НАСКОЛЬКО НЕУЯЗВИМА ВАША БЕСПРОВОДНАЯ СЕТЬ?

Масштабное внедрение беспроводных устройств протекает довольно болезненно. То тут, то там появляются сообщения об их взломе, который уже давно превратился в настоящий радиоспорт для тинейджеров. Попробуем разобраться, насколько велика угроза и что можно противопоставить коварным хакерам.

КРИС КАСПЕРСКИ

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-уязвимости, такие, например, как подложный ARP-сервер, не интересно, лучше обсудим «беспроводной» аспект (**рис. 1**).

Для защиты от злоумышленников разработчики IEEE 802.11 протоколов предприняли целый комплекс противохакерских мер: аутентификация, шифрование 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 обнаруживались 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 подключиться к Интернету за чужой счет. Если точка беспроводного доступа принадлежит крупной компании, ущерб будет не так уж и велик, но вот в домашних сетях этим пренебрегать нельзя.

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

Аутентификация и шифрование

Согласно стандарту IEEE 802.11, существует три базовых режима безопасности, выбираемых беспроводным устройством в зависимости от уровня секретности:

- открытый режим (ни шифрование, ни аутентификация не используются);
- защищенный режим без аутентификации, но с шифрованием трафика;
- защищенный режим с аутентификацией и шифрованием трафика.

Шифрование в обоих случаях осуществляется по WEP-протоколу (Wired Equivalent Privacy – эквивалент проводной защищенности), опирающемуся на потоковый криптоалгоритм RC4. Исходные данные (data) нарезаются на фреймы (fames) с размером 1.518 бит (впрочем, размер задан не жестко и в зависимости от конфигурации оборудования он может существенно отличаться). Для каждого фрейма определяется и укладывается в пакет 32-битная контрольная сумма (ICV), вычисляемая по алгоритму CRC32. Эффективный ключ шифрования (PRNG – Pseudo-Random Number Generator – генератор псевдослучайных чисел) генерируется на основе двух ключей – 40-битного секретного ключа (secret key или WEP key), назначаемого пользователем, и 24-битного вектора инициализации (IV – Initialization Vector), генерируемого случайным образом для каждого пакета. Все вместе это называет-

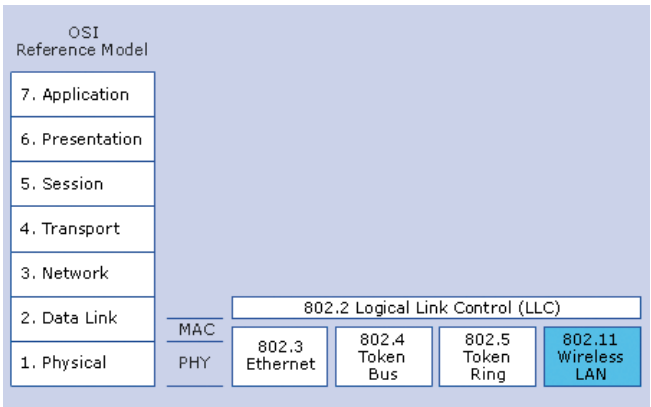


Рисунок 1. OSI-модель, подтверждающая родственные связи между протоколами 802.3 (Ethernet) и 802.11 (WLAN)

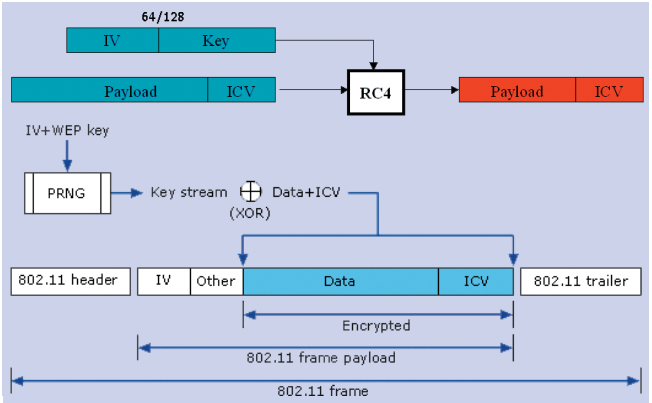
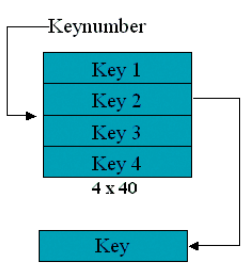


Рисунок 2. Расчет контрольной суммы и шифрование трафика по протоколу WEP

ся 64-битным шифрованием и представит 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 (см. **рис. 2**).

