взлом без проводов
ALT: беспроводные сети и их взлом

крис касперски ака мыщъх

масштабное внедрение беспроводных устройств протекает довольно болезненно и то тут, то там появляются сообщения об их взломе, который уже давно превратился в настоящий радио-спорт для тинейджеров. попробуем разобраться насколько велика угроза и что можно противопоставить коварным хакерам.

введение

Беспроводные технологии прочно вошли в нашу жизнь и похоже не собираются никуда уходить. С их помощью организуются точки доступа в Интернет, строятся полноценные локальные сети, лишенные змеящихся кабелей, и делается множество других удивительных вещей. Семейство стандартов IEEE 802.11 описывает протоколы передачи данных, работающие на частоте 2,4 ГГц и обеспечивающие скорость вплоть до 11 Мбитс/с (протокол 802.11b) или даже 54 Мбит/с (протокол 802.11g). Все вместе они образуют WLAN (Wireless Local Area Network – Беспроводная Локальная Сеть).

Фактически, WLAN представляет собой обыкновенный Ethernet, только без проводов (см. рис. 1). Это значит, что беспроводные сети наследуют все уязвимости обыкновенных проводных сетей и добавляют к ним свои собственные. Описывать классические Ethernet-атаки, такие, например, как подложный ARP-сервер никому не интересно, лучше обсудим "беспроводной" аспект.

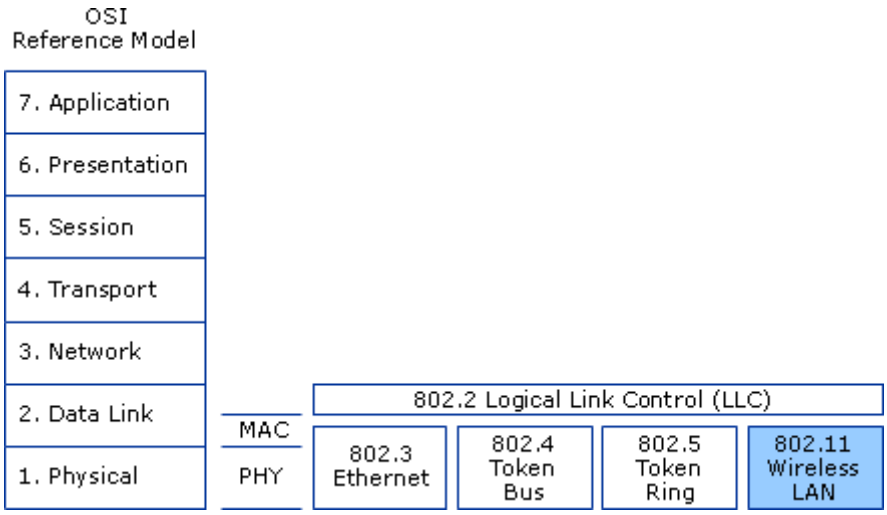

Рисунок 1 OSI-модель, подтверждающая родственные связи между протоколами 802.3 (Ethernet) и 802.11 (WLAN)

Для защиты от злоумышленников, разработчики IEEE 802.11 протоколов предприняли целый комплекс противохакерских мер: аутентификация, шифрования трафика, привязка к MAC-адресам и т. д., однако это не остановило атакующих. На протяжении четырех последних лет разработчики непрерывно совершенствовали защиту, но каждый раз в ней обнаруживалась все новые и новые дыры.

Подавляющее большинство атакующих действуют без злого умысла, воспринимая это как шалость или интеллектуальную игру, но среди них встречаются настоящие охотники за чужим трафиком, из которого можно извлечь различную конфиденциальную информацию (пароли на почтовые ящики, номера кредитных карт и т. д.). Встречаются и просто желающие подключится к Интернету за чужой счет. Если точка беспроводного доступа принадлежит крупной компании, ущерб будет не так уж и не велик, но вот в домашних сетях этим пренебрегать уже нельзя.

Чем вооружены хакеры и как им противостоять, вот вопрос, достойный нашей статьи!

аутентификация и шифрование

Согласно стандарта IEEE 802.11, существует три базовых режима безопасности, выбираемых беспроводным устройством в зависимости от уровня секретности: а) открытый режим (ни шифрование, ни аутентификация не используется); б) защищенный режим без аутентификации, но с шифрованием трафика; с) защищенный режим с аутентификацией и шифрованием трафика;

Шифрование в обоих случаях осуществляется по WEP-протоколу (Wired Equivalent Protocol — Эквивалент Проводного Протокола), опирающегося на потоковый криптоалгоритм RC4. Исходные данные (data) нарезаются на фреймы (fames) с размером 1.518 бит (впрочем, в размер задан не жестко и в зависимости от конфигурации оборудования он может существенно отличатся). Для каждого фрейма определяется 32-битная контрольная сумма (ICV), вычисляемая по алгоритму CRC32 и укладывается в пакет. Эффективный ключ шифрования (PRNG — Pseudo-Random Number Generator — Генератор Псевдослучайный Чисел) генерируются на основе двух ключей — 40-битного секретного ключа (secret key или WEP key) и 24-битного вектора инициализации (IV — Initialization Vector). Все вместе это называется 64-битным шифрованием и представят собой классический пример американского маркетинга по одурачиванию доверчивых пользователей. В самом деле, зачем потребителю знать, что для взлома ключа злоумышленнику достаточно подобрать всего лишь 40 бит из 64!

