ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В WI-FI СЕТЯХ

Алексеенко А.Э.

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

Саломатин С.Б. – канд. техн. наук, доцент

В работе рассмотрено современное состояния средств защиты информации в беспроводных сетях на основе групп протоколов IEEE 802.11, а также разработка комплекса мер для усиления безопасности на основе практических пошаговых рекомендаций.

Одной из важных задач, стоящих перед администраторами и разработчиками коммуникаций является защита беспроводных сетей по технологии групп протоколов IEEE 802.11 (Wi-Fi). В общем случае, защита должна обеспечивать невозможность доступа в сеть без разрешения администратора сети, выражаемого в выдаче кодов или специальных устройств доступа. Использование беспроводных сетей на базе протоколов IEEE 802.11 приводит к следующим особенностям защиты [1]:

1) Для подключения к беспроводной сети, не требуется физический доступ к кабелю витой пары или оптоволокну – достаточно находиться в зоне приёма сигнала маршрутизатора;

2) Передача данных по беспроводному каналу может быть перехвачена и обработана даже без устройства доступа с помощью специальных аппаратных или программных средств.

К стандартным мерам защиты относятся программные и аппаратные средства, предназначенные для решения следующих задач:

1) Предотвратить несанкционированное подключения к беспроводной сети пользователей;

2) Предотвратить доступ к запрещенным ресурсам уже подключившихся пользователей;

3) В случае проникновения, выполнить меры по сбору информации для предотвращения следующего инцидента доступа.

Для повышения уровня защиты беспроводной сети выполняются следующие меры [2]:

1) Замена ключей доступа на более комплексные;

2) Смена протоколов шифрования на более современные и устойчивые к взлому методом перебора;

3) Установка программного обеспечения для протоколирования доступа пользователей к ресурсам внутри сети.

Для администраторов беспроводных сетей, предлагается расширенный комплекс мер на основе автоматизированного контроля за доступом к сети, программируемой смены ключа доступа и перехода на последние стандарты шифрования. Комплекс предназначен для повышения всех уровней защиты беспроводной сети. Перечислим каждый шаг по усилению защиты.

На персональные компьютеры, доступ к которым осуществляется через сеть, устанавливается дополнительное «проксирующее» программное обеспечение, которое записывает в базу данных сведения о случаях доступа к ресурсам, как одобренные, так и отклоненные системой. Запись событий доступа ведется за пределы защищаемой сети, что даже в худшем случае совершенного несанкционированного доступа, позволит сохранить и расследовать историю проникновения.

Традиционным алгоритмом шифрования данных в сети Wi-Fi является WEP (Wired Equivalent Privacy) [3]. Обязательной мерой для повышения безопасности беспроводной сети является перевод всех маршрутизаторов и клиентских терминалов на протоколы шифрования данных WPA и WPA2, которые представляют собой следующее поколение алгоритмов шифрования [3].

WPA3 является преемником WPA2. WPA3 является программой сертификации и поддерживает четыре основных функции, из которых обязательна только одна: новое рукопожатие стрекозы. Эти четыре особенности следующие:

1) Новое рукопожатие под названием «стрекоза» (также называется «Одновременная аутентификация равных»), устойчивое к атакам по словарю и обеспечивающее секретность. Использует нулевые доказательства знаний.

2) Простой способ безопасного добавления устройств в сеть. Ссылка на Wi-Fi CERTIFIED Easy Connect.

3) Защитные механизмы в открытых сетях основаны на шифровании без аутентификации. Оппортунистическое беспроводное шифрование.

4) Увеличенные размеры клавиш с 192-битными ключами. Обязательно только при сертификации WPA3-Enterprise

Кроме того, WPA3 поддерживает защищенные кадры управления (PMF), что делает невозможным запуск атак отмены аутентификации. WPA2 уже поддерживает это, поэтому это не новинка WPA3. Однако с WPA PMF включаются с самого начала в программу сертификации.

