Атаки на клиентов WEP

Сергей Гордейчик

gordey @ ptsecurity.com

Содержание

Введение

Казалось бы, говорить об уязвимостях протокола WEP в 2007 году можно только с точки зрения исторической ретроспективы. Однако, несмотря на все свои недостатки, протокол WEP все еще широко используется в беспроводных сетях. Что обуславливает необходимость демонстрации опасности его применения в ходе тестов на проникновение.

Существующие методы взлома WEP ориентированны, прежде всего, на точки доступа и требуют наличия возможности интерактивного взаимодействия с AP. В данной статье приведена техника, позволяющая восстановить ключ WEP без доступа к AP, находясь в диапазоне радиовидимости станции, ищущей сеть.

Например, ключ WEP к домашней точке доступа может быть получен в то время, как её владелец работает на ноутбуке в самолете или офисе.

Атаки на клиентов беспроводных сетей

Атаки, направленные на клиентов беспроводных сетей являются эффективным инструментом в арсенале злоумышленников. Одним из наиболее распространенных методов является создание атакующим точки доступа, ожидание соединения с ней клиента и подключение к станции на сетевом уровне. Для эмуляции точки доступа, соответствующей требованиям станции могут быть использованы утилиты Karma Tools (http://www.theta44.org/karma/index.html), probemapper (http://www.securitystartshere.net/downloads/tool-probemapper0.5.htm) или airsnarf (http://airsnarf.shmoo.com/) и т.д.

Как показывают исследования с использованием техники Gnivirdraw (http://www.securitylab.ru/analytics/278309.php), до 80% клиентов содержат в профиле незащищенные подключения или по другим причинам соединяются с ложными точками доступа. Однако использование станцией любых механизмов защиты, даже таких как WEP уже серьезно снижают вероятность успеха атакующего. Это связанно с тем, что клиенты будут требовать от ложной точки доступа применения WEP.

Большинство клиентов используют аутентификацию Open System, что увеличивает вероятность успешного установления ассоциации и в случае применения WEP. Однако все данные на вышестоящих уровнях модели OSI будут зашифрованы с помощью неизвестного ключа. То есть злоумышленник может установить ложную точку доступа с произвольным ключом WEP и многие клиенты подключатся к ней на канальном уровне, но без возможности обмена информацией.

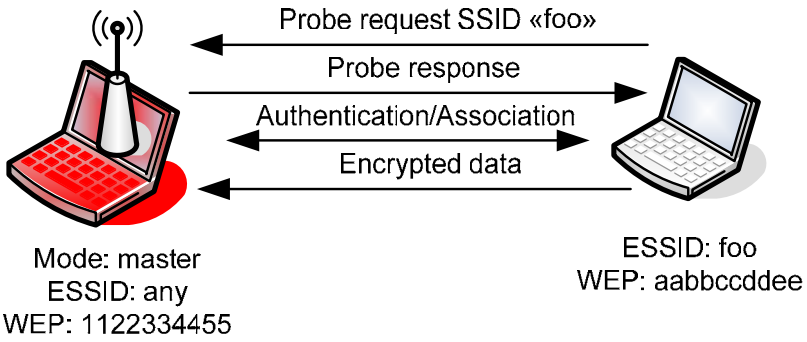

Рисунок 1. Подключение к ложной точке доступа

В некоторых публикациях, например (http://www.securitylab.ru/analytics/262596.php) приводится описание атак с ложной точкой доступа, при которых для восстановления ключа используется трафик, генерируемый клиентом. Однако автору описанные атаки представляются скорее теоретическими, чем пригодными для практического применения.

Большинство современных реализаций стека TCP/IP генерируют некоторый объем сетевого трафика при подключении к сети. Примером могут служить сообщения протоколов DHCP, NetBIOS, IPv6 NDP и так далее. Однако количество передаваемых в этом случае пакетов (как правило, до нескольких десятков) недостаточно для проведения KoreK-атак, требующих десятки тысяч пакетов с различными векторами инициализации (IV).

Стандартный подход, заключающийся в передаче перехваченных ранее широковещательных пакетов, в рассматриваем случае также бесполезен. Поскольку точка доступа контролируется злоумышленником, все ретранслированные ею пакеты будут использовать ключ WEP, не представляющий интереса для злоумышленника.

Таким образом, для взлома WEP необходимо спровоцировать подключившегося клиента на передачу достаточного количества пакетов с различными значениями векторов инициализации. Решить эту задачу можно путем передачи клиенту сообщений, требующих ответа (ARP, ICMP-Echo, IPv6 NDP). Но сделать это необходимо без знания ключа WEP.