Вектора инициализации назначаются самим WLAN-устройством и передаются в открытом виде. Зачем они нужны? А затем, что используемый криптоалгоритм легко вскрывается атакой по открытому тексту. Если злоумышленнику известен хотя бы один исходный байт в каждом фрейме, ключ шифрования восстанавливается без труда, поскольку различные части ключа многократно применяются к различным частям зашифрованных фреймов. Чтобы этого избежать, никакой ключ шифрования не должен использоваться дважды. Вектора инициализации автоматически изменяются с каждым пакетом, что обеспечивает "прозрачную" смену ключа, без ведома и участия пользователя.

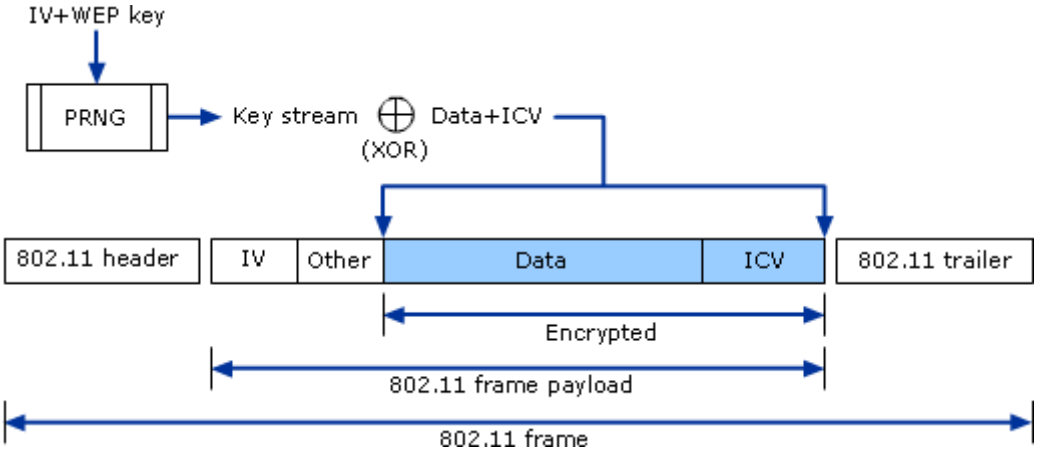

Рисунок 2 расчет контрольной суммы и шифрование трафика по протоколу WEP

Строго говоря, для шифрования используется не один секретный ключ, а целых четыре ключа, последовательно назначаемые пользователем при конфигурации беспроводного оборудования. Смена ключей происходит произвольным образом (номер ключа передается вместе с зашифрованным пакетом), но на безопасность передачи данных это никак не влияет. Если хакер может сломать один ключ, он сломает и четыре.

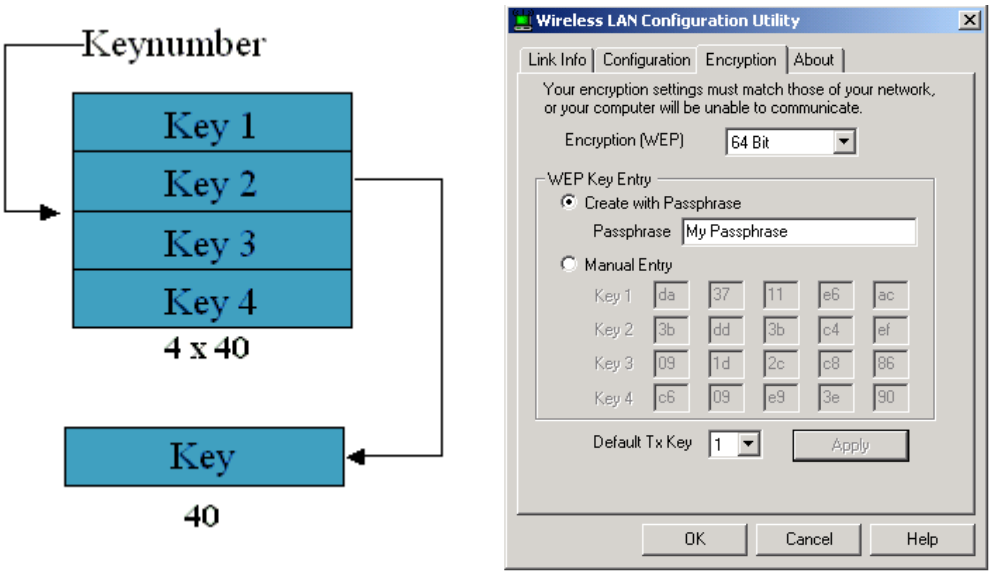

Рисунок 3 четыре секретных WEP-ключа, выбираемых пользователем и автоматически сменяющих друг друга по истечении некоторого промежутка времени

Упрощенно, процесс шифрования потока данных выглядит так (расчет контрольной суммы здесь не показан): `K=IV.WEPkey` → `KSA(K)` → `PRNG(K)XOR data stream`, где функции `KSA(A)` и `PRNG(K)` выражаются следующим псевдокодом:

```
// инициализация
for(i = 0; i < N; i++) S[i] = i;
j = 0;

// скремблирование
for i = 0; i<N; i++
{
        j = j + S[i] + K[i % length];
        swap(S[i], S[j]);
}
```

Листинг 1 псевдокод функции KSA(A), инициализирующей массив S, используемый впоследствии для генерации псевдослучайной последовательности

```
// инициализация:
static int i = 0;
static int j = 0;

// цикл генерации:
i = i + 1;
j = j + S[i];
swap(S[i], S[j]);
return  S[S[i] + S[j]];
```

