

Министерство науки и высшего образования Российской Федерации

Калужский филиал
федерального государственного бюджетного образовательного
учреждения высшего образования
**«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»**
(КФ МГТУ им. Н.Э. Баумана)

Ю.С. Белов, А.Н. Молчанов

**ПРИМЕНЕНИЕ СТАНДАРТОВ ШИФРОВАНИЯ
В БЕСПРОВОДНЫХ СЕТЯХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ**
Методические указания к выполнению лабораторной работы
по курсу «Беспроводные технологии передачи данных»

Калуга – 2019

УДК 004.71
ББК 32.972.5
Б435

Методические указания составлены в соответствии с учебным планом КФ МГТУ им. Н.Э. Баумана по направлению подготовки 09.03.04 «Программная инженерия» кафедры «Программного обеспечения ЭВМ, информационных технологий».

Методические указания рассмотрены и одобрены:

- Кафедрой «Программного обеспечения ЭВМ, информационных технологий» (ИУ4-КФ) протокол № 51.4/5 от «23» января 2019 г.

Зав. кафедрой ИУ4-КФ _____ к.т.н., доцент Ю.Е. Гагарин

- Методической комиссией факультета ИУ-КФ протокол № 4 от «28» 01 2019 г.

Председатель методической комиссии факультета ИУ-КФ _____ к.т.н., доцент М.Ю. Адкин

- Методической комиссией КФ МГТУ им.Н.Э. Баумана протокол № 4 от «5» 02 2019 г.

Председатель методической комиссии КФ МГТУ им.Н.Э. Баумана _____ д.э.н., профессор О.Л. Перерва

Рецензент: _____ А.В. Фиошин
к.т.н., доцент кафедры ИУ3-КФ

Авторы _____ Ю.С. Белов
к.ф.-м.н., доцент кафедры ИУ4-КФ
ст. преп. кафедры ИУ6-КФ _____ А.Н. Молчанов

Аннотация

Методические указания по выполнению лабораторной работы по курсу «Беспроводные технологии передачи данных» содержат описание механизмов обеспечения безопасности в беспроводных сетях и стандартов шифрования в беспроводных сетях.

Предназначены для студентов 4-го курса бакалавриата КФ МГТУ им. Н.Э. Баумана, обучающихся по направлению подготовки 09.03.04 «Программная инженерия».

© Калужский филиал МГТУ им. Н.Э. Баумана, 2019 г.
© Ю.С. Белов, А.Н. Молчанов, 2019 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
ЦЕЛЬ И ЗАДАЧИ РАБОТЫ, ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ЕЕ ВЫПОЛНЕНИЯ.....	5
КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА ИЗУЧЕНИЯ, ИССЛЕДОВАНИЯ	6
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ	30
КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ	31
ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ	31
ОСНОВНАЯ ЛИТЕРАТУРА.....	32
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА	32

ВВЕДЕНИЕ

Настоящие методические указания составлены в соответствии с программой проведения лабораторных работ по курсу «Беспроводные технологии передачи данных» на кафедре «Программное обеспечение ЭВМ, информационные технологии» факультета «Информатика и управление» Калужского филиала МГТУ им. Н.Э. Баумана.

Методические указания, ориентированные на студентов 4-го курса направления подготовки 09.03.04 «Программная инженерия», содержат краткое описание механизмов обеспечения безопасности в беспроводных сетях, стандартов шифрования в беспроводных сетях и задание на выполнение лабораторной работы.

Методические указания составлены для ознакомления студентов с возможностями оборудования для беспроводных локальных сетей. Для выполнения лабораторной работы студенту необходимы минимальные знания архитектуры ЭВМ, компьютерных сетей и технологии локальных вычислительных сетей.

ЦЕЛЬ И ЗАДАЧИ РАБОТЫ, ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ЕЕ ВЫПОЛНЕНИЯ

Целью выполнения лабораторной работы является получение практических навыков применения шифрования для обеспечения безопасности передачи данных в беспроводных сетях.

Основными задачами выполнения лабораторной работы являются:

1. Разобрать основные алгоритмы шифрования, используемые для обеспечения безопасности в беспроводных сетях.
2. Определить надежность различных методов шифрования данных.