Атаки с фрагментацией

Существует достаточно много методов формирования пакетов WEP без знания ключа шифрования. Наиболее эффективным является использование фрагментации на канальном уровне 802.11 (http://tapir.cs.ucl.ac.uk/bittau-wep.pdf).

Суть этого метода заключается в эксплуатации атаки с известным открытым текстом. Используя предсказуемый формат заголовков LLC, существует возможность восстановить 8 байт гаммы (выхода алгоритма PRGA в RC4, далее PRGA). Для этого первые восемь из зашифрованных байт складываются по модулю два с константой, содержащей стандартное значение заголовков LLC (см. рисунок 2).

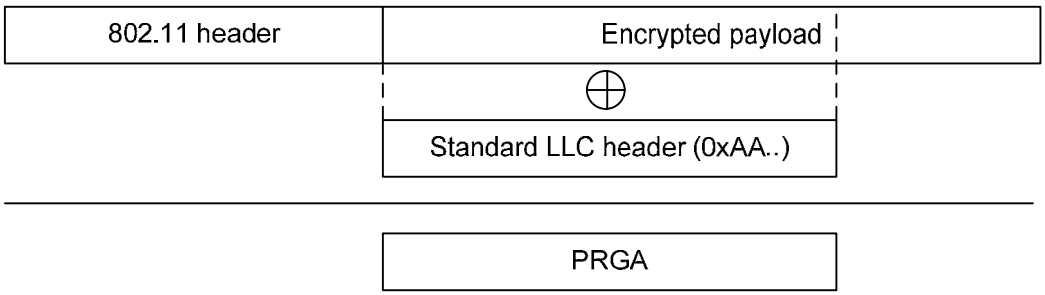

Рисунок 2. Восстановление отрезка гаммы

Как видно из рисунка 3, в заголовке LLC два последних байта могут меняться. Их значение определяет тип используемого протокола вышестоящего уровня. Возможные значения данных полей описаны в документах IANA (http://www.iana.org/assignments/ethernet-numbers).

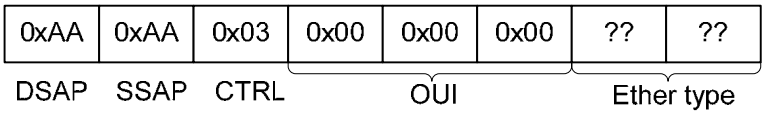

Рисунок 3. Стандартный заголовок LLC (802.2 snap)

В большинстве случаев беспроводные сети используются для передачи IP-трафика. Следовательно, поле Ether type может принимать одно из трех возможных значений:

- **0x0800** – при передаче IP пакетов;
- **0x0806** – для пакетов ARP;
- **0x86DD** – для пакетов IPv6.

Пакеты ARP легко отличить от других по их фиксированному размеру (28 байт данных). Использование протокола IPv6 достаточно просто идентифицируется по наличию широковещательных пакетов на MAC-адреса 33:33:xx:xx:xx:xx, используемых протоколом IPv6 NDP.

Полученные 8 байт гаммы могут быть использованы для передачи в сеть произвольных данных той же длины. Но с практической точки зрения это не представляет большого интереса, поскольку все 8 байт в передаваемом пакете будет занимать заголовок LLC. Чтобы обойти это ограничение, может использоваться функция фрагментации на канальном уровне. Беспроводные сети реализуют механизм, позволяющий передать один пакет вышестоящего уровня в нескольких (до 16) фрагментах 802.11. После перехвата одного из пакетов клиента и восстановления PRGA, отправляемый пакет разделяется на несколько фрагментов, содержащих по 4 байта данных (см. рисунок 4).