Строго говоря, для шифрования используется не один секретный ключ, а целых четыре, последовательно назначаемых 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 сможет взломать один ключ, он сломает и четыре (см. **рис. 3**).

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 (см. **листинг 1, 2** и **рис. 4**).

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 отправляет 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 имеющий-

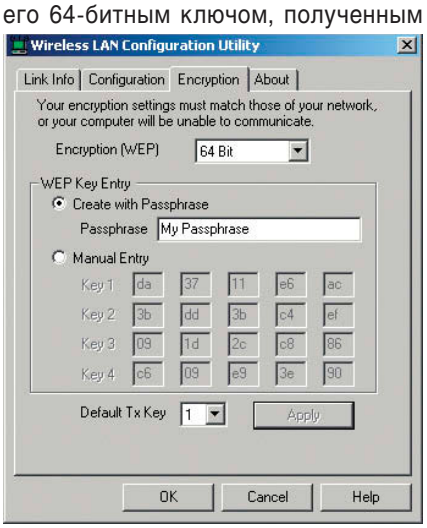


Рисунок 3. Четыре секретных WEP-ключа, выбираемых пользователем и автоматически сменяющих друг друга по истечении некоторого промежутка времени

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

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

// перемешивание байт, оно же
// скреблирование (scrambling)
for i = 0; i<N; i++
{
      j = j + S[i] + K[i % length];
      swap(S[i], S[j]);
}

