Московский физико-технический институт

Эссе по курсу «Защита информации»
на тему:

«Безопасность беспроводных сетей стандарта 802.11»

Выполнил:
студент 111 группы
Яковлев Алексей

г. Долгопрудный
2005г

Содержание

Введение

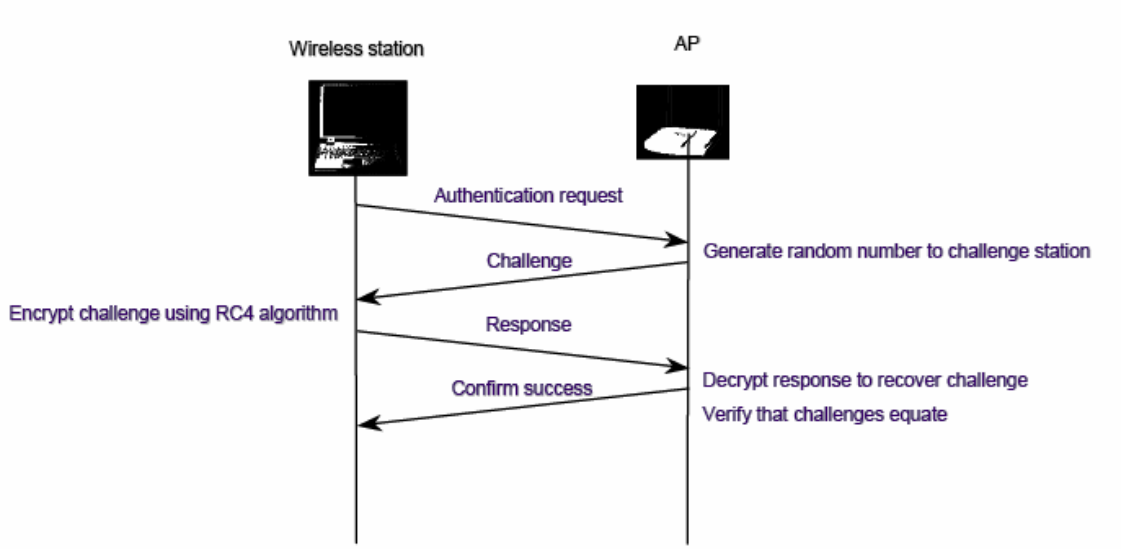
Сети, основанные на протоколе 802.11 , являются наиболее распространенными беспроводными сетями на данный момент. Причём масштабы их развертывания уже не ограничиваются пределами одной комнаты или офиса. Довольно распространены услуги предоставления беспроводного канала в пределах целого города или микрорайона. Вопросы безопасности и конфиденциальности беспроводных сетей не потеряли своей актуальности с момента их появления и до сегодняшнего дня.

В этой работе будет рассмотрен исторический ход развития механизмов защиты от несанкционированного доступа беспроводных сетей 802.11. Обзор начинается описанием основных механизмов защиты «старых» протоколов 802.11a,b и заканчивается самым современным на сегодняшний день протоколом 802.11i.
Первоначально, основным встроенным механизмом защиты беспроводных сетей была технология WEP (Wired Equivalent Privacy - секретность на уровне проводной связи).

WEP (Wired Equivalent Privacy)

Исходный 802.11 предусматривает режим работы вообще без всякого шифрования («открытая аутентификация»), клиентской станции достаточно знать SSID (Service Set Identity - идентификатор комплекта услуг) для прохождения аутентификации. WEP здесь не используется. Причём этот SSID легко получить, прослушивая сеть сниффером.
Другой режим работы 802.11 «Аутентификация на общем ключе»
Данный механизм основан на симметричном шифровании с использованием RC-4. Точка доступа и оконечная станция должны заранее договориться об одном общём секретном ключе. Аутентификация происходит следующим образом:

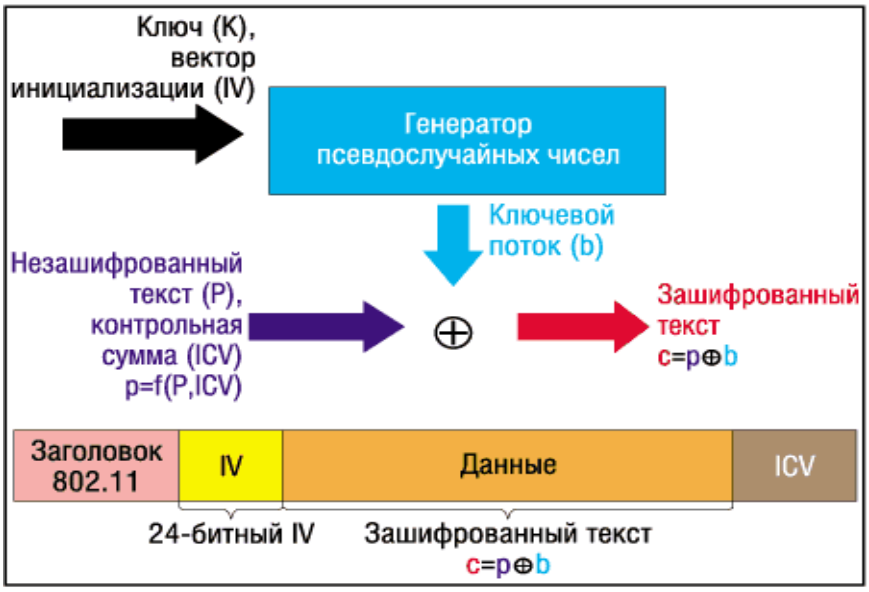
1) Оконечная станция шлёт запрос на аутентификацию
2) Точка доступа генерирует «оказию» и пересылает её оконечной станции
3) Оконечная станция получив «оказию», шифрует её с помощью алгоритма RC-4 на общем секретном ключе и пересылает зашифрованное сообщение точке доступа.
4) Точка доступа, получив сообщение, расшифровывает его и сравнивает с первоначальной посланной ею оказией. Если они совпадают, то данный клиент считается авторизованным



Очевидно, что данный механизм авторизации – односторонний, оконечная станция не имеет возможности убедиться, что точка доступа именно та, защищённое соединение с которой, ей необходимо получить.

После прохождения авторизации используется потоковое симметричное шифрование (на том же общем секретном ключе, что и авторизация) с 24 битным инициализирующим вектором (IV).

Для обеспечения целостности сообщения вычисляется его контрольная сумма (ICV). Здесь используется алгоритм Cyclic Redundancy Check (CRC-32). После добавления суммы полученный пакет шифруется следующим образом: на вход генератора псевдослучайных чисел поступает секретный ключ (длиной 40 бит) и случайный инициализирующий вектор (длиной 24 бита). Затем выходной поток генератора суммируется по модулю 2 с шифруемым сообщением. (Рис. 2)



Для того чтобы принимающая сторона имела возможность расшифровать полученное сообщение, в

пакет в открытом виде передаётся инициализирующий вектор (IV).

Недостатки («слабости») протокола WEP

1) вектор инициализации имеет малую длину (24 бита) и передаётся в открытом виде. Легко показать, что уже при скорости в 5 Mbps, если принять среднюю длину пакета в 2 kb, то время, через которое повторится инициализирующий вектор, оценивается как $\frac{2^{24}}{5000000\ /(2000\ *8)} \approx$ 15 часов.
2) Все абоненты должны иметь один общий статистический ключ, причём протокол не описывает механизмом его обновления.
3) Клиенты не производят никакой авторизации точки доступа.
4) Контрольная сумма, вычисляемая на основе CRC-32, обладает линейным свойством. Она направлена скорее на обнаружение ошибок при передаче, чем на защиту целостности информации

Рассмотрим самую простую, очевидную атаку (основанную на свойствах RC-4 и малой длине IV) . Предположим, что мы имеем два пакета, IV которых совпадает.
Тогда:
$c_1 = p_1$ XOR b_1; $c_2 = p_2$ XOR b_2
Теперь просто делаем XOR этих двух пакетов, получим:
c_1 XOR $c_2 = p_1$ XOR p_2
(b1 и b2 сократились, так как при использовании RC-4 паре ключ и инициализирующий вектор однозначно соответствует значение b, т.е. в нашем случае $b_1 = b_2$)
Имея теперь XOR двух незашифрованных сообщений. Учитывая тот факт, что сообщения обладают некоторой избыточностью и известна структура пакета, существуют методы по получению каждого из сообщения в отдельности, имея лишь их XOR.
Имея пару «шифротекст – исходное сообщение» и IV возможны варианты разных атак:
1) сделав XOR шифрованного текста и исходного сообщения, получаем ключевую последовательность. Её можно использовать для прослушивания трафика, если данная станция не меняет IV для каждого пакета.
2) попытаться произвести атаку со словарем для определения ключа. Далее, имея ключ, прослушиваем весь дальнейший трафик.

Эти уязвимости WEP давно были известны и привели к разработке новых механизмов защиты беспроводных сетей. На смену WEP пришёл WPA.

802.1X

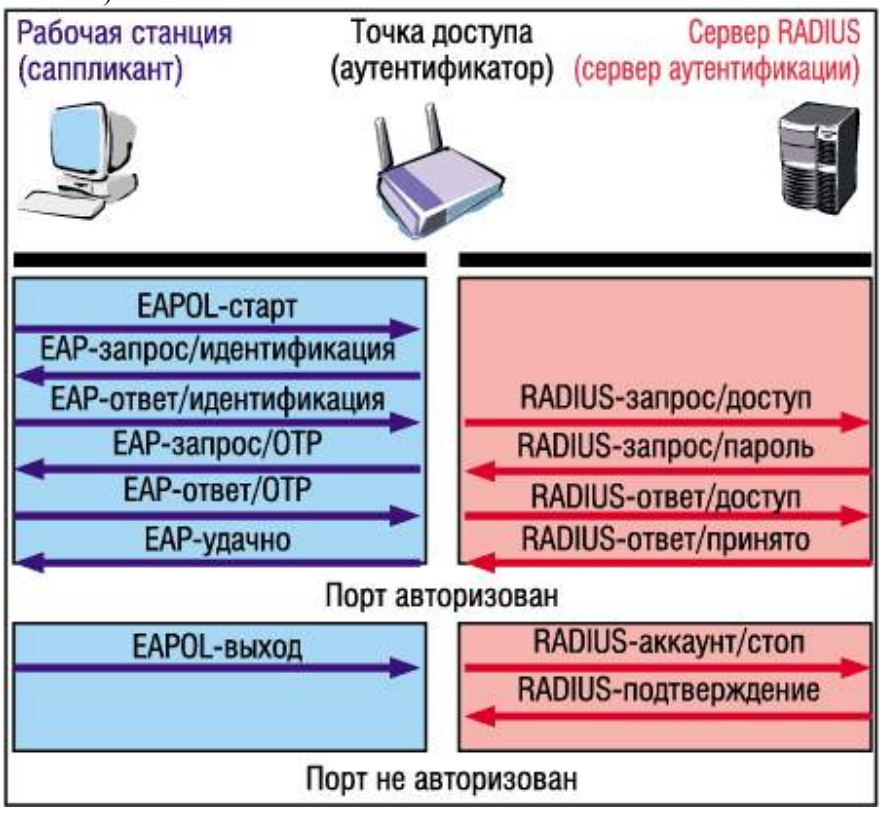
Это стандарт для проведения аутентификации, как в беспроводных, так и в проводных сетях. 802.1X базируется на протоколе расширенной аутентификации EAP (Extensible Authentication Protocol), протоколе защиты транспортного уровня TLS (Transport Layer Security) и сервере RADIUS (Remote Access Dial-in User Service.)

Протокол EAP был создан для стандартизации процедуры аутентификация для продуктов разных производителей. Он позволяет проводить аутентификацию на основе одноразовых паролей, токенов, цифровых сертификатов, смарт-карт, протокола Kerberos. Вследствие данной инкапсуляции, точка доступа не обязана знать о конкретной применяемой методике аутентификации.

802.1X реализует механизм доступа на базе «портов»: полностью исключая возможность доступа неавторизованных пользователей. До прохождения авторизации клиент может передавать только учетные данные и другую информацию, необходимую для прохождения аутентификации.

Причём 802.1X позволяет делать аутентификацию пользователей, а не систем, как это делает WEP.

Рассмотрим механизм аутентификации в общем виде, т.е. ту часть, которая не зависит от выбранного способа. (Возможные методы EAP - это LEAP, PEAP, TTLS и FAST)



Прежде чем получить доступ к сети, клиент должен пройти проверку на сервере RADIUS и только в случае успешной аутентификации ему разрешается доступ в сеть. Процесс аутентификации может протекать, например, следующим

образом (это только пример, в зависимости от типа EAP, типа используемого сервера аутентификации описанный ниже механизм может изменяться)

1) При попадании беспроводного устройства (саппликанта) в зону действия точки доступа, она шлёт устройству запрос.
2) Саппликант отвечает на данный запрос своим идентификатором, который базовая станция пересылает его Radius серверу
3) Сервер аутентификации делает запрос необходимых идентификационных данных через точку доступа.
4) Саппликант отвечает согласно выбранному алгоритму аутентификации. Точка доступа пересылает ответ серверу аутетификации
5) В случае, если саппликант предоставил правильный ответ на запрос, ему пересылается сообщение об успешной авторизации и только после этого аутентификатор «открывает порт», т.е. разрешается не только трафик 802.1X, как это было до прохождения аутентификации.

Протокол 802.1X оказался довольно удачным, он нашёл своё применение как в проводных, так и беспроводных сетях. Он используется в WPA, 802.11i.

Wi-fi Protected Access (WPA)

Протокол WPA (Wi-fi Protected Access — защищенный беспроводный доступ)
Для обеспечения безопасности и целостности в WPA используется протокол TKIP (Temporal Key Integrity Protocol). Данный протокол также использует RC-4 для шифрования, но в нём описан более эффективный механизм управления ключами. Используется 48 битный вектор инициализации, причём его биты меняются каждый раз в соответствии с правилами, описанными в протоколе.
Каждый пакет имеет порядковый номер (48 разрядов), который увеличивается при передаче очередного пакета и используется в качестве вектора инициализации и для генерации ключей. Таким образом, получаем, что каждый передаваемый пакет шифруется своим собственным ключом. (Исключаем коллизионную атаку)
Размер ключа равен 128 битам, т.е. решается проблема короткого ключа в WEP.
Сам ключ получается из базового ключа, MAC-адреса передающего узла и порядкового номера пакета.
Итак, осталось только понять, откуда получается базовый ключ.
Базовый ключ не является статическим, он генерируется каждый раз, когда оконечная станция устанавливает соединение с точкой доступа.
При формировании базового ключа используется хеширование секретного ключа сеанса, случайных чисел, генерируемых и точкой доступа, и клиентской станцией, а также MAC-адресов обоих устройств. Уникальный секретный ключ сеанса точка доступа и оконечная станция получают в результате процесса аутентификации по протоколу 802.1X.
WPA можно рассматривать как некий промежуточный этап от WEP к 802.11i.
Он разработан таким образом, чтобы он мог применяться на старом оборудовании, которое поддерживало WEP. Именно этим фактом можно объяснить применение при шифрование RC-4, а не, например, более устойчивого AES. Но, тем не менее,

уровень безопасности, который обеспечивается данным проколом, как нетрудно заметить, намного выше, чем, например, в WEP.
Сказался так же тот факт, что разработка нового стандарта шла довольно медленно, а необходимость защищать всё разрастающиеся беспроводные сети росла с каждым днём.

802.11i.

25 июня 2004 г. IEEE ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях - 802.11i.
WPA во многом реализовал требования 802.11i. Рассмотрим отличия 802.11i от WEPa

1) использование AES для шифрования (вместо RC-4)
2) система «запоминания паролей»: при выходе пользователя из зоны действия точки доступа и повторного входа в неё, не требуется аутентификация.
3) пре-аутентификация: для ускорения процесса аутентификации при переходе клиента от одной точки доступа к другой.
4) Обязательна двусторонняя аутентификация (802.1X может работать как в двустороннем, так и в одностороннем режиме аутентификации)

Данный стандарт разработан на базе проверенных технологий. Уровень его защищённости вполне удовлетворяет сегодняшнему дню.
Нельзя гарантировать, что он полностью защищен от любых возможных сегодня атак, но практически все уязвимости, существовавшие в WEP и WPA, в 802.11i отсутствуют.
Но для его реализации требуется использование нового, современного оборудования, поддерживающего данный стандарт. В случае если есть необходимость продолжать использование старого оборудования, то можно комбинировать использование разных технологий защиты, например, WEP + VPN (virtual private network).
Данный протокол иногда также называют WPA2, подчёркивая тот факт, что многое в нём взято из WPA.

Литература

[1] Cherita Corbett: Current Flaws, New Standards, and Today's Alternatives: Security for 802.11 Wireless Networks
http://www.prism.gatech.edu/~gt0369c/Security_survey.pdf
[2] Компьютерное Обозрение: Мы вас слушаем, или Безопасность в беспроводных сетях
http://itc.ua/article.phtml?ID=17055&IDw=49&pid=19
[3] Сети, #15/2004: Механизмы защиты беспроводных сетей
http://www.osp.ru/nets/2004/15/055_1.htm

[4] InterlinkNetworks: Introduction to 802.1X for Wireless Local Area Networks
www.lucidlink.com/media/pdf_autogen/ 802_1X_for_Wireless_LAN.pdf