Проблемы безопасности беспроводных сетей стандартов 802.11a/b/g

**Константин Валерьевич Гавриленко, MSc, Директор.
Андрей Александрович Владимиров, PhD, CISSP, CCNP, CCDP, CWNA, TIA Linux+, Глава по безопасности. Архонт Ltd, Бристоль, Великобритания. http://www.arhont.com, info@arhont.com**

1. Введение

Беспроводные технологии передачи данных уже долгое время используются в современном мире ИТ. На протяжении многих лет, прерогативой применения таких типов сетей являлась передача данных на линках типа точка-точка между двумя зданиями/офисами или точка-многоточие в случаях подключения к беспроводным провайдерам Интернета. Высокая стоимость оборудования, используемые лицензионные частоты и невысокая скорость передачи данных являлись ограничивающими факторами, препятствующими широкому распространению такого типа сетей. Ситуация изменилась коренным образом, когда был разработан и принят стандарт 802.11b, а впоследствии, и 802.11a и g, увеличивающие теоретическую скорость передачи данных до 54Мбит/сек. Основным фактором, способствующим продвижению беспроводных сетей этого стандарта, явилась используемая нелицензионная частота и дешевизна оборудования. По некоторым оценкам, число выпускаемых аппаратных устройств с поддержкой стандарта 802.11 достигнет 80 миллионов штук в 2006 году, в то время как цены на них продолжают падать и наличие устройства для беспроводной связи становится де-факто в каждом современном компьютере, и не только. Столь широкое распространение технологии обычно привлекает внимание не только законных пользователей, но и различного рода лиц криминальной направленности. Мы рассмотрим причины, толкающие людей на покупку и настройку необходимого оборудования и заставляющие их выбираться из дому для того, чтобы совершить акт несанкционированного подключения к чужой сети, тем самым идя на нарушение закона.

2. Мотивация беспроводных кракеров

Существует по крайне мере три основные причины такого "иррационального" и "необъяснимого" поведения потенциальных взломщиков:

- *Совмещение приятного с полезным*

Беспроводное хакерство так или иначе связано и с копанием в программах (анализаторах протоколов, инструментах проникновения в чужие сети), и в различной аппаратуре (клиентские карты, шлюзы, антенны и усилители), и это более интересное времяпрепровождение, чем обычный проводной взлом. Более того, по сути марафон по городу с

лаптопом, собирая информацию по беспроводным сеткам, можно считать своего рода азартной игрой, спортом и полезной физической нагрузкой для ослабленного организма компьютерного хакера.

- *Анонимность доступа*

В настоящее время достаточно тяжело находится в Интернете, оставаясь действительно анонимным. Стандартная практика, используемая атакующими - пройтись через цепочку взломанных узлов до цели. Несмотря на кажущуюся сложность, потенциально возможно сопоставить и отследить всю цепочку соединений и выйти на след атакующего. В случае использования атакующим беспроводного канала связи чужой сети, он не оставляет следов и цепочка обрывается на владельце беспроводной сети, который и может ответить согласно всей строгости закона.

- *Бесплатный широкополосной доступ*

Многих прельщает большое количество мультимедийной и другой объёмной информации, находящееся на просторах Интернета. Отсутствие или дороговизна широкополосного доступа вынуждает искать обходные пути, и корпоративные сети с присутствующими точками беспроводного доступа служат первоочередными целями у хакеров, ищущих широкополосной доступ.

3. Классификация беспроводных кракеров.

В свою очередь, иметь представление о людях, которые способны атаковать вашу сеть, не менее важно, чем знать то, чем они руководствуются. Зная их основные мотивы, можно распределить атакующих на три основные категории:

- *"Любопытствующие"*

Преследуют обычно единственную цель - обнаружить как можно большее количество беспроводных сеток. Обычно они не преследуют деструктивных целей и занимаются этим ради забавы и самоутверждения. Этот тип атакующих не представляет серьёзной угрозы и может быть остановлен простой фильтрацией MAC адресов, закрытыми ESSID и WEPом.

