Московский физико-технический институт.
Факультет радиотехники и кибернетики.

Реферат

Безопасность в беспроводных сетях и мобильных устройствах.

Выполнил:
Недайборщ И.Е.
911 гр.
Проверил:

25.04.03

Введение.

Требования к информационной безопасности за последние три десятилетия претерпели три больших изменения. Первым таким изменением стало появление компьютера. Необходимость защиты файлов и информации стала очевидной. Набор средств, созданных для защиты данных и для противодействия хакерским атакам, получил общее название ***компьютерная безопасность***. Вторым большим изменением стало появление распределенных систем, сетей и средств связи для передачи данных. Меры ***сетевой безопасности*** необходимы для защиты передаваемых данных. Третье изменение - это текущее стремительное развитие радиосетей и мобильных телекоммуникаций. Таким образом, ***радиобезопасность*** (wireless security) сегодня высокоприоритетна.

Радиобезопасность.

Любая сеть является объектом существенного риска и проблем с точки зрения безопасности. Они включают в себя такие проблемы, как угрозы физической безопасности, прослушивания и атак самих пользователей сети. Три главных угрозы:

- Дискредитация данных – любая форма раскрытия информации непредусмотренной стороне.
- Неавторизованный доступ – любые средства, при помощи которых неавторизованная сторона получает доступ к ресурсам сети.
- Отказ в обслуживании – действие, предназначенное для блокирования или нарушения нормальной работы сети.

В настоящее время большое внимание уделяется безопасности в беспроводных сетях. Принимаемые в беспроводных и проводных сетях меры безопасности почти одинаковы. Но беспроводные LANs вводят дополнительный набор уникальных элементов обеспечивающих безопасность. Этого требуют специализированные протоколы физического и канального уровней.

Различия в решениях по безопасности для проводных и беспроводных сетей являются следствиями следующих свойств радиосетей:

- Использование специализированных протоколов физического и канального уровней,
- Беспроводные сети не могут быть полностью защищены физическими средствами.
- Связь с существующими сетями осуществляется через точки доступа, которые обеспечивают функцию моста (bridging);
- Возможность роуминга из одной зоны покрытия в другую;
- Уникальные требования к безопасности внутри самой WLAN.
- Специфичные требования к взаимодействию сетей;
- Радио устройства портативны, переносимы и легко могут попасть к злоумышленнику.

Безопасность в WLAN обеспечивают три основных сервиса:

- Аутентификация – процесс проверки подлинности абонента.
- Конфиденциальность – защита информации от несанкционированного доступа (прослушивание).
- Целостность – гарантирует то, что сообщение не было изменено во время передачи по радиоканалу.

Мобильные системы второго поколения.

Цифровые 2G системы, такие как GSM, TDMA и CDMA, используют криптографические методы для аутентификации и конфиденциальности.

Механизмы обеспечения безопасности в GSM реализованы при помощи трех системных элементов:

- идентификационный модуль пользователя (SIM);
- GSM телефон (MS);
- GSM сеть;

На SIM содержится IMSI, индивидуальный ключ идентификации пользователя (Ki), алгоритмы идентификации(A3) и генерации ключа шифрования (A8), а также персональный идентификационный номер (PIN). На GSM телефоне содержится алгоритм шифрования (A5). Алгоритмы шифрования (A3, A5, A8) присутствуют также и в GSM сети. Центр аутентификации (AuC), часть системы операций и поддержки GSM сети, состоит из базы идентификационных и аутентификационных данных пользователей. Эта информация состоит из IMSI, TMSI, идентификатора местности (LAI) и индивидуального ключа идентификации (Ki) каждого пользователя. Такое распределение ключей и алгоритмов шифрования обеспечивает дополнительные меры безопасности как в обеспечении конфиденциальности использования телефона, так и в предотвращении мошенничества.

Рис. 1 показывает распределение скрытой информации по трем системным элементам – SIM, MS, GSM сеть. В GSM сети эта информация размещена в центре идентификации (AuC), домашнем регистре HLR, гостевом регистре VLR. AuC отвечает за генерацию RAND, SRES и Kc, которые размещаются в HLR и VLR для дальнейшего использования в процессах идентификации и шифрования.

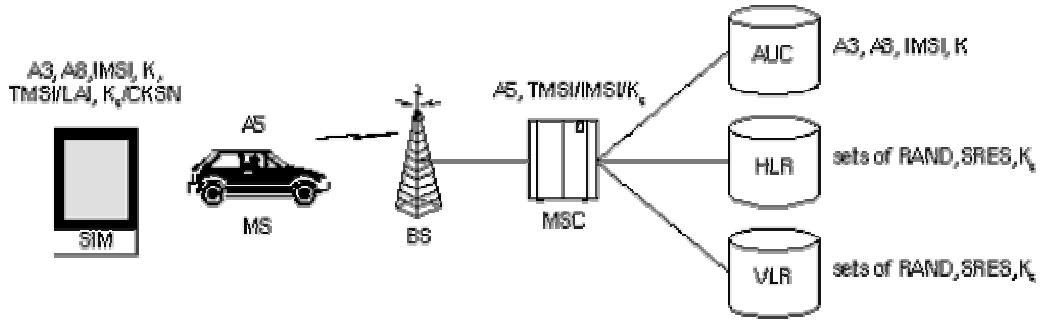

Рис.1

Аутентификация.

GSM сеть идентифицирует подлинность пользователя, используя механизм отклик-отзыв. На MS посылается случайное 128-битное число (RAND). Мобильная станция вычисляет 32-битный подписанный отклик абонента (SRES), основанный на шифрации RAND при помощи алгоритма A3, с использованием ключа Ki. После получения подписанного ответа (SRES) от абонента, GSM сеть повторяет вычисление для проверки подлинности абонента. Важно отметить, что индивидуальный ключ идентификации абонента Ki никогда не передается по радио каналу. Если полученный SRES совпадает с вычисленным значением, то MS считают успешно аутентифицированной. Если же значения не совпадают, то соединение разрывается и мобильной станции указывается на ошибку при аутентификации. Рис. 2 показывает механизм идентификации.

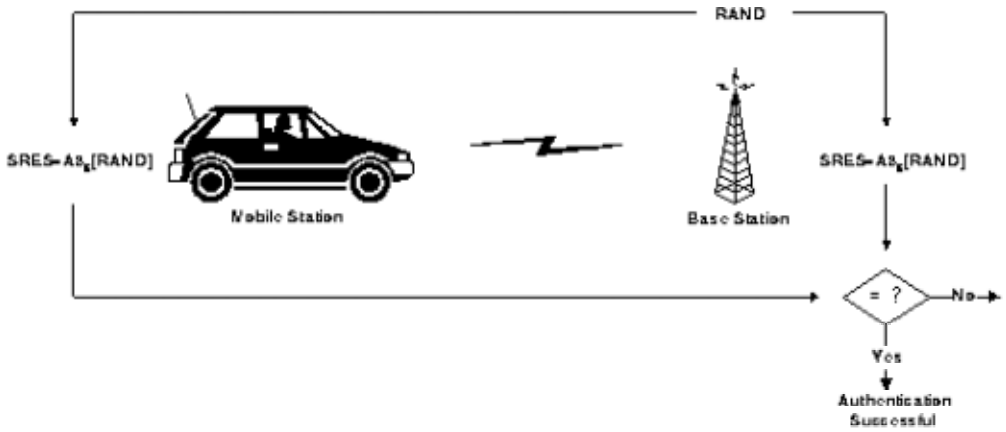

Рис.2

Конфиденциальность данных.

SIM карта содержит алгоритм генерации ключа шифрования (A8), который используется для создания 64-битного ключа шифрования (Kc). Этот ключ вычисляется с использованием того же, что и при аутентификации, случайного числа (RAND), и индивидуального идентификационного ключа абонента Ki. Дополнительная степень безопасности обеспечивается возможностью смены ключа, что делает систему более стойкой к прослушиванию. Ключ Kc можно изменять периодически, если этого требует соображения безопасности. Рис 3. показывает вычисление ключа Kc.

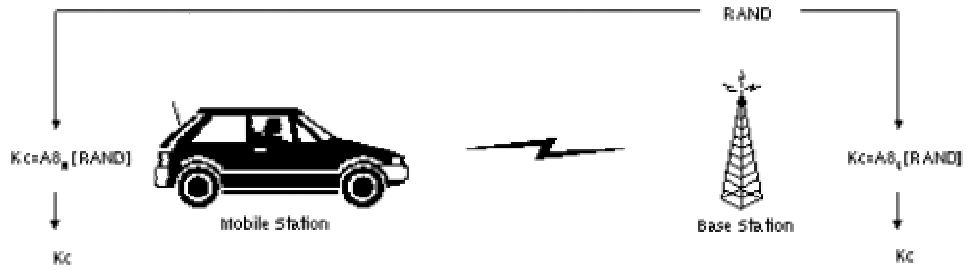

Рис.3

Вычисление ключа Kc, как и при аутентификации, производится внутри SIM. Поэтому такая секретная информация, как идентификационный ключ Ki, никогда не раскрывается SIM картой.

Шифрация голоса и данных между мобильной станцией и сетью выполняется при помощи алгоритма A5. Шифрация информации инициируется командой от GSM сети на переход в режим шифрования. Получив такую команду, мобильная станция начинает шифровать отправляемые и дешифровать получаемые данные, используя алгоритм A5 и ключ Kc. Рис.4 показывает механизм шифрования.

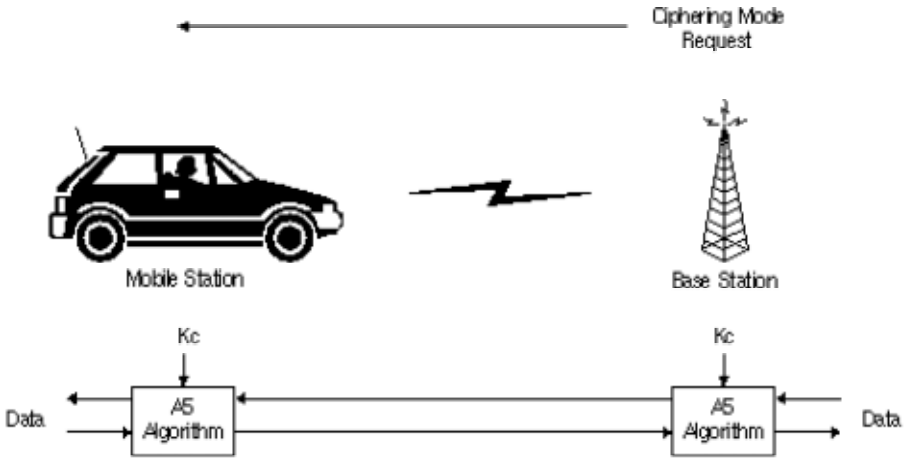

Рис.4

Конфиденциальность идентификатора абонента.

Для того, чтобы гарантировать конфиденциальность абонента, используется временный идентификатор мобильного абонента (TMSI). TMSI посылается на мобильную станцию после проведения процедур аутентификации и начала шифрования. TMSI действителен только в местности, в которой был назначен. Для связи за ее пределами, к TMSI нужно добавлять идентификатор местности (LAI).

Хотя алгоритмы A3, A5, A8 являются закрытыми, кое-что про них известно:

- A3 и A8 алгоритмы являются зависимыми от ключа, однонаправленными хеш-функциями.

Они похожи по функциональности и обычно реализуются в виде одного алгоритма, называемого COMP128.

- A5 – потоковый шифр, состоящий из трех линейных регистров с обратными связями со степенями 19, 22, 23.

Сумма степеней регистров 64. Используется 64-битный сессионный ключ для инициализации начального состояния регистров.

По слухам этот алгоритм имеет эффективную длину ключа 40 бит.

Мобильные системы третьего поколения.

Развертывание 3G систем, таких как UMTS и CDMA2000, будет основано на IP сетях, т.е. открытых сетях, которые не разделяют сигнализацию от данных. Это может позволить злоумышленникам получить доступ к данным и/или сетевым ресурсам. В 3G системах будет применяться Internet-подобная система безопасности. Но поскольку системы третьего поколения должны будут поддерживать роуминг с системами второго поколения, то требования совместимости, возможно, несколько понизят уровень безопасности 3G систем.

Смарт-карта (USIM) также будет являться непременным персональным модулем безопасности. Как и в GSM, алгоритмы аутентификации и генерации ключа будут находиться на этой карте.

Добавлены новые свойства, чтобы учесть изменения в сетевой архитектуре и обезопасить новые сервисы, предоставляемые 3G. По сравнению с GSM, были сделаны два главных усовершенствования:

- Используемая криптография усилена введением 128-битных ключей. Установлены 128-битный ключ шифрования и 128-битный ключ целостности. Шифрация производится по алгоритму Kasumi.
- Для установления подлинности и абонента, и базовой станции введена взаимная аутентификация при соединении. Аутентификация для абонентов, проходящих между различными сетями, также защищается при помощи криптографической системы с открытым ключом. Алгоритм основан на Rijndael.

По сравнению с GSM, важная сигнализация шифруется. Криптографическая проверочная сумма используется в обоих направлениях. Меры безопасности при сигнализации между различными сетями также будут стандартизированы.

Беспроводные локальные сети.

Меры безопасности в 802.11 беспроводных сетях.

В спецификации IEEE 802.11 определены несколько служб, обеспечивающих безопасность рабочей среды. Эти сервисы по большей части предоставляются протоколом Wired Equivalent Privacy (WEP) для защиты данных во время передачи по радио каналу между клиентами и точками доступа.

Три основных сервиса, описанные IEEE для WLAN:

- Аутентификация;
- Конфиденциальность данных;
- Целостность данных;

Аутентификация.

Спецификация IEEE 802.11 определяет два способа проверки достоверности радиопользователя, пытающегося получить доступ к сети:

- Аутентификация открытых систем;
- Аутентификация с общим ключом.

Один способ (аутентификация с общим ключом) основан на криптографии, а другой нет. Метод аутентификации открытых систем не является в полном смысле аутентификацией, точка доступа принимает мобильную станцию без проверки подлинности станции. Важно отметить

также, что аутентификация лишь однонаправленная: аутентифицируется только мобильная станция. Мобильная станция должна верить, что она связывается с реальной AP.

Систематика методов аутентификации 802.11 изображена на рис.5

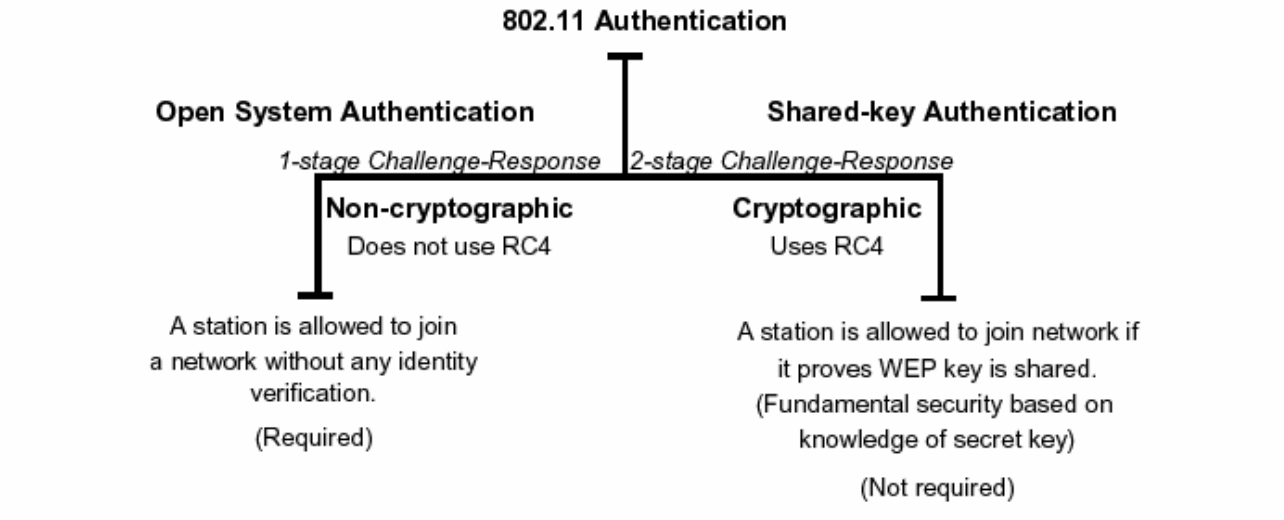

Рис.5

В методе аутентификации открытых систем, клиент аутентифицируется, если он просто присылает MAC адрес во время обмена сообщениями с точкой доступа. Очевидно, что без использования криптографической проверки подлинности, аутентификация по методу открытых систем сильно уязвима и, практически, провоцирует неавторизованный доступ. Но этот метод является единственной требуемой формой аутентификации по спецификации 802.11.