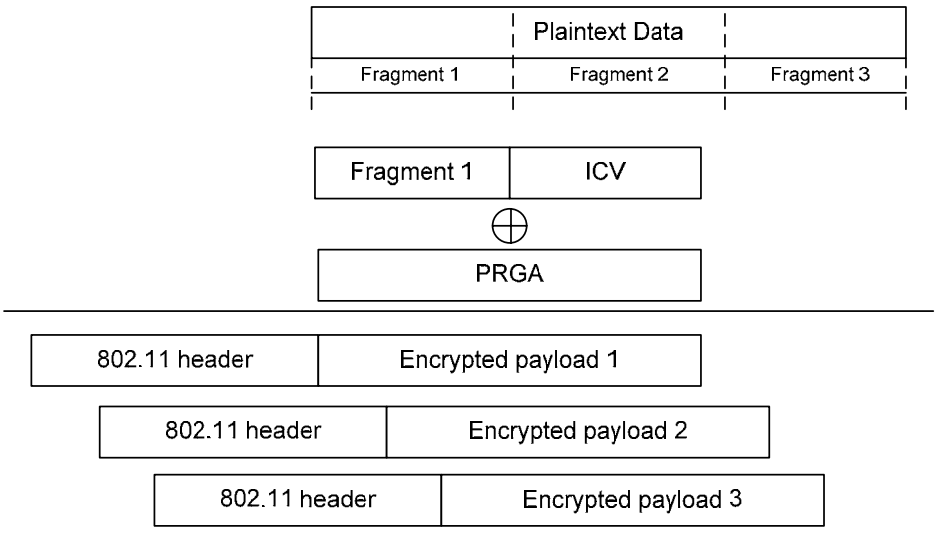

Рисунок 4. Передача фрагментированных фреймов

Каждый их них передается как отдельный фрейм с использованием функции фрагментации 802.11. Пакеты дополняются контрольной суммой (WEP ICV) и зашифровываются с использованием отрезка восстановленной гаммы. Таким образом, без знания ключа WEP в сеть можно передать пакеты длиной до 64 байт.

На практике в сеть можно передать пакеты большего размера. Для этого используется IP-фрагментация, а также структура некоторых служебных пакетов. Например, при перехвате пакета ARP пакета можно восстановить не 8, а 24 байта гаммы (см. рисунок 5). Для этого используются крайне предсказуемые значения заголовков LLC, ARP, а также MAC-адрес отправителя, указанный в заголовках 802.11 в открытом виде.

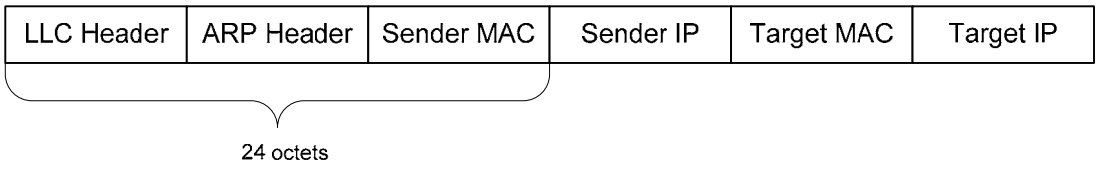

Рисунок 5. Пакет ARP

При использовании в сети IPv6, можно восстановить и больший отрезок гаммы. Например, при перехвате пакетов IPv6 NDP Neighbor Solicitation или Router Solicitation можно восстановить до 50 байт гаммы (заголовки LLC + заголовки IP + 2 байта заголовков ICMP). Это связанно с тем, что в заголовке IPv6 отсутствует поле контроля целостности. Кроме того, при использовании Local-Link адресации адрес IPv6 можно восстановить по MAC-адресу в заголовках 802.11 (см. http://www.securitylab.ru/contest/264659.php), если узлом не используется механизмы рандомизации адресов (http://www.ietf.org/rfc/rfc3041.txt). Отличить разные типы сообщений IPv6 можно по MAC-адресам получателей и размеру. Например, пакет, IPv6 Router Solicitation имеет длину 70 байт и передается на MAC-адрес 33:33:00:00:00:02.

С использованием 50 байт PRGA в сеть можно передать пакеты размером до 736 байт ((50-4)*16), что более чем достаточно для практических целей.

Генерация трафика

При использовании атаки с фрагментацией у злоумышленника, установившего ложную точку доступа, появляется возможность передать подключившейся станции зашифрованный пакет, которой будет гарантированно обработан получателем. Таким образом, остается только сформировать пакет, на который клиент ответит. Примером подобного пакета является ARP-запрос. Дополнительным плюсом является тот факт, что ARP-пакеты не блокируются персональными межсетевыми экранами.

Однако, для того, чтобы станция ответила на ARP-запрос, необходимо, чтобы поле *Target IP* содержало текущий IP-адрес интерфейса. Этой информацией злоумышленник не обладает, поскольку адрес передается в пакетах в зашифрованном виде.

Чтобы получить IP-адрес станции, можно воспользоваться ARP-сканированием, то есть отправкой ARP-запросов на различные адреса получателей, и ожиданием ответа на один из них. Если ответ был получен, значит, станция использует запрошенный IP-адрес (например, 169.254.5.9, см. рисунок 6).