Листинг 2 псевдокод функции PRNG(K), генерирующей псевдослучайную последовательность, используемую для шифрования потока данных операцией XOR

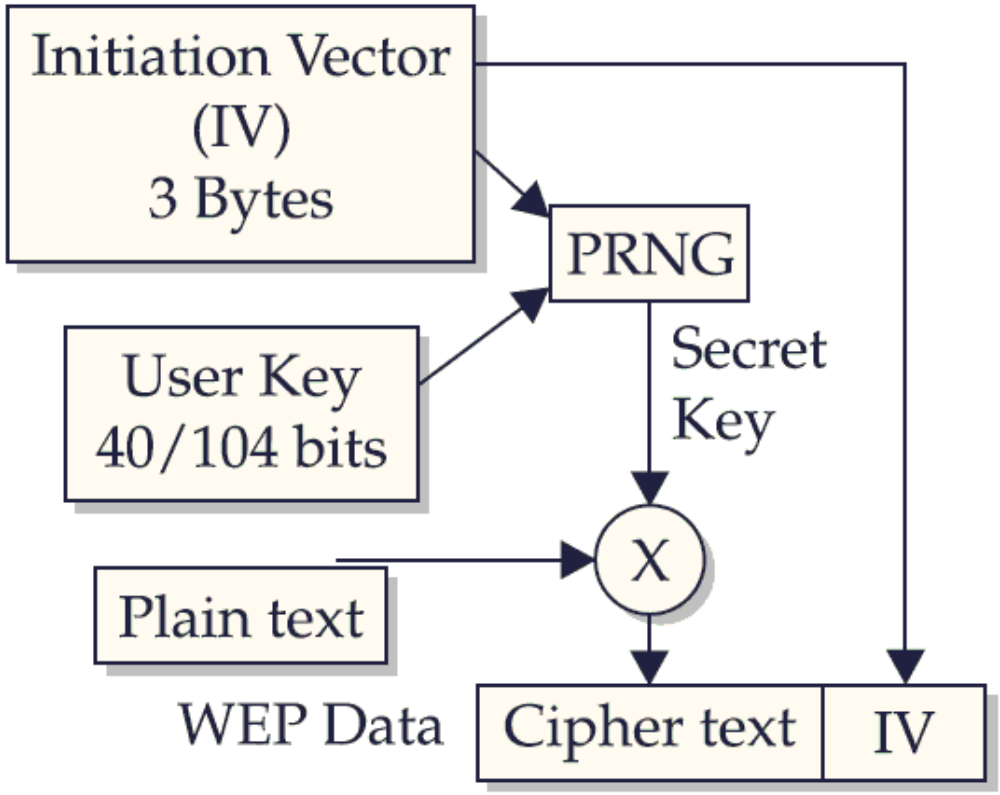

Рисунок 4 блок-схема алгоритма шифрования WEP, используемого для шифрования трафика и аутентификации

Аутентификация осуществляется по старой доброй схеме запрос/отклик (challenge/response). Клиент (Client или Station), желающий подключится к Точке Доступа (Access Point), посылает запрос на аутентификацию (Authentication Request). Точка доступа генерирует 128 байтовый псевдослучайный "испытательный текст" (Challenge Text) и оправляет его Клиенту. Получив "испытательный текст", клиент шифрует его 64-битным ключом, полученным на основе секретного WEP-ключа и произвольного вектора инициализации. Зашифрованный испытательный текст (Encrypted Challenge Text) вместе с вектором инициализации передается на Точку Доступа, где происходит обратный процесс: используя имеющейся в ее распоряжении секретный WEP-ключ и открытый вектор инициализации, Точка Доступа расшифровывает пакет и сравнивает полученный текст с оригинальным испытательным текстом. Если они совпадают, аутентификация считается успешной и Клиенту отправляется подтверждение доступа (Confirm Success).

