Анализ защищенности беспроводных сетей 802.11

Гудилов Андрей, гр. 011

1. Введение

В последнее время беспроводные локальные сети(WLAN) являются основным направлением развития сетевой индустрии. Область применения беспроводных сетей растет невероятными темпами. Беспроводные технологии активно используются в бизнесе и компьютерной индустрии. Самым распространенным стандартом для построения беспроводных сетей стал IEEE 802.11.

Коммерческие задачи беспроводных локальных сетей могут быть разделены на пять категорий:

- Расширение LAN, т.е. решение проблемы «последней мили».
- Организация взаимодействия между пространственно разнесенными локальными сетями
- Организация Campus Area Networks (CAN) – беспроводные сети с инфраструктурой
- Организация Ad-hoc networking – беспроводные сети без инфраструктуры
- Обеспечение доступа мобильных клиентов

Обеспечение безопасности в беспроводных сетях гораздо более трудная задача, нежели в обычных проводных сетях. Многие беспроводные локальные сети сейчас не имеют никакой защиты, даже в протоколе IEEE 802.11 безопасность определена опционально.

Вероятность взлома в беспроводных сетях равна сумме вероятностей взлома обычных локальных сетей и взлома связанного с мобильностью клиента. Поэтому организации должны принимать дополнительные меры безопасности, чтобы понизить эту вероятность до приемлемого уровня.

Здесь будут рассмотрены два типа организации безопасности сети:
IEEE 802.11 (Wired Equivalent Privacy (WEP)) и IEEE 802.1x Security Protocol (Extensible Authentication Protocol (EAP)).

2.Беспроводные сети

Беспроводные локальные сети обычно делятся на три типа:

1. *Wireless Wide Area Network* (WWAN) – сети, покрывающие большие географические пространства (город, страна, материк и т.д.).
2. *Wireless Local Area Network* (WLAN) – сети, охватывающие территорию офиса или небольшой корпорации.
3. *Wireless Personal Area Network* (WPAN) – радиус действия этих сетей порядка 10 метров.

Протокол IEEE 802.11 является интернациональным и часто используемым стандартом для построения WLAN. Этот протокол обеспечивает передачу данных со скоростью от 1 Мб/с до 54 Мб/с на частотах 2.4 ГГц или 5 ГГц. Другим довольно часто используемым стандартом для WLAN является HiperLAN (*High performance radio LAN*), работающий на

частоте 5 ГГц. Есть две модификации этого стандарта HiperLAN/1 и HiperLAN/2 передающие со скоростью 19 Мб/с и 54 Мб/с соответственно.

Наиболее известная технология для построения WPAN – *Bluetooth,* которая базируется на маломощном сигнале на частоте 2.4 ГГц и очень схожа со стандартом 802.11b, но использует отличный подход для обработки сигналов, нежели 802.11. Другие значительные функциональные отличия Bluetooth от 802.11b -- это различия в пропускной способности,1Mbps против 11Mbps, и в радиусе действия, 10 метров против 100 метров.

2.1 Преимущества и недостатки

Беспроводные локальные сети обеспечивают несколько основных преимуществ, такие как мобильность пользователей, быстрое подключение к сети, маштабируемость и расширяемость. Однако имеются и несколько значительных недостатков:

- Скорость беспроводных сетей ограничена доступной полосой пропускания. Можно оценить предел пропускной способности беспроводной сети.WLAN устройства обычно медленнее, чем проводные устройства, т.к. в отличие от Ethernet стандартов, беспроводные стандарты должны более тщательно проверять получаемые фреймы для того, чтобы избежать потери данных из-за ненадежности беспроводной среды передачи данных.

- Используя электромагнитные волны в качестве среды передачи данных приходиться решать несколько проблем, например: отражение волн от зданий, наличие помех и участков, куда волны не проникают, так называемых теневых зон.

- Почти полное отсутствие защиты.

2.3 Типы сетей

Протокол 802.11 определяет два вида сетей: «*infrastructure mode*» и «*ad hoc mode*».

В «infrastructure mode» беспроводная сеть состоит, по крайней мере, из одной точки доступа присоединенной к проводной сети и некоторого количества беспроводных клиентов. Любые взаимодействия между клиентами происходят только через базовую станцию.

