Юрий Бубнов, гр. 914

Analyzing the Security of 802.11 Wireless Networks

1.1 Обзор Wireless сетей

WLAN технология и WLAN индустрия появились в середине 80х, когда Федеральная комиссия связи (США, Federal Communications Commission, FCC) сделала доступной соответствующие радио частоты. В 80х и в начале 90х рост индустрии был относительно низок. Однако сегодня WLAN технологии испытывают огромный рост. Существует несколько предчин роста, но основной является возростание пропускной способности стандарта 803.11.

1.2 История развития

Motorola разработала одну из первых WLAN систем - Altair. Тем не менее, ранние WLAN технологии имели несколько проблем, мешающих их развитию. Такие LAN системы были дорогие, обеспечивали низкие скорости передачи, были склонный к вмешательству в другие радио частоты, и были разработаны главным образом для взаимодействия с приборами той же фирмы. IEEE начал разработку 802.11 в 1990, чтобы “разработать Medium Access Control (MAC) и Physical Layer (PHY) спецификации для беспроводных соединений для стационарных, портативных и мобильных станций”. В 1997, IEEE впервые одобрило международный стандарт связи 803.11. Затем, в 1999, IEEE одобрило 802.11a и 802.11b стандарты безпроводных сетей. Цель состояла в том, чтобы создать технологию, основанную на стандартах, которая могла охватывать многие типы кодирования, частоты, и приложения, подобные тому, что было сделано с 802.3 стандартами локальных сетей на основе протокола CSMA-CD. 802.11a стандарт использует мультиплексирование на ортогональном разделении частоты (OFDM), чтобы уменьшить вмешательство от других станций. Эта технология использует 5GHz частоты и может обрабатывать данные до 54Mbps. Прямым потомком 803.11a технологии является 803.11b технология.

1.3 Частроты и скорости предечи данных

IEEE развивал 802.11 стандарты, для обеспечить организации wireless сетей подобно сетям на основе протокола CSMA-CD, которые доступны много лет. 802.11b стандарт использует нелицинзированную 2.4GHz-2.5GHz ISM полосу частот, используя технологию с прямой последовательностью спектров. ISM полоса стала популярной для безпроводной связи, потому что она доступна во всем мире. 802.11b стандарт сосредоточен на MAC и PHY протоколах. 802.11b WLAN технология позволяет передавать данные со скоростью до 11Mbit в секунду. Это делает его значительно быстрее чем первоначальный IEEE 802.11 стандарт (который посылает данные со скоростью до 2Mbps).

1.3 Архитектура

IEEE 802.11b стандарт позволяет устройствам создавать как peer-to-peer (P2P) сети, так и сети, основанные на стационарных точках доступа (access points, AP), с которыми связываются мобильные узлы. Таким обазом, стандарт определяет две основы сетевой топологии: сеть инфраструктуры и специальная сеть. Сеть инфраструктуры, как предполагается, расширяет диапазон проволочного LAN к беспровдным ячейкам. Портативная ЭВМ или другое передвижное устройство могут двигаться от ячейки до ячейки при поддержании доступа к ресурсам LAN. Ячейка - область, охваченная AP и называется основным сервисным набором (basic service set, BSS). Совокупность всех ячеек сети инфраструктуры называется расширенным сервисным набором (extended service set , ESS). Эта топология полезна для обеспечения беспроводного охвата областей университетского городка или здания. Устанавливая множестро AP с пересекающимеся областями покрытия, можно достигнуть широкой зоны обслуживания.

WLAN оборудование включает в себя беспроводные станции клиента, которые используют радиомодемы, чтобы связаться с AP. Станции клиента обычно оборудуются безпроводной сетевой картой, который состоит из радиомодема и логической части, чтобы обеспечить взаимодействие машины клиента и программным обеспечением. AP включает в себя радио-модем на одной стороне и мост к магистральной сети на другой. AP, стационарное устройство, которое является частью проводной инфраструктуры, является аналогом базовой станции в сотовой связи. Вся связь между клиентскими станциями и между клиентами и сетью проходит через AP. Основная топология WLAN изображена на Ритунке 1.