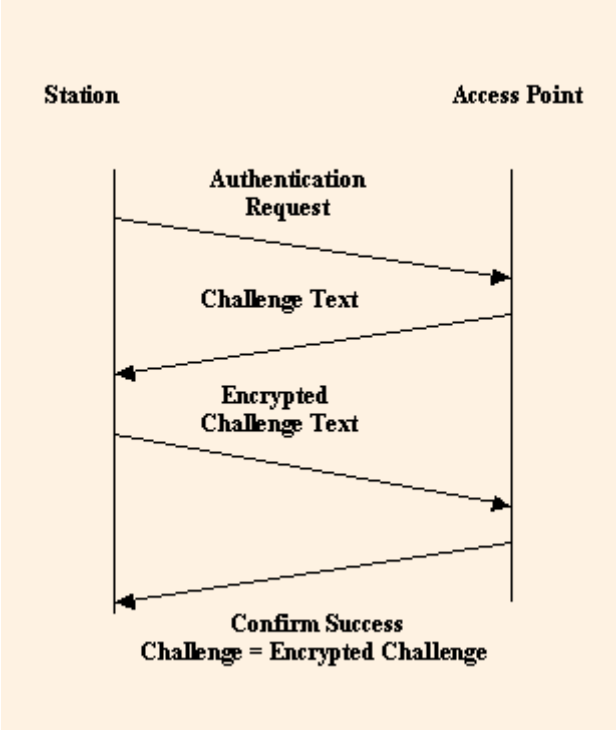

Рисунок 5 схема аутентификации Клиента, используемая в протоколе WEP

Независимо от выбранного режима секретности, Точка Доступа может использовать привязку к MAC-адресам и проверку SSID/ESSID ([Extended] Service Set IDentification – Идентификация [Расширенного] Комплекта Услуг, условно называемая "именем сети"), отсекая всех непрошеных нарушителей еще на стадии подключения (технология Access Control List — Список Управления Доступом). Для самоуспокоения такая мера может быть и сгодится, но вот злоумышленников она остановит навряд ли. И MAC, и SSID передаются по сети открытым текстом, так что их перехват не представляет никакой проблемы. Перепрограммировать MAC-адрес своей карты чуть сложнее, но хакеры с этим легко справляются (даже если карта не позволяет сделать этого явно, атакующий всегда может "перешить" ПЗУ). Что же касается SSID, то он и вовсе прописывается с пользовательского интерфейса, поскольку используется исключительно как "маркер", позволяющий беспроводному устройству отличить одну сеть от другой. Борьба с хакерами в его задачу не входит. Тем не менее, это еще не значит, что SSID можно не заполнять (а большинство пользователей именно так и поступает)!

начинаем атаковать

Стандартный 64-битный ключ шифрования легко взламывается лобовым перебором. Учитывая, что фактическая длина секретного ключа составляет всего лишь 40 бит, в среднем нам достаточно перебрать $2^{40}/2$ == 549.755.813.888 комбинаций. При скорости перебора в сотню миллионов ключей в секунду (вполне умеренная скорость для современных процессоров), атака займет всего час — полтора. Злоумышленнику достаточно перехватить всего 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 необязательно! (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. Добавьте сюда 24 бита Вектора Инициализации и вы получите так называемое 128-битное шифрование. Подобрать 104-битный ключ вслепую уже нереально (при прежней скорости перебора в среднем на это уйдет 281.70.013.338.405.097.811 часов или 3.215.754.947.306.518 веков, что значительно превышает не только оставшееся время существования Солнца, но и всей 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 "Weaknesses in the Key Scheduling Algorithm of RC4" ("Слабые места алгоритма распределения ключей RC4"), мгновенно ставшую знаменитой и определившую название всего семейства атак этого типа: FMS-attack — по первым буквам 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 должен отобрать несколько пакетов, зашифрованных слабыми ключами (такие пакеты называются "слабыми" или "интересными" — interesting). Каждый слабый пакет с 5% степенью вероятности восстанавливает один байт секретного ключа, поэтому общее количество пакетов, которые атакующему необходимо собрать для реализации атаки, в первую очередь зависит от степени его везучести. В среднем, для взлома требуется порядка 6 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 закачивается уже через несколько минут. И это при 104-битном ключе! Так работает AirSnort и многие другие хакерские утилиты, которые свободно можно 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. Для этого достаточно просто перехватить "правильный" пакет и не расшифровывая ретранслировать его вновь. В частности, ARP-запрос, вызовет неизбежный ARP-ответ. Отличить APR-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 см), хотя некоторые карты ухитряются перехватывать трафик и одновременно с этим бомбардировать жертву пакетами.

Хакеры из лаборатории H1kari of Dasb0den Labs усилили FMS-алгоритм, сократив количество необходимых пакетов с 6 миллионов о 500 тысяч, а в некоторых случаях 40/104 битный ключ взламывается всего с 3 тысячами пакетов, что позволяет атаковать даже домашние Точки Доступа, не напрягая их избыточным трафиком. Усиленный алгоритм атаки реализован в утилите dwepcrack, входящий в состав пакета BSD-airtools, а так же другом хакерском инструментарии.

Рисунок 6 внешний вид утилиты dwepcrack, реализующий усиленную разновидность FMS-атаки на WEP-ключи

Разработчики оборудования отреагировали вполне адекватным образом, изменив алгоритм генерации векторов инициализации так, чтобы слабые ключи уже не возникали. Теперь даже dwepcrack'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 древние модели решают эту проблему путем обновления прошивки (правда, не все производители выпустили такое обновление). Впрочем, даже сегодня, в середине 2005 года, в эксплуатации находится огромное количество уязвимых устройств, особенно на периферии, куда уходят все нереализованные складские запасы. Тем не менее, ситуация такова, что хакерам пришлось искать новые пути для атаки. И они были найдены!

В августе 2004 года хакер по имени KoreK выложил на форумах NetStumbler'a исходный код нового криптоанализатора, взламывающего даже "сильные" векторы инициализации. Для восстановления 40-битного ключа ему требовалось всего 200 тысяч

пакетов с уникальным векторами инициализации, а для 104 битного — 500 тысяч. Количество пакетов с уникальными IV в среднем составляет порядка 95% от общего количества зашифрованных пакетов, так что для восстановления ключа атакующему потребуется совсем немного времени. Данный алгоритм реализован в chopper'e, aircrack'e, WepLab'e и других хакерских утилитах, недостатка в которых испытывать не приходится.

В новом оборудовании, построенном по технологии WPA – Wi-Fi Protected Access (Защищенный Wi-Fi Доступ), защищенность беспроводных устройств вновь была усилена. На место WEP пришел TKIP (Temporal Key Integrity Protocol — Протокол Краткосрочной Целостности Ключей), генерирующий динамические ключи, сменяющие друг друга пару минут. 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 восьмибайтный код целостности сообщения, рассчитанный по алгоритму Michael, предотвращающий отправку подложных пакетов. Процедура аутентификации осуществляется по протоколу EAP (Extensible Authentication Protocol – Расширенный Протокол Аутентификации), использующим либо RADIUS-сервер (Remote Authentication Dial-In User Service — Служба Дистанционной Аутентификации Пользователей по Коммутируемым Линиям), либо 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 все еще недостаточно отлажен и потому в некоторых случаях он не срабатывает.