В «Ad hoc mode» нет точки доступа, через которую происходит взаимодействие, а есть просто набор станций, которые взаимодействуют напрямую.

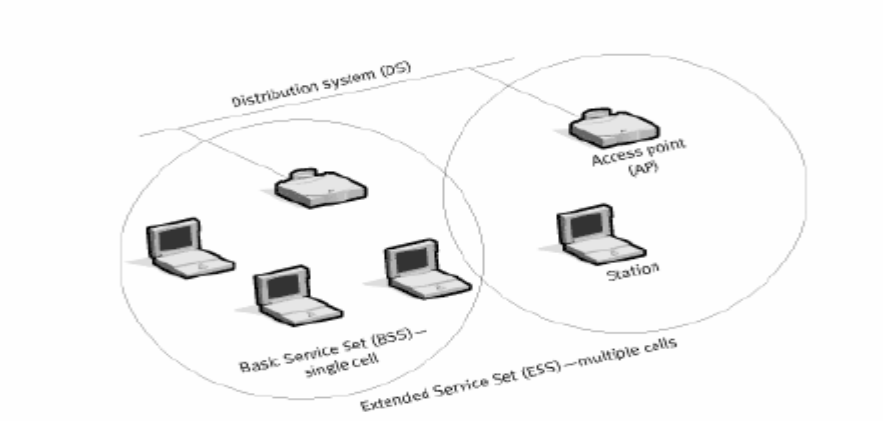

Figure 2-4: Infrastructure mode

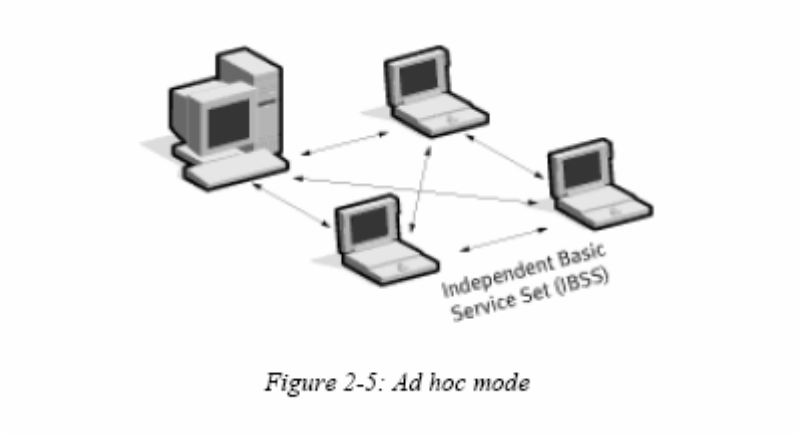

Figure 2-5: Ad hoc mode

3.1 Wired Equivalent Privacy (WEP)

Радиопередачи могут проходить по незащищенной территории, перехват радиосигнала злоумышленниками − это реальная опасность. Для того чтобы защитить данные от несанкционированного доступа, применяются различные методы.

Спецификация 802.11 MAC описывает протокол названный Wired Equivalent Privacy (WEP). Цель данного протокола − это сделать беспроводные сети такими же безопасными как проводные сети. В этом протоколе используется симметричный механизм шифрования RC4. Ключ, который клиент использует для аутоентинфикации и шифрования должен быть такой же, как и использует точка доступа. Сам стандарт 802.11 определяет длину ключа равной 40 битам, но многие компании используют ключ 104 бита, для того чтобы повысить защищенность.

Шифрование потока данных обеспечивает конфиденциальность данных передаваемых между двумя устройствами в сети. Механизм шифрования, используемый в WEP, является симметричным шифром. Если оба устройства не имеют одинакового ключа, то передача данных оканчивается неудачей. В стандарте не оговорено каким образом будет распределяться ключ между пользователями сети.

Итак, в сети появляется новый пользователь, что происходит?

1. Пользователь шлет начальный аутентификационный запрос точке доступа.
2. Когда точка доступа получила начальный запрос, она формирует случайный текст длинной 128 бит и посылает его пользователю.
3. Пользователь копирует этот текст, затем шифрует его с помощью публичного ключа, который был получен заранее (например, лично от администратора), и посылает зашифрованный текст опять точке доступа.
4. Точка доступа расшифровывает полученное сообщение с помощью ключа, который находится у нее, и затем сравнивает получившийся текст с тем текстом, который был отослан пользователю ранее. Если тексты совпали, то точка доступа шлет пользователю сообщение о том, что аутентификация прошла успешно, в противном случае отсылается сообщение о провале аутентификации.

