить их радиаторами,



★★★★★

BEST BUY 2005

это наверняка позволит выжать десяток-другой дополнительных мегагерц. Хочешь узнать производительность - обращайся к графикам. А здесь напишем только то, что при относительно невысокой цене видеокарта весьма и весьма на уровне.

CHAINTech APOGEE AE6800

» По части комплектации эта плата обошла все представленные в тесте устройства и оставила далеко позади даже модели от Asus. И дело не в большом количестве прилагаемого софта и игр, упакованных в удобный, но невзрачный пластиковый бокс. И даже не в инструкции на русском языке и большом клубке кабелей и переходников на все случаи жизни. Все гораздо проще: компания положила в коробку с платой простой, но приятный сувенир - мягкий плюшевый мячик! Так что, купив эту плату, ты убива-

Технические характеристики:
Интерфейс: PCI Express
Ядро: NVIDIA NV42
Количество пиксельных конвейеров, шт: 12
Шина памяти, бит: 256
Объем памяти, Мб: 256
Частота ядра, МГц: 325
Частота памяти, МГц: 300 (600)
Тип памяти: GDDR-3
Выходы: 1xDVI, 1xD-Sub, S-Video
Цена: \$300

ешь сразу двух зайцев: получаешь не только отличную производительность, но и подарок девушке, которая наверняка простит тебе то, что последние полгода ты так

редко водил ее в кино, собирая деньги на это чудо инженерной мысли :). Сама плата снабжена 256 Мб памяти, работающей на 256-битной шине и охлаждаемой небольшими радиаторами. Что до основной системы охлаждения, то она представлена довольно внушительным и мощным турбинным кулером производства компании Arctic Cooling. И все в нем хорошо, но вот размер, рассчитанный на два слота, определенно навеял мысли о потерянном PCI-разъеме. В целом это достойная высокопроизводитель-



★★★★★

ная плата, у которой, кстати, есть шанс стать еще производительнее - все благодаря хорошей разгоняемой памяти и удачному кулеру. Да и забывать о возможности подключения в SLI, пожалуй, не стоит...

Вывод

За лучшую производительность, отличное качество и комплектацию награду "Выбор редакции"

получает плата Asus EN7800 GT. "Лучшая покупка" достается PowerColor X800GT - за

сравнительно небольшие деньги эта плата предлагает современный уровень производительности,

достаточный для любых, даже самых требовательных игр.

МАТПЛАТА ДЛЯ ЖЕЛЕЗНОГО ЭКСТРЕМАЛА

ECS PF5 EXTREME



о планете продолжает победоносное шествие новейших чипсетов от Intel - i955X и i945P/G. Нет поводов жаловаться на это! Ты

только подумай: эти решения технической мысли находятся в тесных отношениях с самыми современными технологиями вроде памяти DDR2, 64-битной архитектуры, поддержки двухъядерных процессоров и т.д.! Вот и компания ECS, мегапопулярная среди любителей недорогого, но качественного железа, выпустила на рынок новую модель материнской платы, основанной на самой "младшей" модели в линейке - чипсете Intel i945P.

Хотя чипсет обладает наименьшим списком "фич" среди собратьев по модельному ряду, плата удалась на славу. Из процессоров поддерживаются модели с частотой системной шины 566/800/1066 МГц (как одно-, так и двухъядерные), наличие двух слотов PCI Express x16 позволяет установить соответствующее количество видеокарт, а поддержка RAID-массивов всех популярных типов и интерфейса Serial ATA придает девайсу имидж весьма заманчивого приобретения, если ты задумал апгрейд.

Модель снабжена восьмиканальным звуковым кодеком на базе микросхемы Realtek ALC880, динамически управляющим аудиовыходами. Проще говоря, теперь, чтобы подключить к системе, скажем, микрофон, вовсе не обязательно искать соответствующий коннектор на задней стенке корпуса - достаточно воткнуть провод в любой разъем, и драйвер начнет принимать сигнал именно с него. Не подкачала плата и по части сетевых возможностей: на ней имеется целых два контроллера - как гигабитный, так и Fast Ethernet производства все той же Realtek.

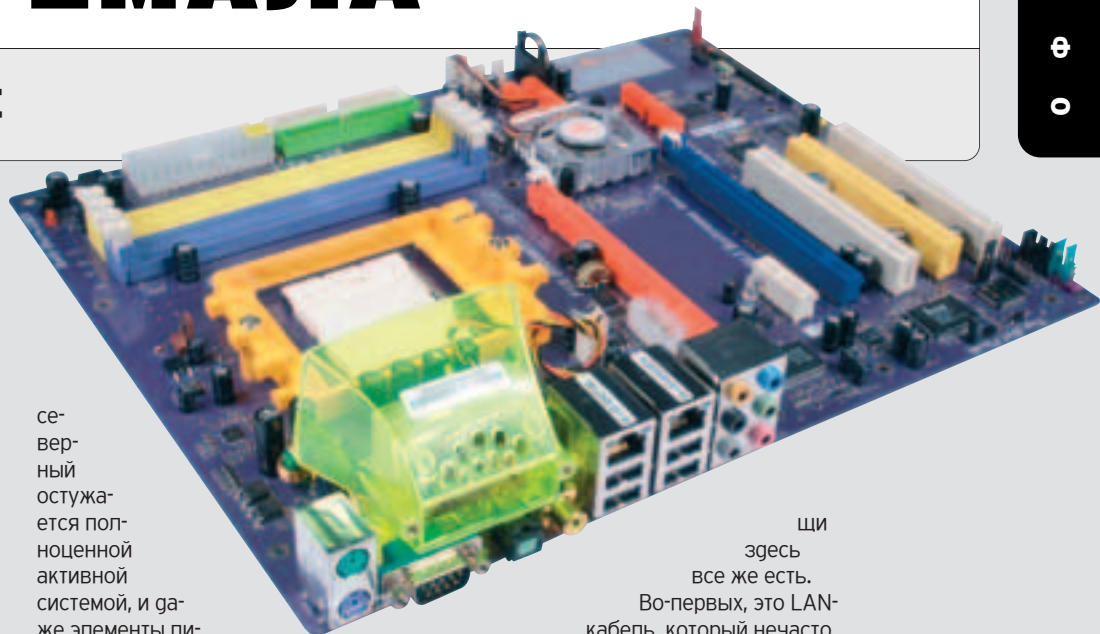
Внешне ECS PF5 Extreme наверняка понравится любителям разгона, так как здесь присутствует охлаждение на всех хоть сколько-нибудь греющихся элементах. Южный мост Intel ICH7R снабжен обычным радиатором,

северный охладится полноценной активной системой, и даже элементы питания обдуваются небольшим вентилятором, что приятно удивило нас. Оверклокерскую направленность также выдают функции ECSONIC2 и I.O.C. (Instant Overclocking Controller). Первая обеспечит пользователю удобную возможность повысить производительность всех компонентов системы, вторая - сделает это динамически в зависимости от нагрузки.

Комплектация платы на фоне других подобных устройств особенно не выделяется: в коробке лежат несколько планок с дополнительными портами расширения, необходимые кабели и диски с программным обеспечением. Правда, две приятные ве-


Технические характеристики:
Чипсет: Intel i945P
Южный мост: Intel ICH7R
Процессоры/разъем: (Intel P4 and Celeron D)/LGA775
Память, МГц: Dual Channel 4xDDR-2 max 4Gb 667/600/533
FSB, МГц: 1066/800/533
Слоты расширения: 2xPCI Express x16; 1xPCI Express x1; 3xPCI; 1xUDMA 100/66/33; 6xSATA
Сетевые возможности: 1xGigabit Ethernet 1000/100/10, 1xFast Ethernet 100/10
Разъемы на задней панели: 2xPS/2, 4xUSB 2.0, 2xLAN, 5xAudio, 1xTosLink
Разъемы, расположенные на заглушках PCI: 1xSATA, 1xFireWire, 2xUSB 2.0, 1xLPT

3DMark'01 SE, баллы	3DMark'03, баллы	Far Cry, FPS	UT2004, FPS	WinRAR, Кбайт/с
15208	4718	57	142,5	391
Тестовые результаты				



щи здесь все же есть. Во-первых, это LAN-кабель, который нечасто включают в комплект к материнским платам (хотя он коротковат, для соединения, скажем, с ноутбуком вполне пригодится). Ну а во-вторых, в комплекте обнаружился забавный сюрприз: в то время как производители "мамок" для пушей надежности распаивают на своих девайсах по две микросхемы BIOS, компания ECS поступила проще и положила резервный чип отдельно! В случае краха BIOS (например после неудачной прошивки) достаточно просто "одеть" эту микросхему поверх заводской - и вуаля, система стартует!

Естественно, мы не преминули протестировать эту материнскую плату на небольшом наборе бенчмарков, и результаты ты можешь увидеть в прилагаемой таблице. Игры прогонялись в разрешении 640x480 - именно в этом режиме основная нагрузка приходится не на видеокарту, а на связку процессор/материнская плата/память.

Девайс робротный и определенно заслуживает покупки. Здесь есть все необходимые функции, полезные и простому пользователю, и хардкорному геймеру. 

ПАЯЛЬНИК

СТАНЬ PHREAK'ОМ: ТЕ САМЫЕ КОРОБОЧКИ

В век цифровых технологий, конечно, глупо пользоваться таким анахронизмом, как аналоговый проводной телефон. Однако все мы вынуждены пользоваться им, пусть порой за чужой счет. В этой статье будет рассказано и о недостатках аналоговой телефонии, и о методах их устранения.



ПРЕДИСЛОВИЕ

■ Я не сомневаюсь, что ты не только видел обычный аналоговый телефон, но и звонил с него. Конечно, я мог бы усомниться в твоей компетентности и прочесть лекцию на две страницы о принципе телефонной связи, но что-то мне подсказывает, что этого делать не стоит. Поэтому не буду увлекаться графоманством и сразу перейду к делу. Возможно, ты тоже читал сказки Петра Карабина о всеилии и всемогуществе фрикеров. Однако, хотя Матрица где-то рядом, реальная жизнь бьет в чело своей реальностью, и с полнотой своей некомпетентности смею заявить, что при всем богатстве выбора не все боксы одинаково полезны для отечественных телефонных линий. Даже больше: некоторых и в природе никогда не существовало. В предлагаемом ниже обзоре представлены только те устройства, работоспособность которых проверена и гарантируется.

BEIGE

■ Грубо говоря, это прибор монтера-телефониста "на каждый день". Устройство состоит из трубки с номеронабирателем, трансформатора, угольного микрофона и телефона. Схема сабжа дана на рис. 1. Трансформатор TV1 служит для развязки цепей микрофона и телефона по постоянному току и согласования их сопротивлений с телефонной линией. В качестве номеронабирателя можно использовать как дисковый анахронизм, так и более современный кнопочный НН

(его фото на рис. 2). При более профессиональном подходе и с использованием современной элементной базы можно собрать девайс размером с обычный калькулятор, да еще и АОН прикрутить. Не буду говорить о двойном назначении прибора, ибо это и так понятно.

CHARTREUSE

■ Довольно часто возникают ситуации, когда нужен маломощный источник питания, но, как назло, под рукой ничего нет. Если есть телефонная линия, то это не проблема, ибо фриеры уже давно научились добывать электричество из абонентской линии (АЛ). Какое название дано сабжу, наверное, уже понятно, а потому предлагаю взглянуть на рис. 3. Снимаемое переменное напряжение на концах резистора подается на диодный выпрямитель, после чего сглаживается конденсатором С1 и стабилизируется стабилизатором VD1. От напряжения стабилизации стабилизатора зависит выходное напряжение девайса, оно может варьироваться от +1,5 до +9 В. Скажем, если использовать два последовательно соединенных диода, то напряжение будет около 1,5 В. При использовании КС133А, КС147А, КС156А, КС175А, КС191А выходное напряжение будет соответственно 3,3 В; 4,7 В; 5,6 В; 7,5 В; 9,1 В. Конечно, можно использовать и микросхемные стабилизаторы напряжения, однако в данном случае не имеет смысла. Конструктивно сабж можно выполнить на печатной плате из одностороннего фольгированного стеклотекстолита размерами 20x30 мм. Расположение компонен-

тов дано на рис. 4, а разводка проводников - на рис. 5. Плата рассчитана на установку стабилизатора в пластмассовом корпусе малогабаритного конденсатора фирмы TREC емкостью 10 мкФ x 16 В. Выпрямительные диоды могут быть любые подходящие по габаритам. При несложной доработке печатной платы для стабилизации напряжения можно использовать микросхемный стабилизатор на 5..9 В в корпусе ТО220. Естественно, устройство будет работать только при подключенном к линии телефоне.

NOISE

■ Это устройство - не только идеальный инструмент западлостроителя, но и мощный помощник в исследовании телефонной линии и помехозащищенности модема. Устройство генерирует псевдослучайный "белый шум", так что идеально подходит для своих целей. Взгляни на рис. 6.

