Безопасность беспроводного периметра сети

Вячеслав Фадюшин, *старший консультант центра информационной безопасности компании "Инфосистемы Джет"*

Сегодня деятельность многих бизнес-подразделений зависит от доступности сетевых информационных ресурсов. Все большее число компаний не могут просто отказаться от использования технологий беспроводного доступа, несмотря на связанные с ними дополнительные ИБ угрозы. Мы рассмотрим основной вопрос безопасности беспроводных сетей — возможность осуществления доступа к внутренним информационным ресурсам ЛВС компании через ее беспроводной периметр.

Ни для кого не секрет, что в настоящее время беспроводные сети не просто становятся все более популярными в корпоративной среде – они приобретают во многих компаниях статус инфраструктуры, поддерживающей целые бизнес-процессы.

Механизмы защиты

Прослушивание беспроводных коммуникаций не требует от атакующего серьезных усилий для физического включения между клиентом и беспроводным сетевым устройством, через которое осуществляется подключение к корпоративной сети. Несмотря на то что данные, передаваемые в процессе взаимодействия Wi-Fi-устройств, защищены с применением криптографии, атакующий легко может перехватить всю информацию об участниках взаимодействия, необходимую и достаточную для осуществления атаки. Единственным существенным препятствием в данном случае можно считать силу сигналов. Она зависит от физического расстояния между беспроводными интерфейсами атакующего и атакуемых.

В настоящее время в беспроводных сетях используется три механизма защиты: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) и WPA2. В свою очередь, WPA и WPA2 могут использоваться с общим закрытым ключом Pre-Shared Key (WPA-PSK) и с аутентификацией 802.1X.

Благодаря нескольким опубликованным уязвимостям архитектуры WEP получение атакующим ключа для подключения к беспроводной сети – лишь вопрос сбора определенного количества пакетов и их анализа. Поэтому WEP в 2004 г. был признан устаревшим и встречается все реже не только в корпоративных, но и в домашних беспроводных сетях.

WPA и WPA2: в чем различие?

Среди специалистов информационной безопасности существует распространенное мнение о том, что WPA и WPA2 практически не различаются по надежности защиты и неважно, какой из этих двух механизмов лучше подходит для защиты сети. Скорее всего, именно это мнение и является причиной до сих пор очень часто встречающегося использования механизма WPA в практике оценки защищенности беспроводных сетей. Действительно, при атаках на соединения WPA и WPA2 используются одинаковые алгоритмы, отличающиеся лишь в деталях на разных стадиях выполнения. При этом WPA имеет несколько архитектурных уязвимостей, существенно снижающих его надежность по сравнению с WPA2 и позволяющих выполнять некоторые типы атак, результат которых не зависит от длины и сложности используемого общего ключа PSK.

WPA2 на сегодня имеет лишь одну опубликованную архитектурную уязвимость, обнаруженную сравнительно недавно (была описана летом 2010 г.), – Hole 196. Данную уязвимость называют инсайдерской, так как для ее использования атакующий и жертва должны быть аутентифицированы в одной беспроводной сети, следовательно, Hole 196 не может быть использована для подключения к сети.

Отталкиваясь от вышесказанного, надежным, с точки зрения ИБ, механизмом для подключения к беспроводной сети является WPA2, который, как уже было сказано, может быть использован с общим закрытым ключом и с аутентификацией 802.1X.

Перебор по словарю

Надежность защиты от несанкционированного подключения в варианте с общим закрытым ключом (WPA2-PSK) прямо пропорциональна сложности и длине выбранного ключа и имени сети (SSID). Для подключения к сети, использующей WPA2-PSK, атакующему в общем случае требуется дождаться момента подключения клиента к беспроводной сети и перехватить данные аутентификации, а именно так называемое рукопожатие (handshake), содержащее результат необратимого криптографического преобразования SSID и PSK. Далее остается только произвести атаку перебора по словарю и, если PSK найдется в словаре атакующего, использовать его для проникновения в беспроводную сеть.