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

// 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]];
```

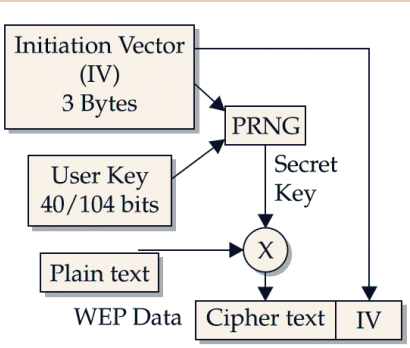


Рисунок 4. Блок-схема алгоритма шифрования WEP, используемого для шифрования трафика и аутентификаци

ся 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) (см. **рис. 5**).

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 программным образом – а подавляющее большинство карт это позволяет – 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)!

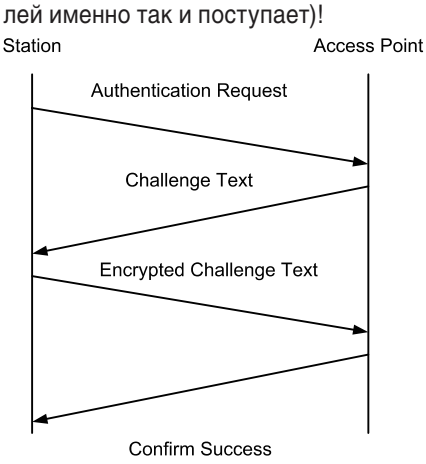


Рисунок 5. Схема аутентификации клиента, используемая в протоколе WEP

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. В этом ему невероятно поможет тот факт, что трафик к почтовому серверу генерируется периодически (например, проверка почты осуществляется каждые 5 минут), поэтому его очень легко отличить ото всех остальных. 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).

Ошибки разработчиков WEP-протокола

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 возраст Вселенной), 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 сделавшую их знаменитыми. Впоследствии все атаки этого типа стали обозначаться аббревиатурой FMS – 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 отбирает пакеты, зашифрованные 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 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 досту-

па 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, ретранслировать его вновь. В частности, ARP-запрос вызовет неизбежный ARP-ответ. Отличить APR-запросы от всех остальных пакетов очень просто: frame.pkt_len == 68 (размер кадра) и wlan.da == FF:FF:FF:FF:FF:FF (адрес назначения). Обычно для передачи запросов используется отдельная WLAN-карта (при этом расстояние между антеннами приемной и передающей карт должно составлять по меньшей мере 15 см, чтобы избежать взаимных наводок), хотя некоторые карты ухитряются перехватывать трафик и одновременно с этим бомбардировать жертву пакетами.

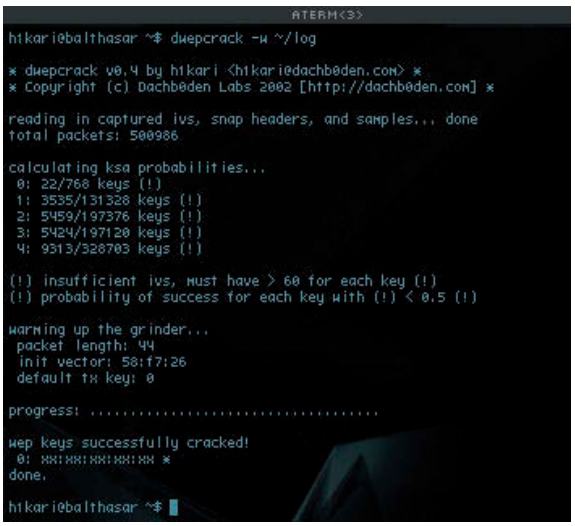


Рисунок 6. Внешний вид утилиты dwepcrack, реализующей усиленную разновидность FMS-атаки на WEP-ключи

Хакеры из лаборатории H1kari of Dasb0den Labs усилили FMS-алгоритм, сократив количество необходимых пакетов с 6 миллионов до 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, входящей в состав пакета BSD-airtools, а также в другом хакерском инструментарии (**рис. 6**).

Разработчики оборудования отреагировали вполне адекватным образом, изменив алгоритм генерации векторов инициализации так, чтобы слабые ключи уже не возникали. Теперь даже dwepcrack требовалось перехватить свыше 10 миллионов пакетов, но даже в этом случае успешная расшифровка ключа не гарантирована! Устройства, выпущенные после 2002-2003 гг., 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 множество 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 продемонстрировал исходный код нового криптоанализатора, взламывающего даже «сильные» векторы инициализации. Для восстановления 40-битного ключа ему требовалось всего 200 тысяч пакетов с уникальными векторами инициализации, а для 104-битного – 500 тысяч. Количество пакетов с уникальными векторами инициализации 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, aircrack, WepLab 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 через 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 ретрансляцию подложных пакетов. Процедура аутентификации осуществляется по протоколу EAP (Extensible Authentication Protocol – расширенный протокол аутентификации), использующему ли-