Этот генератор шума содержит последовательный 8-разрядный регистр сдвига, выполненный на микросхеме К561ИР2, сумматор по модулю 2 (DD2.1), тактовый генератор (DD2.3, DD2.4), выполненный по схеме мультивибратора, и цепь запуска (DD2.2), выполненная на микросхеме К561ЛП2. Шум снимается с вывода 2 микросхемы DD1. Устройство может быть выполнено на печатной плате из фольгированного стеклотекстолита. Аналогом Noise служит устройство под псевдонимом "Scarlet".

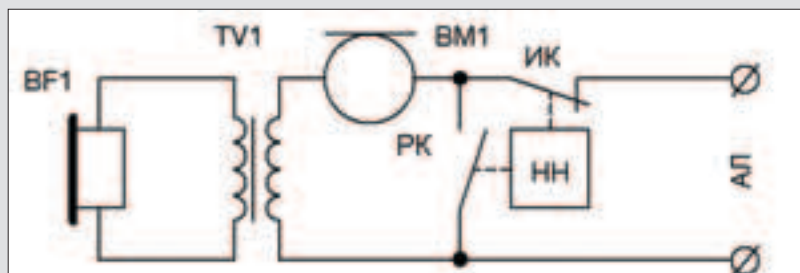


Рис.01: Beige. Вид изнутри



Рис.02: Кнопочный номеронабиратель

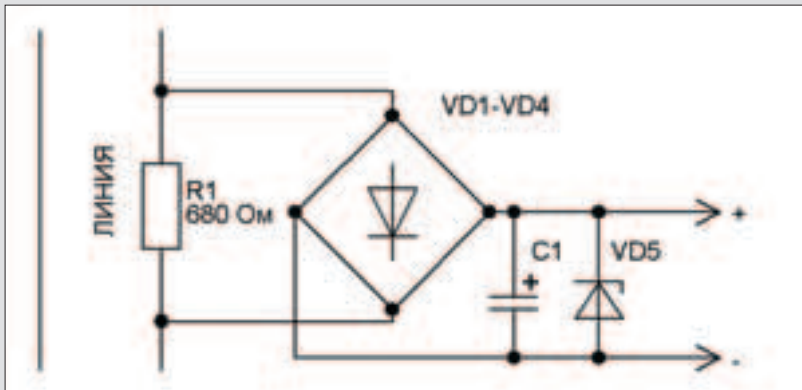


Рис.03: Chartreuse. Вид изнутри

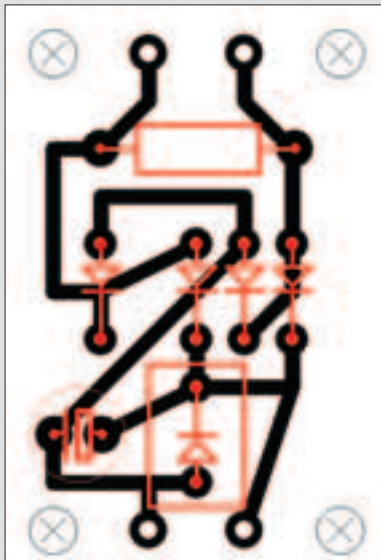


Рис.04: Расположение компонентов

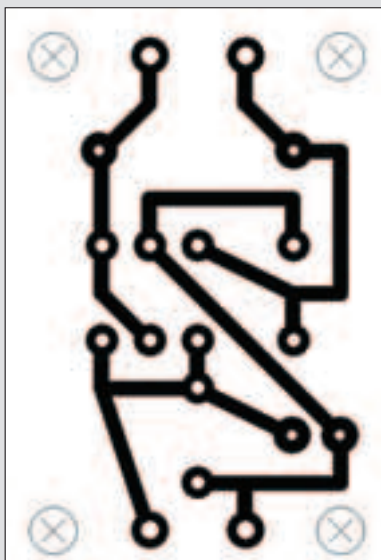


Рис.05: Трассировка проводников

COLOR

Конечно, включать Noise напрямую в абонентскую линию нельзя - для этого необходим специальный адаптер, который также несложен в самостоятельном изготовлении. На рис. 7 как раз изображена схема такого устройства. Трансформатор служит для согласования выходного сопротивления Noise с сопротивлением абонентской линии. Конденсатор ем-

костью 1,0 мкФ необходим для развязки по постоянному току. Конструктивно трансформатор может быть выполнен из обмотки реле РЭС49. Конечно же, контактные группы реле удаляются, как и металлическая оболочка. Штатная обмотка реле играет роль вторичной обмотки трансформатора. Поверх нее наматывается еще одна, которая содержит 400 витков провода ПЭВ 0.1. Именно этой обмоткой устройство Color подключается к линии. Хотелось бы отметить, что данное применение Color далеко не единственное. Если включить трансформатор в разрыв абонентской линии, то вполне возможно осуществлять запись телефонных переговоров, используя диктофон, управляемый голосом (то есть с системой VOX). У данного девайса есть только один маленький недостаток - трудоёмкость намотки трансформатора, однако звунаправленность данного варианта бокса Color легко решит проблему.

DAYGLO

Конечно, человек, знакомый с радиотехникой, сразу узнает в схеме на рис. 8 блокиратор параллельного телефона. Ну а в мире телефонных флибустьеров этот девайс называют dayglo. Принцип работы устройства прост: при снятии, скажем, трубки с телефонного аппарата ТА2, в цепи задействованного аппарата ТА2 напряжение линии 60 В пробивает аналог диода, выполненный на двуханодном стабилитроне VD3, диоде VD4, тиристоре VS2 и резисторе R2. Напряжение падает до 5-20 В, и его уже недостаточно для пробоя каскада ТА1.

При использовании внешних полнофункциональных модемов (не софтовых), например Courier, имеющий довольно высококачественные усилители входящего с АП сигнала, данный девайс может существенно снизить вероятность нервного расстройства, геморроя и полового бессилия. Теперь, даже если домохозяцы снимут трубку подключенного через блокиратор параллельного телефона во время закачки тобой свежей пор... информации и попытаются крикнуть в трубку что-нибудь типа "Клава, зацени, какие я бигуди себе накрутила", в ответ они услышат одну тишину. Им останется только дожидаться окончания удачной закачки и лицезреть в свете ночника розовую птицу обломинго. Однако с дешёвыми софтовыми модемами ты можешь потерпеть фиаско, ибо производители таких модемов экономят буквально на всем, в том числе и на качестве входных цепей. Конечно же, начинающие фрике-ры используют dayglo для несколько

Ну а в мире телефонных флибустьеров этот девайс называют dayglo.

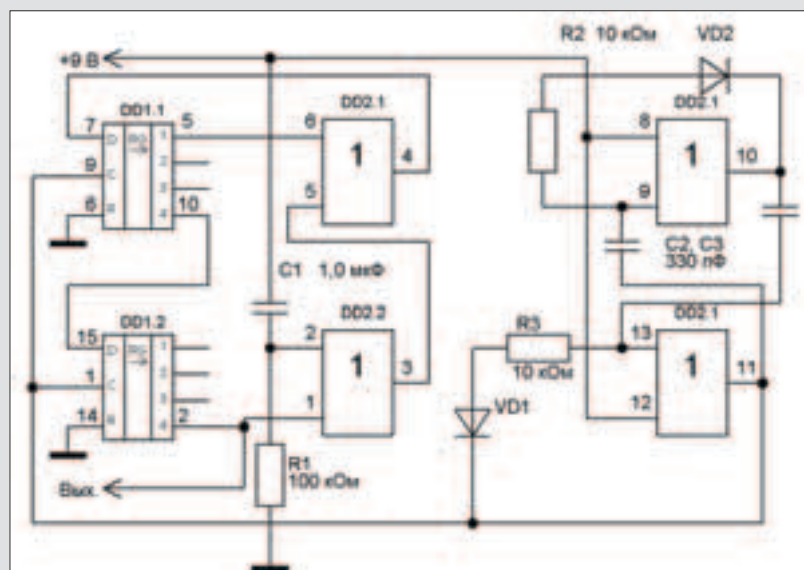


Рис.06: Noise. Вид изнутри

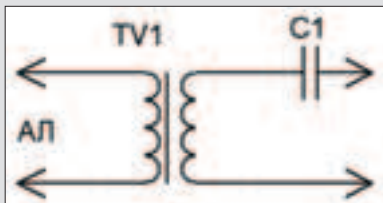


Рис.07: Двухнаправленный Color. Вид изнутри

иных целей, но так как мы законопослушные граждане, ни о чем подобном даже не помышляем :-). Недостатком девайса является необходимость соблюдения полярности включения, однако он с успехом лечится при наличии тестера, включенного в режиме вольтметра постоянного напряжения. В заключение хотелось бы отметить, что указанный девайс можно использовать для подключения до трех ТА и одного модема/четырёх ТА. Для этого достаточно добавить по аналогии необходимые каскады. В устройстве допустимо использовать любые двуханодные стабилитроны (например КС170, КС191). Диоды и тиристоры также любые кремниевые с допустимым током не менее 0,1 А и напряжением пробоя не менее 100 В (например КД105 и КУ112 соответственно). В данной реализации dayglo использованы резисторы R1 и R2 марки ОМЛТ сопротивлением 330 Ом и номинальной мощностью 0,5 Вт. Этот сабж как никакой другой подходит для навесного монтажа. Все детали можно разместить в телефонной розетке, зафиксировав перед спайкой каким-нибудь "моментальным" клеем, например "СуперМомент" (надеюсь, ты клей по назначению используешь :-)). Экспериментально доказано, что абсолютно все детали можно найти на помойке вблизи мастерских по ремонту электронной аппаратуры.

BLAST

■ Встречай! Усилитель микрофона телефонного аппарата. Это устройство можно назвать фрикерским с большой натяжкой, однако на зашум-

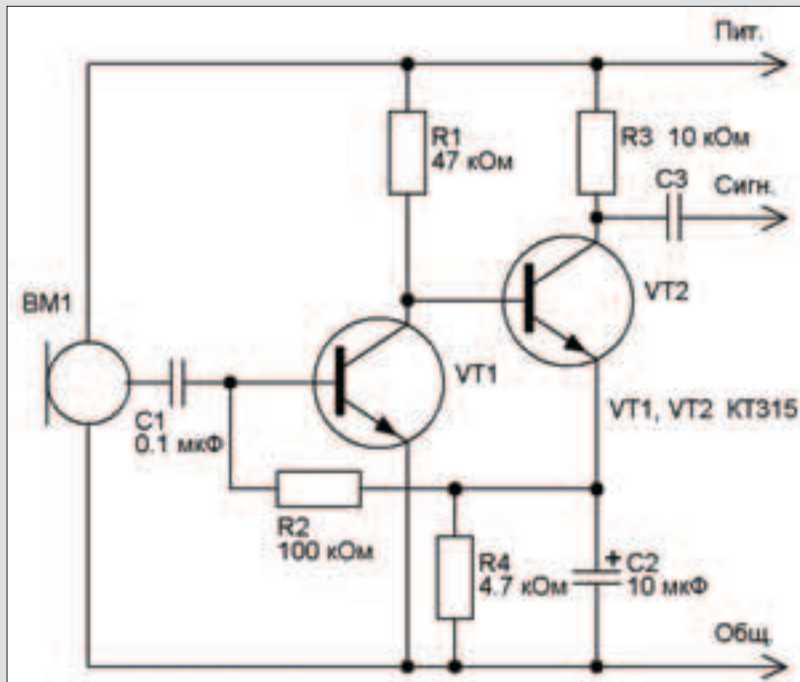


Рис.09: Blast. Вид изнутри

Встречай! Усилитель микрофона телефонного аппарата.

