БЕЗОПАСНОСТЬ СЕТИ БЕСПРОВОДНОГО ДОСТУПА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Высоцкая В.В.

Лыньков Л.М. – д.т.н., профессор

Большинство современных портативных устройтсв (ноутбуки, КПК, смартфоны) уже имеют встроенные средства для работы в беспроводных сетях. Если беспроводная сеть останется незащищенной, она будет уязвима для доступа из других компьютеров. Защитить домашнюю сеть и сеть малого бизнеса от почти любых форм несанкционированного доступа можно, используя для этого методы защиты.

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

– прямые – угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11;

– косвенные – угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей.

Есть следующие виды персональной защиты:

1 Открытая и общая сетевая аутентификация. Спецификация 802.11 поддерживает два метода сетевой аутентификации: открытую систему и с использованием общего ключа.

С использованием открытой аутентификации любая станция беспроводной сети может запросить аутентификацию. Аутентификация – это процесс установления подлинности и подтверждения запроса клиента (обычно это ноутбук) для доступа к сети или сетевой точке доступа. После выполнения аутентификации и предоставления доступа клиент получает доступ к сети. Станция, для которой необходима аутентификация для связи с другой станцией беспроводной сети, отправляет управляющий аутентификационный запрос, содержащий ее идентификационную информацию. Приемная станция или точка доступа принимает любой запрос на аутентификацию.

С использованием общего ключа аутентификации каждая станция обязана получить секретный общий ключ через защищенный канал, который независим от коммуникационного канала беспроводной сети 802.11.

2 WEP-шифрование. WEP-шифрование (Wired Equivalent Privacy) использует специальное преобразование данных для предотвращения несанкционированного доступа к данным беспроводной сети. WEP-шифрование использует ключ шифрования для кодирования данных перед их отправкой. Если используется шифрование, все устройства в беспроводной сети должны использовать одинаковые ключи шифрования.

3 WPA-, WPA2-персональная. Режим персональной защиты WPA используется в домашних условиях или сетях малого бизнеса. Для персональной защиты WPA необходимо вручную сконфигурировать предварительно опубликованный общий ключ (PSK) в точке доступа или клиентах. Аутентификация в сервере не используется. Этот пароль, введенный в точке доступа, должен использоваться в этом компьютере и на всех беспроводных устройствах сети для подключения к этой точке доступа. Защита зависит от надежности и секретности пароля. Чем больше длина используемого пароля, тем надежнее защита беспроводной сети.

4 WPA-, WPA2-Enterprise (WPA-предприятие). Корпоративный режим аутентификации предназначен для использования в масштабах предприятий или сетях государственных учреждений. WPA-предприятие проверяет пользователей сети, используя сервер RADIUS или другой сервер аутентификации [1].

Аутентификация 802.1X (корпоративная защита). Аутентификация по стандарту 802.1x – это процесс, независимый от аутентификации по стандарту 802.11. Стандарт 802.11 обеспечивает основы для различных видов аутентификации и протоколов манипулирования ключами. В стандарте 802.1X присутствуют различные типы аутентификации, каждый из которых обеспечивает свой подход к установлению подлинности, но все они используют один протокол 802.11 и структуру для взаимодействия между клиентом и точкой доступа. В большинстве протоколов после выполнения процесса аутентификации стандарта 802.1X приемная сторона (клиент) получает ключ, который она использует для шифрования данных. При аутентификации по стандарту 802.1X используется метод установления подлинности между клиентом и сервером (например, удаленная аутентификация RADIUS – Remote Authentication Dial-In User Service), к которому подключена точка доступа. Процесс аутентификации использует идентификационную информацию, например, пароль пользователя, который не передается через беспроводную сеть. Большинство видов аутентификации 802.1X поддерживают динамические ключи для пользователя, сеанса и для усиления защиты ключа. Аутентификация 802.1X имеет преимущества перед использованием существующего протокола аутентификации EAP (Extensible Authentication Protocol).

Аутентификация стандарта 802.1x для беспроводных сетей имеет три главных компонента:

– аутентификатор (точка доступа);

– запросчик (программное обеспечение клиента);

– сервер аутентификации.