Результатами работы являются:

- Сетевое оборудование, настроенное на работу с различными алгоритмами шифрования.
- Подготовленный отчет.

КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА ИЗУЧЕНИЯ, ИССЛЕДОВАНИЯ

WEP

Wired Equivalent Privacy (WEP) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизованных пользователей беспроводной сети от прослушивания. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. Для безопасности в сетях Wi-Fi рекомендуется использовать WPA.

Кадр WEP включает в себя следующие поля (Рис. 1.):

1. Незашифрованная часть
 1. Вектор инициализации (Initialization Vector) (24 бита)
 2. Пустое место (Padding) (6 бит)
 3. Идентификатор ключа (Key ID) (2 бита)
2. Зашифрованная часть
 1. Данные
 2. Контрольная сумма (32 бита)

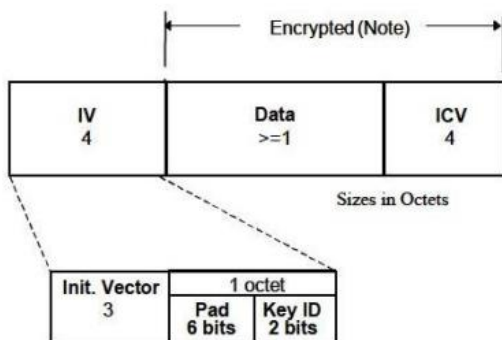


Рис. 1. Кадр WEP

Ключи имеют длину 40 и 104 бита для WEP-40 и WEP-104 соответственно. Используются два типа ключей: ключи по умолчанию и назначенные ключи. Назначенный ключ отвечает определенной паре отправитель-получатель. Может иметь любое, заранее оговоренное сторонами значение. Если же стороны предпочтут не использовать назначенный ключ, им выдается один из четырех ключей по умолчанию из специальной таблицы. Для каждого кадра данных создается сид (Seed), представляющий собой ключ с присоединенным к нему вектором инициализации.

Инкапсуляция данных проходит следующим образом:

1. Контрольная сумма от поля «данные» вычисляется по алгоритму CRC32 и добавляется в конец кадра.
2. Данные с контрольной суммой шифруются алгоритмом RC4, использующим в качестве ключа криптоалгоритма.
3. Проводится операция XOR над исходным текстом и шифротекстом.
4. В начало кадра добавляется вектор инициализации и идентификатор ключа.

Декапсуляция данных проходит следующим образом:

1. К используемому ключу добавляется вектор инициализации.
2. Происходит расшифрование с ключом, равным сиду.
3. Проводится операция XOR над полученным текстом и шифротекстом.
4. Проверяется контрольная сумма.

Все атаки на WEP основаны на недостатках шифра RC4, таких, как возможность коллизий векторов инициализации и изменения кадров. Для всех типов атак требуется проводить перехват и анализ кадров беспроводной сети. В зависимости от типа атаки, количество кадров, требуемое для взлома, различно. С помощью программ, таких как Aircrack-ng, взлом беспроводной сети с WEP шифрованием осуществляется очень быстро и не требует специальных навыков.

В 2004 году IEEE выпустил поправку к стандарту 802.11, включающую в себя новые рекомендуемые к использованию алгоритмы обеспечения безопасности WPA и WPA2. WEP был объявлен устаревшим.

WPA-Personal (WPA-PSK)

Данный режим подходит для большинства домашних сетей. Когда на беспроводной маршрутизатор или на точку доступа устанавливается пароль, он должен вводиться пользователями при подключении к сети Wi-Fi.



Рис. 2. Схема сети

В режиме PSK беспроводной доступ не может управляться индивидуально или централизованно (Рис. 2). Один пароль распространяется на всех пользователей, и он должен быть вручную изменен на каждом беспроводном устройстве после того, как он вручную изменяется на беспроводном маршрутизаторе или на точке доступа. Данный пароль хранится на беспроводных устройствах. Таким образом, каждый пользователь компьютера может подключиться к сети, а также увидеть пароль.

Плюсами WPA являются усиленная безопасность данных и ужесточенный контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств как на аппаратном уровне, так и на программном. На данный момент WPA и WPA2 разрабатываются и продвигаются организацией Wi-Fi Alliance. В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации).

