УДК 004.7

Виды протоколов шифрования Wi-Fi

Зайцев Сергей Сергеевич
Брянский государственный университет имени академика И.Г. Петровского
магистрант

Аннотация
В данной статье речь идет о разных видах протоколах шифрования информации беспроводной сети Wi-Fi.
Ключевые слова: Wi-Fi, протоколы шифрования, беспроводная сеть, WEP, WPA, WPA2, WPS, OPEN.

Types of encryption protocols Wi-Fi

Zaitsev Sergey Sergeevich
Bryansk State Academician I.G. Petrovski University
Undergraduate

Abstract
In this article we are talking about different kinds of protocols, data encryption wireless network Wi-Fi.
Keywords: Wi-Fi, encryption protocols , wireless network , WEP, WPA, WPA2, WPS, OPEN.

Все больше информации передается по средствам всемирной паутины, и данной информации требуется защита. Сейчас очень популярные интернет соединения при помощи Wi-Fi соединения. Возникает вопрос насколько безопасно можно использовать Wi-Ficоединение, и какие протоколы защиты Wi-Fi сети существуют. Рассмотрим типы шифрования Wi-Fi сети (WEP, WPA, WPA2, WPS).

Прежде чем начнем рассматривать протоколы шифрования Wi-Fi, разберем, как работает аутентификация с сервером (роутером).

На рис. 1 изображен клиент- участник сети, который передает и получает информацию, сервер – участник сети, который предоставляет доступ в Интернет. Прежде чем клиент получает доступ интернет, он должен отправить серверу пароль, если он установлен на сервере. Как только введен верный пароль, то сервер высылает ключ, при помощи которого будет все шифроваться. Последующая информация будет идти по зашифрованному каналу. Подробней рассмотрим типы шифрования Wi-Fi соединения.

Рисунок 1 – Аутентификация с сервером (роутером)

Выделяют такой тип шифрования как OPEN. В данном типе шифрования отсутствует защита канала вовсе, как со стороны клиента, так и со стороны роутера. Данный тип шифрования используется в проводных сетях, так как для получения информации необходимо врезаться к физической сети. К беспроводной сети можно подключиться из любой точки в радиусе 15 метров, возможно и более дальнее подключение, все зависит от мощности антенн. Поэтому строго не рекомендуется использовать данный тип шифрования для беспроводных сетей.

В конце 90-х был создан тип шифрования беспроводных сетей WEP, хотя он и предоставлял кое-какую защищенность сети, но его все ровно не рекомендуется использовать. Одна из причин в том, что для взлома пароля защиты требуется маленькое количество времени, парой несколько секунд, так как пароль состоит из 40-104 бит- это очень короткая комбинация. Основная же проблема данного протокола защиты заложена в его проектировании. WEP протокол с каждым пакетом информации передает часть ключа, тем самым вне зависимости от сложности ключа, раскрыть передаваемую информацию можно, имея достаточное количество перехваченных пакетов информации.

На смену WEP протокола шифрования, пришли протоколы WPAи WPA2. В данных протоколах уже пароль состоял от 8 до 63 байт, что существенно затрудняет его подбор. Стандарт поддерживает несколько способов шифрования. Один из них TKIP использовался для перехода от протокола WEP к протоколуWPA и в принципе это тот же WEP. Протокол шифрования WPA2 поддерживает не только разные виды шифрования информации, но поддерживает функцию двух разных режимов начальной аутентификации.

Рассмотрим два режима начальной аутентификации в протоколе WPA2. Первый режим аутентификации называется PSK (порой называют WPAPersonal) – вход по единому паролю. Если это небольшая сеть, то данной функции достаточно и удобно пользоваться. Но если беспроводная

сеть используется в большой компании, где при уходе сотрудника, необходимо менять пароль и передать новый всем остальным сотрудникам компании. Это достаточно неудобно и замедляет работу компании. Поэтому есть второй режим аутентификации Enterprise.Второй режим начальной аутентификации Enterprise снимает проблему в больших компаниях следующим образом, каждому сотруднику выдается свой персональный пароль доступа к сети. Таким образом, при уходе из компании одного сотрудника, стирается его персональный код доступа, не затрагивая других сотрудников компании.

Следующий протокол шифрования беспроводной сети рассмотрим WPS.Данная технология позволяет подключиться к сети, не вводя пароля. Данный протокол получил широкое распространение, хотя у него тоже есть просчет в программирование, как и в технологии WEP. Протокол WPSподключается к роутеру по 8 символьному коду (PIN). Но из-за ошибки проектирования нужно отгадать всего 4 символа данного кода и получиться подключиться и к тому же мы так же узнаем полный код доступа. Получается для доступа к сети через данный протокол, нам необходимо 10000 попыток подбора. Данные действия проходят до каких-либо проверок безопасности, поэтому в секунд можно отправить 10-50 запросов на вход в сеть через WPS. Таким образом, через 3-15 часов удается получить ключ доступа к сети интернет.

После того как данная уязвимость была раскрыта, производители начали вводить лимиты на число попыток входа в сеть, при превышении данного лимита точка доступа отключалась. Однако лимиты на количество попыток входа, не решили проблемы и лишь увеличили время взлома сети. В среднем с лимитом потребуется около 7 дней.

Рассмотрев протоколы шифрования беспроводной сети Wi-Fi, делаем выводы, что протоколы OPEN и WEP категорически не рекомендуются к использованию, если хотите, чтобы не было доступа к беспроводной сети. Протокол WPS обеспечит безопасность сети, но из-за просчета в проектировании данной системы, за часов 12 он будет взломан, если это протокол в котором не установлена функция лимита попыток и в течение 7 дней, если функция лимита предусмотрена в данном протоколе. Если же решили использоватьWPS, то необходимо включать непосредственно при входе в сеть, а в остальное время, необходимо держать в выключенном состоянии. Можно использовать протокол шифрования WPA. Он лучше обеспечить вашу безопасность сети. Но лучше всего использовать протокол шифрования WPA2. Данный протокол максимально обеспечит безопасность беспроводной сети.

Библиографический список

1. Несколько слов о шифровании Wi-Fi протокола: что к чему и зачем: [Электронный ресурс]. URL:http://sonikelf.ru/neskolko-slov-o-shifrovanii-wi-fi-protokola-chto-k-chemu-i-zachem/ (Дата обращения: 31.08.2016)

2. Технологии защиты WI-FI сетей. Стандарт IEEE 802.11X: [Электронный ресурс]. URL:http://confonline.susu.ru/index.php?option=com_content&view=article&id=95:--wi-fi--c-ieee-80211x&catid=16:-2----&Itemid=18(Дата обращения: 31.08.2016)
3. Уязвимости Протокола WEP. Защищенный доступ к Wi-Fi (WPA)[Электронный ресурс]. URL:http://osnovy-setei.ru/uyazvimosti-protokola-wep-zashhishhennyj-dostup-k-wi-fi-wpa.html(Дата обращения: 31.08.2016)