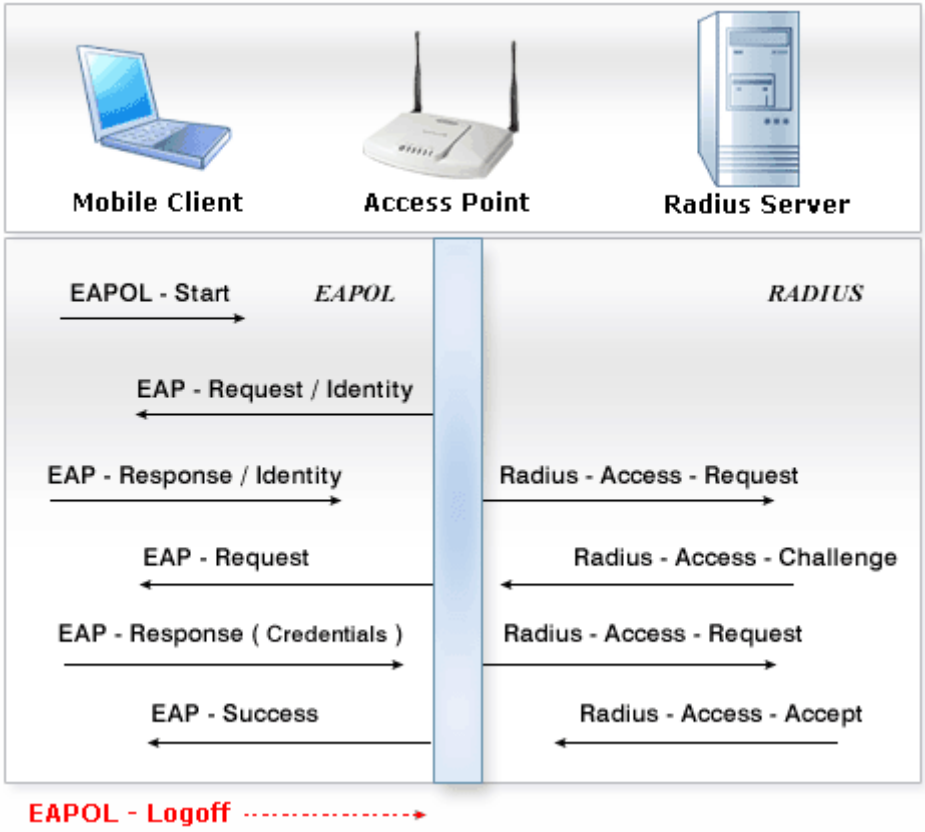

Рисунок 7 схема аутентификации, осуществляемой по WPA-протоколу с выделенным Radius-сервером

Стандарт IEEE 802.11i описывает более продвинутую систему безопасности, основанную на криптоалгоритме AES и известную под именем WPA2. 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 рекомендуется пробить VPN-тоннели (Virtual Private Network – Виртуальная Частная Сеть), задействовать SSL-шифрование или подключить любые

другие способы защиты, изначально ориентированные на небезопасные каналы передачи данных.

>>> врезка: атака по открытому тексту

Если беспроводная сеть имеет выход в Интернет и злоумышленнику известен электронный адрес хотя бы одного из ее абонентов, он может послать жертве письмо, выловить относящиеся к нему зашифрованные пакеты и восстановить секретный ключ по известному содержимому. Полный цикл криптоанализа не займет и нескольких минут! Главное, чтобы жертва согласилась принять письмо, а не удалила его на сервере как спам.

Существуют и другие эффективные атаки против WLAN, описание которых можно найти, например, в статье "What's Wrong With WEP?" (http://www.ilabs.interop.net/WLANSec/What_is_wrong_with_WEP-lv03.pdf)

амуниция и снаряжение

Радиус действия большинства беспроводных устройств ограничен дистанцией в 10 — 100 метров (точная цифра зависит от класса и конструктивных особенностей конкретного оборудования), поэтому атакующий должен находится в непосредственной близости от жертвы. Для этого хорошо подходят карманные компьютеры, они же "наладонники" или Pocket PC. Как вариант, можно воткнуть к десктоп WLAN-карту, подключенную к внешней антенне. Добротная антенна направленного типа, снабженная усилителем мощности, уверенно держит связь на расстояниях до 1,5 — 2 км, а в некоторых случаях и больше того!

Рисунок 8 направленная антенна и усилитель мощности к ней

Такую антенну вместе с усилителем можно купить и легально. Их выпускает Hyper Technology, Broadcast Warehouse, Радиал и многие другие компании. Среди хакеров большой популярностью пользуется направленная антенна HG2415Y типа Radome-Enclosed от компании HyperLink Technology, которую за можно заказать по Интернету. Рассчитанная на стационарный монтаж, она, тем не менее, неплохо чувствует себя на фотографическом штативе или даже обыкновенном ружейном прикладе, превращающим ее в мобильный инструмент для слежения за подвижными жертвами. Параболические антенны действуют на расстояниях, ограниченным фактически одним лишь горизонтом видимости, однако, они катастрофически немобильны, а для хакера самое главное вовремя смотаться с места преступления. Ищите направленные антенны на 2,4 ГГц (они же антенны стандарта IEEE 802.11b/802.11g или WLAN).

При выборе WLAN-карты необходимо убедиться, что выбранные хакерские утилиты (и в первую очередь сниффер) умеет работать с данным чипсетом. Список поддерживаемого оборудования обычно публикуется на сайтах разработчиков соответствующих программ или содержится в документации. Наибольшей любовью пользуется чипсет Prism/Prism2 и беспроводные карты на его основе (например Senao 2511-CD-PLUS). Он отлично документирован, причем документация распространяется не по подписке, а бесплатно раздается всем желающим!

Из программного обеспечения нам понадобится сетевой сканнер, сниффер и взломщик паролей. Их можно найти практически на любой платформе. 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 что недостаточно).

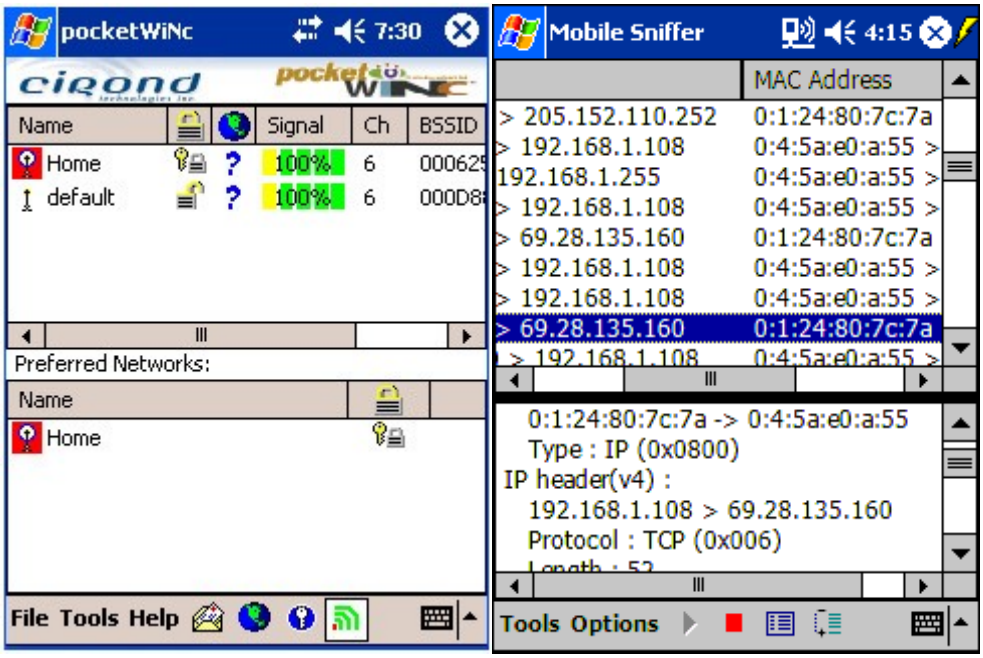

Рисунок 9 оружие наладонников — снифферы pocketWiNc (слева) и Mobile Sniffer (справа)

Основной сниффер под LINUX и BSD это, конечно же, Kismet, изначально ориентированный на хакерские цели. Он поддерживает большое количество оборудования и беспроводных протоколов, удобен в использовании и к тому же абсолютно бесплатен. Перехватывает сетевой 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 WepLap, причем, первый работает значительно лучше.

Рисунок 10 Kismet, установленный на ноутбук

Под Windows перехват беспроводного трафика реализуется гораздо сложнее и кроме сниффера вам потребуется хакнутые версии драйверов для WLAN-карты. Из коммерческих снифферов можно порекомендовать Airopeek, из некоммерческих — утилиту airdump, входящую в состав aircrack и портированную под Windows. Еще можно использовать Sniffer Pro или любой другой подходящий сниффер.