Дальше происходит шифрование каждого пакета, передаваемых между станциями.

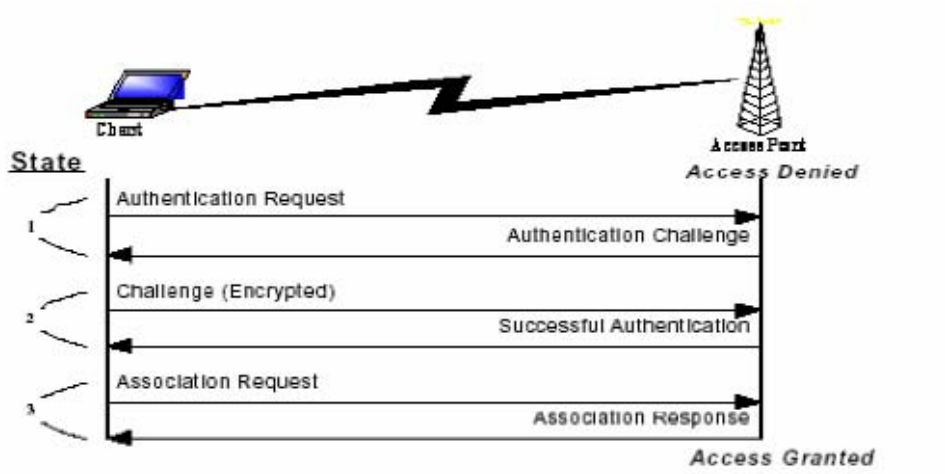

Figure 2-6: Authentication and Association States

3.2 Недостатки WEP

1. Короткий вектор инициализации(IV(24-бита)).
Это приводит к повторению IV значений, что делает возможным провести «атаку с известным открытым текстом». При скорости 5 Мб/с и средней длине пакета 500 бит все значения IV исчерпаются за полдня.

2.Малая длина секретного ключа(40-бит).
Такая длина позволяет найти ключ простым перебором. Чтобы обеспечить приемлемый уровень безопасности, длинна ключа должна быть, по крайней мере, 80-бит.

3.Секретный ключ не может обновляться автоматически и часто.
Секретный ключ должен меняться достаточно часто, чтобы избежать подбора.

4.Нет механизма аутентификации пользователей, есть только аутентификация устройств.
Следовательно, к сети может получить доступ злоумышленник, который украл сетевое устройство.

5.Формирование вектора инициализации происходит не случайно.
Часто производители устройств используют наипростейший алгоритм построения IV,т.е. прибавляют, либо отнимают единицу от начального вектора, использовавшегося при предыдущей передаче.

6.Уязвимость RC4.
Существуют целые классы «ненадежных» ключей, которые позволяют вычислить весь ключ, если известна небольшая часть ключа (например, вектор инициализации).

7. Линейность CRC.
Это позволяет злоумышленнику вносить контролируемые изменения в сообщения.

4.1 IEEE 802.1x Security Protocol

Структура безопасности в 802.11, WEP и аутентификация, основанная на WEP, не предназначенная для масштабирования и поддержки больших, открытых сетей, а так же слабая защищенность WEP создали условия для дальнейшего развития стандартов безопасности. И следующим шагом в развитии безопасности беспроводных сетей стала

разработка стандарта 802.1x, который является расширяемый, портоорентированным протоколом.

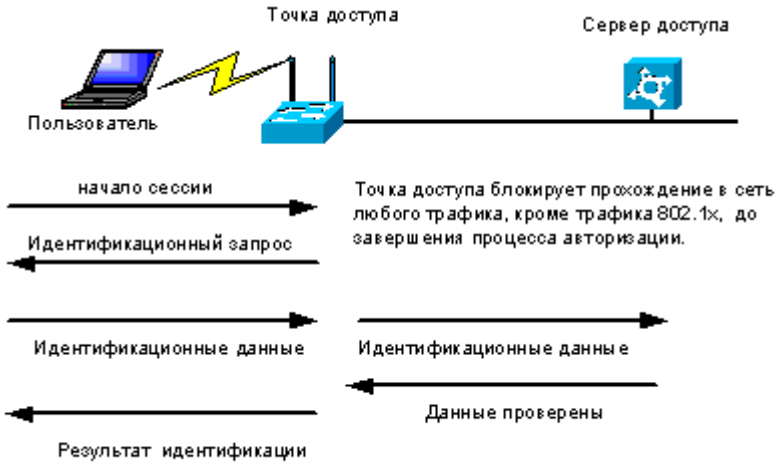

Рис.1 Схема авторизации 802.1x

IEEE 802.1x стандарт предлагает эффективную структуру для защиты системы от несанкционированного доступа, для контроля клиентских потоков информации, а так же для использования динамического распределения ключей доступа. Этот стандарт использует протокол EAP, который используется как в проводных сетях так и в беспроводных, поддерживает аутентификацию группы станций/пользователей (множественную аутентификацию) и аутентификацию типа "открытый ключ".

В структуре 802.1x можно выделить три составные части:
1) Пользователь или клиент, который хочет быть авторизован.
2) Сервер доступа, обычно RADIUS сервер.
3) Точка доступа.

Протокол распределения ключей в 802.1x называется «EAP over LANs» (EAPOL).
Итак, 802.1x работает следующим образом:

1. Клиент(Supplicant) (например клиентская беспроводная карта) посылает начальный запрос точке доступа, затем этот пакет перенаправляется серверу доступа.
2. Сервер доступа посылает идентификационный запрос обратно точке доступа. Точка доступа посылает запрос дальше пользователю.
3. Клиент отвечает на запрос, посылая свой логин и пароль серверу доступа, через точку доступа. Сервер доступа использует специальный алгоритм аутентификации, чтобы проверить подлинность клиента.
4. Если логин и пароль пользователя были верными, сервер доступа посылает сообщение клиенту о том, что аутентификация прошла успешно. Теперь точка доступа открывает порт для клиента для того, чтобы тот мог получить доступ к сервисам сети.

802.1x(EAPOL) протокол обеспечивает эффективный сервис авторизации, безотносительно от того используется ли 802.11 WEP или нет вообще никакого шифрования. Если сервер сконфигурирован чтобы обеспечивать динамический обмен ключами, 802.1x сервер доступа может возвращать сессионный ключ точке доступа вместе с сообщением об удачной аутентификации. Точка доступа использует сессионный ключ для того, чтобы создать, подписать и зашифровать EAP «key message», которое отправляется сразу после посылки сообщения об успешности аутентификации. Клиент может использовать содержимое «key message», чтобы определить приемлемый ключ для шифрования.

802.1X (EAPOL) это только механизм доставки и не обеспечивает фактически механизм аутентификации. Когда вы используете 802.1X , вы должны выбрать вид EAP протокола, т.е. Transport Layer Security (EAP-TLS) или EAP Tunneled Transport Layer Security (EAP-TTLS), который определит как действительно будет проходить аутентификация. Вид EAP протокола «живет» в сервере доступа и внутри операционной системы на стороне клиента. Точка доступа только перенаправляет пакеты между клиентами и сервером доступа и не требует изменения настроек или даже оборудования на данной точке доступа при смене вида EAP.

Ссылки:

1. Sami Uskela. Security in Wireless Local Area Networks.
   http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html

2. М. Филиппов. Вопросы обеспечения безопасности корпоративных беспроводных сетей стандарта 802.11.Специфика России.
   http://www.security.strongdisk.ru/i/148&all=1/

3. Wireless LAN: Security
   http://www.esat.kuleuven.ac.be/~h239/reports/2001/wlan/security.php

4. Mishra, A., N. L. Petroni, & B. D. Payne. Open1x -- Open Source Implementation of IEEE 802.1x.
   http://www.open1x.org/

5. IEEE 802.1X: EAP over LAN (EAPOL) for LAN/WLAN Authentication & Key Management
   http://www.javvin.com/protocol8021X.html

6. Nilufar Baghaei. IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients.
   Department of Computer Science and Software Engineering.University of Canterbury, Christchurch, New Zealand