Некоторые отличительные особенности WPA:

1. усовершенствованная схема шифрования RC4

- обязательная аутентификация с использованием EAP.

- система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.

2. Механизмы шифрования, которые используются для WPA-Enterprise и WPA-PSK, являются идентичными. Единственное отличие WPA-PSK состоит в том, что аутентификация производится с использованием пароля, а не по сертификату пользователя.

WPA-Enterprise

Данный режим предоставляет необходимую в рабочей среде защиту беспроводной сети. Данный режим сложнее в настройке и предлагает индивидуальное и централизованное управление доступом к вашей сети Wi-Fi. Когда пользователи попытаются подключиться к сети, им понадобится предоставить свои учетные данные для аутентификации.

Данный режим поддерживает аутентификацию по протоколу 802.1x через RADIUS-сервер и подходит в том случае, если установлен сервер RADIUS. Режим WPA-Enterprise должен использоваться исключительно в том случае, если для аутентификации устройств подключен сервер RADIUS (Рис. 3).



Рис. 3. Схема сети RADIUS сервером

Пользователи фактически не имеют дела с ключами шифрования. Они создаются защищенно и назначаются во время каждой пользовательской рабочей сессии в фоновом режиме после того, как пользователь предоставляет свои аутентификационные данные. Это не допускает извлечения пользователями сетевого ключа из компьютера.

В стандарте WPA используется Расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (иначе называют мандатом), подтверждающего его право на доступ в сеть.

TKIP, MIC и 802.1X (части уравнивания WPA) внесли свою лепту в усиление шифрования данных сетей, использующих WPA.

TKIP отвечает за увеличение размера ключа с 40 до 128 бит, а также за замену одного статического ключа WEP ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Кроме того, в TKIP используется специальная иерархия ключей и методология управления ключами, которая убирает излишнюю предсказуемость, которая использовалась для несанкционированного снятия защиты WEP ключей.

Сервер аутентификации, после получения сертификата от пользователя, использует 802.1X для генерации уникального базового ключа для сеанса связи. TKIP осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний ключ для динамической генерации ключей шифрования данных, которые в свою очередь используются для шифрования каждого пакета данных. Подобная иерархия ключей TKIP заменяет один ключ WEP (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

Другим важным механизмом является проверка целостности сообщений (Message Integrity Check, MIC). Её используют для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети. MIC построена на основе мощной математической функции, которая применяется на стороне отправителя и получателя, после чего сравнивается результат. Если проверка показывает на несовпадение результатов вычислений, данные считаются ложными и пакет отбрасывается.

WPA2

WPA2 определяется стандартом IEEE 802.11i, принятым в июне 2004 года, и призван заменить [WPA](#). В нём реализовано CCMP и шифрование AES, за счёт чего WPA2 стал более защищённым, чем свой предшественник. С 13 марта 2006 года поддержка WPA2 является обязательным условием для всех сертифицированных Wi-Fi устройств.

Разница между **WPA2 Personal** и **WPA2 Enterprise** состоит в том, откуда берутся ключи шифрования, используемые в механике алгоритма AES. Для частных (домашних, мелких) применений используется статический ключ (пароль, кодовое слово, PSK (Pre-Shared Key)) минимальной длиной 8 символов, которое задается в настройках точки доступа, и у всех клиентов данной беспроводной сети одинаковым. Компрометация такого ключа (проболтались соседу, уволен сотрудник, украден ноутбук) требует немедленной смены пароля у всех оставшихся пользователей, что реалистично только в случае небольшого их числа. Для корпоративных применений, как следует из названия, используется динамический ключ, индивидуальный для каждого работающего клиента в данный момент. Этот ключ может периодически обновляться по ходу работы без разрыва соединения, и за его генерацию отвечает дополнительный компонент — сервер авторизации, и почти всегда это RADIUS-сервер.