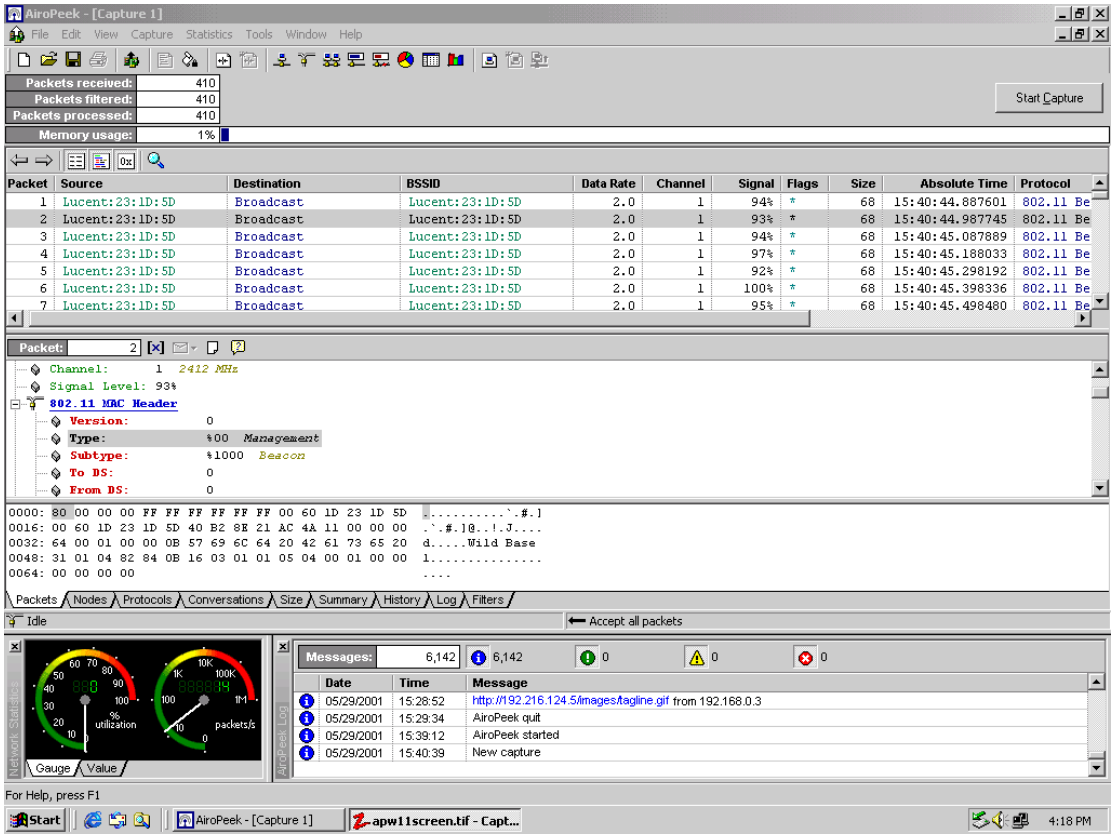

Рисунок 11 внешний вид сниффера AiroPeek

На Mac'ах весь хакерский инструментарий собран в одном флаконе — утилите по имени KisMAC, которая настолько проста, что ей сможет пользоваться даже ребенок. Здесь есть и сетевой сканер, и сниффер, и парольный переборщик (brute force), и криптоанализатор слабых векторов инициализации. Предусмотрена даже такая мелочь, как планировщик, позволяющий осуществлять атаки по расписанию.

В общем, на недостаток хакерского инструментария жаловаться не приходится, в глазах так и рябит от разнообразия.

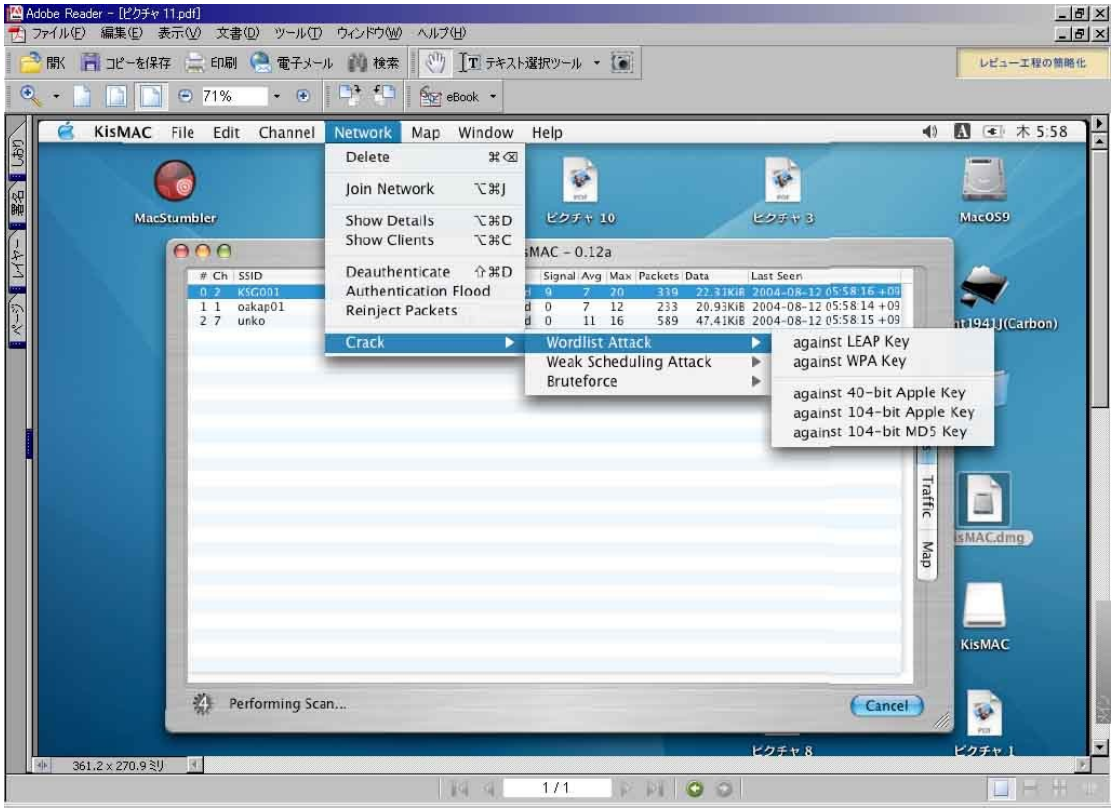

Рисунок 12 так выглядит утилита kisMAC, соединившая в себе сниффера с парольным взломщиком

Загрузочный лазерный диск Auditor Security Collection уже содержит весь необходимый инструментарий и модифицированные драйвера, поддерживающие большое количество разнообразных беспроводных устройств. 518-мбайтный ISO-образ можно бесплатно скачать с WEB-сайта компании Moser Informatik, расположенного по адресу: http://www.moser-informatik.ch

заключение

Так все-таки безопасны беспроводные сети или нет? Устройства, поддерживающие стандарт IEEE 802.11i (WPA2) еще никому взломать 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, отпугивающего новичков и просто любопытствующих пользователей, впервые взявших сниффер в руки.