Наибольший интерес в WPA3 представляет технология dragonfly (стрекоза). Dragonfly использует архитектуру клиент-сервер, где MessageManager является центральным сервером, а программные модули, которые хотели бы общаться друг с другом, являются клиентами. MessageManager поддерживает сокет прослушивания для подключения модулей и начала отправки сообщений. Все сообщения проходят через MessageManager, который перенаправляет их в подключенные модули на основании их подписок. Модули подключаются к MessageManager, подписываются на интересующие их типы сообщений, отправляют сообщения, которые будут пересылаться MessageManager всем модулям, которые подписались на эти типы сообщений, и получают сообщения, на которые они сами подписались. Модули остаются независимыми друг от друга и не должны знать, какие модули будут использовать свои сообщения или откуда поступают сообщения, которые они потребляют.

Рукопожатие стрекозы – это обмен ключами с использованием криптографии с дискретным логарифмом, которая аутентифицируется с использованием пароля или ключевой фразы. Он устойчив к активной атаке, пассивной атаке и атаке по автономному словарю.

WPA3 обладает идеальной секретностью пересылки (чего нет у WPA2) и защищает от атак методом «грубой силы» в автономном режиме.

В отличие от WPA2, WPA3 разрешено использовать только «Расширенный стандарт шифрования» (AES) и больше не использовать устаревшие протоколы, такие как «Протокол целостности временного ключа» (TKIP) или «Проводная эквивалентная конфиденциальность» (WEP).

Метод предварительного ключа (PSK) в WPA2 заменен на *одновременную аутентификацию* (SAE), которая предлагает более надежную аутентификацию на основе пароля. Сама парольная фраза больше не используется для получения ключа (ключевое слово: Pairwise Master Key (PMK)), получение ключа основано на криптографии с эллиптической кривой (ECC) или специальной форме ECC с целочисленными числами, называемыми только конечным полем.

WPA3 использует доказательство с нулевым разглашением, что гарантирует, защиту паролей при рукопожатии SAE, при этом участники рукопожатия могут быть уверены, что другая сторона знает, что они имеют такой же и правильный пароль. Рукопожатие Dragonfly по сути является протоколом SPEKE.

Помимо установки новых алгоритмов для оборудования, необходимо также усиление собственной сети за счет введения виртуальной внутренней сети, известной как технология VPN (Virtual Private Network). Создание VPN вводит дополнительное шифрование поверх уже используемых уровней, что на порядок повышает сложность взлома и делает практически невозможным силовой подбор ключей и паролей.

Также одним из способов защиты информации в Wi-Fi является автоматическая регенерация ключей доступа, производимая по расписанию и заданному алгоритму на всех устройствах доступа и клиентских терминалах. Данный способ требует разработки и установки специального программного обеспечения, которое выполняет следующие действия:

1) Создает новый ключ доступа в соответствии с правилами, заданными администратором сети;

2) Устанавливает этот ключ на все устройства, используя для подключения еще действующий предыдущий ключ;

3) Повторяет действия не реже периода, заданного администратором сети.

Ведение собственной базы ключей позволит избежать повторного использования ранее примененной последовательности, а использование аппаратно-программного генератора случайных чисел сделает создаваемый ключ непредсказуемым. При правильной настройке такого комплекса, силовой подбор ключа доступа становится практически невозможен, даже при полном доступе злоумышленника к каналу связи.

Рассмотренные меры позволяют сделать невозможным чисто силовые методы взлома беспроводной сети Wi-Fi и существенно затрудняют прочие способы, такие, как социальные и логические. Для обеспечения максимальной степени защиты, рекомендуется комбинировать предложенные меры с другими, например, контролем доступа персонала и расширенные методы идентификации пользователей с использованием электромагнитных карт или датчиков отпечатков пальцев.

Список использованных источников:

1. Пролетарский, А.В. [и др.]. Беспроводные сети Wi-Fi / А.В. Пролетарский, И.В. Баскаков, Д.Н. Чирков, Р.А. Федотов, А.В. Бобков, В.А. Платонов/ М.: Интернет-университет информационных технологий – ИНТУИТ.ру, 2013. – 216 с.

2. Пол Беделл. Сети. Беспроводные технологии. – М.: НТ Пресс, 2008. – 448 с.

3. Визавитин, О. И. Практика защиты информации в Wi-Fi сетях на основе современных программно-аппаратных средств // Молодой ученый. – 2016. – №5. – С. 182–184.