АВТОР: ВЛАДИМИР ЛЕПИХИН

ЗАЩИТА беспроводных сетей СЕГОДНЯ И ЗАВТРА

ПРАКТИЧЕСКИ С МОМЕНТА ПОЯВЛЕНИЯ БЕСПРОВОДНЫХ СЕТЕЙ БЫЛИ ОЧЕВИДНЫ УГРОЗЫ, СВЯЗАННЫЕ С ИХ ИСПОЛЬЗОВАНИЕМ: ОТНОСИТЕЛЬНАЯ ЛЕГКОСТЬ ПОДКЛЮЧЕНИЯ И ВОЗМОЖНОСТЬ ПРОСЛУШИВАНИЯ ТРАФИКА. ЗА КОРОТКИЙ ПЕРИОД РАЗВИТИЯ БЕСПРОВОДНЫХ СЕТЕЙ СМЕНИЛОСЬ НЕСКОЛЬКО ПОКОЛЕНИЙ МЕТОДОВ ЗАЩИТЫ, НАЧИНАЯ ОТ ОБЩИХ РЕКОМЕНДАЦИЙ СТАНДАРТА 802.11 ДО ТЕХ, ЧТО ОПИСАНЫ В ИЗВЕСТНОМ СТАНДАРТЕ 802.11I, ЦЕЛИКОМ ПОСВЯЩЕННОМ ВОПРОСАМ БЕЗОПАСНОСТИ. ЧТО ЖЕ ТРЕБУЕТСЯ УЧИТЫВАТЬ ПРИ ЗАЩИТЕ БЕСПРОВОДНОЙ СЕТИ СЕГОДНЯ И КАКИЕ ВОЗМОЖНОСТИ ЕСТЬ ДЛЯ ЭТОГО?

АВТОР: ВЛАДИМИР ЛЕПИХИН

Построение полностью «беспроводного» офиса сегодня — скорее исключение, чем правило, поэтому беспроводные сети сейчас являются дополнением «проводных». В зависимости от цели, поставленной при развертывании беспроводной сети, обычно различают корпоративный и гостевой доступ. Соответственно, и требования по защите формулируются отдельно, причем часто это оговаривается уже в политике безопасности. Следовательно, если это возможно, необходимо уже на этапе развертывания беспроводной сети «отделить» корпоративный и гостевой доступ друг от друга.

Далее речь пойдет о защите корпоративного доступа.

Порядок защиты корпоративного беспроводного доступа на сегодняшний день довольно очевиден и включает три основных пункта:

1. Внедрение защитных мер с учетом рекомендаций стандарта 802.11i.
2. Построение инфраструктуры мониторинга событий безопасности с учетом специфики беспроводной сети.
3. Дополнительная защита на уровне пользователя.

Внедрение защитных мер

Что касается первого пункта, то сегодня построение сетей, полностью удовлетворяющих требованиям стандарта 802.11i, уже не кажется непосильной задачей. Организации, использующие беспроводные технологии, постепенно уходят от WEP к WPA/WPA2, а препятствия, создаваемые необходимостью поддержки устаревших клиентов, и проблемы совместимости постепенно смещаются на задний план.

Беспроводные сети, работающие по протоколу WEP, практически не встречаются в корпоративном секторе. Его применяют только в случае необходимости, например для поддержки устаревших устройств, когда обновить программное или аппаратное обеспечение не представляется возможным. Протокол WEP может быть задействован для защиты сетей AdHoc, так как при их построении использование WPA/WPA2 невозможно. Использование протокола WEP можно наблюдать и в так называемых «домашних» сетях, где он может быть выбран совершенно случайно.

Конечно, построение сети с учетом стандарта 802.11i требует наличия соответствующей инфраструктуры, но не стоит забывать про «облегченный» вариант — WPA-PSK/WPA2-PSK, при котором мы получаем вполне приемлемый уровень защиты, но в этом случае все устройства, подключенные к такой сети, используют один и тот же ключ. Следовательно, потеря или кража одного устройства компрометирует и остальную сеть. Кроме того, эта схема уязвима к атакам по словарю. Перехваченные в момент подключения клиента к сети запрос и отклик позволяют провести «офлайновую» словарную атаку. В связи с этим стоит упомянуть о недавнем предложении компанией Elcomsoft новой технологии подбора паролей в беспроводных сетях, базирующихся на стандартах безопасности WPA и WPA2. По заявлениям разработчиков, указанная методика обеспечивает в десятки раз более высокую скорость подбора пароля по сравнению со стандартными средствами (www.securitylab.ru/news/361077.php).