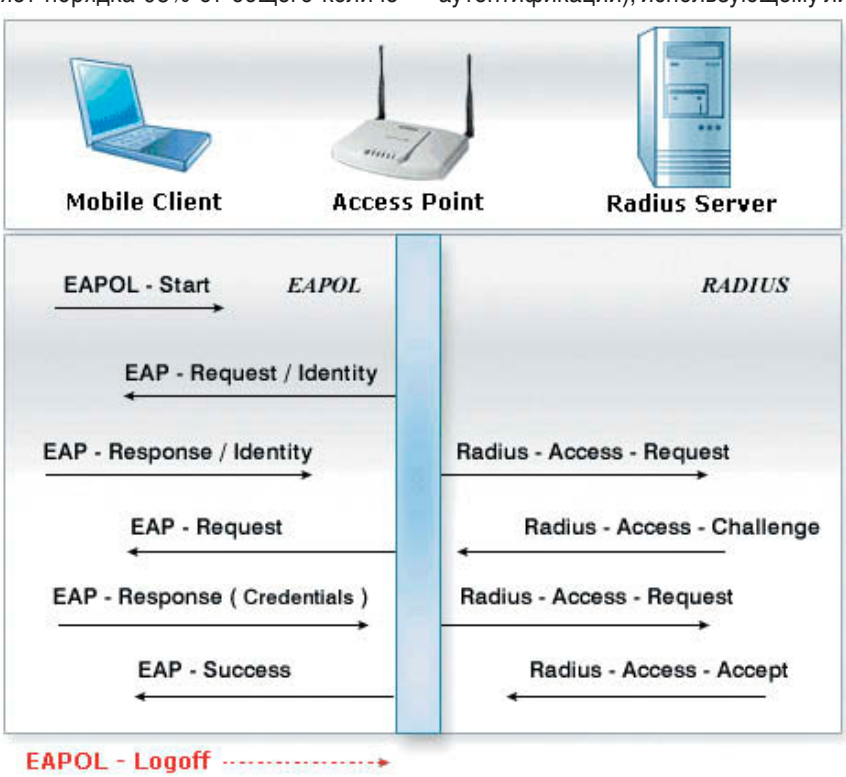


Рисунок 7. Схема аутентификации, осуществляемой по WPA-протоколу с выделенным Radius-сервером

бо 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 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 (см. **рис. 7**).

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, задействовать SSL-шифрование или подключить любые другие способы защиты, изначально ориентированные на небезопасные каналы передачи данных.

Существует только один способ проверить, насколько безопасно приобретаемое вами беспроводное устройство – это атаковать его! Каждый уважающий себя администратор должен отчетливо представлять, какой инструментарий находится на службе у хакеров, знать его сильные и слабые места. Бояться хакерских утилит не нужно! Ни один закон не запрещает «взламывать» свою собственность, принадлежащую вам по праву, поэтому никаких юридических проблем здесь не возникает, а под категорию «вредоносных» программ обсуждаемые утилиты не попадают. Как показывает практика, больше всех волнуется тот, кто не контролирует ситуацию, образно говоря, находясь в темноте с завязанными глазами. Когда-то боялись привидений, сейчас боятся хакеров, вирусов и червей. А все почему? Потому что не знают, как построить надежную защитную систему, как из всех WLAN-карт, разбросанных по витрине, выбрать ту, которая будет неподвластна взлому. Производители оборудования, как уже было показано выше, постоянно лукавят. Верить им нельзя, и приходится рассчитывать только на самих себя.

От антенны до программы

Радиус действия большинства беспроводных устройств ограничен дистанцией в 10-100 метров (точная цифра зависит от класса и конструктивных особенностей конкретного оборудования), поэтому атакующий должен находиться в непосредственной близости от жертвы. Одни хакеры вооружаются карманными компьютерами (они же «наладонники» или Pocket PC), другие предпочитают десктоп с WLAN-картой, подключенной 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, так что простой бдительности для его обнаружения уже будет недостаточно!

При выборе WLAN-карты атакующий должен убедиться, что выбранные хакерские утилиты (и в первую очередь сниффер) умеют 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 захватывают 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) (см. **рис. 8**).

Основной сниффер под LINUX и BSD это, конечно же, Kismet, изначально ориентированный на исследовательские 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.

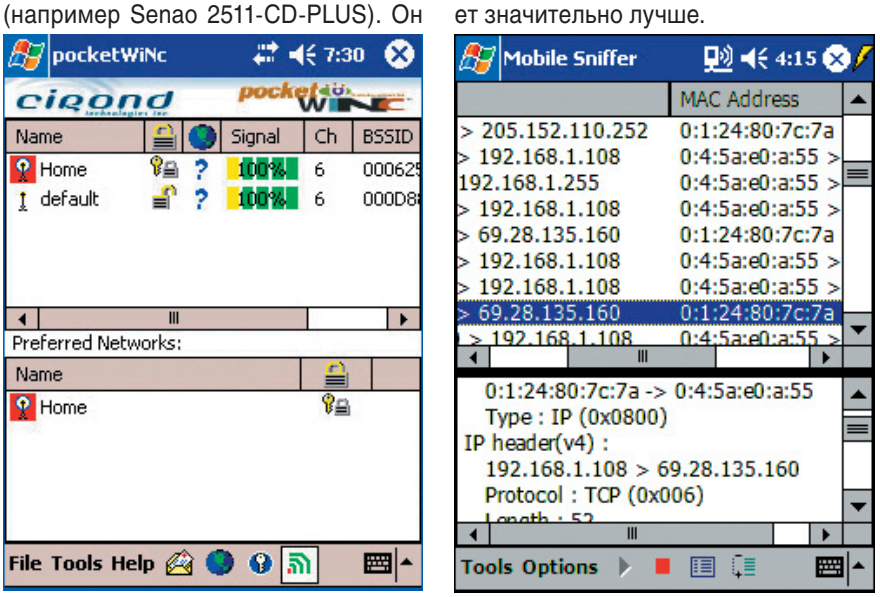


Рисунок 8. Оружие наладонников – снифферы pocketWiNc (слева) и Mobile Sniffer (справа)

Под Windows перехват беспроводного трафика реализуется гораздо сложнее и кроме сниффера нам потребуются модифицированные 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.

На Mac 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.

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

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.