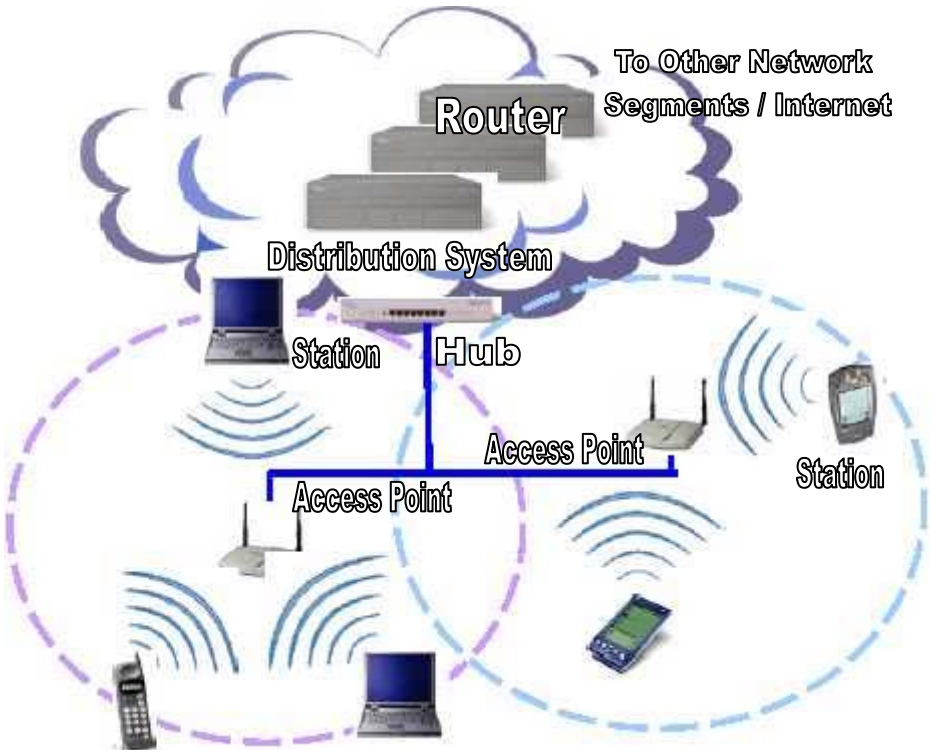


Рисунок 1. Основы 802.11b Wireless LAN технологии

Хотя большинство WLAN работает в режиме и архитектуре "инфраструктуры", описанной выше, возможна также другая топология. Это второя топологии, специальная сеть связывает передвижные устройства, которые находятся в той же самой области (т.е., в той же самой комнате). В этой архитектуре, станции клиента сгруппированы в отдельную географическую область и могут быть связаны в сеть без доступа к сети инфраструктуры. Связанные устройства в специальном режиме указываются как IBSS (независимый основной сервисный набор, independent basic service set). Специальная топология изображена на Рисунке2.

Специальная конфигурация подобна peer-to-peer сети, в которой не требуется что бы какой-то узел функционировал как сервер. Как специальный WLAN, портативные ЭВМ, рабочие станции и другие 802.11 устройства могут совместно использовать файлы без использования AP.

1.4 Компоненты Wireless сети

WLAN включает два типа оборудования: беспроводная станция и точки доступа. Станция, или клиент, являются, обычно, портативной ЭВМ или карманным компьютером с беспроводной сетевой картой. WLAN клиент может также быть настольным компьютером, на производственном этаже, или другой публичной области. Беспроводная сетевая карта обычно вставляется в PCMCIA или в USB порт. NIC используют радио частоты или инфракрасные лучи, чтобы установить подключения к WLAN. Точка

доступа, которое действует как мост между беспроволочными и обычными сетями, обычно включает радио часть, сетевой интерфейс типа 802.3, и программное обеспечение. Функции AP, как основной станции для беспроводной сети, соединять беспроволочные станции с обычной сетью.

1.5 Расстояния

Надежный диапазон охвата для 802.11b WLAN зависит от нескольких факторов, включая требуемую скорость передачи данных, источники радио интерференции, физической области и ее характеристики, мощности, связи, и использованной антенны. Теоретические диапазоны - от 29 метров (для 11Mbps) в закрытой области офиса до 485 метра (для 1Mbps) в открытой области. Однако, типичный диапазон для обеспечения связи 802.11b - приблизительно 50 метров в закрытом помещении. Всенаправленной антенной на открытом воздухе, обеспечение связи может быть увеличено до 400 метров. Диапазон 400 метров, почти 1/4 мили, делает WLAN идеальную технологию для применения в университетских городках.

AP могут также обеспечивать функцию "соединения". Соединение подключает две или более сети вместе и позволяет им связываться, чтобы обмениваться сетевым трафиком. Соединение позволяет point-to-point или multipoint конфигурацию. В архитектуре point-to-point два LAN связаны с друг другом через соответствующие AP LAN. В multipoint соединении, одна подсеть LAN связана с несколькими другими подсетями LAN через каждое сетевую AP.

Предприятия могут использовать соединение, чтобы сделать LAN между различными зданиями в городке. AP обычно помещаются на вершине зданий, чтобы достигнуть большего охвата. Типичное расстояние, по который AP может быть связано с другим - приблизительно 2 мили

2 Преимущества

"Непривязанный" метод WLAN связи, делает их очень привлекательный, что может привести к увеличеннию эффективности и уменьшению стоимости.

WLAN предлагают четыре выгоды пользователям:

1. UserMobility - Пользователи может обращаться к файлам, сетевым ресурсам, и Internet без необходимости физически соединяться с сетью. Пользователи могут быть мобильны и все же иметь доступ в реальном времени к LAN предприятия.
2. Быстрая установка - время, требуемое для инсталляции уменьшен, потому что сетевые подключения могут быть сделаны без перемещения или добавления проводов.
3. Гибкость - Предприятия могут также быть удовлетворены гибкостью установки и развертывания WLAN по мере их необходимости. Пользователи могут быстро развертывать небольшие WLAN для временного использования: конференции, показа, или встречи.
4. Масшабируемость - WLAN сетевая топология легко конфигурируется, чтобы выполнить определенные прикладные задачи и масштабиррується от маленьких P2P сетей до очень больших сетей предприятия, которые допускают передвижения в широкой области.

Из-за этих фундаментальных приемуществ, рынок WLAN увеличился за прошлые несколько лет, и WLANS все еще возростает в популярности. IDC утверждает, что продажи WLAN технологии, будет больше чем $ 3.2 миллиардов к 2005. WLAN становятся реальной альтернативой традиционным решениям. Фактически, больницы, университеты, аэропорты, гостиницы, и магазины используют WLAN для доступа к Internet.

3 Безопасность 802.11 Wireless LANS

IEEE 802.11b определяет несколько служб для обеспечения безопасности среды. Службы безопасности обеспечиваются в значительной степени WEP протоколом, чтобы защитить данные канального уровня в беспроводной передачи между точками доступа и клиентами. То есть WEP не обеспечивает непрерывную защиту, а только для беспроводной части подключения.

3.1 Безопасность, реализоваееая в стандарте 802.11

В стандарте IEEE определены три основных службы безопасности для WLAN:

1. Идентификация - первичная цель WEP состояла в том, чтобы обеспечить службу безопасности, которая проверяет идентичность общающихся станций клиента. Это должно обеспечить управление доступа к сети посредством отказа в доступе станциям, которые не могут подтверждать подлинность должным образом.