>>> врезка: ссылки на инструментарий

- **Hyperlink Technology**:
  - фирма, выпускающая антенны и торгующая ими через Интернет: http://www.hyperlinktech.com;
- **Broadcast warehouse**:
  - еще один производитель антенн для WLAN-устройств: http://www.broadcastwarehouse.com;
- **RADIAL**:
  - отечественный производитель антенн: http://www.radial.ru;
- **NetStumbler**:
  - монитор беспроводной сети, работающий под Windows 2000/XP, версия для Windows CE называется MiniStumbler и работает на Pocket PC: http://www.netstumbler.com/downloads;
- **Airscanner Mobile:**

- бесплатный сниффер для Pocket PC: http://www.snapfiles.com/get/pocketpc/airscanner.html;

- **PocketWarrior**:
  - еще один бесплатный сниффер под Windows CE и Pocket PC: http://pocketwarrior.sourceforge.net;
- **kismet**:
  - сниффер номер один под Linux, BSD и MacOS, ориентированный на хакерскую деятельностью и распространяющийся в исходных текстах, версия под Windows обладает ограниченными возможностями и потому не рекомендуется: http://www.kismetwireless.net/;
- **Airopeek**:
  - достойный сниффер под Windows: www.wildpackets.com/products/airopeek;
- **Sniffer Portable**:
  - http://www.snmp.co.uk/nai/amnesty.htm;
- **aircrack**:
  - лучший взломщик WEP и WPA-паролей на сегодняшний день, распространяющийся на некоммерческой основе; в комплект поставки входит сниффер, работающий на Linux и Windows 2000/XP: http://www.cr0.net:8040/code/network/aircrack/;
- **AirSnort**:
  - устаревший взломщик WEP-паролей: http://airsnort.shmoo.com;
- **kisMAC**:
  - утилита для атаки на беспроводные сетеи под MAC OS: снифер и взломщик паролей в одном флаконе: http://binaervarianz.de/projekte/programmieren/kismac/download.php;

>>> врезка: ссылки на интересные статьи

- **Weaknesses in the Key Scheduling Algorithm of RC4**:
  - библия всех взломщиком WEP-ключей, написанная тройкой магов Scott Fluhrer, Itsik Mantin и Adi Shamir (на английском языке): http://www.smallnetbuilder.com/Weblink-req=visit-lid=66.php;
- **Practical Exploitation of RC4 Weaknesses in WEP Environments by David Hulton**:
  - статья, описывающая усиленный вариант FMS-атаки на WEP с примерами исходного кода (на английском языке): http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt;
- **Wireless Security Auditor (WSA)**:
  - статья из исследовательского центра IBM, описывающая проблемы безопасности беспроводных протоколов (на английском языке): http://www.research.ibm.com/gsal/wsa/;
- **Атаки на WEP**:
  - практическое пособие атакующего, сравнение различных хакерских утилит, советы по их настройке (на русском языке): http://www.securitylab.ru/53508.html и http://www.securitylab.ru/54769.html;
- **Dispelling the Myth of Wireless Security**:
  - слегка устаревшая статья о способах взлома беспроводных сетей, но комментарии к ней вполне актуальны (на английском языке): http://www.oreillynet.com/pub/a/wireless/excerpt/wirlsshacks_chap1/index.html;
- **NetStumbler-форум**:
  - форум, на котором общаются WLAN-хакеры (на английском языке): http://www.netstumbler.org;

>>> врезка: книги по безопасности беспроводных сетей

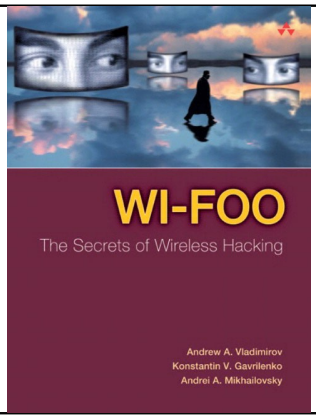	**Wi-Foo** By Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky Publisher : Addison Wesley Pub Date : June 28, 2004 ISBN : 0-321-20217-1 Pages : 592

Рисунок 13 лучшая книга по взлому беспроводных сетей с большим количеством практических примеров, ориентированная на хакеров и криптоаналетиков,

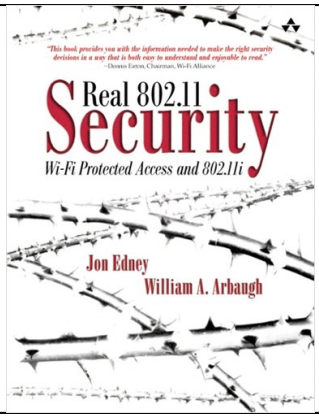	Real 802.11 Security: Wi-Fi Protected Access and 802.11i By Jon Edney, William A. Arbaugh Publisher : Addison Wesley Pub Date : July 15, 2003 ISBN : 0-321-13620-9 Pages : 480

Рисунок 14 неплохая книга по безопасности беспроводных сетей, ориентированная на теоретиков и системных администраторов

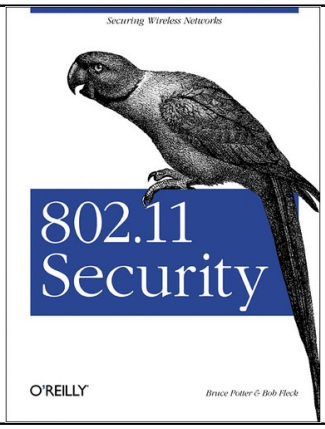	802.11 Security By Bob Fleck, Bruce Potter Publisher : O'Reilly Pub Date : December 2002 ISBN : 0-596-00290-4 Pages : 208

Рисунок 15 еще одна сильно теоритизированная, но в целом весьма не плохая книга по атакам на WLAN