- *"Пираты"*

К данной категории мы относим в первую очередь преследующих цель использовать чужие каналы связи для скачивания или распространения пиратской продукции, порнографии или рассылок СПАМа. Установка простейшего шифрования WEP позволит обезопасить сеть от большинства атакующих такого рода, но не следует быть слишком самонадеянным.

- *"Профессионалы"*

Имея хорошие знания и навыки, это самый серьёзно настроенный тип атакующих. Имея перед собой чётко поставленную задачу, они прекрасно знают что нужно для её реализации. Стандартные методы

защиты способны остановить такого рода нападающего всего на пару часов. Скрытность, фланговые атаки и доступ через чёрный ход – это то, что их привлекает в атаках на беспроводные сети.

4. Методы беспроводных атак

Далее мы рассмотрим основной инструментарий, используемый атакующими. Не секрет, что преобладающая часть серьёзных кракеров будет использовать одну из открытых операционных систем, скорее всего Линукс. Для этого есть много веских причин, среди которых можно выделить драйвера, поддерживающие режим мониторинга, возможность посылки произвольных фреймов и, главное, - бесплатность и открытый код, позволяющий кракерам адаптировать драйвера и утилиты под свои нужды. Кроме того, большинство атакующих не будет тратить свои кровно заработанные средства на покупку последней версии анализатора сетевого трафика за 15'000 у.е., а пиратские копии узкоспецифических продуктов подобного рода далеко не всегда существуют. В придачу, большинство из коммерческих продуктов просто не могут предоставить разнообразие функций, необходимых для взлома беспроводных сетей, таких как введение модифицированных фреймов в WEP-защищённую сеть без знания WEP пароля.

4.1. Обнаружение беспроводных сетей

Существует два метода обнаружения беспроводных сетей: активное и пассивное. Активное сканирование подразумевает под собой отправку пробного фрейма с запросом и ожидание ответа на него. Из полученного пакета извлекается ESSID сети, канал, индикатор шифрования и поддерживаемая скорость. Одна из наиболее известных программ, реализующих активное обнаружение сетей и работающая под ОС Windows – Netstumbler. Такой вид сканирования не очень эффективен. Так называемые закрытые сети не будут отвечать на пробные запросы и, соответственно, не будут обнаружены данным типом сканирования. Вы также ограничены мощностью передатчика карточки, и сможете обнаружить только сети которых достигнет ваш пробный пакет, таким образом вы можете находится прямо в центре точка-точка соединения, но сигнал с вашей карточки не будет достигать точек доступа; соответственно такая сеть также не будет обнаружена.

Гораздо эффективней использовать пассивный режим обнаружения сетей при помощи режима мониторинга в сочетании с перебором всех DSSS-каналов. Это позволяет обнаруживать беспроводные сети путём перехвата и анализа проходящего трафика, в том числе всех управляющих и административных фреймов. Единственным фактором, ограничивающим возможность обнаружения сети, в этом случае

становится приемная чувствительность карты. Мы можем её "улучшить" за счёт применения антенн с большим коэффициентом усиления и использования двунаправленных усилителей, а также одновременного применения двух и более беспроводных карт для покрытия большего спектра одновременно. Одной из наиболее полнофункциональных программ в данной категории является Kismet. Она особенно интересна в связке с GPSDrive, с помощью которой вы можете без труда собрать координаты найденных сетей и нанести их на карту.

Исходя из нашего достаточно богатого опыта "боевых выездов", только 30-40% всех беспроводных сетей имеют минимальный уровень защиты – один из типов WEP. Остальные 60-70% абсолютно открыты, и не надо прилагать больших усилий для того, чтобы перехватить транслируемую информацию или подключиться к точке доступа. Но что возможно сделать с "защищёнными" сетями? WEP – не помеха. Даже самые последние имплиментации WEP'а можно вскрыть за достаточно небольшой промежуток времени. В нашей тестовой лаборатории, используя модифицированную программу Aircrack, мы смогли получить ключ менее чем за 5 минут анализа проходящего трафика.

4.2. Атаки на WEP - прошлое, настоящее и будущее.