Почему на практике речь идет лишь о переборе по словарю? Во-первых, из-за используемых в WPA2 алгоритмов криптографического преобразования атака полным перебором займет огромное количество машинного времени, при использовании для создания PSK большого алфавита и при ограничении длины PSK не менее 10 символов. Время, необходимое атакующему для полного перебора "надежного" PSK, значительно превышает количество времени, которым он располагает для атаки, что делает ее нецелесообразной.

Во-вторых, так как при подключении используется хэш не только PSK, но PSK и SSID, возникают и сложности с использованием предварительно сгенерированных таблиц хэшей (rainbow tables). Таблицы должны быть составлены для двух множеств исходных строк, что экспоненциально увеличивает объем занимаемого ими дискового пространства, а генерация новых таблиц для каждого нового SSID сводится к атакам полным перебором по алфавиту. При этом использо-

вание таблиц для "вскрытия" ключа WPA2-PSK не становится полностью невозможным, но обычно ограничивается набором из 1000 наиболее распространенных SSID.

Платные сервисы

В настоящее время в сети Интернет существуют платные сервисы, использующие собственные гибридные словари (содержащие не только словарные слова, но и ряд модификаций каждого слова с добавлением и/или изменением некоторых символов) большого объема и сервисы облачных вычислений для осуществления подбора ключа. Время подбора по словарю зависит от загруженности сервиса (количества "рукопожатий" в очереди) и обычно занимает не более 4 часов. Цена подбора одного ключа составляет от $10. Подобные сервисы используют словари, содержащие в общей сложности не менее 250 млн слов, а объем словарей некоторых сервисов приближается к 1 млрд слов и их комбинаций. В индивидуальном порядке с использованием облачных сервисов можно произвести атаку полным перебором по алфавиту, длительность и цена которой прямо пропорциональны объему используемого алфавита.

Атаки на WPA-Enterprise

Использование WPA-Enterprise повышает защищенность беспроводного периметра сети от несанкционированного подключения благодаря своей архитектуре, но вопреки часто встречающемуся заблуждению механизм WPA-Enterprise также подвержен ряду атак. Общий смысл этих атак заключается в создании фиктивной копии точки доступа и сервера аутентификации, ожидании подключения клиента и сохранении его аутентификационных данных с последующим использованием их для проникновения в сеть. Данный тип атак значительно сложнее в подготовке и исполнении, чем атаки на WPA2-PSK, но при удачном выполнении предоставляет атакующему гораздо большие возможности по атаке на внутренние информационные ресурсы сети. Этому способствует еще и то обстоятельство, что аутентификация пользователей беспроводной сети часто является доменной аутентификацией и, получив учетные данные пользователя беспроводной сети, злоумышленник получает доступ к домену с этими учетными данными.

Частично проблему решает использование беспроводной системы обнаружения вторжений (Wireless intrusion detection system – WIDS), способной отслеживать появление незарегистрированных точек беспроводного доступа, распространенных типов беспроводных атак и других аномалий беспроводного эфира.

Снижаем риски

Перечислим рекомендуемые меры по снижению рисков проникновения в корпоративную сеть через ее беспроводной периметр:

- использование уникального SSID;

Сила сигналов зависит от физического расстояния между беспроводными интерфейсами атакующего и атакуемых.

- использование сложных ключей длиной не менее 10 символов (в идеале – случайный набор символов, включающий заглавные и прописные буквы, цифры и знаки препинания и исключающий клавиатурные последовательности);
- регулярная смена ключей;
- по возможности использование WPA-Enterprise в комплексе с WIDS и процессами мониторинга событий ИБ и реагирования на инциденты ИБ;
- проведение периодических тестов на проникновение.

Надо сказать, что все существующие на данный момент технологии защиты беспроводных сетей подвержены своим типам сетевых атак. По нашему опыту, для эффективного снижения риска проникновения в корпоративную сеть через беспроводной периметр недостаточно использовать только технические механизмы защиты. Важно организовать поддерживающие их процессы мониторинга событий ИБ и реагирования на инциденты ИБ. Это станет частью комплексной системы управления информационной безопасностью компании. ●

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru