УДК 621.391

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В WI-FICETЯХ

ФеоктистовД.С., ХрущевВ.Ю.

Научный руководитель: ***Черников Дмитрий Юрьевич.***

Институт инженерной физики и радиоэлектроники СФУ

Россия, 660074, Красноярск

За последние годы роль Wi-fi сетей значительно возросла - в скором времени трафик беспроводных сетей может превзойти трафик проводных сетей. Поэтому проблема безопасностиWi-fi сетей занимает важное место в сфере телекоммуникационных систем.

Ключевые слова: Wi-fi, шифрование, угрозы безопасности, подлинность, информация.

In recent years, the role of Wi-fi networks has increased significantly - in a short time traffic of wireless network can surpass traffic of wired networks. Therefore, the problem of security Wi-fi networks plays an important role in the field of telecommunication systems.

Keywords: Wi-fi, encryption, security threats, authenticity, information.

Сегодня очень сложно найти человека, не использующего все блага беспроводных сетей. Это действительно очень удобно, доступно и быстро подключаемся и чем дальше, тем процесс приобщения к мировой паутине становиться еще проще для бытового пользователя. А если у этого самого пользователя есть еще и смартфон, планшет или ноутбук, то посещение общественных мест с наличием бесплатного открытого Wi-Fi доступа очень часто сопровождается использованием возможности подключиться к бесплатному интернету. Wi-Fi стал неотъемлемой частью жизни жителей большого города, при этом мы просто перестали об этом думать: подключаемся и используем.

Однако в случае подключения к открытым Wi-fi сетям отсутствует всякая защита. Т.е. точка доступа и клиент никак не маскируют передачу данных. Почти любой беспроводной адаптер Wi-fiможет быть установлен в режим прослушивания, когда вместо отбрасывания пакетов, предназначенных не ему, он будет их фиксировать и передавать в ОС, где их можно спокойно просматривать.Поэтому открытая передача данных по беспроводной сети гораздо более опасна.

Открытость сети не означает, что любой желающий может с ней работать. С целью обезопасить сеть передачи данных используются определенные методы аутентификации и шифрования.

Аутентификация – это проверка подлинности предъявленного пользователем идентификатора.Существуют следующие способы аутентификации:

- WEP;
- WPA;
- WPA 2;
- WPS/QSS.

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время,авторизованным пользователям доступа к ней.Шифрование обеспечивает три состояния безопасности информации:

- конфиденциальность, шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении;
- целостность, шифрование используется для предотвращения изменения информации при передаче или хранении;
- идентифицируемость, шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Алгоритмы шифрования таковы:

- none – отсутствие шифрования;

- WEP – основанный на алгоритме RC4 шифр с разной длиной статического или динамического ключа (64 или 128 бит);

- TKIP – улучшенная замена WEPс дополнительными проверками и защитой;

- AES/CCMP – алгоритм, основанный на AES256 с дополнительными проверками и защитой.

WEP (*Wired Equivalent Privacy*) –первыйстандартзащиты Wi-Fi. На деле он даёт намного меньше защиты, чем эти самые проводные сети, так как имеет множество огрехов и взламывается множеством разных способов. В 2004 IEEE объявили WEP устаревшим из-за того, что стандарт имеет множество слабых мест в алгоритме распределения ключей RC4. Каждый пакет, содержащий такой ключ, с 5%-ной степенью вероятности восстанавливает один байт секретного ключа. В среднем для взлома требуется порядка шести миллионов зашифрованных пакетов. В настоящее время создан алгоритм, сокративший количество необходимых пакетов до 500 тысяч. Данный алгоритм так же называют атакой Фларера-Мантина-Шамира.

WPA (*Wi-FiProtectedAccess*) – второй стандарт, пришедший на смену WEP. Качественно иной уровень защиты благодаря принятию во внимание ошибок WEP. Стандарт поддерживает различные алгоритмы шифрования передаваемых данных после рукопожатия: TKIP и CCMP. TKIP так же, как и WEP, страдает от некоторых видов атак, поэтому в целом не безопасен. WPA отличается от WEP и тем, что шифрует данные каждого клиента по отдельности. После рукопожатия генерируется временный ключ – PTK – который используется для кодирования передачи этого клиента, но никакого другого. Поэтому даже если вы проникли в сеть, то прочитать пакеты других клиентов вы сможете только, когда перехватите их рукопожатия – каждого по отдельности.

CCMP – протокол шифрования 802.11i созданный для замены TKIP, использует алгоритм AdvancedEncryptionStandard (AES). В отличие от TKIP, управление ключами и целостностью сообщений осуществляется одним компонентом, построенным вокруг AES с использованием 128-битного ключа, 128-битного блока, в соответствии со стандартом шифрования FIPS-197.

WPA2 является заменой WPA. Отличие этих методов в используемых алгоритмах шифрования, WPA2 использует метод шифрования AES. Данный метод позволяет использовать более длинные ключи, что увеличивает безопасность сетии ее устойчивость к взлому.

Алгоритм шифрования AES (*AdvancedEncryptionStandard*), также известный как Rijndael – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). По состоянию на 2009 год AES является одним из самых распространённых алгоритмов симметричного шифрования.Алгоритм состоит из часто повторяющихся раундов шифрования. Сначала на основе 128/192/256-битового ключа получают одиннадцать так называемых ключей раундов, каждый из которых имеет размер 128/192/256 бит. Каждый раунд включает в себя преобразование с использованием соответствующего криптографического ключа, для того чтобы обеспечить секретность шифрования.

Технология Wi-fiполучила широкое распространение в следствие своего удобства иуниверсальности для организации беспроводного доступа к информации. Однако она несёт в себе множество серьёзных угроз информационной безопасности пользователей.Рассмотренные механизмы обеспечения безопасности открытых Wi-ficетей являются наиболее распространенными на сегодня. В тех случаях, когда этого недостаточно существует возможность использования метод ограничения доступа посредством авторизации пользователя, что востребовано в корпоративном секторе.

Библиографический список

1 Wi-Fi сети: проникновение и защита. URL: http://habrahabr.ru/post/224955/

2Protecting Wi-Fi networks. URL: http://www.cisco.com/c/dam/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd807395b9.pdf

3 Белорусов Д.И. Корешков М.С.WiFi-сети и угрозы информационной безопасности. Журнал: Специальная техника, выпуск №6, 2009г.