Об авторе

Владимир Лепихин – заведующий Лабораторией сетевой безопасности Учебного центра «Информзащита». Под его руководством разрабатываются тренинговые курсы по сетевой безопасности. За годы работы Лабораторией накоплен значительный исследовательский и практический опыт построения защищенной беспроводной инфраструктуры и оценки защищенности беспроводного доступа. Результаты работ систематизированы в курсе «Безопасность беспроводных сетей», который поддерживается и оперативно обновляется по мере появления новых проблем и технологий защиты беспроводного доступа.

Построение инфраструктуры мониторинга

Второй шаг — мониторинг. И здесь существует своя специфика. Не случайно в не так давно опубликованном документе американского национального института стандартов и технологий (NIST), посвященном системам обнаружения и предотвращения атак, беспроводные системы мониторинга выделены в особую группу. При этом цель мониторинга в данном случае — не только обнаружение «беспроводных» атак, но и выявление новых устройств (точек доступа, клиентских станций). Сегодня при внедрении инфраструктуры мониторинга необходимо обращать внимание на следующие моменты.

— Точки доступа Bluetooth

Они работают в том же частотном диапазоне, что и устройства 802.11 b/g, но могут не обнаруживаться существующими системами мониторинга беспроводных сетей. Таким образом, злоумышленник может создать угрозу нарушения защиты периметра, подключив такое устройство к сети. Скорость вполне приемлема для передачи небольших объемов информации.

— Технология 802.11n

Она вносит новые сложности в процесс мониторинга. Устройства 802.11n будут поддерживать как 20-, так и 40-мегагерцовые каналы. При этом последние будут образовываться из двух смежных по 20 МГц, и, если частотный спектр окажется перегруженным или надо будет связаться по старому стандарту, устройство может перейти на узкие каналы 20 МГц. Для систем обнаружения беспроводных атак это означает более частое переключение между каналами и меньшее время работы на одном канале. Разумеется, все это повышает вероятность пропуска атаки. Стандарт 802.11n вводит новый режим работы устройств — «Greenfield mode», что делает невозможным их обнаружение обычными системами, рассчитанными на стандарты a/b/g. Для целей обратной совместимости устройства 802.11n могут работать в трех режимах: a/b/g, смешанном (a/b/g/n) и Greenfield (только n).

Наконец, для некоторых точек доступа можно использовать специальное программное обеспечение WKnock, которое делает их «незаметными» в течение долгого периода времени, до тех пор пока ими не пользуются.

АВТОР: ВЛАДИМИР ЛЕОНКИН

Защита на уровне пользователя

Самое сложное — это «третий пункт». Построение беспроводной сети с учетом требований стандарта 802.11i и правильная организация фильтрации трафика позволяют достичь вполне приемлемого уровня защищенности. Неудивительно, что в такой ситуации вектор атак смещается в сторону беспроводных клиентов. Ведь, как и во многих других ситуациях, «слабым звеном» при защите беспроводной сети оказываются пользователи и их рабочие места. Так что этот вопрос рассмотрим более подробно.

Вот перечень возможных атак на беспроводных клиентов:

- атаки с использованием уязвимостей ОС и прикладного ПО;
- атаки на защитные механизмы канального уровня (аутентификация, шифрование);
- атаки с использованием уязвимостей драйверов сетевых адаптеров;
- DoS-атаки.

В силу специфики беспроводного доступа беспроводной клиент и потенциальный злоумышленник оказываются по отношению друг к другу в одном сегменте. Аналогично клиентам VPN, для которых характерно подключение к ресурсам корпоративной сети из неизвестного сетевого окружения, для клиентов беспроводных сетей существует угроза атак со стороны нарушителей, находящихся в зоне действия точки доступа.

Следовательно, в отношении беспроводного клиента могут быть выполнены «классические» сетевые атаки, направленные на нарушение «навигации»:

- удаленное изменение таблицы ARP (ARP-Spoofing);
- удаленное изменение таблицы маршрутизации (ICMP Redirect);
- внедрение ложного DHCP-сервера;
- подмена DNS-ответов (DNS-spoofing).

В случае успеха перечисленных атак могут быть реализованы и атаки «человек посередине» на используемые в беспроводной сети криптографические протоколы, например SSH и SSL. Кроме того, пользуясь уязвимостями сетевых сервисов, нарушитель может пытаться получить доступ к узлу на уровне ОС или прикладного ПО. Однако для совершения таких атак необходимо выполнение одного из следующих условий:

- нарушитель и объект атаки подключены к одной и той же точке доступа;
- объект атаки подключен к точке доступа, контролируемой нарушителем (например, к ложной точке доступа).