ленных телефонных линиях это устройство так же, как и Dayglo, может сэкономить немало нервов. Вариантов исполнения устройства может быть множество, но типов всего два: для электретных микрофонов и для угольных. Мы не будем рассматривать угольные микрофоны по объективным причинам, а схему Blast для электретного микрофона ты можешь идентифицировать на рис. 9. Если ты правильно идентифицировал blast, то твое мнение должно совпадать с моим: это обычный двухкаскадный транзисторный усилитель. Правда, от совсем обычного его отличает наличие

цепочки R2, R4, C2. На языке радиосхем это называется цепью отрицательной обратной связи. Она нужна для того, чтобы усилитель не перевозбудился (ga-ga, Бивис!.. - прим. рег.). Резистор R2, ограничивая усиление blast'a в целом, расширяет диапазон усиления. C2 - не что иное, как простейший емкостный фильтр, ну а R4 обеспечивает рабочую точку транзистора VT2. Впрочем, остальные резисторы служат тоже для этого. А то, что конденсаторы C1, C3 разделительные и служат для развязки по постоянному току, ты и сам прекрасно знаешь. Теперь по сигналам. Девайс питается от 3-9 В. Если напряжение питания электретного микрофона - около 1,5 В, то, дабы не спалить последний, в его питающую цепь вводится токоограничительный резистор сопротивлением 10 кОм. Раз уж речь зашла о деталях, позволь разъяснить. В устройстве могут быть использованы резисторы любых марок (например ОМЛТ, МОН), с мощностью рассеивания не менее 0,125 Вт. Конденсаторы C1, C3 типа К10-17а или аналогичные импортные, например фирмы TREC. Электролитический конденсатор C2 может быть типа К50-35 с рабочим напряжением не меньшим, чем напряжение питания. Транзисторы могут быть любыми из серии КТ315. При использовании более современных транзисторов с большим коэффициентом усиления по току, при возникновении возбуждения (харак-

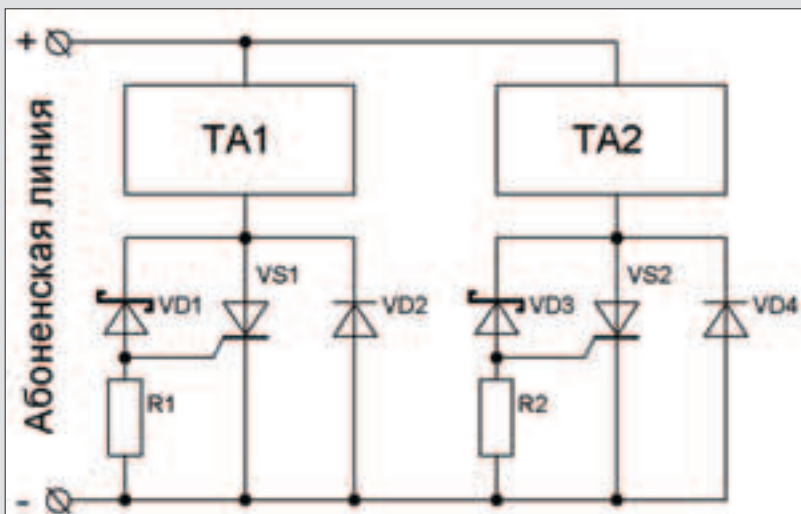


Рис.08: Dayglo. Вид изнутри

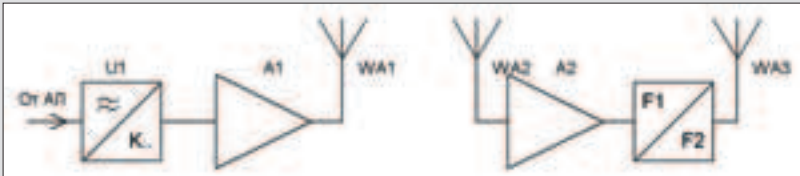


Рис.10: Вариант организации аппаратного sniffinga

Проверить работоспособность RadioColor можно с помощью бытового УКВ-приемника.

терный свист) или при появлении ограничения сигнала (звуки, издаваемые как будто отхаркивающим туберкулезником) необходимо будет заново подобрать резистор R2, на время заменив его подстроечником. Легко догадаться, что в этом случае после настройки нужно замерить сопротивление подстроечного резистора и впаять вместо него постоянный с таким же сопротивлением.

ВМЕСТО ОТСТУПЛЕНИЯ

■ Все перечисленные выше девайсы можно отнести к разряду устройств двойного назначения. Если соответствующие органы обнаружат эти сабжи, они вряд ли смогут доказать что-либо противозаконное в твоих действиях. Однако устройство, описанное ниже, - исключительно диверсионной направленности. На форуме <http://forum.xakep.ru> промелькал тред о вероятной возможности создания аппаратного sniffера. Конечно, я не предлагаю перечитать этот тред сугубо фреймовой направленности, но и мне есть что сказать по этому поводу. Как всегда, разговор об устройстве, тем более в столь непривычном для фрикера направлении, следует начинать с обсуждения его принципа работы. Предлагаю взглянуть на рис. 10. Сигнал, снимаемый с абонентской линии, подается на модулятор U1 и, после небольшого усиления узлом A1, излучается антенной WA1. Усиление должно быть настолько маленьким, насколько это возможно для обеспечения уверенной связи с ретранслятором. Сам ретранслятор может быть распо-

жен, например, на крыше соседнего здания. Он снимает сигнал антенной WA2 и через преобразователь передается уже на совсем другой частоте с совсем другими уровнями сигнала. Дабы не "легить горбатого" и снизить ручной труд изготовления высокочастотной части ретранслятора, можно использовать Wi-Fi-адаптер. Если использовать узконаправленную антенну с усилителем типа "волновой канал", можно получить уверенную связь на расстоянии нескольких километров. При таком исполнении получается максимально защищенная система наблюдения за проходящим в данной сети трафиком. Далее, развернув схему наоборот, выделяем полезный сигнал из радиосигнала и обрабатываем его с помощью компьютера каким-нибудь sniffером типа ethereal. Для перехвата трафика Dial-up-соединения та часть, которая именуется радиозакладкой, может быть исполнена, например, так, как показано на рис. 11. Скажу сразу, что схема публикуется "с колес", поэтому местами пахнет сырьем. Однако сабж, название для которого я пока не придумал, вполне пригоден для практического применения.

RADIOCOLOR

■ В принципе, за названием дело не стало - пусть будет RadioColor, потому что если животное бежит на четырех лапах, как ежик, летит, как ежик, и сопит, как ежик, то, скорее всего, это и есть ежик. То, что это СУПЕРЕжик, не суть важно. Данный девайс использует Color для своего подключения в

разрыв абонентской линии. Далее сигнал поступает на предварительный усилитель, выполненный на транзисторе VT1 и, извиняюсь за банальность, усиливается. Снимаемого с коллектора VT1 сигнала достаточно, чтобы получить девиацию частоты (она обеспечивается вариакпом VD1) до 75 кГц (если тебе не изменяет память, то максимальная скорость передачи в Dial-Up-соединении - около 50 Кбит) в модуляторе, выполненном на транзисторе VT2. К базе VT2 и к вариакпу VD1 подключен кварцевый резонатор, работающий на частоте 22-36 МГц по осцилляторной схеме, составляя с конденсатором C1 и контуром L1C2 "емкостную трехточку". Кстати, сам контур настроен на частоту, в три раза превышающую рабочую частоту кварцевого резонатора ZQ1. На языке радиотехники это называется третьей гармоникой. Далее через катушку связи L3 промодулированный по частоте сигнал поступает на оконечный усилитель, выполненный на транзисторе VT3 типа КТ610. Данный каскад работает в режиме класса "С" (цэ), что позволяет получить зверский КПД при минимуме потребления. Он усиливает сигнал до 150 мВт, поэтому позволяет уверенно передавать цифровые сигналы на расстояние до 150 м при использовании штыревой телескопической антенны WA1 длиной 1 м. В данной конструкции используются малогабаритные керамические конденсаторы. Резисторы могут быть типа ОМЛТ с мощностью рассеивания не менее 0,125 Вт. Дроссель Др1 - самодельный, намотанный на резисторе ОМЛТ-0,25 Вт с сопротивлением более 100 кОм. Он содержит 60 витков провода ПЭВ-0.1. Катушки L1 и L2 намотаны на полистироловом каркасе диаметром 5 мм с латунным подстроечником. Катушка L1 содержит 10 витков провода ПЭВ-0.31, катушка L2 - 5 витков такого же провода. Настройка RadioColor сводится к установке частоты работы контура L1C2. При использовании кондиционных деталей какой-либо дополнительной настройки не требуется. Проверить работоспособность RadioColor можно с помощью бытового УКВ-приемника, работающего на частоте 68-108 МГц. На данный момент пока никакой печатной платы не разведено, конструкция была изготовлена на макетной плате.

Если RadioColor предполагается использовать в радиусе его действия, то необходимость в дополнительном ретрансляторе отпадает. Я не буду говорить, что при наличии смекалки этот сабж можно сделать двунаправленным. Даже больше: работы в этом направлении ведутся. Кто знает, возможно, скоро по России прокатится новая волна фрикинга, подобно хакерской волне, которая была вызвана RTK 0.4 ;-).

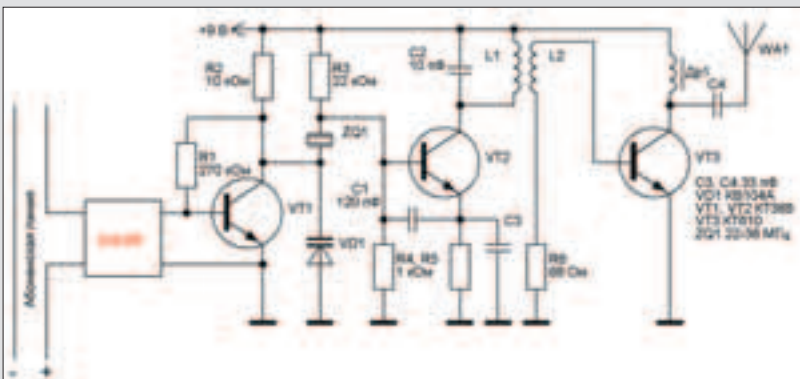


Рис.11: RadioColor - аппаратный sniffер

ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по всем
вопросам подписки для регионов:
8-800-200-3-999
(в том числе для абонентов МТС,
Билайн, МегаФон), для Москвы:
935-70-34

ВЫГОДА

Цена подписки на 20% ниже, чем в розничной продаже
Бонусы, призы и подарки для подписчиков
Доставка за счет редакции

ГАРАНТИЯ

Ты гарантированно получишь все номера журнала
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка
Доставка осуществляется заказной бандеролью или курьером



Стоимость заказа на Хакер Спец

900 руб. на 6 месяцев

1740 руб. на 12 месяцев

Стоимость заказа на комплект Хакер Спец + Хакер*

1830 руб. комплект на 6 месяцев

3600 руб. комплект на 12 месяцев



*Хакер с 2CD или Хакер с DVD на выбор

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ!

На письма отвечал SkyWriter (sky@real.hacker.ru)

Е-МЫЛО

(spec@real.hacker.ru)

ОТ: СЕРГЕЙ [PSV@ATKNET.RU]
ТЕМА: НЕ УКАЗАНА

Здравствуй, спец.
Вот такой вопрос у меня. Послал SMS на №4445. Пришел пароль к сюрпризу (<ensored>), однако он не открывает этот сюрприз. Пишет, что пароль неверный.

ОТВЕТ:

Приветствую тебя, Сергей!
Этот вопрос уже становится достойным FAQ'a, в лучшем, конечно, смысле этого слова. Дело в том, что он уже практически застрял в анналах журнальной истории, ибо его задают очень многие. А ответ на него в большинстве случаев оказывается несложным:

1. Читатель хочет хакнуть нас, воспользовавшись методом банальной социальной инженерии (ай как нехорошо!).
2. Просто пароль может быть прочитан по-разному (простите нас, рога :-), например буква "i" (эль малое латинское) и циферка "1" (единица арабская) на экране многих мобильных выглядят одинаково, этой посылкой стоит пользоваться, когда подбираешь пароль к архиву после получения SMS :-). С нашей же стороны торжественно клянемся (на первом номере "Хакер Спец"), что постараемся не опускать таких непоняток в дальнейшем.
Keep yourself out of trouble, Sergey.

ОТ: RAMBLER [TEM@RAMBLER.RU]
ТЕМА: КРИК ДУШИ

Идет бабка по улице и видит, как целая толпа избивает одного человека.
- Зачем же вы его все бьете? Что он вам плохого сделал! - говорит бабка.
- Уйди, бабка, не мешай. Мы спамера поймали!!!! - возражает толпа.
- Да что же вы его жалуете? Ногами его надо, ногами!!!! - кричит бабка.

(народный фольклор)

Я начал с этого эпиграфа не случайно, а так как злобные спамеры завладели моим почтовым ящиком и повадились каждый день отсылать всякую гадость с него, супостаты проклятые!!! И с каждым днем количество корреспонденции, отсылаемой с моего ящика, увеличивается в несколько раз. Уж не знаю как прогнать этих c^&#%\$)* @\$(@)*(&@%^&#)(&#^&*@)^#@\$%.
(Простите. Дал волю эмоциям...)

ОТВЕТ:

Ну, здравствуй, Рамблер! Знаешь, эта проблема гложет многих, в том числе нас. Знаешь, какие письма мне присылает AvaLANche?! А все, что мне предлагает увеличить Gorgum или Андрюша, я даже перечислять не возьмусь... Самое интересное, что все они открещиваются: говорят, мол, не писали мы такого... Думают, я наивный.

А если серьезно, то никто паролей от их ящиков я не крад, дело просто в том, что SMTP не проверяет адрес отправителя, а это значит, что ты можешь погостить туда хоть billgates@microsoft.com. Но если ты не веришь в это, то советую поменять пароль от ящика, переставить Винду, поставить персональный файрвол, и да будет тебе счастье!
Use condoms and PGP, наш юный поисковый груп!

