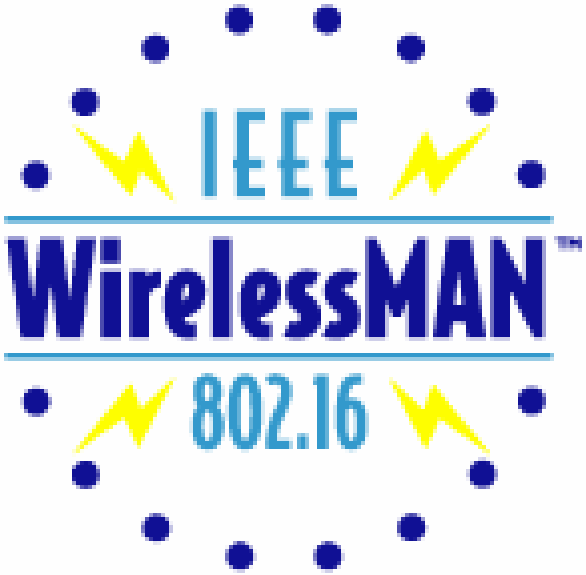

Протокол 802-16.

Обзор сетевого уровня безопасности.

Выполнил студент 911 группы Дмитриев Константин.
гДолгопрудный
2003г.

1. Сетевой уровень безопасности.

Механизм безопасности предоставляет станциям беспроводной сети секретность данных. Он обеспечивается при помощи шифрования каналов между Базовой Станцией(БС) и Станциями-Подписчиками(СП).
Вдобавок, Механизм Безопасности предоставляет операторам связи высокую защиту от кражи сервиса связи. БС защищает сервисы передачи данных от несанкционированного доступа путем шифрования связанных с ними сетевыми сервисами. Механизм Безопасности представляет аутентифицированный протокол управления ключами клиент/сервер, в котором БС, сервер, контроллирует распределение ключей СП. Вдобавок, к основным механизмам защиты к протоколу управления ключами добавлена аутентификация станций, основанная на цифровых сертификатах.

1.1 Архитектура.

Механизм безопасности состоит из 2х компонентов:
а) Протокол энкапсуляции для шифрования пакетов данных в сети с беспроводной связью. Этот протокол определяет (1) набор поддерживаемых криптографических пакетов, т.е., пар алгоритм шифрования данных – алгоритм аутентификации, и (2) правила применения данных алгоритмов к содержимому MAC-уровня PDU.
б) Протокол управления ключами(Privacy Key Management или PKM) обеспечивающий безопасную передачу ключей от БС к СП. Посредством этого протокола, СП и БС синхронизируют данные о ключах; вдобавок, БС использует протокол для осуществления условный доступ к сетевым сервисам.

1.1.1 Шифрование пакетов данных.

Сервисы шифрования определяются как набор характеристик субуровня безопасности MAC. Информация MAC-заголовка, отвечающая за шифрование, располагается в Generic MAC Header формате.
Шифрование всегда производится над содержимым MAC PDU; Generic MAC Header не зашифровывается. Все упрравляющие MAC- сообщения следует пересылать открытым текстом для облегчения регистрации, распределения диапазона и нормальной работы MAC-субуровня.

1.1.2 Протокол управления ключами.

СП использует PKM протокол для авторизации и получения ключей от БС, и для поддержания периодической реавторизации и ибновления ключей. Протокол управления ключами использует сертификаты X.509[IETF RFC 2459], алгоритм шифрования с открытым ключом RSA[PKCS #1] и сильные симметричные алгоритмы кодирования для обменя ключами между СП и БС.
Протокол PKM относится к модели PKM, где СП, “клиент” PKM, запрашивает информацию о ключе, а БС, PKM-«сервер», отвечает на запрос, при этом гарантируя, что индивидуальная станция получает только те ключи, которые ей предназначаются. Протокол PKM использует передачу управляющих MAC-сообщений.
PKM протокол использует шифрование с открытым ключом для обмена Авторизационным Ключом между СП и БС. Этот ключ потом используется для обмена ключами шифрования передаваемых данных. Этот механизм позволяет обновлять ключи шифрования избежав при этом больших вычислительных затрат, связанных с открытым ключом.

БС удостоверяет личность СП во время начальной авторизации. У каждой СП имеется свой уникальный сертификат формата X.509, который выдается изготовителем устройства станции. Сертификат содержит в себе открытый ключ станции и ее MAC-адрес. При запросе авторизационного ключа, СП отправляет свой сертификат БС. БС проверяет сертификат, а затем шифрует Авторизационный Ключ открытым ключом СП и отправляет его обратно.
БС устанавлмвает связь между удостоверенной СП и клиентом и тем самым с соответствующим сервисом, доступным клиенту. То есть, после обмена Авторизационным Ключом, БС устанавливает аутентифицированную сущность клиента СП и сервисов(т.е. определенные ключи шифрования данных), к которым СП имеет доступ.
Т.к. БС проверяет сущность СП, она защищает против злоумышленника, применяющего клона СП, выдающего себя за настоящюю СП. Использование сертификата X.509 предотвращает клонам СП вход под поддельным удостоверением.
Все СП должны иметь установленных изготовителем пару открытый/закрытый RSA ключей или обеспечивать алгоритм динамической генерации пары ключей RSA. Если СП полагается на внутренний алгоритм генерации RSA ключей, СП должна созадть ключи при первом получении Авторизационного Ключа. Все СП с предустановленными изготовителем RSA ключами должны также иметь предустановленные изготовителем сертификаты X.509. Все СП, реализующие собственную генерацию RSA ключей, должны поддерживать механизм установки выпущенных изготовителем сертификатов.

1.1.3 Security Associations

Security Association(SA) это информация о безопасности, которую использует БС и одна или несколько клиентских СП для поддержания безопасных соединений в сети IEEE Std 802.16-2001. Определены три типа SA: Основной, Статический и Динамический. Каждая СП устанавливает Основную SA в процессе инициализации. Статическая SA обеспечивается в пределах БС. Динамические SA устанавливаются и обрываются на лету в зависимости от установления и завершения определенных сервисных потоков. Как Статические, так и Динамические SA могут быть общими для нескольких СП.
Общая информация SA должна включать в себя Криптографический набор, используемый в пределах SA. Общая информация может содержать Ключи Шифрования Трафика (Traffic Encryption Keys, TEK) и Инициализационные Векторы. Точное содержание SA зависит от ее Криптографического Пакета.
SA идентифицируются при помощи SAID.
Каждая СП должна установитьс со своей БС особую Основную SA. SAID Основной SA любой СП должна равняться Основному CID СП.
Используя протокол PKM, СП запрашивает у БС ключи SA. БС должна удостовериться, что СП имеет доступ только к тому SA, к которому она относится.
Ключевая информация SA(напр. Ключ DES и Инициализационный Вектор CBC) имеет конечноый срок жизни. При предоставлении Базовой Станцией ключевой информации SA, информация имеет ограниченное время жизни. СП сама должна запросить у БС ключевую информацию SA при истечении срока годности. Если же срок действия SA для данной станции истечет раньше, чем станция получит новый SA, станции придется выполнить вход в сеть заново. Протокол PKM описывает то, каким образом СП и БС поддерживают синхронизацию ключей.

1.1.4 Назначение соответствия соейдинений<-> SA.

Существуют следующия проавила назанчения соответствий:
1) Все транспортные Соединения должны относится к существующему SA.
2) Мультикастовые Соединения могут относиться к Статическому или Динамическому SA.
3) Вторичное Соединение Управления должно относиться к Первичному SA.
4) Основное и Первичное соединение Управления не должны соотвествовать SA.

1.1.5 Криптографический Инструментарий

Криптографический инструментарий это набор методов шифрования данных, их аутентификации и обмена TEK. В стандарте определены 2 инструметария:

1. Шифрование данных отсутствует, аутентификация данных отсутствует и 3-DES.128
2. CBC-режим 56-бит DES, аутентификация данных отсутствует и 3-DES.128

1.2 PKM протокол

1.2.1 Аутентификация СП и обмен АК. Обзор.