Первое условие может быть выполнено в следующих случаях:

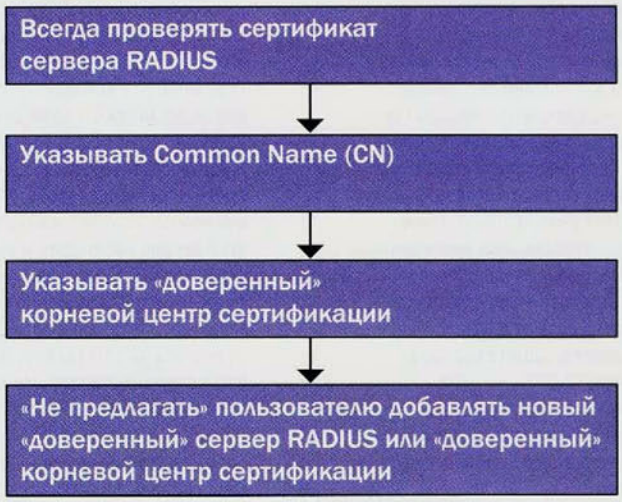
- гостевой доступ, при котором аутентификация осуществляется через веб-портал;
- корпоративный доступ с применением технологий VPN; в этом случае обычно на канальном уровне соединение устанавливается без каких-либо препятствий, а все защитные механизмы начинают работать на сетевом уровне и выше.

Таким образом, уязвимыми для таких атак оказываются пользователи «хотспотов» и беспроводные клиенты, осуществляющие доступ в корпоративную сеть с использованием VPN-технологий. В этом, кстати, и состоит опасность «гибридов» корпоративного и гостевого доступа, которые обычно строят на базе уже хорошо сложившейся инфраструктуры VPN.

В качестве меры защиты от рассмотренных угроз может служить набор средств, который называют «Endpoint Security» и который включает в себя такие компоненты, как персональный межсетевой экран и систему предотвращения атак. Фактически, в этом случае ситуацию следует рассматривать как подключение из «неизвестного» сетевого окружения и принимать соответствующие меры защиты.

Однако результат рассмотренных выше атак на ОС и прикладное ПО (например, задействуя ложную точку доступа) сильно зависит от состояния защитных механизмов канального уровня. Как правило, применение станцией любых механизмов защиты, даже WEP, уже серьезно снижает вероятность успеха атакующего, поскольку в этом случае клиент будет требовать от ложной точки доступа использования WEP. Даже если клиент использует аутентификацию Open System, что в случае применения WEP позволит ему ассоциироваться с ложной точкой доступа, все равно данные на вышестоящих уровнях модели OSI будут зашифрованы с помощью неизвестного ключа.

«ПРАВИЛЬНАЯ» НАСТРОЙКА PEAP



Метод аутентификации PEAP

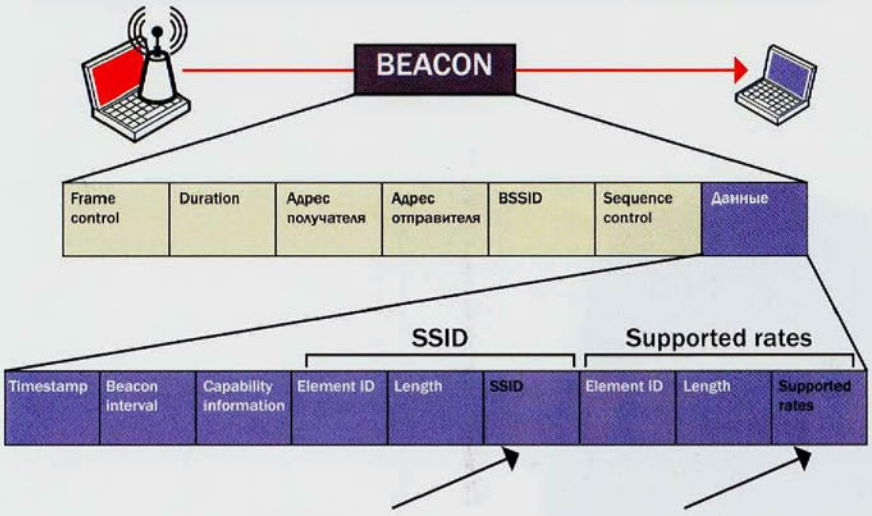
При использовании 802.1x многое зависит от выбранного метода аутентификации. Сегодня, безусловно, наиболее популярен метод аутентификации PEAP. Однако его применение обеспечивает должный уровень защиты только при условии правильной настройки всех участников схемы. Вот основные «слабые» места PEAP:

- Проверка подлинности сервера RADIUS основана на проверке подлинности его сертификата. Это требует корректной настройки процедуры проверки;
- Человеческий фактор. Довольно часто конфигурация параметров беспроводного доступа оставляет клиента «наедине» с решением «доверять/не доверять». Фактически, в этом случае «безопасность» оказывается в руках пользователя.