ОТ: SCAINEN@RAMBLER.RU
ТЕМА: ОПЯТЬ ПОЛЕНИЛСЯ НАБРАТЬ :-)

Взял я ваш журнал "Хакер" октябрьского выпуска 2004 года, когда просматривал диск, нашел журнал "Хакер Спец" в электронной подшивке. Тема там была - переполнение буфера. Там предлагалось попробовать уронить буфер: откомпилирую следующий демонстрационный пример или возьми исполняемый файл с диска.

А у меня диска нет - помогите. Пришлите этот файл или напишите, как его откомпилировать. Код такой:

```
#include <stdio.h>
root()
{
    printf("your have a root!\n");
}

main()
{
    char passwd[16]; char login[16];

    printf("login:"); gets(login);
    printf("passwd"); gets(passwd);
    if (!strcmp(login, "bob") &&
        ~strcmp(passwd, "god"))
        printf("hello, bob!\n");
}
```

ОТВЕТ:

Ну, здравствуй, Скайнен-собака-рамблер-точка-ру! Вот так вот, с корабля на бал: ни здрасьте тебе, ни го свиданья. "Взял я Ваш журнал" и не спросил разрешения.

Но дело, в общем-то, не в этом. Не будем обращать внимания на синтаксис и семантику приведенного куса кода, сконцентрируемся на главном: так как данный файл предполагает наличие привилегий и пользователя с именем root, то совершенно очевидно, что файл должен запускаться в ОС UNIX/Linux, а раз так, то, скорее всего, и компилировать его стоит в этой ОС (так удобнее, братья).

Так вот, ты загружаешь свой UNIX/Linux и набираешь команду:

```
cc file.c -o file
Или:
gcc file.c -o file
```

Какая-нибудь наверняка сработает. Естественно, по легенде в файле file.c лежит корректный исходник :-). После этого запускай file и наслаждайся первой собранной программой. Что такое UNIX/Linux - см. другой номер нашего издания :-).
Добрых свершений, Скайнен!

ОТ: P4GEWIN@YANDEX.RU
ТЕМА: ОПЯТЬ ПУСТО :-(-

» Я, значит, на компе журналы читаю в натуре! Я <censored> от журналов! Классные журналы в натуре! А <censored> еще круче не видел! Балдею! Вроде как журналы у вас с дивидюхой рубают. А ЧувО на диск пишете? Я рублюсь <censored>, скока можно влихнуть на 4 гига в натуре! Я <censored> скока <censored> со всеми журналами диск DVD? Ну типа журнал - <censored>!!! Только там в журнале маловато порнухи, приходится из Яндеха выбивать и из Гугла, я о нем прочитал из журнала.

Ну типа чисто в натуре ваще, если конкретно, то я узнал о вашем журнале случайно, читая на пиратском компактe help-файл. Там было написано, как чистить Мастгай 98 от всякого <censored>. Я <censored>, как обалденно написано, классно придумено и <censored>, без него <censored> я бы в <censored> не <censored>. Я, значит, балдею. Да! Кто кинет мне по мылу нормальный KEYRUS.COM? Я уже со своим <censored>, у которого язык через <censored> переключается (в винде почти не переключает, CTRL+ALT будешь нажимать 10 минут - может, переключится, в гоце Shift+CTRL, га и то тоже работает глюкаво).

У меня есть крутая прога Restorator. Как всерга, по моему <censored> качать. Но скачал! Крутая прога! Можно вскрывать программы и DLL'ки, а потом изменять чего хочешь!!! Я балдею. Особенно с программой EType Dialer. Ее можно открыть как исходник формы, я та-кую версию создал!! На таком хорошем языке (РусскийЧутьИзмененный). Если хочешь, могу по мылу кинуть, запросто. Но только чтоб никто посторонний не видел, а то мне <censored> получать ото всех... Да, а примерно сколько старых журналов (.PDF) вы закидываете на диск? Интересно стало. Я читал письма в журнале, короче, там и увидел это. Ээээ... Был вопрос в журнале, как сделать сеть из двух компов через телефонную линию. Я там все понял, но файлы другого компа после подключения увидеть не могу! Я, может, что недоделал? Мне сказали, что надо в режиме сетевом окружении одинаковую рабочую группу поставить на обоих компах. Да и фижня-то у меня в том, что я на Windows XP. А чувак-чувачевский сидит под Windows 98. Нет, я могу. Точнее, я сконнектиться не могу, то есть могу, но не могу, конкретно при проверке имени и пароля хоть <censored> чаши. Я <censored>. Глюки у кого-то (у меня?). Да <censored>. Чего как настроить? А! <censored> чуть не забыл. Я читал, конечно, в Хакере (Спец), что ехе'шники часто сжимают, и перед заго в 16-ричник разжимают. Вопрос - чем? Какой прогой, обычной, или такую <censored> найдешь? Это сделать легко чайнику (это я про того чувака-чувачевского, коннектора <censored>). Ему тоже надо кой-чего взломать. А у меня. Ой, <censored>, скока я тут написал, коннект выдержит? Да, у вас в журнале (ой, в журнале) очень часто упоминается про эмуляторы. А эмуляторы мобил где скачать можно? Я чего-то найти не могу <censored>. <censored> - это не то, что проги по вычищению <censored>. Здесь мозги нужны... И не скажете ли как мне: на С++ написать крутую прогу с оригинальным интерфейсом, выдвигающую в определенное время CD-ROM и просьбой вставить "Диск багнутый <censored> номер 1" с одновременным проигрыванием "крутого" музона через спикер (ведь его просто так без отрубания проги не выключить). У, <censored> как завернул-то. Мне пора. По возможности намылите ответ. Жду. Если надо, могу намылить еще чего-нибудь, га скажу кое-кому, чтоб тоже намылил... Если надо... Вроде вам мало пишут, читаю я в журнале...

ЗЫ: Так и хочется написать: "Отучим Ская от просмотра Санкт-Петербургского порно, женим его, купим машину, отрастим ему пивное брюхо, приобретем трости с латунным набалдашником, фиолетовые кальсоны и бюст Льва Толстого". Но я воздержусь.

ЗЫ_2: Санкт-Петербургское порно??? И не нужен ли ему грачовый напильник :)?

ОТВЕТ:

Здравствуй, милый мой читатель!

Я долго и мучительно вычитывал твой опус. Ты действительно очень много и по делу написал, поэтому очень сложно уместить ответ в одной короткой статье - каждый вопрос заслуживает, по крайней мере, темы номера. У нас сейчас как раз период, когда мы выбираем темы на следующий год, так что жми в следующем году ответы на все твои вопросы, в частности:

- "Как <censored> в <censored>, чтобы все было <censored>";
 - "Задвигаем <censored> в <censored>";
 - "Я ним, <censored>, я бы в <censored> не <censored>!";
- И многое другое...

Что касается Санкт-Петербургского кинематографа, к сожалению, именно им я никогда не увлекался, я предпочитаю продукцию студии Private :-)) и просматриваю ее исключительно в образовательных целях!

Ну, ждем новых свершений, до встречи в <censored>!

ОТ: ADMINISTRACIA CB [ADMINISTRACIACB@LIST.RU]
ТЕМА: ПРОСЬБА



ПОМОГИТЕ!!!

Ребята!!! СРОЧНО НУЖНА ВАША ПОМОЩЬ!!!!

Я тут недавно в одну онлайн-игру стал играть - <censored> называется!!! Я вас очень прошу, вы не могли бы прокачать моего героя или создать нового, более сильного!!! Я уверен, для таких мастеров, как вы, это просто плевое дело, а сам я этого сделать не могу!!!

Я читаю ваш Журнал, и он мне очень нравится!!!! Там много интересного и познавательного!!!!

Еще прошу, пожалуйста, ответьте на мое письмо, буду ждть, заранее спасибо!!!

ОТВЕТ:

Поможем!

Мы обязательно поможем! Дело в том, что Ашот и Горлум в последнее время тоже увлеклись игрой <censored> и начали зарабатывать деньги фармингом - целыми днями сидят и прокачивают героев, чем и зарабатывают, статьи не сдают и колоссально бездельничают :-). Так что по всем вопросам прокачки - к ним. Еще наша редакция предоставляет услуги по:

- Переводам текстов;
 - Уборке мусора;
 - Благоустройству территорий;
 - Быстрому и недорогому строительству.
- Обращайтесь!

ОТ: THURMAN BLAND [RAE-JAMXRUBANL@LATINO.COM]
ТЕМА: LAST CHAAAAANCE



Your woman needs an 8 inch man.

Be that man for her.

Learn how here.

ОТВЕТ:

Вот! Как раз одно из таких писем.

Моей женщине нужен восьмидюймовый человек! Может, купить ей небольшого "человека-паука"? Наверное, тогда она будет чувствовать себя лучше?

Но в любом случае я таким человеком становиться не собираюсь, даже во имя любви. И тебе не советую руководствоваться этой рекламой :-).

Удачного личного роста тебе, Thurman Bland :-).



Niro (niro@real.xakep.ru)

ОВЕРДРАЙВ



ту машину заметили еще на прошлом рынке. Тогда факту ее появления не придали особого значения: ну мало ли кто приезжает на рынок выбирать себе машину, имея с собой в качестве секретного оружия консультантов из сервиса, ГИБДД или еще откуда-нибудь, при этом стараясь не светить людей без крайней необходимости. Скромная белая "Карина", давно не мытая,

на лысой резине, медленно ехала вдоль рядов с выставленными на продажу автомобилями. Кто-то в этой машине время от времени опускал стекло водительской двери, внимательно читываясь в информацию, написанную на лобовых стеклах выставленных на продажу "точил". Далеко не все продавцы старались указать сведения в полном объеме, и в таких случаях из машины раздавался короткий вопрос вроде "Какой ценник?" или "Что под капотом?" Ответ выслушивался, стекло закрывалось.

"Карина" остановилась в конце ряда, на лобовое стекло брызнули две струйки воды, включились "дворники", разгребая пыль по углам. Водитель удовлетворенно кивнул; его сосед даже не поднял глаз от ноутбука, лежащего на коленях. Его пальцы небыстро, но внимательно проходили по клавишам, на экране периодически появлялись фотографии автомобилей и какая-то информация, в основном на японском языке.

- Борис, - продолжая смотреть в экран, сказал человек с ноутбуком. - Борис, подъем!

С заднего сиденья поднялся заспанный парень, прикрывший от солнца лицо газетой. Он аккуратно сложил свою защиту вчетверо, положил рядом с собой, после чего протер глаза и спросил:

- Нашли?
- Нет, скоро найдем. Я чувствую, что в этом привозе их будет много.
- Тогда чего разбудил, Леха? - Борис был явно недоволен происходящим. - Еще спал бы и спал...
- Да поговорить не с кем, - рассмеялся водитель. - Все молчком, молчком... Анекдот хоть расскажи, что ли.

Борис наморщил лоб и выдал:
- Объявление в газете: "Одинокий бегемотик ищет заботы, ласки, понимания... и чего-нибудь пожрать!"

Водитель подавился смехом, после чего вдруг сказал:
- А насчет пожрать - это идея. Где-то пару рядов назад видел шашлык-ную. Мясо, наверное, дерьмо, но сам факт...

- Ага, - кивнул Борис, - устраиваясь поудобнее. - Дрессировщик выпил, лвы закусили.
- Точно, - Леха решительно закрыл крышку компьютера и приоткрыл окно.
- Зачем? - удивился водитель. - Кондиционер работает.
- Буду шашлычную по запаху искать. Кажется, нам назад и направо.

Водитель аккуратно развернулся и сам уже увидел легкий дымок, поднимающийся над тем местом, где разговорчивые и веселые азербайджанцы жарили своего неизвестного зверя.

- Знаете, что в этом деле самое главное? - спросил Леха. - Ну, в шашлыках?
- Что? - спросил Борис, разглядывая ряды сквозь тонированное стекло машины.

- Собачьи кости надо лучше прятать...
- Да пошел ты, - отмахнулся Борис. - Смотри, какая "Виста"!
- "Виста" как "Виста", ничего особенного, девяносто восьмой год, один и восемь кубатура, хороший движок, удачный... Автомат - на руле, типа "кулиса". Вот только крыло у нее крашеное - заднее правое. И раз я это заметил, значит, ее здесь делали. Если японцы красят, ни одна собака тон не отличит.

- Как ты все это видишь? - удивился водитель, протискиваясь между двумя сверкающими полированными "Краунами".

- А я, Димон, четыре года в сервисе отработал - на кузовных работах. Чего только не видел. Мы такие ужасные машины с того света вытаскивали, что потом сами удивлялись, как они вообще ездят. И кто-то же их покупает. Слепые, наверное... Так что для меня заметить, что именно на машине делали, - раз плюнуть. Вот на той "Короле" - бампер, а во-он там, на темно-синей "Хонде" вверх водительская. Ну разве не видно?

- Нет, - коротко ответил Дима, вглядываясь в то, что ему указал специалист. Действительно не было видно: чтобы глаз различал разницу в цвет-верть тона, его обладатель должен был заслужить звание профессионала.

- А вот лионские ткачи различают до сотни оттенков одного только черного цвета, - гордо поделился своими знаниями Борис. - Вот бы их сюда - всех бы вывели на чистую воду одним только взглядом.