Что же касается WPA1, то по этому поводу существуют различные мнения. Начнем с того, что схема аутентификации непосредственно в сам протокол WPA1 не входит и осуществляется сторонними средствами. Это может быть и EAP-MD5, и EAP-TLS и MS-CHAP... То есть сама по себе поддержка WPA1 ничего не решает! Безопасность обеспечивается лишь правильной настойкой оборудования, а это требует соответствующей квалификации обслуживающего персонала! Поэтому, если вы не уверены в себе, от использования WPA1 лучше воздержаться.

Литература:

1. Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. Wi-Foo. – Addison Wesley, ISBN : 0-321-20217-1, 592 с. – лучшая книга по взлому беспроводных сетей с большим количеством практических примеров, ориентированная на хакеров и криптоаналитиков.
2. Jon Edney, William A. Arbaugh. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. – Addison Wesley, ISBN : 0-321-13620-9, 480 с. – неплохая книга по безопасности беспроводных сетей, ориентированная на теоретиков и системных администраторов.
3. Bob Fleck, Bruce Potter. 802.11 Security. – O'Reilly, ISBN: 0-596-00290-4, 208 с. – сильно теоретизированная, но в целом весьма не плохая книга по атакам на WLAN.
4. Weaknesses in the Key Scheduling Algorithm of RC4: библия всех исследователей WEP-ключей, написанная тройкой магов Scott Fluhrer, Itsik Mantin и Adi Shamir (на англ.): http://www.smallnetbuilder.com/Weblink-req=visit-lid=66.php.
5. Practical Exploitation of RC4 Weaknesses in WEP Environments by David Hulton: статья, описывающая усиленный вариант FMS-атаки на WEP с примерами исходного кода (на англ.): http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt.
6. Wireless Security Auditor (WSA): статья из исследовательского центра IBM, описывающая проблемы безопасности беспроводных протоколов (на англ.): http://www.research.ibm.com/gsal/wsa.
7. Атаки на WEP: практическое пособие атакующего, сравнение различных хакерских утилит, советы по их настройке (на рус.): http://www.securitylab.ru/53508.html и http://www.securitylab.ru/54769.html.
8. Dispelling the Myth of Wireless Security: слегка устаревшая статья о способах взлома беспроводных сетей, но комментарии к ней вполне актуальны (на англ.): http://www.oreillynet.com/pub/a/wireless/excerpt/wirlsshacks_chap1/index.html.
9. NetStumbler-форум: форум, на котором общаются WLAN-хакеры (на англ.): http://www.netstumbler.org.

Ссылки на инструментарий:

1. 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.
2. Airscanner Mobile: бесплатный снифффер для Pocket PC: http://www.snapfiles.com/get/pocketpc/airscanner.html.
3. PocketWarrior: бесплатный снифффер под Windows CE и Pocket PC: http://pocketwarrior.sourceforge.net.
4. kismet: снифффер 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.
5. Airopeek: достойный снифффер под Windows: http://www.wildpackets.com/products/airopeek.
6. Sniffer Portable: http://www.snmp.co.uk/nai/amnesty.htm.
7. aircrack: лучший взломщик WEP и WPA-паролей на сегодняшний день, распространяющийся на некоммерческой основе; в комплект поставки входит снифффер, работающий на Linux и Windows 2000/XP: http://www.cr0.net:8040/code/network/aircrack.
8. AirSnort: устаревший взломщик WEP-паролей: http://airsnort.shmoo.com.
9. kisMAC: утилита для атаки на беспроводные сети под MAC OS: снифффер и взломщик паролей в одном флаконе: http://binaervarianz.de/projekte/programmieren/kismac/download.php.