Защита аутентификации стандарта 802.1X инициирует запрос на аутентификацию от клиента беспроводной сети в точку доступа, которая устанавливает его подлинность через протокол EAP в соответствующем сервере RADIUS. Этот сервер RADIUS может выполнить аутентификацию пользователя (с помощью пароля или сертификата) или компьютера (с помощью адреса MAC). Теоретически, клиент беспроводной сети не может войти в сеть до завершения транзакции. (Не все методы аутентификации используют сервер RADIUS. WPA-персональная и WPA2-персональная используют общий пароль, который вводится в точке доступа и в устройствах, запрашивающих доступ к сети). Существует несколько аутентификационных алгоритмов, используемых со спецификацией 802.1X. Эти методы используются при идентификации клиента беспроводной локальной сети в сервере RADIUS. Во время аутентификации в сервере RADIUS пользователи проходят проверку в специализированных базах данных. Аутентификация RADIUS основана на наборе стандартов, предназначенных для аутентификации, авторизации и ведения учетных записей (Authentication, Authorization и Accounting – AAA). Сервер RADIUS содержит прокси-процесс для проверки клиентов в многосерверной среде. Стандарт IEEE 802.1X предоставляет механизм для управления и аутентифицированного доступа к беспроводным сетям на основе портов 802.11 и проводных сетей Ethernet. Управление сетевым доступом, основанным на использовании портов, подобно инфраструктуре локальной сети, управляемой с помощью коммутаторов, которая идентифицирует устройство, подключенное к порту ЛС, и запрещает доступ к этому порту, если процесс аутентификации был неудачен [2].

Протокол аутентификации RADIUS. RADIUS (Remote Authentication Dial-In User Service) – это сервис протокола клиент-сервер для авторизации, аутентификации и ведения учетных записей (Authorization, Authentication и Accounting – AAA), который используется для регистрации клиентов в сервере сетевого доступа по коммутируемой линии. Обычно сервер RADIUS используется поставщиками услуг доступа в Интернет (Internet Service Providers – ISP) для выполнения задач AAA. Далее описаны фазы AAA:

1 Фаза аутентификации (Authentication): Проверяется имя пользователя и пароль в базе данных. После проверки идентификационной информации начинается процесс авторизации.

2 Фаза авторизации (Authorization): Определяется, было ли дано разрешение на запрос доступа к ресурсам. Назначается IP-адрес для клиента, выполняющего доступ по коммутируемой линии (Dial-Up).

3 Фаза ведения учетной записи (Accounting): Выполняется сбор информации об используемых ресурсах для оценки, аудита, учета времени сеанса или учета стоимости затрат.

В сетях Wi-Fi используются следующие виды шифрования данных:

1 AES – CCMP. Advanced Encryption Standard – Counter CBC-MAC Protocol (улучшенный стандарт шифрования – протокол Counter CBC-MAC). Это новый метод защиты при беспроводной передаче данных, определенный в стандарте IEEE 802.11i. Протокол AES-CCMP обеспечивает более надежный метод шифрования в сравнении с TKIP. AES-CCMP используется в качестве метода шифрования, когда необходима повышенная безопасность данных. Протокол AES-CCMP доступен для сетевой аутентификации
WPA/WPA2-персональная/предприятие.

2 TKIP. Протокол TKIP (Temporal Key Integrity Protocol) использует функцию смешения содержимого ключа для каждого пакета, проверку целостности сообщений и механизм манипуляций с ключом. Протокол TKIP доступен для сетевой аутентификации WPA/WPA2-персональная/предприятие.

3 CKIP. Cisco Key Integrity Protocol (CKIP) – это собственный протокол защиты Cisco для шифрования в среде 802.11. Протокол CKIP использует следующие особенности для усовершенствования защиты 802.11 в режиме «infrastructure»:

- Key Permutation (KP) – манипуляции с ключом;
- Message Sequence Number – номер последовательности сообщения.

4 WEP. WEP-шифрование (Wired Equivalent Privacy) использует специальное преобразование данных для предотвращения несанкционированного доступа к данным беспроводной сети. WEP-шифрование использует ключ шифрования для кодирования данных перед их отправкой. Только компьютеры, использующие этот же ключ, могут получить доступ к сети и расшифровать переданные другими компьютерами данные. Корпоративная WEP-защита отличается от персональной WEP-защиты тем, что для нее может быть выбрана открытая сетевая аутентификация, а затем можно выбрать 802.1X и указать нужный тип аутентификации клиентов [3]. Выбор типов аутентификации недоступен для персональной защиты WEP.

Список использованных источников:

1. Шифрование wi-fi сети, какой метод выбрать? [Электронный ресурс]. – https://wifiget.ru.
2. Configuring IEEE 802.1X Port-Based Authentication.
3. Обзор возможностей защиты [Электронный ресурс]. – Режим доступа: http://support.elmark.com.pl.