БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ БЕСПРОВОДНЫХ СЕТЯХ

Кириченко А.В.
Донецкий национальный технический университет

Рассматриваются вопросы безопасности wi-fi сетей. В частности протоколы сетей, принципы их работы, достоинства и недостатки. Также рекомендации по улучшению защиты передачи данных по беспроводным сетям.

Введение

В беспроводной сети возможны следующие способы доступа к информации:

- доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через неё – и к ресурсам LAN;
- подслушивание трафика, извлечение из него конфиденциальной информации;
- искажение проходящей в сети информации;
- воровство интернет-траффика;
- атака на ПК пользователей и серверы сети (например, Denial of Service или даже глушение радиосвязи);
- внедрение поддельной точки доступа;
- рассылка спама, противоправная деятельность от имени вашей сети.
- и самое популярное среди всего выше сказанного - атака ПК или сервера, не относящегося к сети которую он прослушивает.

В последнее время широко используется стандарт 802.11b/g для построения КС.

Благодаря средствам аутентификации и шифрования данных, злоумышленнику почти невозможно получить доступ к сети или перехватить передаваемые данные. В сочетании с мерами безопасности на сетевом уровне протокола (подключение к беспроводной сети парольного доступа и т.д.), а также функциями безопасности тех или иных конкретных приложений (шифрование, парольный доступ и т.д.).

В 802.11 реализованы следующие протоколы безопасности:

1 WEP(Wired Equivalent Privacy)

Первый протокол, реализующий безопасность, используется для обеспечения безопасности передачи данных. Шифрование данных осуществлялось с использованием алгоритма RC4 на ключе со статической составляющей от 40 до 104 бит и с дополнительной случайной динамической составляющей (вектором инициализации) размером 24 бит; в результате шифрование данных производилось на ключе размером от 64 до 128 бит. Перед WEP не стоит задача полностью скрыть передаваемую информацию, требуется лишь сделать ее недоступной для прочтения.

Часть WEP-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамичекая (вектор инициализации), то есть меняющаяся в процессе работы сети. Основной уязвимостью протокола WEP является то, что вектора инициализации повторяются через некоторый промежуток времени, и взломщику потребуется лишь собрать эти повторы и вычислить по ним статическую часть ключа.

Данный вектор является 24-битным. Таким образом, в результате мы получаем общее шифрование с разрядностью от 64 до 128 бит.

WEP работает на втором уровне модели OSI и применяет для шифрования минимум 40-битный ключ, что явно недостаточно.

Проблемы алгоритма WEP носят комплексный характер и кроются в целой серии слабых мест:

- механизме обмена ключами (а точнее, практически полном его отсутствии);
- малых разрядностях ключа и вектора инициализации (Initialization Vector - IV);

– механизме проверки целостности передаваемых данных;
– способе аутентификации и алгоритме шифрования RC4.

Процесс шифрования WEP выполняется в два этапа:

– Вначале подсчитывается контрольная сумма (Integrity Checksum Value -- ICV) с применением алгоритма Cyclic Redundancy Check (CRC-32), добавляемая в конец незашифрованного сообщения и служащая для проверки его целостности принимаемой стороной.
– На втором этапе осуществляется непосредственно шифрование.

Ключ для WEP-шифрования общий секретный ключ, который должны знать устройства на обеих сторонах беспроводного канала передачи данных. Этот секретный 40-битный ключ вместе со случайным 24-битным является входной последовательностью для генератора псевдослучайных чисел.

Существует несколько процедур, при помощи которых возможно улучшить безопасность своей сети.

– Использование длинных WEP ключей, это затруднит хакеру работу. Если оборудование поддерживает 128-битное шифрование, то следует его использовать.
– Периодическая смена ключей.
– Размещение точек доступа за фаерволом, вне локальной сети.
– Использование VPN для всех протоколов, которые могут передавать важную информацию.

Последующим развитием безопасности стало появление WPA.

2 WPA (Wi-Fi Protected Access)

Протокол безопасности, применяемый для обеспечения безопасности в беспроводных сетях. Он был создан в качестве замены для WEP, в которой были обнаружены серьёзные уязвимости. WPA реализует большую часть стандарта IEEE 802.11i и предназначен для замены WEP.

Существует два вида WPA:

– WPA-PSK (Pre-shared key).

Для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети, при его использовании необходимо ввести один пароль на каждый узел беспроводной сети (точки доступа, беспроводные маршрутизаторы, клиентские адаптеры, мосты). До тех пор, пока пароли совпадают, клиенту будет разрешён доступ в сеть.

– WPA-802.1x.

Вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

WPA – это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

– IEEE 802.1X определяет процесс инкапсуляции данных EAP,
– WPA – технология защищённого доступа к беспроводным сетям (Wi-Fi Protected Access),
– EAP – протокол расширенной аутентификации (Extensible Authentication Protocol),
– TKIP – протокол интеграции временного ключа (Temporal Key Integrity Protocol),
– MIC – технология проверки целостности сообщений (Message Integrity Check).

Ключевыми здесь являются новые модули TKIP и MIC.

Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищённой.

Технология проверки целостности сообщений MIC(Message Integrity Check) обороняет от внешнего проникновения и изменения информации. Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая уже давно используется в VPN.

Важно отметить, что механизмы шифрования, используемые для WPA и WPA-PSK, являются одинаковыми. Единственное отличие WPA-PSK заключается в том, что там аутентификация производится по какому-либо паролю, а не по мандату пользователя. WPA-PSK уязвима для атаки методом подбора. Но WPA-PSK снимает путаницу с ключами WEP, заменяя их целостной и чёткой системой на основе цифробуквенного пароля.

3 WPA2

В отличие от WPA, в WPA2 используется более стойкий алгоритм шифрования AES. По аналогии с WPA, WPA2 также делится на два типа: WPA2-PSK и WPA2-802.1x.

Стандартом предусмотрены две функциональные модели: с аутентификацией по IEEE 802.1x, т. е. с применением протокола EAP, и с помощью заранее предопределенного ключа, прописанного на аутентификаторе и клиенте (такой режим называется Preshared Key, PSK). Так как алгоритмы шифрования, использующие процедуру TKIP, уже принято называть WPA, а процедуру CCMP – WPA2, процедура установления соединения и обмена ключами для алгоритмов TKIP и CCMP одинакова.

Сам CCMP (Counter mode (CTR) with CBC-MAC Cipher-Block Chaining (CBC) with Message Authentication Code (MAC) Protocol) так же, как и TKIP, призван обеспечить конфиденциальность, аутентификацию, целостность и защиту от атак воспроизведения. Данный алгоритм основан на методе CCM-алгоритма шифрования AES. Все AES-процессы, применяемые в CCMP, используют AES со 128-битовым ключом и 128-битовым размером блока.

Последним нововведением стандарта является поддержка технологии быстрого роуминга между точками доступа с использованием процедуры кэширования ключа PMK и преаутентификации.

Процедура кэширования PMK заключается в том, что если клиент один раз прошел полную аутентификацию при подключении к какой-то точке доступа, то он сохраняет полученный от нее ключ PMK, и при следующем подключении к данной точке в ответ на запрос о подтверждении подлинности клиент пошлет ранее полученный ключ PMK. На этом аутентификация закончится, т. е. четырех стороннее рукопожатие (4-Way Handshake) выполняться не будет.

Процедура преаутентификации заключается в том, что после того, как клиент подключился и прошел аутентификацию на точке доступа, он может параллельно (заранее) пройти аутентификацию на остальных точках доступа (которые он «слышит») с таким же SSID, т. е. заранее получить от них ключ PMK. И если в дальнейшем точка доступа, к которой он подключен, выйдет из строя или ее сигнал окажется слабее, чем какой-то другой точки с таким же именем сети, то клиент произведет пере подключение по быстрой схеме с закэшированным ключом PMK.

Выводы

Безопасности беспроводных сетей стоит уделять особое внимание. Ведь wi-fi это беспроводная сеть и притом с большим радиусом действия. Соответственно, злоумышленник может перехватывать информацию или же атаковать сеть, находясь на безопасном расстоянии. К счастью в настоящее время существуют множество различных способов защиты и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности.

Литература

[1] Wi-Fi. Материал из Википедии – свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/Wi-Fi

[2] rfc5416. Материал из RFC – серии пронумерованных информационных документов. Электронный ресурс. Режим доступа: http://tools.ietf.org/html/rfc5416

[3] Олифер В.Г.,. Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – Спб.: Питер, 2006. – 958 с.