WPA2 Enterprise

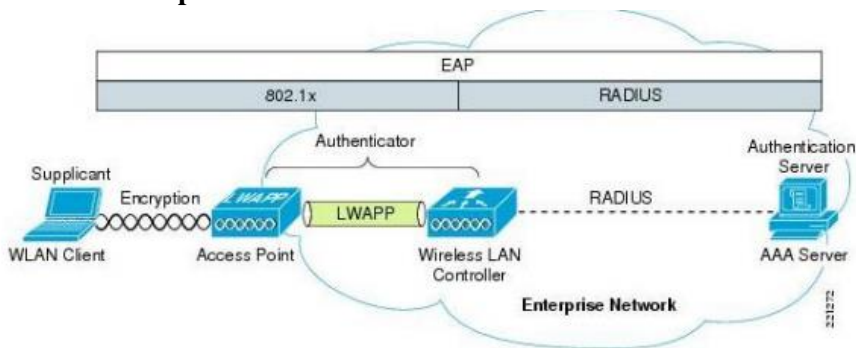


Рис. 4. Схема работы сети

Здесь мы имеем дело с дополнительным набором различных протоколов. На стороне клиента специальный компонент программного обеспечения, supplicant (обычно часть ОС) взаимодействует с авторизующей частью, AAA сервером. В данном примере отображена работа унифицированной радиосети, построенной на легковесных точках доступа и контроллере (Рис. 4). В случае использования точек доступа «с мозгами» всю роль посредника между клиентами и сервером может на себя взять сама точка. При этом данные клиентского суппликанта по радио передаются сформированными в протокол 802.1x (EAPOL), а на стороне контроллера они оборачиваются в RADIUS-пакеты.

Применение механизма авторизации [EAP](#) в вашей сети приводит к тому, что после успешной (почти наверняка открытой) аутентификации клиента точкой доступа (совместно с контроллером, если он есть) последняя просит клиента авторизоваться (подтвердить свои полномочия) у инфраструктурного [RADIUS-сервера](#) (Рис. 5)

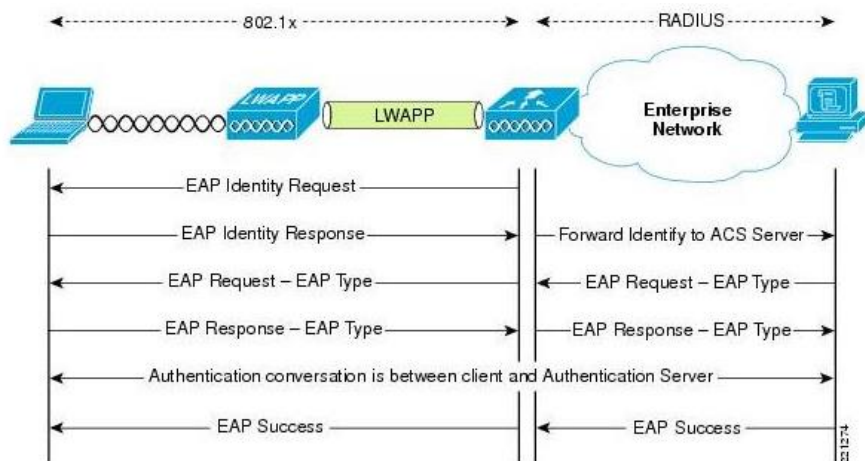


Рис. 5. Механизм авторизации EAP

Использование WPA2 Enterprise требует наличия в вашей сети RADIUS-сервера. На сегодняшний момент наиболее работоспособными являются следующие продукты:

- Microsoft Network Policy Server (NPS), бывший IAS — конфигурируется через MMC, бесплатен, но надо купить Windows
- Cisco Secure Access Control Server (ACS) 4.2, 5.3 — конфигурируется через веб-интерфейс, наворочен по функционалу, позволяет создавать распределенные и отказоустойчивые системы, стоит дорого
- FreeRADIUS — бесплатен, конфигурируется текстовыми конфигами, в управлении и мониторинге не удобен.

При этом контроллер внимательно наблюдает за происходящим обменом информацией, и дожидается успешной авторизации, либо отказа в ней. При успехе RADIUS-сервер способен передать точке доступа дополнительные параметры (например, в какой VLAN поместить абонента, какой ему присвоить IP-адрес, QoS профиль и т.п.). В завершении обмена RADIUS-сервер дает возможность клиенту и точке доступа сгенерировать и обменяться ключами шифрования (индивидуальными, валидными только для данной сессии) (Рис. 7).