2. Конфиденциальность - Конфиденциальность, или секретность, была вторая цель WEP. Было разработано, чтобы обеспечить “секретность, достигнутую в обычной сети “. Цель состояла в том, чтобы предотвратить “пассивные атаки” (просмотр данных неидентифицированными клиентам).
3. Целостность - Другая цель WEP, как службы безопасности, состояла в том чтобы гарантировать, что сообщения не изменены в процессе передачи между клиентами и точкой доступа (активное нападение).

Стандарт не предполагал другие службы безопасности типа ревизии, авторизации.

3.1.1 Идентификация

802.11b спецификация определяет два типа средств, чтобы определить пользователей, пытающихся получить доступ к сети. Одни средства основаны на шифровании, а другие - нет. Для нешифрованого подхода, существует два различных способа идентифицировать клиента. Однако, оба из этих подходов основанны на механизме идентефикации. Беспроводнве станции, требующие доступ просто отвечают Сервисным Идентификатором Набора (SSID) wireless. Эти два пути упомянуты как Open System authentication and Closed System authentication.

С Open System, клиент определен, если он просто отвечает с пустой строкой для SSID - следовательно, название " ПУСТАЯ идентификация." Со вторым методом, Closed Authentication, клиенты должны ответить с фактическим SSID сети. То есть клиенту позволяют доступ, если это отвечает с правильной 32-байтной строкой, опознающей BSS сети. Это примитивный тип идентификации - только схема идентификации. Фактически, никакая из этих двух схем не предлагают нормальную защиту против неправомочного доступа.

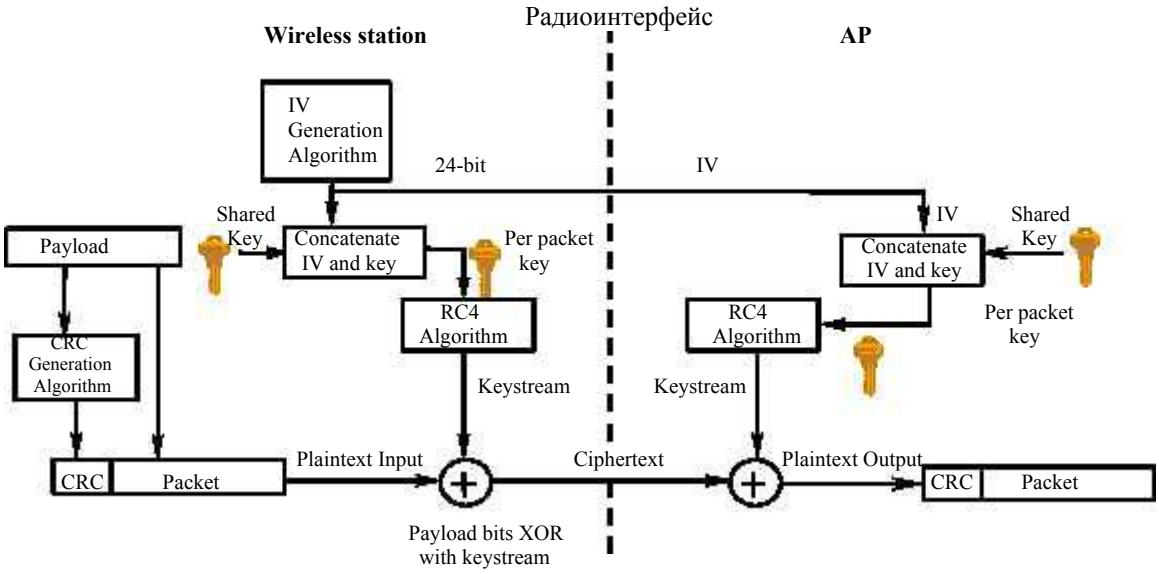
Идентификация публичным ключем - криптографическая методика идентификации. Это схема, основанная на том, имеет ли клиент публичный ключ. В этой схеме вызов производится точкой доступа и посылается клиенту. Клиент, используя ключ (ключ WEP) зашифрует вызов и возвращает результат AP. AP расшифровывает результат, вычисленный клиентом и позволяет доступ только, если расшифрованное значение то же самый как переданный вызов. Алгоритм, используемый в вычислении - RC4, разработанный Роном Ривестом MIT. Этот опознавательный метод - элементарная криптографическая методика, и это не обеспечивает взаимную идентификацию. То есть клиент не подтверждает подлинность AP и поэтому нет никакой гарантии, что клиент поддерживает связь с нужной AP и сетью.

3.1.2 Секретность

Стандартная конфиденциальность в 803.11b поддерживается с помощью криптографических методов. WEP методика использует RC4 с симметричным ключом, алгоритм потокового шифрования, чтобы сгенерировать гамму шифра. Этот “поток” добавляется по модулю 2 к данным, которые будут переданы. По WEP методике, данные могут быть защищены от раскрытия в процессе передачи. WEP применяется ко всем данным верхних уровней, чтобы защитить трафик типа TCP / IP, IPX, и HTTP.

WEP поддерживает размеры ключей от 40-бит до 104-бит. 104-разрядный ключ WEP, например, с 24-битом IV становится 128-разрядным ключом RC4. Вообще, увеличение размера ключа увеличивает защищенность методики. Исследование показало, что размеры ключей больших чем 80-бит делают грубую силу криптоанализа невозможной задачей. Однако, практически, большинство WLAN использует 40-разрядные ключи. Кроме того, недавние атаки показали, что подход WEP, к сожалению, уязвим к некоторым атакам независимо от размера ключа.