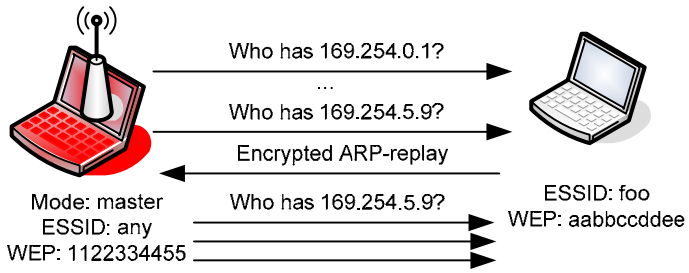

Рисунок 6. ARP сканирование

В качестве диапазонов для сканирования могут выбираться адреса из диапазона APIPA (169.254/32) или распространенные адреса RFC 1918 (например, 192.168.0/24). После того, как IP-адрес станции был определен, используется повторная передача ARP-запроса с целью получения необходимого для KoreK-атак количества пакетов с различными векторами инициализации. Для того, чтобы отличить ARP-запросы, отправленные на разные IP-адреса, могут использоваться различные MAC-адреса отправителя.

В случае поддержки станцией IPv6 ситуация упрощается. Поскольку большинство реализаций стека IPv6 отвечает на широковещательные (например, направленные на адрес ff02::01) ICMPv6-echo запросы, то злоумышленнику достаточно отправить подобный пакет в сеть.

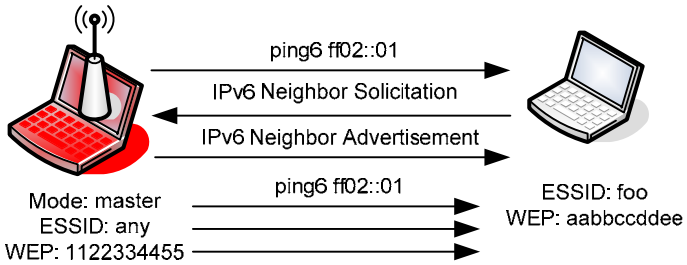

Рисунок 7. Использование IPv6

Также в IPv6 может применяться пакет IPv6 Neighbor Solicitation (аналог ARP-Request в IPv4). В этом случае осуществлять подбор IP-адреса нет необходимости, поскольку Local-Link IP-адрес может быть определен по MAC-адресу стации.

В ходе исследования использовались клиентах на основе следующих ОС:

- **Windows XP Service Pack 2**
- **Linux 2.6.x**
- **Windows Mobile 2003 SE**

Во всех трех случаях подход показал высокую эффективность работы. Особенно это относится к Linux и Windows Mobile, стеки TCP/IP которых поддерживают IPv6 «по умолчанию». Сводные данные по ОС приведены в таблице.

	Windows XP Service Pack 2	Linux 2.6.x	Windows Mobile 2003 SE
Поддержка APIPA	Да	Зависит от настройки	Да
Поддержка IPv6	Требует настройки	Встроенная	Встроенная
Ответ на ping6 ff02::1	Да	Да	Да
Поддержка RFC3041	Нет	Нет	Нет

Практическая реализация

Для демонстрации практической возможности описанной атаки была разработана утилита wep0ff (http://www.ptsecurity.ru/wepoff.asp). После запуска, программа ожидает пакетов от соединившихся клиентов. Из полученного пакета извлекается значение вектора инициализации и MAC-адреса станции, восстанавливается PRGA. Затем программа в течении полутора минут оправляет широковещательные ICMPv6-Echo запросы, после чего пытается провести ARP-сканирование сети для диапазона APIPA (169.254/32). Как показали эксперименты, сканирование всех адресов данного диапазона в режиме 802.11g only занимает мене двух минут.