- Этого мало...

- Чего мало?
- Одного только взгляда, - сказал Дима. - Люди не понимают.
- Чего не понимают?
- Того, что они... Короче, какая разница?
- Да никакой, - коротко ответил Леха. - Паркуемся.
Он остановился вблизи шашлычной, с той стороны, куда не дул ветер. Выглянув из окна, он внимательно посмотрел на тех, кто готовил мясо, потом сказал в салон, не обращаясь ни к кому конкретно:

- Я им никогда не доверял... Кому сколько заказывать?
Борис попросил один и картошку. Дима думал чуть дольше, потом решил взять шаурму.

- И попить чего-нибудь, - добавил он Лехе, когда тот готовился сделать заказ. - Уж очень душно сегодня. Интересно, они долго готовят?

- Минут десять, - ответил Борис, который вытащил неизвестно откуда газету и стал внимательно изучать ее. - Но, может быть, и быстрее - как получится.

Через десять минут, как Леха и обещал, они дружно жевали мясо. Дима аккуратно отгibal края целлофанового пакета, в который была завернута шаурма, и закрывал глаза от удовольствия.

- Умеют же, если захотят...
- Любого человека надо заинтересовать, - кивнул Борис, вгрызаясь в свой шашлык. - Ведь семьдесят рублей за эту фригню многовато, не кажется? Вот они и делают хорошо, чтобы родник не иссяк.

- Такой родник никогда не иссякнет... - протянул Леха, откинув кресло немного назад. - Такой родник - вечный. Если только какой-нибудь гурацкий закон не примут.

Дима посмотрел на него, потом открыл ноутбук и ткнул пальцем в одно из окон, что были на экране.

- Уже приняли. Паспорт моряка отменили. Аукционы, сам знаешь, закрывают для доступа...

"Одинокий бегемотик ищет заботы, ласки, понимания... и чего-нибудь пожрать!"

- А ты-то нам на что?
- Это не обсуждается. Вообще, то, что в нашей машине происходит, несколько отличается от происходящего в остальной жизни. Короче, проблеме можно создать на ровном месте. На то оно и правительство, чтобы нашими делами особо не заморачиваться. Они там делают то, что только им самим и нужно.

- Ну, ты на своего любимого конька сел, - протянул Борис. - Чего за лекция-то? К чему? Мы все и так знаем. Пусть сдохнет тот, кто нас не любит, правильно?

- Правильно, - ответил ему Дима. - Я просто хотел сказать, пока в стране бардак, будет все так, как на этом рынке. Будут продавать всякое дерьмо, и никто никогда не разберется, чего ему подсунули. Поддельвают все: документы, машины, агрегаты, доллары! Все! Ты можешь на секунду, Борис, представить, какая масса денег сейчас находится в карманах тех людей, что по рынку ходят или в машинах сидят? А сколько из них фальшивых? А сколько машин, привезенных из Японии, вылечено от разных болезней - только чтобы програть? Сколько сделано разных бумаг, сколько подшаманено железа, сколько выдраено прокуренных, затопленных салонов, сколько людей будет обмануто и чертовски пожалеет о покупке спустя какое-то время?

Борис аккуратно макнул кусок мяса в соус, отправил его в рот и соглас-но кивнул. Леха тоже особо не отвлекался от еды во время этого монолога.

- Я просто хочу понять, - не унимался Дима. - Ведь это вполне нормальное желание? Скажите мне, какого черта все это происходит? Почему всем затуманила мозги жажда наживы, причем за счет других? Нет бы самому что-нибудь делать руками, производить общественно полезный продукт... Так нет же, обмануть, надуть, заставить расстаться с деньгами любой ценой! И ведь спят же потом спокойно!

- Дим, остынь, - вдруг сказал Леха. - Ты сам-то понял, что сказал?
- Понял, - отмахнулся Дима. - Ладно, это я так... Наболело.
- Не надо эмоций, - криво улыбнулся Борис и похлопал Диму по плечу.
- Ты, главное, делай свое дело. Мы здесь не зря собрались.

Дима отвернулся и стал смотреть в окно на окружающие их машины.
- Я думаю, что тебе надо просто заняться делом, - кивнул Леха сам себе. - Борис, иди глянь хоть какую-нибудь тачку, пусть Дима на клавиши надавит, а то он тут нас задолбает своей философией.



Борис согласно подмигнул водителю в зеркало и выбрался наружу. - Хватит чушь молоть, как будто меня здесь нет, - огрызнулся Дима. - Не задолбаю я никого. А вот поработать правда хочется. Давайте документы...

Тем временем Борис уже обхаживал кругами довольно дорогой, даже на первый взгляд, "Марк". Хозяин "тачки" смотрел на него с водительского сиденья подозрительным взглядом: чувствовал, что у такого человека явно нет денег на подобную машину. Борис внимательно осмотрел автомобиль со всех сторон, отметил про себя все царапины на кузове, после чего спросил:

- Что стоит?
- Двенадцать пятьсот на старте. Если есть интерес, немного подвинем.
- "Немного" - это сколько?

Хозяин вылез из машины, подошел ближе:

- Ты брать будешь? Тогда и поговорим.

- А можно документы посмотреть? - спросил Борис. - Чего-то она как-то подозрительная...

- Чего? - пожал плечами хозяин. - Три дня назад таможня прошла, это у нее первый рынок!

- Да я не против, чего ругаешься... Просто я с детства такой... Все проверяю. Меня, может, в этом самом детстве напугали один раз и на всю жизнь. Так что? Документы не дашь посмотреть?

- Сам смотреть будешь?

- Да нет, есть кому взглянуть... - Борис кивнул в сторону своей машины. - Документы один посмотри, машину - другой. На все есть специалисты.

- Ну-ну, скептически покачал головой хозяин, но машину закрыл, вытащил документы из внутреннего кармана и вместе с Борисом, не выпуская их из рук, направился туда, куда его пригласили.

Леха увидел их раньше Димы, пихнул того коленом:

- Идет, дверь закрой и стекло подними. Тебя видеть не должны.

Леха включился в процесс быстро, пальцы сами закрыли кнопку на двери и включили стеклоподъемник. Потом он вытащил из нагрудного

И когда японцы прекратили публичный доступ к серверам, Дима удержался и остался на высоте.

кармана маленький пульт и нажал пару кнопок. Где-то в районе багажника еле слышно взвизгнули сервомоторы.

- Я же просил проверить на бесшумность, - сквозь зубы огрызнулся он Лехе. - Бездельники... Тарелка шумит, как будто "Боинг" на посадку заходит!

- Чего нудишь, гнус, - так же сквозь зубы, улыбаясь подходящему продавцу, ответил Леха. - На улице такой шум - никто не услышит... Привет, начальник, - кивнул он хозяину "Марка". - Продаешь? А мы покупаем... Давай документы, глянем... А лист аукционный есть?

- И лист есть. Вот любопытные! Смотрите, - хмыкнул продавец. - В последнее время все только и говорят "Аукцион! Аукцион!". Чего ж вы там поимете?

- А ты нам, начальник, и расскажешь, - улыбнулся во все зубы Леха, отдавая бумаги Диме. - Мы же хотим, чтобы все было как у людей - красиво.

Было видно, что этот самый "начальник", да и то, что документы скрылись где-то в глубине "Карины", порядком нервировало продавца. От Лехи за версту разило какими-то тюремными замашками, да он и сам словно старался выставить их напоказ. Хозяин машины переминался с ноги на ногу и отыскивал глазами в толпе кого-нибудь из знакомых.

Тем временем Борис сел в машину на свое место на заднем сиденье и стал всматриваться в то, что происходило сейчас на экране ноутбука Димы.

- На спидометре пятьдесят пять тысяч... С небольшим, - шепнул он как бы невзначай, наблюдая за тем, как ловко Дима обходит все ограничения на японских серверах, содержащих базу данных по прошедшим аукционам. - Так, внимательно сейчас, не так быстро...

Борис пробегал глазами страницы, заполненные иероглифами. Он был единственный в их группе, кто ничего не понимал ни в автомобилях, ни в компьютерах, но он прекрасно знал японский язык. Курсы, которые он закончил пару лет назад во Владивостоке, подтолкнули его к более детальному изучению японской культуры; он ушел с головой в "их" книги, ездил в Страну Восходящего солнца по обмену студентов, занимался восточными единоборствами - короче, был насквозь пропитан японским духом. Он зло всемчал американского "Последнего самурая", считая, что более глупой интерпретации японского величия и гордости нет и не было (Борис был уверен, что "Танцы с волками" намного лучше показали проникновение белого человека в мир индейцев, чем Том Круз сумел перевоплотиться в самурая).

Заниматься чтением аукционных листов Бориса пригласил Леха - его бывший одноклассник, который никогда не выпускал из поля зрения сво-

их наиболее ценных школьных товарищей. Он просто подошел к нему на улице, поинтересовался здоровьем, семьей, личной жизнью, увлечениями и как-то ловко повернул разговор на достаточно легкий и быстрый заработок - мотаться по выходным с ним и еще одним его другом на авторывок и помогать "нормальным пацанам" покупать "нормальные тачки". Этот друг - Дима - будет прямо на рынке ломать базы данных, ибо он хакер, каких еще поискать надо, а Борис станет у них переводчиком.

- Уж больно у них язык заковыристый, - сказал тогда Леха. - Даже со словарем одно слово можно полдня расшифровывать. А ты, я знаю, парень продвинутый...

Борис тогда согласился: подобная практика показалась ему очень и очень интересной. Тем более что технических терминов он знал не очень много - пришлось вплотную заняться самоподготовкой, перед первой поездкой на рынок он провел пару бессонных ночей за учебниками и в интернете. Уже в прошлые выходные он сумел помочь ребятам, за что его отблагодарили довольно приличным вознаграждением.

Сегодня он был готов намного лучше. Дима указал ему несколько адресов со страницами, на которых объяснялись условия работы японских аукционов, давались подробные расшифровки листов, выданных на аукционе. Сам хакер готовился к работе не менее тщательно. Когда стало известно, что японцы, ранее имевшие отношение в публикации информации о машинах, решили закрыть базы для доступа, Дима сразу понял, что в этой закрытости есть "золотое дно". Если некая информация становится засекреченной, всегда есть люди, которым она, по стечению обстоятельств, жизненно необходима. И, следовательно, надо сделать так, чтобы он, Дима, мог в любое время получить ее.

Подготовительный этап прошел достаточно быстро: он, пока гоступ был еще легальным и свободным, изучил структуру серверов в Осаке, Токио и еще паре прибрежных городов, в которых и брали машины у пакистанской мафии русские торговцы. Самим японцам весь этот железный хлам был по барабану, они отдали его на откуп. Оказалось, что защита у японцев стоит так себе, те и предстать себе не могли, что кто-то поставит себе цель сливать их архивы, чтобы в другой стране заняться тем, чем они с Лехой занимаются в настоящее время. Дима везде, где только можно, раскопал свои бэкдоры, проверил их через несколько дней - все было на месте, функционировало исправно и ждало своего часа.

И когда японцы прекратили публичный доступ к серверам, Дима удержался и остался на высоте. А Леха, нашедший переводчика, удачно разрулил ставшую безвыходной ситуацию: имея информацию, они просто не могли прочитать ее. Теперь их команда могла делать все, что они хотели...

... Вот-вот, какое там число стоит? - кинул взгляд на аукционник Борис. - Восьмое июня этого года? Точно, это она. Читаем... "Toyota-Mark III", девяносто девятого года, автоматическая коробка передач, родной пробег сто двенадцать тысяч, аукционная оценка три балла, стартовая цена 750 тысяч йен (ушла почти за миллион триста). Еще не все, - остановил он Диму, который хотел крутануть страницу дальше - туда, где была фотография. - Тут еще есть примечания: люк, литые, незначительные царапины на заднем левом крыле и левом пороге, небольшая вмятина на левой двери, производилась замена переднего левого крыла. Начало торгов: восьмое июня, а время... Пятнадцать часов ноль минут московское, у нас, соответственно, ночь. Судя по его виду, покупал не он: это надо было в интернете весь день просидеть, чтобы ночью неликвид хапнуть по бросовой цене.

- Ага, - протянул Леха, который все это слышал, но продолжал улыбаться хозяину, понимая, что тот не разобрал ни слова прозвучавшего сейчас в салоне их машины. Тем временем Дима все-таки посмотрел на снимок машины, внимательно сравнил его с оригиналом и остался доволен.

- Она. И у нас есть повод поговорить, - тихо сказал он Лехе, ткнув пальцем в жирную "четверку", нарисованную на аукционнике зеленым карандашом. - Пробег - раз, лист "левый" - два. Ну, и битая. Это прицепом пойдет. Или деньги, или машина. Будешь говорить?

Леха вытащил сигарету, закурил и опустил свое стекло полностью.

- Что хочешь за машину?

- Я же сказал, - огрызнулся хозяин, которому все это перестало нравиться. - Двенадцать пятьсот. Не устраивает - на рынке машин много, подберете себе.

- Это точно, - хмыкнул Леха. - Двенадцать пятьсот... А пять лет с конфискацией за свой "Маркушник" не хочешь?

- Чего? - попятился от машины продавец. - Документы давай и вали отсюда, сейчас быстро найдем на тебя управу...

Он завертел головой, пытаясь увидеть хотя бы одного парня в камуфляже, которые представляли здесь следящих за порядком людей хозяина рынка, но, как назло, ни одного из них поблизости не было. Да тут еще, как на грех, неподалеку остановился фургон, развозящий по рынку горячую пищу для торговцев автомобилями, и из динамика, установленного на крыше его кабины, разносилось по рядам:



Можешь стрелять, ничего я тебе не дам!

- Пицца, пирожки, холодное пиво!.. Пицца, пирожки...

Продавец вдруг понял, что не докричится сейчас ни до кого, и хотел было начать самостоятельно бороться за документы на свою машину, но внезапно увидел, как из окна "Карины" на него смотрит ствол пистолета. Леха аккуратно, не афишируя оружие, показал его продавцу:

- Садись в машину. Не думай, я выстрелю запросто, в десанте служил.

Продавец напрягся. Было похоже, что пистолета он никогда в своей жизни не видел. Страх в его глазах был, но было и еще что-то, подаренное нашей стране Голливудом. В глубине души этот человек, насмотревшийся боевиков, верил в какое-то чудо и садиться в машину не собирался.

Тогда Леха щелкнул предохранителем. И хотя вокруг было достаточно шумно, человек его услышал.

- Ты только глянь, где я стою, - кивнул Леха в сторону ворот рынка. - Бабах, потом выеду, пока заметишь, пока поймут... Я уже бугу далеко. Да никому ты и не нужен, первым делом мародеры у тебя баксы вытащат, а уже потом "скорую" вызовут. Жизнь твоя - тьфу! Садись или нет? - прикрикнул он.

Продавец сломался. В последний раз оглянувшись, он открыл заднюю дверь и сел рядом с Борисом. Тот немного отодвинулся и сунул руку во внутренний карман куртки, делая вид, что там у него пистолет, хотя на самом деле там ничего не было. Продавец покосился на этот жест и вжался в сиденье.

- Твоя машина? - спросил, не поворачивая головы, Дима.

- Мо... Моя, - проблеял продавец.

- На тебя записана?

- На меня.

- Сюда смотри, - он махнул рукой за спину, привлекая внимание продавца к компьютеру. - Это она?

Мужчина слегка наклонился вперед. Увидев фото своего "Марка", он быстро закивал.

- Зачем, сука, людей обманываешь? - на этот раз спросил Леха. Он положил пистолет себе на колени, закрыл окно и заблокировал двери.

- Я не обманываю, - ответил продавец.

- Тебя как зовут?

- Николай...

- Послушай, Николаша, - протянул Леха, делая паузу. - Мы про твою машину все знаем - даже больше, чем ты сам. Вот человек, - он похлопал по руке Димы, - он сейчас, можно сказать, не с нами. Он, если честно, Николаша, сейчас в Японии. А если точнее, где?

- В Осаке, - ответил Дима.

- Вот видишь, Коленька, прямо в Осаке. И вот оттуда, из этой самой, прости господи, Осаки, он нам говорит, что ты, Николаша, гад.

"Коленька", которому было лет сорок, беребил пальцы рук и непонимающе смотрел в затылок тому, кто сейчас, оказывается, был в Японии.

- Что значит "гад"? Вы чего, мужики, здесь так не делают... - пытался он возразить, но Леха, развернувшись в кресле, приставил ему пистолет ко лбу и сказал:

- "Здесь" - только так и наго с вами, козлами.

- Пушку убери, - сказал Николай. - Хватит в войну играть, говори, что тебе наго.

- Вот это другой разговор, - Леха опустил пистолет. - Коля, за тобой столько грехов, что я даже не знаю, как ты их все замаливать будешь. Пробег смотал - раз... Ну-ну, пальцы не загибай, я за тебя сам посчитаю. Смотал? Хорошо, что не возражаешь, глупо спорить, когда факты прямо перед тобой. Лист аукционный подделал - два. Ну, это фиגня, конечно, подумаете "три" на "четыре" переправил. Продолжать?

- Сколько вы хотите? - спросил продавец.

- Я думаю, по десять баксов за каждую смотанную тысячу, - наморщил лоб Леха. - Ну, и три сотни за аукционник.

- А не пошли бы вы нахрен! - внезапно ответил им продавец. - Можешь стрелять, ничего я тебе не дам!

Он даже попытался приподняться на сиденье, но, конечно, встать в полный рост у него не вышло, да и двери не позволили выскочить.

- Вы понимаете, что этот рынок для вас последний? - кричал он, брызгая слюной. - Я же вас засвечу перед всей братвой! Вы же сюда заехать не сможете! Никогда! Да и рожи ваши я срисовал, узнаю из тысячи, как в песне поется!

- Глянь его данные, - сказал Леха, не отрывая глаз от разъяренного лица Николая.

- Сейчас, - отозвался Дима. - Читай, не отвлекайся, - это уже предназначилось Борису. Тот снова наклонился вперед. Николай напрягся и замолчал. Происходило что-то, чего он не понимал.

Дима щелкал клавишами, временами сверяясь с паспортом автомобиля. "Парфенов Николай..." - шептал он себе под нос. - "Сейчас, сейчас..."

- Куда отправить? - спросил он у Лехи.

- Ты же знаешь - в Новую Зеландию, - ответил тот.

- Угачи, - безо всяких эмоций сказал Дима. - Я хоть правильно все разобрал?

- Точно, - согласно кивнул Борис. Он уже понял, что Дима работает чисто по зрительной памяти: ему было все равно, что означают иероглифы, он просто запомнил их расположение и вид на странице.

- Итак, - снова начал разговор Леха. - Ты, Николай, любишь километраж сматывать. Вам бы за это руки отрывать, но мы не такие. Зря ты тут слюной брызгал, не к лицу тебе это. Даю тебе пять минут на то, чтобы исправить свои ошибки. Правда, теперь, поскольку ты не понял меня с первого раза, будет на две сотни дороже.

- Пошел ты!.. - откинулся на сиденье Николай. - Дверь лучше открой и иди себе могилу копать! Документы не просто вернешь - приползешь и в зубах их будешь держать, тварь!

- Пять минут начались, - будто не слыша ничего, сказал Леха. - А через пять минут четыре твоих тачки, Николай Парфенов, со смотанными спидометрами, отгрузят вместо лайнера "Русь" на контейнеровоз, идущий в Новую Зеландию... Да-да, Коленька, два джипа и два микроавтобуса. Твои? Вот о чем я говорю, Николай. А ты знаешь, как в Новой Зеландии относятся к тем, кто занимается коррекцией показателей? А вот это уже, Коля, Интерпол... Чего напрягся?

Николай действительно стал похож на взведенную пружину. О том, что бывает в этой трижды проклятой Новой Зеландии, он знал не понаслышке. И тогда кранты всему бизнесу... В Японию уже точно не поутят.

- Где доказательства того, что машины отгружаются не по адресу? - спросил он, сжав зубы. - Разводите, как лоха?

- Компьютер, Николай, - великая сила. Покажи ему, - он повернулся к Диме. Откуда-то из-под ног у того выехал листок бумаги (принтер был припрятан надежно и очень удобно). Дима подхватил лист и протянул назад.

- Переведи, - приказал он Борису, но Николай сам выхватил бумагу и принялся жадно разглядывать те знаки, буквы и цифры, что были там

пропечатаны. Было похоже, что он и сам немного разобрался в этих грузовых документах. - Ах вы... Ну уроды!..

Дима смотрел в окно. Он прекрасно понимал, что против таких доказательств не пойдут никто. Связаться с Интерполом - на всю жизнь запороть бизнес, какой бы плюгавенький он ни был.

Николай смял лист в кулак, ненавидящим взглядом обвел всех в машине, словно стараясь запомнить их навсегда, потом полез в карман, вытащил деньги, отсчитал тысячу долларов, протянул Лехе:

- Больше не дам, лучше сразу убей.

- Как скажешь, - равнодушно ответил Леха и взял пистолет в руки. - Сам сказал...

- Ты чего?! - закричал Николай, когда Леха поднял ствол на уровень его глаз. - Ты чего?! Забери свои деньги, пагдал!

Он бросил еще сотню, после чего стал дергать ручку двери. Леха лениво протянул руку к кнопке, щелкнул. Николай от неожиданности едва не вывалился на гравий.

- Беги не оборачиваясь, - сказал Леха. - Иди продавай свое барахло.

Было видно, что Николай напуган и разозлен очень и очень сильно. Он побежал к своей машине, ввалился на переднее сиденье и сразу же завел мотор. Его глаза смотрели в их сторону с нескрываемой ненавистью и злобой. Через несколько секунд он рванул с места, подняв облако пыли. Несколько пар удивленных глаз проводили его, после чего тут же забыли о его существовании.

- На прошлой неделе было все не так круто, - вдруг сказал Борис, который держался из последних сил. Вид пистолета в руках Лехи поколебал его уверенность в их праведном деле. - По-моему, мне все это внезапно перестало нравиться.

- На, бери, - протянул ему триста долларов Леха. - Теперь как, снова проникся? Ну, чего ты? Ты просто пару страниц прочитал, перевел и нам рассказал - и за это три сотни вечнозеленых! Ну, где еще так заработаешь? Дима, а ты не забыл его машины обратно в Россию отправить?

- Нет, не забыл, - буркнул хакер. - Если ты сервомоторы не смажешь, в следующий раз без меня поедете.

- Да... Не подмажешь - не поедешь, - сам себе сказал Леха. - Да ладно, самое главное, что часть нашего плана сработала. Осталось жрать.



- Ждать? Что? - удивился Борис. - И вообще, нам не пора отсюда съезжать? Странный какой-то бизнес, ведь он прав был, на следующем рынке нам под машину гексоген подложат, далеко не уедем.

- Да никому он не расскажет, - хлопнул себя по колену Леха. - Ты же видел... То есть, я имею в виду... Он, конечно же, расскажет, просто обязан рассказать. Вот только весь вопрос - кому и как быстро. Ставлю сотню, что он сейчас где-нибудь в километре отсюда сидит под деревом и прочищает кишечник. Слабоват он, мне кажется. Или я ошибаюсь?

- Хрен его знает, - недоверчиво покачал головой Дима. - Человеческий фактор - вещь абсолютно непредсказуемая. Вот, к примеру, моя часть работы. Мы бы сейчас здесь не сидели бы, если б там, в Японии, у кого-то мозги получше работали. Поставили бы какую-нибудь защиту, повыкидывали бы меня из системы... Просто надо захотеть. А им, похоже, все равно. Они обновления ставили на свои компьютеры последний раз три с половиной месяца назад. Если бы я этими администраторами командовал, то они бы сейчас все на бирже труда уже толкались.

Дима был готов рассуждать на эту тему бесконечно долго, как и всегда, когда тема касалась компьютеров, сетей, взломов и прочей киберлабуды. Леха уже чувствовал, что назревает лекция о людях, занимающих чужое место, о бездарях, купивших себе дипломы, об идиотах, никогда не просматривающих информационные бюллетени в интернете и не ставящих очередные обновления, которые бы сделали компьютеры неуязвимыми для хакерских атак. Правда, при желании Дима мог говорить и на совершенно противоположные темы: о продвинутых хакерах, к которым он сам причислял себя (впрочем, совершенно справедливо), о людях, которые совершенствуют свое мастерство, пишут разнообразные серьезные (и не очень) программы, занимаются общественно полезным делом, указывая всяким околосредовым бездарностям на их место в этой жизни и на их совершенно идиотские ошибки.

Скорее всего, кончится пулей в лоб, потом ноги в таз с цементом и на дно Амурского залива.

- Сходи за пивом, Дима, - внезапно сказал Леха. - Если, конечно, не тяжело. Проветрись, не грузи нас. Хочешь, я с тобой схожу. Или Боря.

- Да-а, - протянул Дима, который понял, что его просчитали на ход вперед и заткнули рот пивной соской. - Ничего вы не понимаете. Лагно. Кому сколько, какого и что к пиву? И один не пойду.

Поскольку на рынке в машине всегда нужен водитель, то остался Леха. Борис выбрался на улицу, потянулся, прищурился от яркого света и пригладил волосы.

- Эх, хорошо-то как! - сказал он, ни к кому не обращаясь. - Сейчас бы на море, ветерок, девочки в купальниках, мороженое, волны, матрас... А мы вот тут, в этом пекле, дышим бензиновым смрадом, жрем какой-то непонятный шашлык, запиваем пивом, которое налито в разные бутылки из одной бочки! Ну почему так?

- Потому что на море даром - только волны.