Авторизации СП, контроллируемая государственным аппаратом Авторизации, это процесс, состоит из следующего:

a) БС удостоверяет сущность СП
b) БС предоставляет удостоверенной СП АК, из которого получаются Ключ Шифрования Ключа(KEK) и ключ удостоверения сообщения.
c) БС предоствляет удостоверенной СП SAID и свойства первичного и статического SA, к которому СП разрешен доступ.

После получения первичной авторизации, СП периодически ее обновляет; реавторизация также проводится государственной машиной Авторизации Станции-Подписчика. СП должна поддерживать авторизационный статус для того чтобы обновлять устаревающие TEK. СП начинает авторизацию, посылая Аутентификационную Информацию своей Базовой Станции. Сообщение Аутенитфикационной Информации Содержит сертификат X.509, выданный самим изготовителем или другим Authority. Сообщение Аутентификационной Информации носит строго информативный характер; т.е. БС может игнорировать его. Однако, оно предоставляет БС возможность получить сертификат клиентской БС.
СП посылает сообщение Авторизационного Запроса тотчас после посылки сообщения Аутентификационной Информации. Это запрос АК, также SAID, идентифицирующих любую Статические SA, к которым у СП есть доступ.
Авторизационный Запрос включает в себя:
а) сертификат X.509, выданный изготовителем
б) Описние криптографических алгоритмов, которые поддержмвает запрашивающая СП; поддержка криптографических параметров СП посылается БС в виде списка идентификаторов криптографических наборов, каждый из которых определяет пару алгоритмов шифрование пакетов данных-аутентификация пакетов данных, поддерживаемую СП.
в) Основной CID Станции-подписчика. Основной CID это первый статический CID, который БС назначает СП во время начальной классификации –Первичный SAID равен Основному CID.
В ответ на сообщение Авторизационного Запроса БС удостоверяет сущность запрашивающей СП, определяет алгоритм шифрования и поддержку протокола,

разделяемого с СП, активизирует АК для СП, шифрует открытым ключом СП и отсылает обратно СП в сообщении Авторизационного Ответа.
а) АК, зашифрованный открытым ключом СП.
б) четырехбитный номер , используемый для того, чтобы можно было отличить следующие последовательно друг за другом АК
в) время жизни ключа
г) идентификаторы(т.е. SAID) и свойства единичного первичного и статических SA, к которым у СП есть доступ на получение ключевой информации.
Авторизационный Ответ должен идентифицировать Статические SA в добавок к Основному SA, чей SAID соответствует CID, запрашивающей СП, в то время как Авторизационный Ответ не должен идентифицировать какие-либо Динамические SA.
БС, в ответ на Авторизационный Запрос БС, должна определить, авторизована ли СП, чью сущность можно определить по сертификату X.509, для работы с основными юникастовыми сервисами и к каким еще статически заданным сервисам(т.е. Статическим SAID), подписан клиент станции-подписчика.
Обратите внимание на то, что БС предоставляет защищенные сервисы клиенту СП в зависимости от того, какие определенные криптографические инструменарии поддерживают СП и БС одновременно.
СП должна периодически обновлять свой АК, посылая Авторизационный Запрос БС. Повторная Авторизация идентична авторизации, отличие в том, что СП не посылает сообщение Авторизационной Информации во время циклов повторной авторизации.
Во избежание прерывания сервиса во время повторной авторизации, соседние АК имеют перекрывающиеся времена жизни. И СП, и БС должны иметь поддержку до двух ключей одновременно во время таких переходных периодов.
Функционирование алгоритма планирования Авторизационных Запросов Авторизационной Машины в сочетании с режимом БС обновления и использования Авторизационных Ключей СП гарантирует, что СП может обновлять ключи без задержек в течение периодов повторной авторизации СП.

1.2.2 Передача Ключей Шифрования пакетов с Данными. Обзор.

После завершения авторизации, СП запускает отдельно машину управления Ключами Шифрования пакетов с Данными(КШД) для каждого SAID, определенного в сообщении Авторизационного Ответа. Каждая машина управления КШД, работающая в СП, отвечает за ключевой материал, относящийся к соотвествующему SAID. Машины управления КШД преиодически посылают сообщения Запроса Ключа базовой станции, запрашивающие ключевой материал для своих соответствующих SAID.
БС отвечает на Запрос Ключа сообщением Ключевого Ответа, содержащим активный ключевой материал БС для определенного SAID.
КШД в Ключевом Ответе шифруется 3-DES(encrypt-decrypt-encrypt или режим EDE), используая 2 ключа, ключ шифрования ключа(key encryption key, KEK) 3-DES берется из АК.
Обратите внимание, что БС всегда держит 2 набора ключевого материала на один SAID. Времена жизни двух поколений перекрываются таким образом, что каждое поколение становится активным в середине периода жизни предществующего и деактивизируется в середине периода активизации следующего. БС содержит в своих Ключевых Ответах оба активных набора ключевого материала данного SAID.
Ключевой ответ содержит ,кроме КШД и вектора инициализации CBC, оставшееся время жизни каждого из двух наборов ключевого материала.

Принимающая СП использует эти данные чтобы определить, когда БС сделает недействительным определенный КШД и, тем самым, распланировать следующие Запросы Ключа таким образом, что СП запросит и получит новый ключевой материал прежде, чем истечет срок действия активного ключевого материала СП. Работа алгоритма планирования Запросов Ключа машины управления КШД в сочетании с расписанием БС обновления и использования ключевого материала SAID гарантирует, что СП сможет обмениваться зашифрованными данными с БС. Машина управления КШД остается активной в течение всего периода, когда
а) СП имеет право функционировать области безопасности БС, т.е. обладает действительным АК.
б) СП имеет доступ к определенному SA, т.е. БС продолжает предоставлять новый ключевой материал в циклах обновления ключей.
Родительская машина контроля Авторизации останавливает все дочерние машины управления КШД, когда СП получает от БС Отказ в Авторизации во время цикла повтороной авторизации. Индивидуальные машины управления КШД могут быть запущены или остановлены во время цикла повторной авторизации, если авторизации Статических SAID СП изменились между последовательными повторными авторизациями.
Связь между машинами управления Авторизацмей и КШД происходит посредством передачи событий и сообщений протокола. Машина управления Авторизацией создает события(Стоп, Авторизирован, Выполняется Авторизация и Авторизация Завершена), адресованные дочерним машинам управления КШД. Машины управления КШД не направляют события своим родительским машинам управления Авторизацией. Машина управления КШД воздействует на машину управления Авторизацией косвенноым обращом через сообщения, которые посылает БС в ответ на запросы СП: БС может ответить на Запросы Ключа машины управления КШД сообщением об ошибке(т.е. сообщением Authorization Invalid), обрабатываемым машиной управления Авторизацией.

1.2.3 Выбор средств безопасности

В процессе авторизации СП предоставляет БС список со всеми криптографическими средствами(пара алгоритмов шифрование-аутентификация для данных), которые поддерживает. БС выбирает из этого списка одно из скриптографических средств для использования в первичном SA запрашивающей СП. Авторизационный Ответ, который БС шлет обратно СП, включает в себя дескриптор первичного SA, который,кроме всего прочего, идентифицирует криптографическое средство, которое выбрала БС для первичного SA. БС должна отклонить запрос на авторизацию, если она определит, что ни один из предложенных криптографических наборов не подходит.
Авторизационный Ответ содержит также необязательный список дескрипторов статических SA; каждый дескриптор статического SA идентифицирует криптографический набор, применяемый в SA. Выбор криптографического набора SA обычно делается независимо от криптографических возможностей запрашивающей СП. БС может включить в Авторизационный Ответ дескрипторы статических SA, идентифицирующих криптографические средства не поддерживаемые запрашивающей СП; если это имеет место, СП не следует запускать машины управления КШД для статических SA, криптографические наборы которых СП не поддерживает.

1.2.4 Машина управления Авторизацией.

Машина управления Авторизацией состоит из шести состояний и восьми четких событий (включая прием сообщений), которые могут инициализировать переходы состояний.

1.2.5 Машина управления КШД.

Машина управления Авторизацией состоит из шести состояний и девяти событий (включая прием сообщений), которые могут инициализировать переходы состояний.

Приведенный материал является переводом 1й главы из публикации: IEEE Standard for Local and metropolitan area networks

Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2001