Программа разрабатывалась для драйверов madwifi-old с поддержкой raw device. Для её использования необходимо предварительно настроить драйвер на поддержку данного типа устройств:

```
# iwpriv ath0 mode 3
# echo 1 > /proc/sys/dev/ath0/rawdev
# echo 1 > /proc/sys/dev/ath0/rawdev_type
# ifconfig ath0raw up
```

Программа вполне также работоспособна и на драйверах madwifi-ng. В этом случае необходимо создать два виртуальных адаптера: один для работы в режиме точки доступа, второй – в режиме мониторинга.

```
# wlanconfig ath0 create wlandev wifi0 wlanmode master
# wlanconfig ath1 create wlandev wifi0 wlanmode monitor
```

Затем интерфейс переводится в режим точки доступа. Для этого могут использоваться Karma Tools (для ответа на Probe Request с произвольным значением essid), либо стандартные функции драйвера:

```
# iwconfig ath0 mode master essid foo enc 1122334455 channel 1
```

В случае использования Karma tools необходимо вручную включать режим использования шифрования (значение ключа WEP – произвольное):

```
# iwconfig ath0 enc 1122334455
```


После этого необходимо запустить программу wep0ff и дождаться её перехода в режим **ipv6 flood** или **ARP flood**.

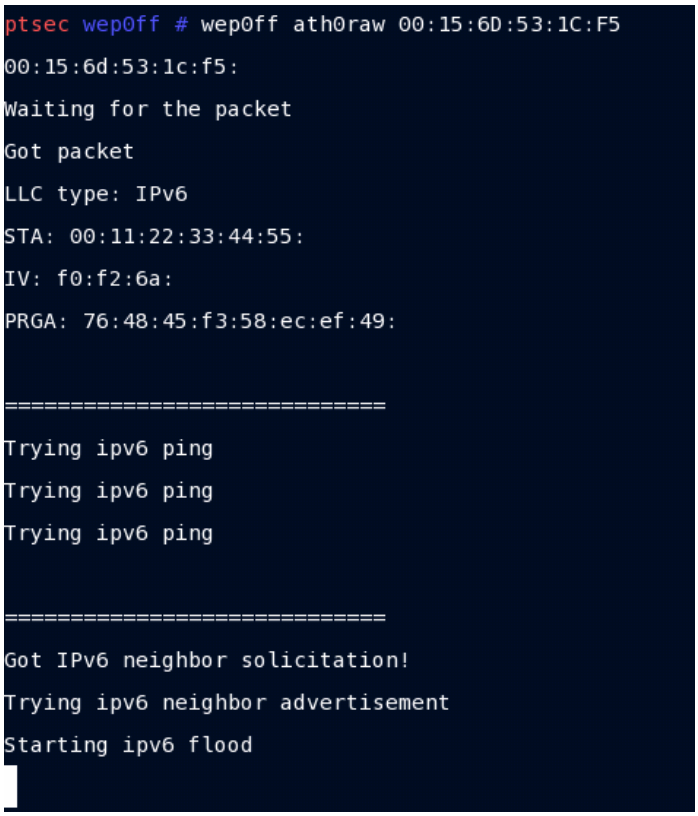

Рисунок 7. Программа wep0ff

После этого, используется любая программа сбора беспроводного трафика, например airodump-ng для накопления необходимого количества пакетов с различными векторами инициализации. После чего используется KoreK-атаки для восстановления ключа WEP.

Об авторе

Сергей Гордейчик работает системным архитектором компании Positive Technologies (www.ptsecurity.ru), где он специализируется в вопросах безопасность приложений, безопасности беспроводных и мобильных технологий. Автор также является ведущим разработчиком курсов «Безопасность беспроводных сетей», «Анализ и оценка защищенности Web-приложений» учебного центра «Информзащита» (www.itsecurity.ru). Опубликовал несколько десятков статей в “Windows IT Pro/RE”, SecurityLab (www.securityfocus.ru) и других изданиях. Является участником Web Application Security Consortium (WASC).

О компании Positive Technologies

Основное направление деятельности компании — защита компьютерных сетей от несанкционированного доступа. Говоря проще, мы помогаем нашим клиентам защититься от хакеров и других непрошенных виртуальных гостей.

Свою основную задачу мы решаем тремя путями:

- предоставляем услуги по аудиту и защите вычислительных сетей, серверов, рабочих станций;
- развиваем один из лучших в мире сканеров безопасности XSpider, который клиент может использовать самостоятельно для поиска и устранения уязвимостей;
- обеспечиваем информационную поддержку профессионалам на страницах принадлежащего нам ведущего российского портала по информационной безопасности securitylab.ru.

Являясь специализированной компанией, мы способны обеспечить самый высокий уровень сервиса в своей области. В то же время, имея богатый и успешный опыт работы в сфере информационных технологий, мы по желанию клиента готовы предоставить и более комплексные решения (начиная от проектирования архитектуры локальной сети, поставки оборудования и кончая поддержкой и сопровождением всей сетевой программно-аппаратной инфраструктуры).