Учитывая тот факт, что большинство беспроводных сетей до сих пор используют WEP для защиты передаваемой информации, то следует более подробно остановится на методах, используемых кракерами для взлома ключей WEP. Мы можем условно разделить атаки на три категории:

- атака методом полного перебора (опционально с оптимизацией) является действительно эффективной только при условии того, что длинна ключа была установлена как 40-бит. Даже при таком небольшом ключе у атакующего, использующего старенький Пентиум III, займет около 50 дней для того, чтобы перебрать все возможные комбинации. Зато вам понадобится перехватить только один зашифрованный пакет данных для дешифровки. Существует оптимизированный вариант атаки перебором, предложенный Тимом Ньюшемом, который использует слабости алгоритма генерации WEP и при благоприятном стечении обстоятельств (перехваченный файл дампа должен быть порядка 24Гб), взлом возможен всего за полминуты. Собрать 24 Гб дамп файл достаточно тяжело и долго, да и сама атака работает только против первых версий алгоритма. Так что её практическое применение очень ограничено. Более практичной является атака на один пойманный пакет перебором по словарю с помощью утилиты WepAttack.
- атака FMS и её улучшенный вариант до сих пор являются самой распространенной атакой на WEP и использует оригинальный метод взлома предложенный Скоттом Флурером, Итцик Мартином и Ади

Шамиром в 2001 году. В основе атаки лежат три основных принципа:
а) при некоторых векторах инициализации шифр RC4 оказывается таким, что информация о ключе проявляется в выходных байтах.
б)слабость, выражающаяся в инвариатности, позволяет использовать выходные байты для определения наиболее вероятных байтов ключа.
в)первые выходные байты всегда предсказуемы, поскольку содержат заголовок SNAP, определенный в спецификации IEEE.

Учитывая специфику генерации и длину ключа, атакующему надо будет проанализировать от 6 до 8 миллионов пакетов, чтобы получить значение ключа. При полной загруженности сетки 802.11b понадобится как минимум два часа для сбора необходимого количества пакетов. Существует улучшенная версия данной атаки (см. исходный код dwepcrack из bsd-airtools), которая использует модифицированный алгоритм поиска "слабых" пакетов и позволяет сократить время для получения и необходимое количества пакетов до полумиллиона, что существенно облегчает жизнь атакующему. Стоит заметить, что практически все основные производители беспроводного оборудования слегка модифицировали алгоритм генерации, дабы избежать выхода "слабых" пакетов наружу и предотвратить данную атаку.

Атаки Корека (так как существует несколько разновидностей этих атак), являются последними наиболее эффективными атаками на WEP. Эти статистические атаки, основанные на "обрезании" зашифрованного пакета байт за байтом, используют не "слабые", а уникальные вектора инициализации, что позволяет снизить количество необходимых для взлома пойманных пакетов до минимума и сократить время взлома ключа до получаса или менее. В настоящее время атаки Корека поддерживаются такими утилитами взлома, как AirCrack, WepLab и последние версии AirSnort. Так как дешифровка единственного пакета с помощью атак Корека выполняется быстро и без особых проблем, реиньекция ARP пакетов в уязвимую сеть для инициирования ответов, включающих в себя уникальные вектора инициализации, становится практичным способом дополнительно сократить время взлома WEP ключа или взломать ключ на сети с очень низкой активностью. Именно эту методологию и использует AirCrack, написанный Кристофером Девайн. Безусловно, помимо ARP для иньекции могут быть использованы другие протоколы, такие как DHCP.

До появления атак Корека, единственной утилитой для иньекции трафика в зашифрованную WEPом сеть был WEPWedgie Антона Рэйджера, использующий генерацию части потока RC4 через перехват и XOR зашифрованной и незашифрованной переменной, передаваемой при аутентикации клиента с использованием распределенного WEP

ключа. Так как этот способ аутентикации не очень распространен в реальном мире, его никак нельзя назвать практичным. Тем не менее, WEPWedgie или, скорее, предложенная методология его использования, освещает ещё одну важную возможность использования иньекции трафика в сети, защищенные WEPом - энумерацию этих сетей (включая сканирование портов) при наличии узла со сниффером на удаленной сети, на который можно перенаправлять ответы на пакеты, введенные в сеть хакером, владеющим частью потока используемого RC4. Перенаправление пакетов осуществляется через подстановку IP адреса удаленного узла в качестве исходного адреса вводимого пакета. Изначально, WEPWedgie был настроен на сканирование Cisco PIX экрана, установленного между точкой беспроводного доступа и проводной локальной сетью. В нашей книге ("Wi-Фу:"боевые" приемы взлома и защиты беспроводных сетей") описывается модификация WEPWedgie для сканирования клиентских устройств на беспроводной сети вместо Cisco PIX.