Аутентификация с общим ключом является криптографическим методом аутентификации. Это простая схема «оклик-отзыв», основанная на проверке знания клиентом общего секрета. В этой схеме, как изображено на рис.6, сгенерированный точкой доступа случайный запрос посылается радио клиенту. Клиент, используя криптографический ключ, общий с AP, шифрует запрос и возвращает результат точке доступа. Точка доступа дешифрует результат, вычисленный клиентом, и, если дешифрованное значение совпадает с отправленным случайным запросом, разрешает доступ. В качестве алгоритма для криптографических вычислений и для генерации 128-битного случайного запроса используется потоковый шифр RC4, созданный Ron Rivest в MIT. Важно отметить, что описанный метод аутентификации представляет собой простейший криптографический метод и не обеспечивает взаимную аутентификацию. То есть, клиент не аутентифицирует AP, а, значит, нет никаких гарантий, что клиент связывается с легитимной AP.

И нет ничего удивительного в том, что известны (и уже давно) слабости простейших односторонних схем «оклик-отзыв». Они подвержены множеству видов атак, включая печально знаменитую атаку «человек посередине». Более того, спецификация IEEE 802.11 не требует даже такой аутентификации.

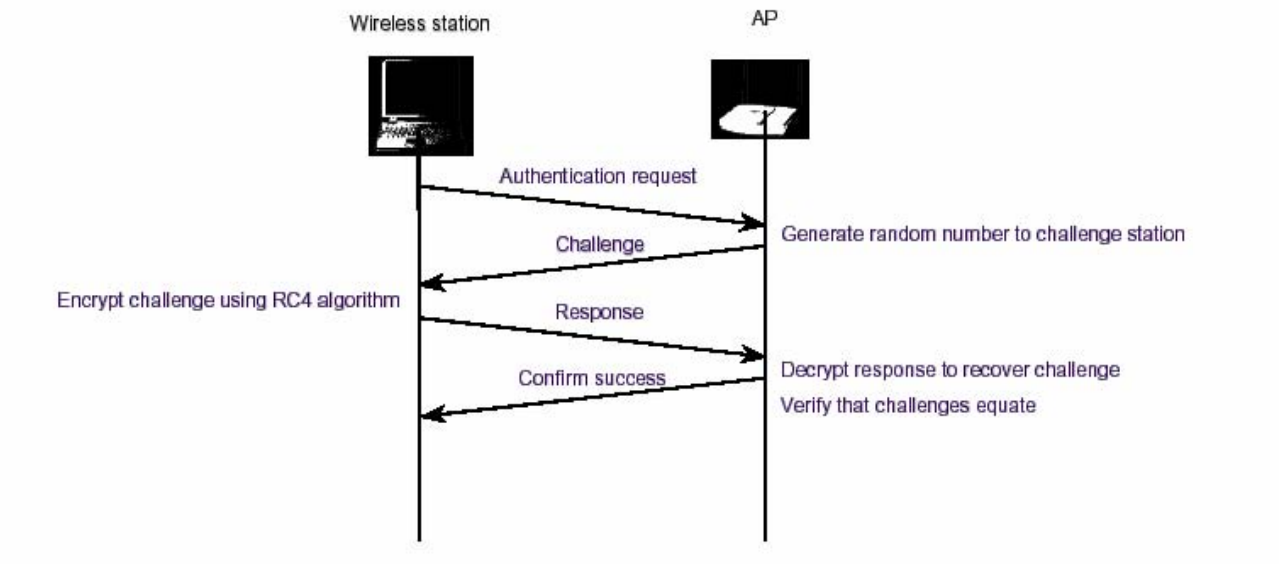

Рис.6

Конфиденциальность.

В стандарте 802.11 конфиденциальность обеспечивается использованием криптографического метода для радиоинтерфейса. Для обеспечения конфиденциальности в WEP используется симметричный, потоковый алгоритм шифрования RC4, генерирующий псевдослучайную ключевую последовательность. Этот ключевой поток просто прибавляется по модулю 2 (XOR) к передаваемым данным. По методу WEP данные могут быть защищены от раскрытия во время передачи по радиоканалу. WEP применяется

ко всем данным, находящимся выше 802.11 WLAN уровней, для того, чтобы защитить трафики TCP/IP, IPX, HTTP и т.д.

В стандарте 802.11 описана поддержка только 40-битных общих ключей. Тем не менее, несколько производителей предлагают нестандартизированные расширения WEP, которые поддерживают длины ключей от 40 до 128 бит. В остальном, в этих решениях все одинаково.

Исследования показали, что ключи длиной больше 80 бит при корректной реализации алгоритма могут сделать грубый криптоанализ неосуществимым. Для 80 битных длин число возможных ключей превышает возможности современных компьютеров. На практике, большинство WLAN реализаций основано на 40 битных ключах. Причем, недавние атаки показали, что в приложении к конфиденциальности WEP, к несчастью, уязвим для некоторых типов атак независимо от размеров ключа.

Концептуально алгоритм изображен на рис.7

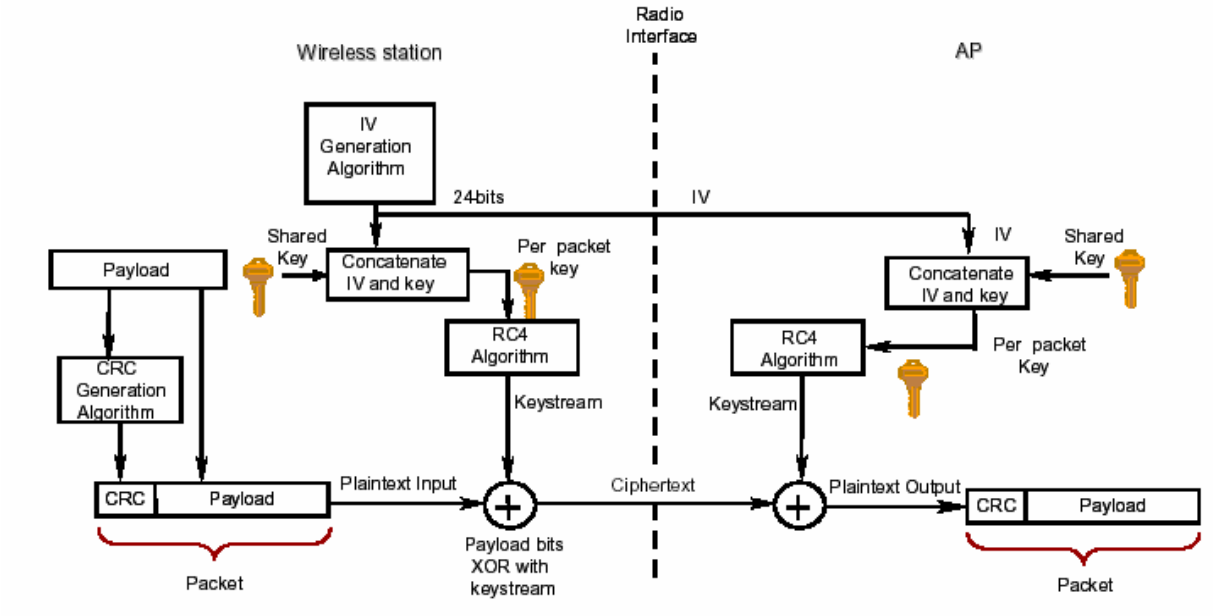

Рис.8

Целостность.

Спецификация IEEE 802.11 также описывает средства обеспечения целостности данных, передаваемых между радиоклиентами и точками доступа. Эта мера безопасности применяется, чтобы отклонять любые сообщения, которые были изменены противником во время передачи по радиоканалу. Этот метод использует контроль при помощи избыточного циклического кода. Как изображено на рисунке (см. выше), CRC-32 (или последовательности проверки кадра FCS), вычисляется для каждого кадра полезных данных перед передачей.

Запечатанный таким образом пакет затем шифруется с использованием ключевого потока RC4. На принимающей стороне выполняется дешифрование и заново вычисляется CRC, которое затем сравнивается с CRC, пришедшим с сообщением. Если эти две CRC не равны друг другу, то это означает нарушение целостности и пакет уничтожается.

Как и в случае с обеспечением конфиденциальности целостность в 802.11 уязвима по отношению к некоторым типам атак независимо от длины ключа. Фундаментальным недостатком в схеме обеспечения целостности в WEP является то, что простейшая CRC не является таким криптографически безопасным механизмом, как, к примеру, хэш-функция.

