УДК 004.056.5

Курмакаев П.А.

Студент

4 курс, факультет «Телекоммуникаций и радиотехники»

Поволжский Государственный Университет Телекоммуникаций и Информатики

Россия, г. Самара

Шилкина М.В.

Студент

4 курс, факультет «Телекоммуникаций и Радиотехники»

Поволжский Государственный Университет Телекоммуникаций и Информатики

Россия, г. Самара

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ Wi-Fi

Аннотация:

Статья посвящена безопасности Wi-Fi сети, которая в настоящее время является самой большой проблемой для неё. В статье были разобраны причины уязвимостей. Также были подробно рассмотрены механизмы защиты и принципы их работы. Автор привёл возможные последствия атак на Wi-Fi сеть. И наконец описаны проблемы безопасности общественных Wi-Fi точек.

Ключевые слова: безопасность, Wi-Fi, WPA, WEP, WPS, защита, беспроводная сеть.

Kurmakaev P.A.
Student
4 course, faculty "Radio Engineering and Telecommunications"
Povolzhskiy State University of Telecommunications and Informatics
Russia, Samara
Shilkina M.V.
Student
4 course, faculty "Radio Engineering and Telecommunications"
Povolzhskiy State University of Telecommunications and Informatics
Russia, Samara

SECURITY OF WIRELESS Wi-Fi NETWORKS

Annotation:
The article is devoted to the security of Wi-Fi network, which is currently the biggest problem for it. The article discussed the causes of vulnerabilities. Protection mechanisms and principles for their operation were also discussed in detail. The author cited the possible consequences of attacks on the Wi-Fi network. Finally, we describe the security problems of public Wi-Fi hotspots.
Keywords: security, Wi-Fi, WPA, WEP, WPA, protection, wireless network.

Введение

Основная причина уязвимости пользовательских данных, передающихся по сетям Wi-Fi, заключается в том, что обмен в таких сетях происходит по радиоканалу. А это предоставляет возможность перехвата данных в любой точке, где физически есть доступ к сигналу Wi-Fi. Проще говоря, если сигнал Wi-Fi реально поймать, то возможно сделать и перехват трафика, будь злоумышленник хоть в соседнем помещении, хоть на улице.

Но несмотря на все трудности на сегодняшний день разработаны и внедрены средства защиты Wi-Fi сетей. Вся защита основана на шифровании передающегося и получаемого трафика между точкой доступа и клиентским устройством, которое подключено к ней.

Механизмы защиты Wi-Fi

Точка доступа может работать в одном из двух режимов - открытом или защищенном.

В режиме открытого доступа, подключение может осуществить любое клиентское устройство. В защищённом режиме – лишь те, кто имеет прошёл аутентификацию.

- ***OPEN*** *— это отсутствие всякой защиты. Точка доступа и клиентское устройство не скрывают передачу данных. Открытая передача данных по беспроводной сети очень опасна.*
- ***WEP (Wired Equivalent Privacy)****. Самый первый механизм защиты. Шифрование потока данных осуществляется с помощью временного ключа. WEP фактически передаёт несколько байт этого самого ключа вместе с каждым пакетом данных. Таким образом, имея достаточное количество перехваченных пакетов данных, вне зависимости от сложности ключа, можно раскрыть любую передачу.*
- ***WPA и WPA2 (Wi-Fi Protected Access).*** *Стандарт поддерживает такие алгоритмы шифрования передаваемых данных как*

TKIP и CCMP. TKIP был придуман на то время, пока IEEE были создавали полноценный алгоритм CCMP. TKIP, как и WEP, уязвим к некоторым типам атак, и не является безопасным. По существу, использование WPA с TKIP это тоже самое, что и использование обычного WEP. WPA так же в отличии от WEP шифрует данные каждого клиента по отдельности. Кроме разных алгоритмов шифрования, WPA(2) поддерживают два режима начальной аутентификации: PSK и Enterprise. PSK — вход по единому паролю, который вводит клиент при подключении к сети. Это легко и удобно, но может стать проблемой, особенно в крупных компаниях. ***Enterprise*** *позволяет решить эту проблему благодаря наличию множества ключей, хранящихся на отдельном сервере — RADIUS. Кроме того, Enterprise стандартизирует сам процесс аутентификации в протоколе EAP (Extensible Authentication Protocol), что позволяет написать собственный алгоритм.*

- ***WPS/QSS*** *— технология, которая буквально позволяет просто нажать на кнопку и тут же подключиться к сети, т.к. не требует ввода пароля. WPS позволяет клиентскому устройству подключиться к точке доступа по 8-символьному коду, состоящему из цифр (PIN). Но из-за ошибки в стандарте нужно угадать лишь 4 из них. Таким образом, хватит всего 10000 попыток подбора и не зависимо от сложности пароля можно будет получить доступ к беспроводной сети Wi-Fi, а с ним в придачу — и этот полный пароль, как он есть. Когда обнаружили уязвимость, производители стали внедрять ограничение на число попыток входа, после превышения которого точка доступа автоматически на какое-то время отключала WPS.*

Последствия атак

Хакеры могут использовать ваш Wi-Fi для совершения противоправных действий. К примеру, взлома сетей и аккаунтов, рассылки спама и т.п.

Наконец, самое страшное – если хакеры решат перехватить и расшифровать ваш трафик. И получить данные, которые вы бы не хотели кому-то предоставлять: пароли от социальных сетей и банковских аккаунтов, личную переписку.

Так же, есть возможность осуществления атаки «человек посередине». Можно перехватывать сеансы TCP, выполнять вставку информации в сеансы HTTP, воспроизводить адресные или широковещательные пакеты.

Вопросы безопасности общественных сетей Wi-Fi

Сегодня очень распространено использование Интернета через Wi-Fi сети в общественных местах - в кафе, общественном транспорте, торговых центрах, аэропортах и т.п. Если вы решили воспользоваться Интернетом через такую сеть, то ваши данные (логин и пароль) могут быть перехвачены другим человеком, который также подключен к сети Wi-Fi. А особенность общественных сетей Wi-Fi как раз и заключатся в том, что к ней может подключиться любой желающий, в том числе злоумышленник.

Защитить свои данные при подключении к Интернету через общественную и не только Wi-Fi сеть можно воспользовавшись протоколом HTTPS. Цель этого протокола - установить зашифрованное соединение между клиентским устройством (браузером) и сервером.

Что касается других случаев использования Интернет - чаты, видеосвязь и т.д, то для защиты этих данных можно использовать бесплатные или платные серверы VPN сервера. То есть сначала подключаться к серверу VPN, а уже затем использовать чат или открытый сайт.

Использованные источники:

1. http://ru.d-ws.biz/articles/security-wifi.shtml
2. https://habrahabr.ru/post/224955/
3. https://www.iphones.ru/iNotes/777130