Безоапсность WEP:



3.1.3 Целостность

IEEE 802.11b спецификация, также обеспечивает целостность данных, переданных между клиентами и точками доступа. Эта служба безопасности была разработана, чтобы отклонить любые сообщения, которые были изменены(заменены) активным противником. Эта методика использует зашифрованную CRC. Как изображено в диаграмме выше, CRC-32, или последовательность проверки фрейма, вычисляется для данных до передачи. Затем пакет шифруется, используя поток ключей RC4. Получатель, расшифровывает, и вычисляет CRC повторно для полученного сообщения. Вычисленный CRC, стравнивается с вычисленным на отправителе. Если CRC не равны, то есть “полученно с ошибкой”, то это указывает на нарушение целостности и пакет будет отвергнут. Как и с службой секретности, к сожалению, целостность в 802.11b уязвима к некоторым нападениям независимо от размера ключа.

Спецификация, к сожалению, не предполагает какие-нибудь средства для управления ключами. Поэтому, генерация, распределение, сохранение, загрузка, архивирование, ревизия, и уничтожение оставлено тому, кто развертывает WLAN. Ключевое управление (вероятно наиболее критический аспект системы) для 802.11b полагается на пользователей сети. В результате, в WLAN может оказаться много видов уязвимостей. Эти уязвимости включают ключи WEP, которые не являются уникальными, никогда не заменяются, слабые ключи (все ноли, все, основанные на легко предполагаемых паролях, или другие подобные тривиальные образцы). Так как управление ключами слабо реализовано в 802.11b, WEP-ЗАЩИЩЕННЫЕ сети страдают от неспособности масштабироваться. Другими словами, даже если предприятие признает необходимость изменения ключей, задача будет огромна в большой WLAN среде. Например, большой университетский городок может иметь 15000 AP. Производство, распределение, загрузка, и управление ключами для среды этого размера - наиболее существенная проблема.

3.2 Проблемы в стандарте безопасности IEEE 802.11b

Как упомянуто выше, WEP протокол используется в WLAN основанных на 802.11. WEP, в свою очередь, использует RC4 алгоритм с переменной длинной ключа, чтобы шифровать трафик. Стандарт 802.11 поддержвает в WEP 40-разрядные ключи. Однако, некоторые поставщики сделали продукты с 104-битными ключами, плюс дополнение 24-бита IV. Ключи часто основаны на паролях, которые выбраны пользователями; это обычно уменьшает эффективный ключевой размер.

Несколько групп компьютерных специалистов по сетевой защите обнаружили проблемы, которые позволяют пользователям ставить под угрозу защищенность WLAN. Они включают пассивные нападения, чтобы расшифровать трафик, основанный на статистическом анализе, активные нападения, чтобы ввести новый трафик от неправомочных станций, активные нападения, чтобы расшифровать трафик. Атаки, основанные на анализе по словарю, возможны только при анализе дневного трафика.

Существуе несколько проблем в безопасности:

1. Использование статических WEP ключей - много пользователей в сети, потенциально совместно использующей идентичные ключи в течение длинных периодов времени, что является известной уязвимостью защиты. Это происходит, в частности из-за недостатка в управлении ключами в WEP протоколе.

2. Вектор инициализации (IV) в WEP, является 24-разрядным полем, представляя простую текстовую часть сообщения. Эта 24-разрядная строка, используемая, чтобы инициализировать ключевой поток, генерированный RC4 алгоритмом, является относительно маленьким полем, когда используется для криптографических целей. Повторное использование тот же самого IV производит идентичные потоки ключей. Использование также коротких IV гарантирует, что они будут повторятся после относительно короткого времени. Кроме того, стандарт 802.11 не определяет, как IV инициализируется или изменяется, и индивидуальные NIC от того же самого производителя могут производить те же самые IV последовательности, или некоторые NIC могут использовать постоянный IV. В результате, хакеры могут делать запись сетевого трафика, определять ключевой поток, и использовать его, чтобы расшифровать текст.
3. IV - часть RC4 ключа кодирования. Легкость узнавания 24-бит ключа пакета, в объединении со слабостью в списке ключей RC4, ведет к аналитическому нападению, которое позволяет узнать ключ, после перехватывания и анализа относительно маленького количества трафика.
4. WEP не обеспечивает никакой криптографической защиты целостности. Однако, 802.11 MAC протокол использует некриптографический CRC, чтобы проверить целостность пакетов. Комбинация некриптографической контрольной суммы с шифрами потока опасна и часто ведет к непреднамеренному нападению типа “побочный канал”, что имеет место для WEP. Это активное нападение, которое разрешает нападавшему расшифровывать любой пакет, систематически изменяя пакет и CRC посылка его AP, и отмечая, подтвержден ли пакет. Опасно проектировать протоколы кодирования, которые не включают криптографическую защиту целостности, из-за возможности взаимодействий с другими уровнями протокола, которые могут отдавать информацию о тексте шифра.

3.3 Требования безопасности

Сетевые нападения обычно разделяются на пассивные и активные нападения. Эти два широких класса подразделены на другие типы нападений.

- Пассивное Нападение - нападение, в котором атакующий просто получает доступ к активу и не изменяет его содержание (т.е. подслушивая). Пассивные нападения могут быть подслушивание или анализ трафика (иногда называемые анализом потока трафика). Эти два пассивных нападения описаны ниже.
  - При подслушивании - нападающий просто просматривает содержания передающихся сообщения
  - Анализ Трафика - нападавший, более тонким способом, получает сведения, контролируя передачи для получения образцов связи. Значительное количество информации содержится в потоке сообщений между общающимися сторонами.
- Активное Нападение - нападение посредством чего атакующий изменяет поток данных. Возможно обнаружить этот тип нападения, но нельзя предотвратить. Активные нападения могут быть одного из четырех типов (или комбинации): нелегальное проникновение, воспроизведение, модификация сообщения, и DoS - атаки.
  - Нелегальное проникновение ── Нападавший исполняет роль уполномоченного пользователя и таким образом получает некоторые привилегии.
  - Воспроизведение - нападавший контролирует передачи (пассивное нападение) и повторно передает сообщения как законный пользователь.
  - Модификация сообщения -нападавший изменяет сообщение, удаляя, добавляя, измененяя, или переупорядовачивая его.
  - DoS - нападавший предотвращает или запрещает нормальное использование или управление средствами связи.

3.3.1 Потеря конфиденциальности

Конфиденциальность - свойство, что информация не сделается доступной или будет раскрыта атакующим. Это, вообще, фундаментальное требование защиты для большинства организаций. Из-за широковещания и природы радио, конфиденциальность более трудное требование защиты. Нельзя управлять расстоянием, по которому происходит передача. Это делает традиционные физические контрмеры защиты менее эффективными.

Пассивное подслушивание абонента 802.11b может вызвать существенные проблемы. Противник может прослушать и получать секретную информацию, включая частную информацию, ID сети, пароли, и данные конфигурации. Этот риск присутствует, потому что 802.11b сигналы могут проникать вне периметра здания и т.п.. Из-за расширенного диапазона радиопередач 802.11, атакующие могут потенциально обнаруживать передачу на стоянке автомобилей или на близлежащих дорогах. Этот вид нападения является особенно простым по двум причинам: 1) часто конфиденциальность WLAN технологии даже не применяются и 2) из-за многочисленной уязвимости в защите 802.11b.

Анализаторы пакетов, типа AirSnort и WEPCRACK, являются инструментальными средствами, которые доступны в Internet. AirSnort - одно из первых инструментальных средств, созданных, чтобы автоматизировать процесс анализа сетей. К сожалению, это также обычно используется для вторжения в сети. AirSnort может воспользоваться недостатками в ключах - планирование алгоритма RC4, который формирует часть WEP стандарта. AirSnort требует только компьютера, с Linux операционной системой и wireless сетевую карту. Программное обеспечение пассивно контролирует WLAN передачи данных и вычисляет ключи кодирования после, по крайней мере, 100МБ сетевых пакетов. В высоко насыщеной сети, собирание этого количества данных может занять 3-4 часа; если объем передач низок, несколько дней.

Возможно так же использования ложного AP. Оно может находится недалего от пользователей безпроводной сети. Дстаточно иметь более сильный сигнал, что бы зарегестрировать себя как настояий AP.

3.3.2 Потеря целосности

DoS атаки происходят, когда атакующий преднамеренно генерирует сигнал, чтобы было отказано в доступе законным клиентам. При DoS атаке клиенты не спобобны связяться с етью. Незлонамеренные пользователи также могут оказаться предчиной DoS атаки. Пользователь, например, может неумышленно монополизировать сигнал, загружая большие файлы, отвергая обрящение других пользователей к сети. В результате, политика безопасности должна ограничить типы и количества данных, которые пользователи способны загрузить в сеть.

3.3.4 Другие проблемы в безопасности

С расространением безпроводной связи, все больше пользователей хотят иметь возможность связаться с сетью своей организации, например для конфиренции, находясь вне действия сети предприятия. Многие аэропорты готовятся к развертыванию wireless сетей организуя в них политику безопасности с помощью VPN.

Такие сети имеют три главных риска: 1)они публичны, и поэтому в сеть имеют доступ все пользоватеи, в том числе атакующие; 2)они служать мостом между пользователем и сетью его предприятия, в результате атакующий может получить достут к сети или подвергнуть атаке прользователя; и 3) они используют мощные сигналы для предачи данных, что облегчает задачу прослушивания.

При соединении сети предприятия с другой сетью должны быть предприняты некоторые меры безопасности: использование Transport Layer Security(TLS), SSL .

3.4 Уменьшение Риска

Организации могут уменьшить риски в сетях, применяя контрмеры. Контрмеры Управления, объединенные с операционными и техническими контрмерами могут быть эффективны в сокращении рисков. Разным организациям нужен разный уровень безопасности. Также, защита увеличивается по стоимости, потраченных на оборудование защиты, в неудобстве и обслуживании, или в эксплуатационных расходах.

3.4.1 Контрмеры Управления

Контрмеры Управления для начинаются с всестороннего рассмотрения политики безопасности. Политика безопасности являются основой, на которой другие контрмеры - операционный и технический - рационализированы и осуществлены. Политика безопасности должна делать следующее:

- Выделять, кто может использовать WLAN технологию в организации
- Выделять, требуется ли доступ Internet
- Описывать, кто может устанавливать точки доступа и другое оборудование
- Обеспечивать, ограничения на местоположение и физической защиты доступа
- Описывать тип информации, которая может быть послана
- Описывать условия, при которых устройствам позволяют входить в сеть
- Определять стандартные параметры настройки защиты доступа
- Описывать ограничения на то, как устройство может использоваться, типы местоположения
- Описывать аппаратную и программную конфигурацию любого устройства доступа
- Обеспечивать рекомендации при потерях устройств и инцидентах в защите

- Обеспечивать рекомендации на использовании кодирования, и другой программной защиты
- Определять частоту и контекст оценок защиты

Другая контрмера управления состоит в том, что весь критический персонал должным образом обучен на использовании технология. Сетевые администраторы должны полностью знать все риски защиты.