Проблемы в системе безопасности стандарта 802.11

Несколько групп специалистов по компьютерной безопасности обнаружили ряд брешей в безопасности 802.11, которые позволяют мошенникам разрушить безопасность WLAN. Рассматривались пассивные атаки направленные на дешифрование трафика, основанные на статистическом анализе, активные атаки направленные на ввод нового трафика от неавторизованных мобильных станций, активные атаки на дешифрование трафика (к примеру основанные на обмане точки доступа), а также атаки строящие словари. Атаки на построение словаря возможны после анализа достаточного количества трафика в загруженной сети.

Ряд проблем связанных с WEP приведен в таблице 1:

Таблица 1

1.*Слишком короток (или вообще статичен*)	Использование коротких 24-битных IVs приводит к повторению ключевого потока в течение достаточно короткого промежутка времени, особенно в загруженных сетях. Повторения позволяют дешифровать данные при помощи атак средней сложности.

2.*Короткие криптографические ключи.*	40-битные ключи не отвечают требованиям к безопасности системы. Обычно подразумевается, что длины ключей должны быть больше 80 бит. Чем больше длина ключа, тем более устойчива система к грубому криптоанализу.
3.*Одинаковые криптографические ключи используются несколькими пользователями*	Использование статичных WAP ключей (несколько пользователей в сети могут использовать одинаковые ключи в течение долгого времени) – хорошо известная слабость в системе безопасности. Этот недостаток обусловлен отсутствием средств управления ключами в WEP. Если, к примеру, будет утерян или украден ноутбук, то ключ будет дискредитирован вместе со всеми другими компьютерами использующими этот ключ. Более того, если несколько станций использует один и тот же ключ, то можно достаточно быстро собрать достаточно трафика для аналитической атаки.
4.Не предусмотрено возможности автоматического или достаточно частого обновления ключей	Криптографические ключи должны меняться достаточно часто, чтобы помешать грубому криптоанализу.
5.RC4 обладает недостатком при составлении ключа и, к тому же, несоответствующим образом используется в WEP.	Комбинация открытости 24 ключевых битов в IV и недостатков в первых нескольких байтах ключевого потока RC4 позволяет реализовать эффективные атаки, открывающие ключ. В большинстве других приложений, использующих RC4, этот недостаток не проявляется, поскольку они не открывают ключевых битов и не переназначают ключ при шифровании каждого пакета.
6.Недостаточное обеспечение целостности данных.	CRC32, как и другие линейные блочные коды, неуместен для обеспечения криптографической целостности. Возможно изменение сообщения. Необходима криптографическая защита для предотвращения умышленных атак.
7.Отсутствие аутентификации пользователя.	Идентифицируется лишь само устройство. Украденное устройство может получить доступ к сети.
8.Идентификация устройства представляет собой простой «отклик-отзыв» с общим ключом.	Однонаправленная «отклик-отзыв» аутентификация – объект для атак типа «человек посередине». Требуется взаимная идентификация для контроля легитимности пользователя и сети.
9.Отсутствует идентификация клиентом точки доступа.	Для гарантирования легитимности точки доступа и предотвращения появления мошеннических точек доступа клиенту нужно идентифицировать AP.

.

Вывод.

Данный обзор показывает, что уровень безопасности в наиболее популярных современных беспроводных (802.11) и мобильных (GSM) сетях недостаточно высок. Для создания более безопасных систем необходим более продуманный выбор протоколов, стандартов, криптографических методов. Остается надеяться, что в разрабатываемых сейчас новых системах (3G, 802.11i и т.д.) это будет сделано, и меры безопасности будут на достаточно высоком уровне.

В ближайшем будущем мы станем свидетелями стремительного развития беспроводных технологий, устройств и оборудования. Без сомнения, аспекты безопасности ускорят это развитие, и окажут на информационные системы большое влияние.

Ссылки.

1. Kaj J. Grahn, Göran Pulkkis, Jean-Sebastien Guillard. *Security of Mobile and Wireless Networks,* July 2002.
2. Tom Karygiannis, Les Owens. *Wireless Network Security*, November 2002.
3. Chih-Chun Chang. *Overview of Wireless Security*, 2002.