Одно из нововведений для защиты передаваемого трафика в сетях, ограниченных использованием WEP, - это автоматическая ротация ключей используя протокол 802.1x. Не важно, какой из расширяемых протоколов аутентикации (EAP) используется, в любом случае для каждого беспроводного клиента используется отдельный ключ, а для широковещательных адресов - общий ключ на всю сеть. Единственная сложность заключается в разделении трафика с такой сети для каждого отдельного клиента до момента смены ключа. Выбранный трафик можно пропустить через стандартные дешифраторы и получить используемый ключ. Момент смены ключа достаточно просто отследить проанализировав файл дамп. На данный момент не существует автоматических программ для дешифрации данных с такого рода сетей и большинство работы приходится делать вручную, что впрочем не делает их более защищёнными от прослушивания. Что интересно, разделение ключей на клиентские и широковещательные в данной системе приводит к наличию дополнительной уязвимости. Тип и характер используемого протокола групповой передачи можно легко определить по используемому MAC адресу, транслируемому в IP адрес класса Д. Дополнительно, атакующий может замерить время регулярной посылки пакетов протокола и сопоставить его со дефалтным временем, описаны(например 30 секунд у IP RIPv1/2). Знание содержания неизменяемых полей такого протокола дает значительное количество пар зашифрованный/незашифрованный текст, позволяющее "отXORить" длинные участки потока RC4 и использовать их для инъекции пакетов обнаруженных протоколов групповой передачи, таких как протоколы маршрутизации, STP или протоколы управления виртуальными локальными сетями. С помощью этой инъекции, хакер способен

перенаправить трафик с локальной беспроводной сети наружу, к узлу, находящемуся под его контролем. Кроме того, подобный несанкционированный ввод пакетов дает неограниченные возможности проведения атак по отказу в обслуживании на всю сеть.

4.3. Уязвимости стандарта беспроводной безопасности 802.11i

Данный стандарт зиждется на двух китах. Первый - уже упомянутый протокол контроля доступа на базе портов 802.1x с надстройками в виде EAP. Использование 802.1x/EAP в основанных на 802.11i протоколах сертификатов беспроводной безопасности WPAv1 и WPAv2 принципиально не отличается. Главное отличие между WPAv1 и WPAv2 - использование принципиально различных систем симметричного шифрования (TKIP в WPAv1, CCMP в WPAv2) и хэширования (MIC в WPAv1, CBC-MAC в WPAv2).

4.3.1 Атаки, не связанные с уязвимостями 802.1x/EAP

В настоящее время WPAv2 является новоиспеченным стандартом, и атаки на WPAv2, не связанные с уязвимостями 802.1x/EAP, остаются теоретическими. Впридачу, пока они сводятся всего лишь к DoS, например путем истощения ресурсов беспроводного шлюза с поддержкой WPAv2 при помощи создания множества процессов аутентикации с использованием произвольных MAC адресов несуществующих клиентов. Еще один вектор DoS атаки против WPAv2 - инъекция подделанного первого пакета четырехпакетного обмена при установлении ассоциации точка доступа - клиент с использованием WPAv2. Эта атака возможна потому, что данный пакет не использует хэширования для проверки целостности пакета во избежания потенциальных атак повтора пакета если используется общий статический ключ CCMP. Так как известных практических имплементаций и доказательств эффективности этих атак пока не существует, мы не будем заниматься их подробным рассмотрением в этом докладе.

WPAv1 является временным решением при переходе от WEP к WPAv2, не требующим модернизации аппаратной части. Помимо теоретических, не связанных с 802.1x, атак против WPAv1, таких как атака на хэш временного ключа (снижающая сложность извлечения ключа с 2^128 до 2^105) и DoS атак искажения контрольной суммы MIC (реализация которых намного сложнее, чем кажется на первый взгляд), существуют и прикладные атаки против WPAv1-SOHO, использующего предварительно разделенный ключ, общий для всех узлов с одним ESSID в большинстве реализаций WPAv1-SOHO. Первая атака представляет из себя генерацию временных ключей других клиентских узлов, если известен постоянный общий ключ (PSK). Таким образом,

практически эта атака представляет ценность для легитимного пользователя сети, который желает прослушивать и манипулировать трафиком других легитимных пользователей (вариант сотрудника, атакующего соединение своего руководителя). Несмотря на то, что каждый узел на сети, защищённой WPAv1-SOHO, имеет свой зашифрованный канал соединения с точкой доступа, временные ключи для защиты этого канала генерируются с помощью PSK, двух случайных величин из двух первых пакетов четырехстороннего квитирования WPAv1-SOHO и MAC адресов участвующих узлов. Таким образом, атакующий, уже обладающий PSK, может легко перехватить MAC адреса вовлеченных узлов, и инициировать процедуру квитирования с помощью DoS атаки фреймами деассоциации для перехвата первых двух пакетов обмена с нужными величинами. Имея эти данные под рукой, несложно сгенерировать временный ключ для атакуемого канала.

Если же атакующий не знает PSK (стандартный кракер снаружи), он может воспользоваться атакой перебора по словарю или даже случайного перебора против временного ключа, а затем, имея величины, упомянутые выше, сгенерировать PSK из угаданного временного ключа, осуществив действия первой описанной атаки в обратном порядке. Вы можете ознакомиться с данной атакой в деталях, прочитав статью её первооткрывателя, Роберта Московица, на сайте http://wifinetnews.com/archives/002452.html. А её программными реализациями являются такие утилиты, как coWPArty (автор Joshua Wright) и WPA Cracker.

4.3.2. Атаки против 802.1x/EAP.

Данные атаки можно подразделить на атаки против 802.1x вне зависимости от используемого типа EAP, и атаки против отдельных EAP разновидностей. К первым относится посылка фальшивых EAP-Failure и EAPOL-logoff (EAP через локальную сеть) фреймов, затопление фреймами EAPOL-Start и циклическим перебором идентификаторов EAP, а также преждевременной отправкой фреймов EAP-Success. Так как принцип работы подобных атак понятен, и мы не особенно заинтересованы в DoS атаках (хотя они могут иметь большое значение в проведении атак "человек в середине", всегда есть старые добрые фреймы деаутентикации), мы не будем акцентироваться на них и перейдем к атакам на специфические типы EAP.

Самый первый стандартизированный тип EAP - это EAP-MD5, который использует схему аутентикации, аналогичную аутентикации CHAP. Сейчас EAP-MD5 практически вышел из употребления и может быть встречен в основном в случае режима подстраховки, когда по какой-то причине более совершенные типы EAP не работают. Основной

уязвимостью EAP-MD5 является отсутствие какой-либо аутентификации с "серверной" стороны, сопряженное с отсутствием туннелирования трафика этого протокола. Таким образом, кракер может представить свою "пиратскую" точку доступа с большей силой сигнала и сопряженным RADIUS сервером, и "переманив" клиентские машины на ее сторону после массовой DoS атаки фреймами деаутентификации перехватить имена и пароли пользователей. На практике эта атака легко реализуема с помощью фальшивой аппликационной точки доступа на основе Линукс драйверов HostAP (собственно точка доступа или аутентификатор) и поднятого демона hostapd с его минималистическим сервером аутентикации, авторизующим любые хосты, способные послать фрейм с корректным ответом EAP. Помимо перехвата паролей, атакующий с помощью данного метода может пытаться взломать подсоединившиеся хосты напрямую.