3.4.2 Операционные контрмеры

Физическая защита - наиболее фундаментальный шаг для обеспечения того, чтобы только уполномоченные пользователи имели доступ к компьютерному оборудованию. Физическая защита объединяет такие меры как средство управления доступа, идентификация персонала, и внешняя граничная защита. Беспроводные сети нуждаются в физическом средстве управления доступа. Например, идентификация по фотографии или биометрические устройства. Биометрические системы для физического управления доступа включают просмотры ладони, геометрию, просмотры сетчатки, отпечаток пальца, образец голоса, подписи, или распознавание лица. Внешняя граничная защита может включать двери блокировки и камеры видео для наблюдения вокруг периметра, чтобы препятствовать неправомочному доступу к безпроводным компонентам сети типаAP.

Также важно расположение AP. Если сигналы от AP проходят вне периметра зданий, то человеку не нужно находится внетри периметра, что бы прослушивать канал. Сущестуют специальные приборы для измерения мощности излучения от точки доступа, некоторые поставщики прилагают их вместе с оборудованием. Возможно использование направленных антен, но они не защищают связь, только ограничивают диапазон обслуживания AP.

Но использование ограниченя покрытия не дает полную гарантию от прослушивания. Нарушитель может использовать антену с большой чуствительностью, поэтому в дополение к ограничению охвата необходимо внедрение криптографических средств.

3.4.3 Технические контмеры

Технические контрмеры привлекают использование аппаратных и программных решений. Программные контрмеры включают надлежащие конфигурации AP, программных патчах и обновлениях, идентификации, системы обнаружения вторжения (IDS), и кодирование. Аппаратные решения включают smart cards, VPNs, публичную ключевая инфраструктура (PKI), и биометрику.

3.4.3.1 Решения на уровне приложений

Технические контрмеры, вовлекающие программное обеспечение включают конфигурирование точек доступа, регулярно обновление программного обеспечения, осуществление идентификации и IDS решений, выполнение ревизий защиты, и принятия эффективного кодирования.

3.4.3.1.1 Конфигурация AP

Сетевые администраторы должны конфигурировать AP в соответствии с установленной политикой безопасности. Должным образом конфигурируя административные пароли, параметры настройки кодирования, управление CSMA-CD (MAC) Списком Управления Доступа (ACL), публичные ключи, и SNMP агентов может устранять многие уязвимости, свойственной программе с заданной по умолчанию конфигурации.

Обновление заданных по умолчанию паролей. Каждое WLAN устройство идет с его собственными параметрами по умолчанию, некоторые из которых содержат уязвимости. Пароль администратора - главный пример. На некоторых AP, фабричная заданная по умолчанию конфигурация не требует пароля. Неправомочные пользователи могут легко получать доступ к устройству, если нет никакой защиты паролем. Администраторы должны изменить параметры по умолчанию, чтобы удовлетворить политику безопасности, которая должна включить требование для “сильных” (т.е. алфавитно-цифровая и специальная символьная строка по крайней мере восемь символов в длине) административных паролей. Если требование защиты достаточно высоко, организация должна рассмотреть использование автоматизированного генератора паролей. Альтернатива на идентификацию пароля – двух факторная идентификация. Одна форма двух факторной идентификации использует симметричный ключевой алгоритм, чтобы производить новый код каждую минуту. Этот код - одноразовый код использования, который соединен с личным номером пользователя (PIN). Другой пример двухфакторной идентификации обединяет smartcard пользователя с PIN пользователя. Этот тип идентификации требует аппаратного устройства smartcard и сервера PIN.

Установление надлежащих параметров настройки кодирования. Параметры настройки Кодирования должны быть установлены для самого сильного кодирования, доступного в оборудовании(программе), в зависимости от требований защиты организации. Как правило, AP имеют

только несколько доступных параметров настройки кодирования: нет кодирования , 40- bit shared key, и 128-bit shared key. Кодирование, которое используется в WEP: потоковое шифрование и осключающие-ИЛИ не налагает дополнительное бремя на компьютерные процессоры, выполняющих функцию.

Управление функцией сброса. Функция сброса налагает специфическую проблему, потому что позволяет индивидууму обнулить любые администраторские параметры, возвращая AP к его заданным по умолчанию фабричным параметрам настройки. Индивидуум может сбрасывать конфигурацию к параметрам по умолчанию просто, вставляя объект типа ручки в отверстие сброса. Наличие физического средства управления доступа может предотвратить от угрозы сброса AP неправомочными пользователями.

Использование функциональных возможностей MAC ACL. Адрес MAC - аппаратный адрес, который уникально идентифицирует каждый компьютер (или устройство) в сети. Поставшики 802.11 оборудования обеспечивают методы к ограничению доступа к WLAN основанные на MAC ACL, которые сохранены и распростроняются между AP. AC ACL предоставляет доступ к компьютеру, используя список разрешений, обозначенных адресом MAC. Однако, локальная сеть на основе протокола CSMA-CD MAC ACL не представляет сильный механизм защиты. Поскольку адреса MAC передаются не зашифроваными, MAC может быть легко зафиксирован. Это может быть эффективно только против случайного подслушивания.

Изменение SSID. SSID AP должен быть изменен от фабричного значения по умолчанию. Хотя оборудованный противник может фиксировать этот параметр по беспроводному интерфейсу, его надо изменять, чтобы предотвратить попытку противника, соединяться с сетью.

Изменение значения по умолчанию криптографических ключей. Использование значения по умолчанию - уязвимость защиты, потому что много поставщиков используют идентичные общедоступные ключи в их фабричных параметрах настройки. Пользователь может знать значение по умолчанию общедоступного ключа и использовать, чтобы получить доступ к сети.

Изменение параметоров SNMP. Некоторые AP используют SNMP, которые позволяют сетевым инструментальным средствам программного обеспечения управления контролировать состояние AP и клиентов. Использование хорошо известных, заданных по умолчанию строк делает устройства уязвимыми.

Изменение заданного по умолчанию канала. Другое соображение, которое непосредственно непригодно для использования - заданный по умолчанию канал. Поставщики обычно используют заданные по умолчанию каналы в AP. Если два или более AP с одиноковыми каналами расположены около друг друга, но находятся в различных сетях, может возникнуть проблема DoS.

Использование DHCP. Автоматические сетевые подключения вовлекают использование DHCP сервера. DHCP сервер автоматически назначает IP адреса на устройства, которые связываются с AP. Например, DHCP сервер используется, чтобы управлять диапазоном TCP/IP адресов для портативных ЭВМ клиента или рабочих станций. После того, как диапазон IP установлен, DHCP сервер динамически назначает адреса на рабочие станции при необходимости. Угроза с DHCP состоит в том, что злонамеренный пользователь мог легко получать неправомочный доступ на сети с помощью портативной ЭВМ с беспроводной NIC. Так как DHCP сервер не обязательно будет знать, какие устройства имеют доступ. Уменьшение риска состоит в отключение DHCP и использование статических IP.

3.4.3.1.2 Аутентификация

Аутентификационные решения включают использование имен пользователя и паролей; smartcards, биометрика, PKI; или комбинация решений. При использовании имена пользователя и паролей для идентификации, важно иметь политику, определяющую минимальную длину пароля, требуемые символы пароля, и истечение срока пароля. Smartcard, биометрика, и PKI имеют их собственные индивидуальные требования.

3.4.3.1.3 Системы Обнаружения Вторжения (IDS)

IDS - эффективный инструмент для определения, пытаются ли неправомочные пользователи обращаться, или уже обратились к сети, поставили ли под угрозу сеть. IDS может или быть host-based или network-based. Агент host-based установливатся на индивидуальной системе (например, сервер базы данных) и контролирует системные файлы при подозрительном поведении, типа повторных неудавшихся попыток входа в систему или изменение на разрешения файла. Агент может также использовать контрольную сумму, чтобы искать изменения в системных файлах. В некоторых случаях, агент может останавливать нападение на систему, хотя первичная функция ведущего агента должна регистрировать и анализировать события и посылать предупреждения. IDS network-based контролирует сетевой трафик, пакет за пакетом, в реальном времени (или близко к реальному времени насколько возможно) чтобы определить, соответствует ли трафик предопределенным типам нападения. Сетевой монитор узнает пакеты, которые соответствуют этому образцу и принимают меры типа прекращения сетевого сеанса, посылка почтового предупреждения администратору, или другому по указанному действию. Поскольку агент постоянно находится на компьютере, host-based система может исследовать данные после того, как они были

расшифровано. Напротив, network-based IDS - не способен расшифровать данные, поэтому, зашифрованный сетевой трафик пропускают без исследования.

3.4.3.1.4 Кодирование

Как упомянуто ранее, AP имеют только три доступные параметра настройки кодирования: без кодирования, 40-бит, и 104-бит. “Без кодирования” представляет наиболее серьезный риск, так как незашифрованные данные, проходящие в сети могут легко быть прочитаны и изменены. 40-бит шифрует сетевые данные, но все еще существуе риск. 104-разрядное кодирование - более безопасное чем 40-разрядное кодирование из-за существенного различия в размере ключей. Хотя это и неверно для сетей на основе 802.11 из-за плохой разработки криптографии WEP, использующей IV.

3.4.3.2 Решения на аппаратном уровне

Аппаратные контрмеры включают smartcard, VPN, PKI, биометрику, и другие аппаратные решения.

3.4.3.2.1 Smart Cards

Smart card могут увеличить уровень защиты, хотя они так же добавляют сложности. Организации могут использовать smart card вместе с именем пользователя или паролем. Они могут использовать smart card при двухфакторной идентефикации.

Организации могут также комбинировать smart card с биометрикой. Smart card выгодны в случаях, требующих идентификацию не только имени пользователя и пароля. Пользовательское свидетельство и другая информация непосредственно сохранены на картах и требуется только, чтобы пользователь помнил PIN.

3.4.3.2.2 VPN

VPN - быстро растущая технология, для обеспечения безопасности передачи данных в сетевых инфраструктурах. VPN позволили корпорациям, использовать Internet для отдаленного доступа. Сегодня, VPN обычно используется в различных случаях: для удаленного доступа, для обеспечение связи типа LAN-LAN. VPN использует криптографические методы для защититы IP информации. Данные находятся внутри VPN “туннеля”.

Большинство VPN, работающих сегодня, использует IPsec протоколы. IPsec, разработанный IETF, является структурой открытых стандартов для обеспечения связи по сетям IP. Предоставляет следующие типы защиты:

- Конфиденциальность
- Connectionless целостность
- Идентификация происхождения данных
- Replay protection
- Защита от анализа трафика

Connectionless целостность гарантирует, что полученное сообщение не изменилось. Идентификация происхождения данных гарантирует, что полученное сообщение было послано создателем а не человеком, идентефицирующим себя как создатель. Replay protection обеспечивает гарантию, что то же самое сообщение не было доставлено многократно и сообщения пришли в порядке. Конфиденциальность гарантирует, что другие не могут читать информацию в сообщении. Защита анализа трафика обеспечивает гарантию, что нарушитель не может определять, кто поддерживает связь или частоту или объем переданной информации. IPsec выполняет задачу маршрутизации сообщений через зашифрованный туннель двумя специальными IPSEC заголовками, вставленными сразу после заголовка IP в каждом сообщении. Encapsulating Security Protocol (ESP) заголовок обеспечивает секретность и защищает против модификации, и Authentication header (AH) защищает от модификации без обеспечения секретности. Internet Key Exchange (IKE) Протокол - механизм, который добавляет ключи и другую защиту - связанную с параметрами, которые будут переданы до связи без вмешательства пользователя.

IPSEC туннель обеспечивается от клиента через AP на VPN устройство. С IPSEC, службы безопасности предоставляются на сетевом уровне стека протокола. Это означает, что все приложения и протоколы, работающие выше того уровня - защищенны IPSEC. IPSEC службы безопасности независимы от защиты, которая встречается в WEP защите. Организация может рассматривать наличие как IPSEC так и WEP.

Также клиенты могут соединяться с сетью предприятия через VPN шлюз. Клиенты устанавливают IPSEC подключение к радио шлюзу - в дополнение или вместо WEP. В данном случае клиент не нуждается в специальных аппаратных средствах; только требуется IPSEC/VPN программное обеспечение. VPN шлюз может использовать предопределенные ключи или цифровые удостоверения для идентификации клиента. Дополнительно, пользовательская идентификация к VPN шлюзу может происходить, используя Remote

Authentication Dial-In User Service(RADIUS) или одноразовым паролем (OTP), сгенерированым, например, с помощью SecureID. Дополнительно, VPN шлюз может создать контрольный журнал всех действий.

3.4.3.2.3 Инфраструктура публичных ключей

PKI обеспечивает структуру и сервисы для производства, распределения, управления, и учета публичных ключевыми удостоверениями. Это обеспечивает приложения безопасным кодированием и проверкой сетевых операций как целостности данных, используя данные удостоверениями. Некоторые изготовители обеспечивают PKI телефонные трубки и smartcard.

PKI обеспечивает идентификацию через пользовательские удостоверения, и пользователи могут использовать те же самые удостоверения с защитой прикладного уровня, типа подписи и шифровки сообщения.

3.4.3.2.4 Биометрика

Биометрические устройства включают отпечатки палицев или ладони, оптические сканеры (включая сетчатку), сканеры распознавания лица, и сканеры распознавания голоса. Биометрика обеспечивает уровень защиты когда используется одина или наряду с другими решениями защиты. Например, для организаций, нуждающихся в более высоких уровнях защиты, биометрика может быть объединена с smartcard и использоваться вместо имени пользователя и пароля.

3.4.3.2.5 Другие аппаратные решения

Промышленность защиты также ответила на уязвимости в WEP. Несколько производителей предлагают объединенные решения защиты. Два таких производителя, являются Bluesocket и Vernier Networks. Bluesocket Wireless Gateway 1000(WG- 1000) создает межсетевую защиту между AP и остальной частью сети. WG-1000 требует идентификации через внутреннюю базу данных или центральный сервер. Для централизованной идентификации, WG-1000 поддерживает RADIUS, Lightweight Directory Access Protocol (LDAP NT 4 Domain и Windows 2000 Active Directory. Кроме того также поддержан, Extensible Authentication Protocol (EAP) для идентификации на основе лексемы. Доступно использование ролей, для поддержки различных кодирований различным пользователям в зависимости от уровня необходимой защиты. Роли также поддерживают максимальную пропускную способность для каждой пользовательской категории типа "служащих" и "посетителей". WG-1000 поддерживает кодирование для преодолевания недостатков в WEP.

Vernier Networks создали Vernier Networks System, которая состоит из двух аппаратных устройств, которые подтверждают подлинность, управляют, переадресовывают, и регистрируют сетевой трафик, произведенный сетью для каждого пользователя, сотовым телефоном, или другим устройством без установления программного обеспечения на клиенте. Устройства - CS 5000 Control Server и AM 5004 Access Manager. Control Server центрально управляет идентификацией для всех пользователей, координирует роуминг на уровене 3. Access Manager соединяется с AP, назначает права для пользователей, и включает другие функциям защиты типа IPSEC, Point-to-Point Tunneling Protocol (PPTP), и Layer 2 Tunneling Protocol (L2TP).

3.5 Развитие стандартов и технологий безопасности

Подобно промышленности, организации по стандартизации также ответили на ненадежность в 802.11b WLAN. В основном проявили активность Internet Engineering TAPk Force (IETF) и IEEE. IEEE в настоящее время работает на трех отдельных направлениях.

Первое направление разрабатывается TAPk Group I (TGi), который предложил существенные модификации в существующем IEEE 802.11 стандарте. TGI определяет вторую версию WEP на основе недавно выпущенном Advanced Encryption Standard (AES). AES решение обеспечит решение проблем, и не будет требовать новых аппаратных средств и изменений протокола. TGi в настоящее время разработало основы, для предотвращения всех известных проблемы связянных с использованием WEP, включая предотвращение подделок и обнаружения нападений Replay.

Вторая группа – меньше чем TGi. Группа определяет the Temporal Key Integrity Protocol (TKIP) для решения проблемы без аппаратных изменений - то есть происходят изменения на микропрограммном и программном уровне.

Третья группа занимается введеним нового стандарта IEEE 802.1x. IEEE 802.1x стандарт определяет структуру для управления доступа на основе порта и ключевого распределения. Используя существующий Extensible Authentication Protocol (EAP), AP подтверждает подлинность NIC, консультируясь с центральным сервером. 802.1x стандарт поддерживает серверы идентификации типа RADIUS или Kerberos. В настоящее время IETF разработывают многочисленные EAP протоколы способные работать с 802.1x.

3.6 Источники

1. **“**Application Development Trends” Magazine. “Cutting the Cable” by John K. Waters. January 2003 Volume 10 Number 1
2. National Institute of Standards and Technology. Special Publication 800-48. “Wireless Network Security 802.11, Bluetooth ™ and Handheld Devices” by Tom Karygiannis and Les Owens