Чувствовалось, что Дима немного не в духе, и это несмотря на то, что у них все получилось. Они направились к ближайшему ларьку, уже издали разглядывая бутылки, выставленные на витрине. Пару раз их заставляли подпрыгивать громкие сигналы от тех, кому они мешали проехать; Борис ругался на чем свет стоит, грозя вслед кулаком и понимая, что это ни к чему не ведет, Дима молча шел и смотрел по сторонам, уделяя внимание людям, которые по каким-то причинам смотрели на них. Пусть это был короткий случайный взгляд или наоборот - долгий, сопровождающий их к ларьку; ему надо было понять, знают что-нибудь о них или до сих пор нет.

Они взяли по две бутылки холодного, сразу запотевшего пива, присели на лавочку рядом с ларьком, не торопясь возвращаясь в душную, несмотря на кондиционер, машину. Оба они, совершенно не сговариваясь, думали сейчас о том, с какой легкостью Леха направлял пистолет в лицо жертве, как нагло и легко он разговаривал с человеком, которого выбрал в качестве жертвы шантажа, - и они оба не хотели идти назад.

- Ты знаешь, что Леха сидел? - внезапно спросил Дима.

- Если честно, нет, - хрустя сухариками, ответил Борис. - Но - догадаться нетрудно.

- А насчет десанта, интересно, он сворал или нет? - Дима поставил бутылку рядом с собой, огляделся по сторонам. - Я этих десантников знаю, они все с пулей в башке.

- Черт его знает, - пожал плечами Боря. - А пистолет у него откуда? На прошлой неделе он безо всякого оружия обошелся. Правда, тогда такой лох попался, что его можно было просто пальцем припугнуть.

Дима вздохнул, глотнул пива и спросил:

- А ты так думаешь, почему он не боится ничего? Почему мы дело сгелали и не уехали?

Борис перестал хрустеть и посмотрел в глаза Димы.

- Я думал, ты знаешь. Вы же меня особо в курс дела не посвящаете.

Сам же Леха сказал... Короче, я так понял, что вы какой-то реакции ждете. Вот только мне чего-то домой хочется. Не нужна мне эта ваша реакция.

- Струсил?

- Нет, я не из пугливых, хоть в детстве и очки носил, и по заборам не лазил, и домой вовремя приходил, и пятерки получал. Думаешь, что если я в шестом классе от тебя получил так, что зуб потерял, то с тех пор только щеки и подставляю?

- Надо же, запомнил... - хмыкнул Дима. - А я и позабыл уже напрочь... Вообще, ты прав. Нам нужна реакция. Смысл в том, что эта штука баксов - практически ничто по сравнению с тем, что будет, если мы свою работу криминальную превратим в легальную.

- Объясни, - Борис открыл вторую бутылку и влил в себя сразу больше половины, не сводя глаз с лица Димы.

- Да очень все просто. Понимаешь, я, без лишнего хвастовства скажу, на компьютере могу все. И то, как я на эти аукционы чертовски пролез, - такая малость, что просто смешно. Готовился я к этому, если честно, не так уж и долго, в основном теорию изучал. Практики-то у меня предостаточно было.

- На чем практиковал? - поинтересовался Борис.

- В основном экономический шпионаж, если выражаться пафосным языком. Добывал всякие базы данных, связанные с товарооборотом по краю, потом по всему Дальнему Востоку. Люди, они ведь не могут честно торговать: им надо друг у друга клиентов переманивать, поставщиков подставлять, ассортимент знать, шаги предугадывать... В России такие вещи не очень развиты, сам понимаешь, люди еще до сих пор на счетах считают и в блокноты ручками пишут. Но если у фирмы есть комп, то считай, я на нем обязательно побываю.

- И много ты на этом шпионаже наработал? - Борис поставил вторую пустую бутылку под лавочку и с тоской оглянулся на ларек - явно хотелось еще.

- Ой, Боря, много... У меня вообще сложилось впечатление, что я здесь такой один. Знаешь, я всегда не понимал: если ты чего-то такое хочешь узнать, о чем в газетах не пишут и по телевизору не говорят, то ты в милицию или еще там в какой государственный орган не пойдешь, логично? Тебя там просто не поймут, - Дима улыбнулся своим мыслям.

- И что тогда делать?

- А тогда можно, Борис, обратиться к частному детективу, и если он не трусоват по натуре и берется за любые дела (лишь бы хорошо платили), то он для тебя любую информацию из-под земли достанет. Правда, если он затронет государственные интересы, то тут придется туговато. Скорее всего, кончится пулей в лоб, потом ноги в таз с цементом и на дно Амурского залива.

- Чего-то ты издали начал, - кивнул Борис, который уже чувствовал во всем теле прохладу и легкость.

- Я тебя пытаюсь к мысли подвести, - допил свое пиво Дима. - Скажи, много людей заинтересовано в том, чтобы знать ту информацию, которую мы сегодня показали хозяину "Марка"? Сколько людей хочет купить машину и не прогореть на этом, не потерять деньги и нервы?

- Я бы точно хотел. Только у меня денег на машину нет, так что эта проблема для меня не стоит.

- Подожди, будут и у тебя эти деньги, - сверкнули у Димы глаза. - И будем мы с тобой, Боря, разъезжать по городу на жипах, будут с нами за руку здороваться и в новостях показывать... Просто надо людей к той же самой мысли подтолкнуть. Мы ведь потому так дерзко себя вели, что нам крайне необходимо, чтобы нас заметили, срисовали, предложили вежливо пообщаться в кулуарах этого рынка. Понял?

- То есть, вы не хотите вот так бомбить продавцов? Вы хотите работать на хозяина? Что-то типа услуги по определению поплинности машины на рынке?

- Ну наконец-то гопер, хоть и с подсказками! - радостно признал Дима.

- Да, да и еще раз да. Мы сидим здесь с тобой, Боря, и ждем, когда же к нам кто-нибудь подойдет. Ведь этот продавец не мог просто так расстаться со своей тысячей долларов, сесть в машину и рвануть отсюда куда-нибудь к черту на кулички. Точно тебе говорю, не мог! Он, наверняка, сразу же побежал звонить кому-то, кто знает кого-то, кто знает хозяина. Сейчас эта информация о нас с тобой через десятые руки тех, кто на это уполномочен, просачивается наверх.

Борис машинально осмотрелся и обратил внимание на трех парней в камуфляже с нашивками на карманах.

- "Охрана", - прочитал он и повернулся к Диме. - Может, они уже за нами?

- Вполне возможно, - взглянул в ту же сторону Дима. - Не бойся, солдат ребенка не обидит. Вот только пива мы больше брать не будем, можешь на ларек не пялиться. Нам еще сегодня разговаривать придется... У тебя мобила с собой, в машине не оставил?

- Да, - Борис полез было за ней, но Дима его остановил.

- Ты можешь позвонить Лехе, не вынимая его из кармана? Ну, ты же такой умный, прикинь, что и сколько раз нажать надо, чтобы именно его номер набрался!

Боря закатил глаза к небу, потом кивнул и принялся шарить пальцами в кармане куртки, нажимая кнопки телефона.

- Я думаю, не зря они здесь... - снова посмотрел на охранников Дима. - Как позвонишь, долго не жди, он поймет. У нас с ним есть кое-какие задумки, так что он будет в курсе...

- Все, - спустя несколько секунд сказал Боря. - Думаю, что позвонил именно ему. А если не попал, то мне, возможно, сейчас перезвонят, у меня после Лехи мама в справочник забита.

- Будем надеяться, - похлопал его по плечу Дима. - Смотри, один из них по радиации чего-то докладывает. Я так понял, они нас пасли, теперь определились, скоро подойдут.

Подошли с другой стороны. Дима и не заметил, как рядом на лавочку кто-то опустился - лишь почувствовал, как ему под ребра уперся ствол пистолета. Тогда он тихо присвистнул, Борис вздрогнул и посмотрел в его сторону.

На лавочке сидел человек в джинсовом костюме и бейсболке с таким изогнутым козырьком, что глаз было совершенно не видно. Он делал вид, будто встретил знакомых, при этом сидел к Диме настолько близко, что пистолета видно не было, похоже, ствол впирался ему в бок сквозь внутренний карман куртки.

- Добрый день, - улыбнулся человек и быстро осмотрелся. Парни в камуфляже приблизились и ждали его распоряжений. - Я за вами.

- А вы, собственно, кто? - спросил Дима, не обращая внимания на пистолет, упирающийся ему под ребра. - Вполне возможно, что вы сейчас обратились не по адресу.

- Ну, вряд ли, - ответил незнакомец. - У нас ошибок не бывает. Это же вы сейчас изьяли из оборота у человека на этом рынке одну тысячу сто долларов США?

- Мы, - согласился Дима. - Причем сгелали это, как мне кажется, совершенно справедливо. Или этот несправедливый человек рассказал вам свою версию событий?

- Мне совершенно все равно, как вы это сгелали, - человек убрал пистолет, почувствовав, что люди, которых он искал, явно настроены на разговор, а не на стрельбу. - Самое главное, что у меня есть четкий приказ - доставить вас по назначению. Здесь недалеко, метров сто. Здание администрации.

- А я уж решил, что мы сейчас прямо в отделение милиции пойдем, да еще и в наручниках, - Дима закинул в рот последнюю пригоршню сухариков и с громким хрустом перемолол их за пару секунд, не жалея зубов. Это был единственный момент разговора, когда стало понятно, что он волнуется. До этой секунды он ничем себя не выдал.

Борис не участвовал в их разговоре, предоставив ему право развиваться так, как хотел Дима. Правда, понять, все ли идет по плану, было непросто, но тот факт, что их ведут не в органы правопорядка, а к боссу этого большого рынка, говорил сам за себя - с ними хотели разобраться без лишнего шума.

Они встали. Парни в камуфляже отошли на приличное расстояние от них, но расположились таким образом, что убежать было практически невозможно, - все направления были перекрыты. Дима усмехнулся, проводив их взглядом:

- Конвой? А кто-то собирается бежать? Я - нет. Может, ты, Борис?

Тот отрицательно замотал головой.

- Ваш товарищ неразговорчив? - спросил человек, который сопровождал их.

- Нет, просто его пока ни о чем не спрашивали, - ответил за Бориса Дима, и они пошагали к двухэтажному зданию у въезда на рынок.

Никто не обращал на них никакого внимания, только единожды кто-то из проезжающего автомобиля поздоровался с их конвоиром. Судя по всему, человек на рынке был не самый известный.

- Скорее, не самый публичный... - прошептал себе под нос Дима. - То, что нам нужно. Борис...

- Чего? - отозвался товарищ.

- Похоже, то, что надо, - сказал Дима. - Разговор будет серьезный.

Они приблизились к белому аккуратному зданию, на котором висела табличка "Администрация". Дима остановился в десяти метрах от него, задрал голову. На крыше сразу бросилась в глаза большая тарелка спутниковой связи, пара простых телевизионных рогов с протянутыми куда-то в неизвестность проводами, три больших прожектора по углам (наверное, их было больше, с этой точки просматривалось не все). Окна второго

этажа были закрыты жалюзи, наружу выведены несколько кондиционеров. Отделка сделана на совесть; Борис тоже остановился, осмотрел дом.

- Не думаю, что стоит здесь задерживаться, - сказал им их конвоир. - Я могу расценить это как нежелание двигаться дальше, а уж этого ну никак нельзя допустить. Ну?

- Идем-идем, - внезапно сказал Дима и решительно шагнул к дверям. Спустя несколько секунд дом поглотив их.

Они вошли и сразу покрылись мурашками от той прохлады, которая была создана внутри дома кондиционерами. Там дышалось приятно и легко, шум рынка сразу исчез, едва дверь закрылась за ними. Человек зашел за ними следом, обогнал их и приблизился к следующей по коридору двери из темного дерева.

- Что-то типа шлюза, - шепнул Борис. Дима молча кивнул.

- Я привел их, - сказал человек куда-то в дверь. Стало заметно, что на уровне роста человека в стену вмонтировано небольшое переговорное устройство.

- Открываю, - раздалось из миниатюрного динамика. Щелчок размагнитченного замка, дверь распахнулась наполовину. Они прошли дальше и оказались на винтовой лестнице, круто поднимающейся на второй этаж. Где-то рядом слышался гомон нескольких человек, звонил телефон; острис трудились вовсю.

Лестница была покрыта темно-зеленой ковровой дорожкой, закрепленной, как в театрах, штангами к ступенькам. Окна выходили прямо на подъездную дорогу, где громоздились сейчас в ряд, пытаясь выехать, десятки машин. После поворота лестницы Дима увидел трассу Владивосток-Уссурийск, пролегающую в пятидесяти метрах от рынка. Десятки, сотни машин мчались по ней в обе стороны, и никому из них не было дела до того, как сейчас сложится жизнь трех Робин Гугов с авторынка.

Подъем закончился еще одной шикарной дверью. На этот раз безо всяких приспособлений, однако прямо над головами у них Дима тут же заметил маленькую веб-камеру, изображение с которой не просто писалось

Именно так и должен выглядеть кабинет автомобильного босса.