Cisco EAP-LEAP, один из широко распространенных типов EAP использует MS-CHAPv2 для аутентикации пользователей, на чём и базируется атака против него. Перехватив обмен запросами между клиентом и точкой доступа, можно использовать оптимизированную атаку перебора по словарю с помощью Asleap-imp, leap или THC-LEAPcracker'a для того, чтобы извлечь пароль. Оптимизация атаки против этого частного протокола возможна потому, что
- имя пользователя незашифровано, защищен только пароль
- третий из используемых для этого DES ключей дефектен и позволяет вычислить два последних байта MD4 хэша пароля пользователя
- сам хэш пароля пользователя не имеет начального значения, и поэтому позволяет атаки по типу радужных таблиц (Rainbow tables). Подобные атаки на MD4 хэши длиной всего 6 байт (см. предыдущий пункт!) отличаются значительной скоростью, позволяющей использовать радужные таблицы больших размеров. В настоящее время Cisco рекомендует использовать более новый и безопасный EAP-FAST вместо EAP-LEAP.

Что же касается считающихся безопасными EAP-PEAP и EAP-TTLS, использующих туннелирование обмена данными аутентификации, они не так хорошо защищены, как кажется. Старая проблема EAP-MD5, а именно отсутствие аутентификации с "серверной" стороны всплывает здесь с новой силой. По крайней мере, сети использующие EAP-TTLS+PAP и EAP-PEAP+MS-CHAPv2 для аутентификации, являются уязвимыми к атакам, основанным на установлении кракером "пиратской" точки доступа, сопряженной с фальшивым RADIUS сервером. Отметим, что EAP-TTLS+PAP является конфигурацией по умолчанию на Windows XP ОС при использовании EAP-TTLS. Сборка PAP логинов происходит после массовой DoS атаки, использующей

фреймы деаутентиакции или EAP DoS методы, упомянутые в начале этой секции. Взлом EAP-PEAP+MS-CHAPv2 менее эффективен и требует множественных DoS атак. Первая волна DoS необходима для добывания имен домэйна и пользователя с помощью связки фальшивая точка доступа/фальшивый RADIUS сервер. Эти имена используются для создания локального файла с паролями для перебора на системе атакующего. Следующие волны DoS сбрасывают пользователя с фальшивой точки доступа и заставляют его повторять аутентикацию к системе атакующего, пока пароль пользователя не совпадет с паролем в созданном кракером файле. Интересным вектором этой атаки было-бы использование ее в сочетании с описанной ранее атакой на MS-CHAPv2 в структуре EAP-LEAP, и исследование этого вектора находится на нашем TODO листе.

5. Заключение.

На настоящий момент, относительно безопасными можно считать только сети стандарта 802.11, защищенные с помощью WPAv1 с 802.1x и WPAv2 с 802.1x при условии использования типов EAP с поддержкой туннелирования и взаимной аутентикацией обоих концов туннеля. К таким типам EAP относятся EAP-TLS и EAP-FAST. При этом, EAP-TLS требует наличия сертификатов аутентификации на всех клиентских хостах, что делает установку и менеджмент массивных сетей, защищенных с использованием этого протокола, весьма трудоемкой. В то же время, EAP-FAST поддерживается по преимуществу аппаратным обеспечением Cisco и требует покупки дополнительного программного обеспечения (суппликанты Funk или Meetinghouse) для поддержки систем, иных чем Windows XP, Windows 2000 и Windows CE. Таким образом, дизайн защищенных сетей стандарта 802.11 является более сложной задачей, чем представляют себе многие архитекторы и администраторы таких сетей, даже при рассмотрении исключительно протоколов 802.11i и без касания альтернатив, таких как IPSec.

6. Ссылки

1. The Radical Realm of RADIUS, 802.1x, and You. 2005. Rodney Thayer, Beetle, Shmoo Group, LayerOne.
2. 1 Message Attack on the 4-Way Handshake. 2004. ChangHua He, John C. Mitchell. Stanford University.
3. Attacks against Michael and Their Countermeasures. 2003. Dan Harkins. Trapeze Networks.
4. Weakness in a Temporal Key Hash of WPA. 2004. Vebjorn Moen at al., Bergen University.

5. Fast and Secure Roaming in WLAN. 2004. Magnus Falk, Linkoping University.
6. "Wi-Фу:"боевые"приемы взлома и защиты беспроводных сетей", 2005. Владимиров, А. А., Гавриленко, К. В., Михайловский, А. А.