Таким образом, источники уязвимостей PEAP — ошибки настройки и чело-

АВТОР: ВЛАДИМИР ЛЕПИХИН

ПОЛЯ ФРЕЙМОВ «BEACON», ИМЕЮЩИЕ ПЕРЕМЕННУЮ ДЛИНУ



вческий фактор. Вот основные ошибки настройки PEAP:
- отсутствие проверки сертификата сервера RADIUS;
- решение о «доверии» сертификату сервера RADIUS принимает пользователь;
- не выполняется проверка параметра CN (Common Name) в сертификате.
Правильная настройка PEAP предполагает выполнение условий, показанных на рисунке.
В противном случае возможно проведение атаки с использованием ложного RADIUS-сервера, который на любой запрос аутентификации возвращает положительный ответ, «эмулирует» соответствующую сетевую инфраструктуру и записывает в журнал данные аутентификации (challenge/response, password/username).
Еще одна интересная проблема «уровня клиента» — драйверы для беспроводных карт. Это программное обеспечение, а оно может содержать ошибки реализации. Если эти ошибки связаны с обработкой управляющих фреймов (beacon или probe response), существует потенциальная возможность выполнения произвольного кода на клиентском узле при получении специальным образом сформированного управляющего фрейма. Например, нарушитель может сформировать фрейм beacon, включив туда соответствующий код. Кроме фреймов beacon могут быть использованы и другие управляющие фреймы, например ответы на запросы probe request или association request.
Отдельные поля управляющих фреймов, имеющие переменную длину, хорошо подходят для включения туда кода, вызывающего ситуацию переполнения буфера. Так, во фреймах beacon имеются «комплекты» из трех полей: тип (Element ID), длина, значение. В частности, в таком виде передается идентификатор сети — SSID (смотрите на рисунке). Таким образом, варьируя длину и значения соответствующих полей и отправляя сформированные фреймы beacon в сеть, можно пытаться вызвать на узле ситуацию переполнения буфера.

В качестве примера можно привести уязвимость драйверов беспроводных адаптеров Intel (2200BG и 2915ABG), причина — ошибка обработки управляющих фреймов (www.wve.org/entries/show/WVE-2006-0059).
Ошибки реализации драйверов для беспроводных сетевых адаптеров опасны по нескольким причинам:
- использование уязвимости «по определению» предполагает получение доступа на уровне ядра, а это означает возможность обхода любых защитных механизмов;
- для беспроводных клиентов значительно легче использование уязвимости удаленно, поскольку многие уязвимости основаны на ошибках обработки широковещательных управляющих фреймов (например, «beacon»), которые обрабатываются всеми станциями;
- для реализации атаки достаточно небольшого числа фреймов;
- процедура обновления драйверов обычно выполняется редко, поэтому системы могут оставаться уязвимыми к атакам довольно продолжительное время.
Наконец, следует заметить, что новый стандарт 802.11n предполагает усложнение драйверов поддерживающих его устройств, что повышает вероятность появления новых уязвимостей такого типа.
Для защиты от подобных атак необходимо отслеживать используемые версии драйверов и своевременно обновлять их. Для сбора информации об используемых драйверах можно применить свободно распространяемую утилиту WiFiDEnum (www.labs.arubanetworks.com/wifidenum).
Кроме того, в процессе мониторинга событий безопасности можно выявлять попытки использования уязвимостей драйверов. Основываясь на аномальном подходе, можно отслеживать нестандартные/некорректные фреймы. Сигнатурный подход, в свою очередь, можно реализовывать для отслеживания попыток использования известных уязвимостей.

И последнее

Безусловно, самый сложный этап в обеспечении безопасности беспроводной сети — дополнительная защита на уровне пользователя. И хотя имеется масса эффективных технических мер, от человеческого фактора никуда не денешься. Поэтому в ряде ситуаций потребуется прибегнуть к крайней мере — повышению осведомленности пользователей. it

Ссылки

- www.csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
  «Guide to Intrusion Detection and Prevention Systems (IDPS)»
- www.wve.org/entries
  Каталог уязвимостей беспроводных сетей
- www.securitylab.ru/analytics/312606.php
  «О взломе WEP. В последний раз...»
- www.blackhat.com/presentations/bh-usa-07/Bulygin/Presentation/bh-usa-07-bulygin.pdf
  «Remote and Local Exploitation of Network Drivers»