куда-то в закрома рогины, но и наверняка проходило некий анализатор, на экране которого можно было вычислить личности некоторых нежелательных особ. Перед дверью их никто не остановил, значит, никакой информации на парней у хозяина рынка не было.

- Как там Леха? - спросил Борис, наклонившись к самому уху Димы.

- Разберется по ситуации, - не таясь, ответил тот. Глупо было предполагать, что на Леху никто до сих пор не вышел. Наверное, он уже с кем-то общается; а скорее всего, ребята с рынка сгелали проще: подперли его машину с двух сторон - никуда не денется.

Они вошли.

Именно так и должен выглядеть кабинет автомобильного босса: в глаза сразу же бросился стеклянный шкаф напротив окна, в котором на нескольких широких полках были расставлены модели машин - десятки, сотни маленьких автомобильчиков, сверкающих яркими расцветками и хромом.

- Ух ты! - непроизвольно выдохнул Борис, увидев это великолепие, и только потом обратил внимание на человека, который стоял к ним спиной в дальнем конце комнаты и закрывал вмонтированный в стену сейф. Маленькая, но тяжелая дверца угрюмо бухнула, щелкнули замки. Человек повернулся к ним лицом, и они впервые в своей жизни увидели самого богатого человека их города - человека, наложившего монополию на едва ли не самое дорогое, что можно было продавать и покупать (не считая рынка недвижимости).

- В кресла. Оба, - махнул он им рукой. Дима отглянулся, увидел рядом два шикарных кожаных кресла, опустился в одно из них. Человек обошел свой рабочий стол из темно-коричневого дерева, остановился в двух шагах от своих гостей.

- Здравствуйте, - сказал он Борису и Диме, рассмотрев их. - Сразу приступим к делу. Виктор, давай сюда этого бедолагу.

Их конвоир вышел на несколько секунд за дверь, после чего в кабинете появился парень из "Марка".

- Кто из них сидел за компьютером? - спросил у него босс.

- Вот этот, - указал тот на Диму. - Я, правда, лица его не видел, он не поворачивался. Но со спины - он, сто процентов. И одежда та же. Точно он.

- А второй что делал?

- Да я и сам могу все рассказать, - попытался вставить слово Дима, но его никто не слушал.



- Второй? - переминался с ноги на ногу продавец. - В смысле, вот этот? Их же трое...

Босс вздохнул - причем сделал это нарочито громко, втянув воздух ноздрями, не раскрывая рта. Чувствовалось, что он очень раздражен.

- Этот читал с экрана, - быстро ответил продавец, боясь навлечь на себя гнев.

- Читал... В смысле переводил?

- Ну да, там же все по-японски...

- Иди, - махнул ему босс. - Нет, погожди... Сколько ты им дал?

- Тысячу сто баксов. Своих, честно заработанных...

- Не ной. Завтра тебе позвонят. На всю сумму не рассчитывай, комиссионные пока никто не отменял, - босс побренчал в руке ключами от сейфа. - Свободен.

Продавец вышел из кабинета, унося с собой смутную надежду на возвращение денег и наказание отмороzków.

- Завтра легендой вы на рынке станете, - босс вернулся за свой стол, опустился во вращающееся кресло, поколдовал с пультом кондиционера, после чего стало заметно холоднее. - Люблю, когда все вот так, на грани, чтобы еще чуть-чуть - и заморзнешь.

Из рта шел пар. Дима потер плечи и прижал руки плотнее к груди, стало чуть теплее.

- Странная у вас какая-то группа... - сказал босс, ни к кому конкретно не обращаясь. - Хакер, переводчик, уголовник. Хотя мне - из опыта боевых действий - известны и не такие преступные сообщества. Помнится, я и сам... Ну да бог с ним, с прошлым. Я вас заметил еще неделю назад, а точнее, не я сам, мне доложили. Знаете, я ведь бывший военный, поэтому у меня здесь достаточно военизировано начинающая иерархия, заканчивая разного рода службами. Есть своя разведка, своя контрразведка, свое... Все у меня свое. Вот мне вас и описали в прошлую субботу - "Карина", в ней трое, у одного на коленях ноутбук, зачем-то сверяют документы с тем,

А знаешь ли ты, Дима, что такое овердрайв?

что читают с экрана. Хакеры, блин... Правда, тот лох, которого вы тогда развели, ничего не сказал - он тут случайным человеком оказался. Привез сам себе машину, подшаманил, вдохнул в нее, так сказать, вторую жизнь, хотел с нее поднять пару сотен долларов...

Борис слушал голос хозяина рынка, будто замороженный: тембр притягивал, заставлял расслабляться и вникать, внимательно... Дима же, напротив, был напряжен и о чем-то умал - это было заметно по отсутствующему взгляду.

- ...Да и черт с ним, с этим несчастным, - махнул рукой в неизвестность босс. - На сколько вы его тогда кинули? Молчите? Правильно делаете, мне это особенно не интересно. Но сегодня... Помните, как Жеглов говорил?

"Сегодня, граждане бандиты, вышла у вас промашка..." Потому что, как в том приснопамятном фильме, "номерочек вы хапнули не тот". И конечно, продавец "Марка" не английский посол и машина у него так себе, но вот только та цепочка, что его от вас ко мне привела, родственной мне оказалась. Может быть, спустил бы я вам и сегодня ваш беспредел, но - не могу. Закон не позволяет.

Он встал с кресла, подошел к кондиционеру на стене и встал под него, как под водопад. Закрыв глаза, он что-то прошептал сам себе, после чего внезапно спросил:

- Кто придумал?

- Я, - ответил Дима.

- Как?

- Опыт есть. Я за компьютером уже много лет, а вот денег все никак не мог через него заработать.

- А теперь, значит, можешь? - босс вышел из-под ледяных воздушных струй. - Я спрашиваю еще раз - кто дал идею? Где прочитал, услышал, подглядел?

- Да нигде, - пожал плечами Дима. - Ехал однажды по Владивостоку, смотрю, объявление висит - "Коррекция показаний электронных спидометров". И телефон внизу. Меня это на мысль натолкнуло: раз уж все это уже вполне легально рекламируется, раз уж продавцы обнаглели вконец, что ради продажи на все идут, значит, можно их на этом наказывать. Ведь можно узнать родной пробег, можно узнать... Да все можно узнать! Ну, я полез японские серверы на лопатки класть...

Глаза у Димы загорелись. Он попал в свою стихию, разговор утягивал его в какие-то технические дебри, но босс не перебивал.

- Собрал статистику привоза автомобилей, потом по всем портам в Японии, из которых тачки везут, прошерстил. Компьютеры там - как будто не японцы работают, а негры какие-то плантационные. Вроде бы информация насущная, многие бы голову дали на отсечение, чтобы знать ее, - и на тебе, защита плевая. Заходи кто хочет, бери что хочешь! И еще сделали вид, что закрыли серверы для публичного доступа. Смешно сказать, закрыли! Я их быстро заново открыл...

- А никто больше не закроет - только теперь уже насовсем? - спросил босс, глядя прямо в глаза Диме.

- Пусть закрывает, - криво усмехнулся тот в ответ. - Нет такой двери, которую нельзя было бы открыть заново.

- Угу... - хмыкнул босс и вернулся к себе за стол. - А друзей своих как в дело втянул?

- Да запросто, - Дима сел в кресле поудобнее. - Добыть информацию - полдела. Наго ее еще и реализовывать. Либо продавать кому-то, либо шантажировать... Тут много вариантов. Вот Леха и подошел для этого дела практически идеально. Язык у него подвешен будь здоров, я порой и не понимал, когда он успевает лапши навешать! Ведь как парень с деньгами расстался! Деваться ему некуда было. Профессионал Леха, нечего сказать!

- А этот? - кивнул босс на Бориса, сжавшегося в кресле от того, что речь зашла о нем.

- Борис? Он просто хороший переводчик, - гордо сказал Дима, будто в знании Борисом языка была и его заслуга. - Очень хороший. Там ведь она бракадабра, иероглифы. А Борис ну просто с листа читает.

- Да чего там, - засмутился тот. - Прям уж с листа... Пробелов в знаниях еще ого-го сколько.

- Пробелов? - нахмурил лоб босс. - Пробелы нам ни к чему. Так значит, идея целиком твоя?

Дима кивнул.

- И реализация твоя? Ну, в смысле, компьютеры японские ломал сам? Никто не помогал, в интернете не светился?

- Нет, если вы о форумах. Вопросов в открытую не задавал, информацией не делился. Военная тайна.

- Молодец, хвалю... А знаешь ли ты, Дима, что такое овердрайв? - босс наклонил голову набок, ожидая ответа.

Дима отрицательно замотал головой, но потом спохватился и ответил:

- Книга такая есть - "Мона Лиза Овердрайв". Там про хакеров. Альтернативная фантастика. Другого ответа не знаю.

- Книга? Нет, причем здесь книга? Я книг давно уже не читаю, времени нет... - босс потер лагони, взял со стола зажигалку, пощелкал, прищурившись, несколько секунд смотрел на огонь.

- Овердрайв - это такая штука в автоматической коробке передач. Кнопочка маленькая сбоку. Вот вроде бы в коробке четыре передачи, а кнопку нажимаешь, и их уже пять... Представляешь?

- Смутно, - непонимающе смотрел на босса Дима.

- Понимаешь, Дима, мне твоя задумка очень нравится, - зажигалка со стуком упала на стол. - Придумал ты все сам. Кроме тебя, никто в этом не понимает...

Он перевел глаза на Бориса, который в этот момент разглядывал коллекцию в шкафу.

- А когда кнопку нажимаешь, передача становится больше всего на одну. Не на три... Ты понимаешь меня?

Дима замороженно замер, потом кивнул.

- Моя команда - это хорошо отлаженный механизм, - босс говорил медленно и тихо. - ОЧЕНЬ ХОРОШО ОТЛАЖЕННЫЙ. Но в нем до сих пор не нажата кнопка "Овердрайв". Я бы не хотел делать это зря - ты можешь дать мне здесь и сейчас гарантию на то, что будешь качать всю информацию только для меня, давать ее мне и получать с этого неплохие дивиденды?

Дима молча кивнул.

Босс подошел к нему, наклонился к самому уху и шепнул:

- И почему-то мне кажется, что ты все это затеял, чтобы вот в этом кресле здесь сейчас сидеть и со мной разговаривать. А переводчики у меня свои есть. И безо всяких пробелов в знаниях...

Борис посмотрел на них как на заговорщиков.

- Ну что, жмем кнопку? Считаю до трех.

- Да, - не дожидаясь начала счета, ответил Дима. За спиной скрипнула дверь и что-то коротко, металлически щелкнуло.

...Когда труп Бориса унесли, босс налил Диме стакан коньяка.

- За овердрайв? - подмигнул он ему.

- За... овер...драйв, - откашлявшись, сказал Дима.

В лесу неподалеку от рынка догорала Лехина "Карина"...

КОНЕЦ





ЧИТАЙ В СЕНТЯБРЕ:

Трейловые байки: бой без правил
Единственное ограничение в этой схватке цена — 2000\$

Домбайские войны
Вероломное вторжение байкеров в горы Большого Кавказа

В поисках сцепления
Оценка 64 лучших трейловых покрышек

На перекрестке лета и «Контеста»
Закулисье «Контеста», а также эксклюзивное интервью Фабьеном Барелем и Трейси Моузли

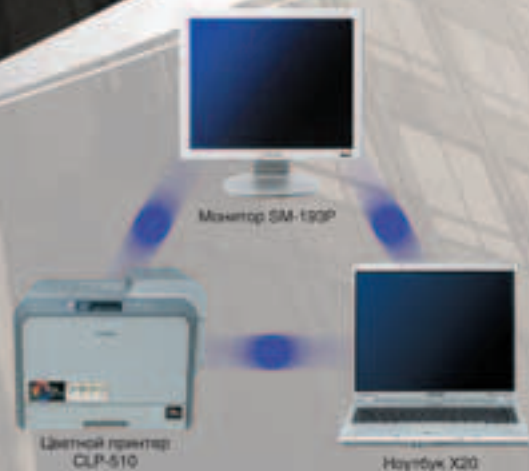
MOUNTAIN BIKE
ACTION www.mountainbike.ru

**ГЛАВНЫЙ ЖУРНАЛ РОССИИ
О МАУНТИНБАЙКЕ**

ИТ-решения Samsung для бизнеса

Не секрет, что многие преуспевающие компании выбрали технику Samsung для построения внутренней информационной структуры. Продукты Samsung помогают добиваться успеха в бизнесе как глобальным корпорациям, так и небольшим фирмам. Революционные технологии, используемые в наших ноутбуках, печатных устройствах и мониторах, позволяют Samsung по праву называться ведущей ИТ-компанией.

Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1.
Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.



SAMSUNG

10 (59) 2005

ХАКЕР БЛЕЦ

ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

●

МОБИЛЬНЫЙ ВЗАЛОМ