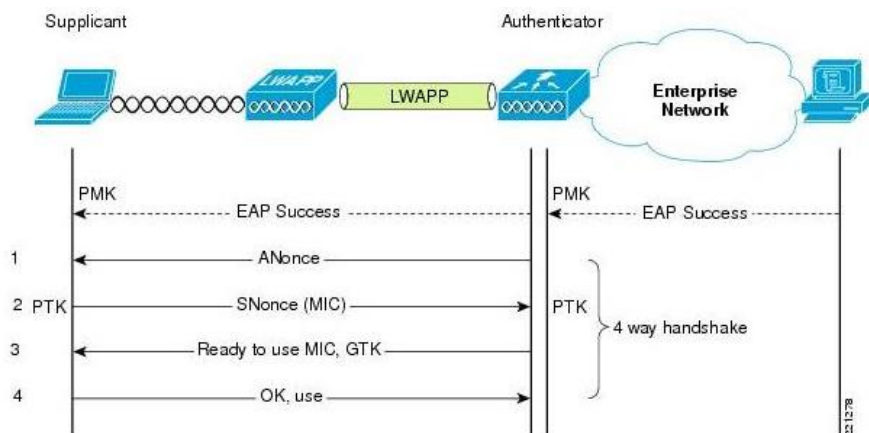


Рис. 7. Механизм авторизации EAP

RADIUS

Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием. Этот

протокол применялся для системы тарификации использованных ресурсов конкретным пользователем/абонентом. Центральная платформа и оборудование Dial-Up доступа (NAS с системой автоматизированного учёта услуг (биллинга)), RADIUS используется как протокол AAA:

- Authentication — процесс, позволяющий аутентифицировать (проверить подлинность) субъекта по его идентификационным данным, например, по логину (имя пользователя, номер телефона и т. д.) и паролю.
- Authorization — процесс, определяющий полномочия идентифицированного субъекта на доступ к определённым объектам или сервисам.
- Accounting — процесс, позволяющий вести сбор сведений (учётных данных) об использованных ресурсах. Первичными данными (то есть, традиционно передаваемых по протоколу RADIUS) являются величины входящего и исходящего трафиков: в байтах/октетах (с недавних пор в гигабайтах). Однако протокол предусматривает передачу данных любого типа, что реализуется посредством VSA (Vendor Specific Attributes).

Будучи частью биллинговой системы, RADIUS-сервер является интерфейсом взаимодействия с телекоммуникационной системой/сервером (например, маршрутизатором или коммутатором) и может реализовывать для такой системы следующие сервисы:

Общие

- Создание и хранение учётных записей пользователей (абонентов)
- Управление учётной записью пользователя (абонента) из персонального интерфейса (например, веб-кабинета)
- Создание карточек доступа (логин/PIN-код) для предоставления услуг, с некоторым лимитом действия (Dial-Up доступа в Интернет и карточной IP-телефонии)
- Ручная и автоматическая блокировка учётной записи абонента по достижению заданного критерия или лимита

- Сбор и анализ статистической информации о сессиях пользователя и всей обслуживаемой системы (в том числе CDR)
- Создание отчётов по различным статистическим параметрам
- Создание, печать и отправка счетов к оплате
- Аутентификация всех запросов в RADIUS-сервер из обслуживаемой системы (поле Secret)

Аутентификация

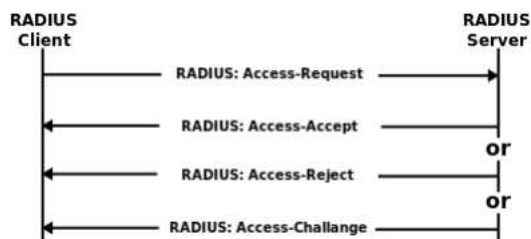


Рис. 8. Аутентификация и авторизация через RADIUS-сервер

Аутентификация и авторизация через [RADIUS-сервер](#) (Рис. 8).

Авторизация

- Выдача состояния блокировки учётной записи пользователя
- Выдача разрешения к той или иной услуге
- Сортировка данных на основе анализа статистической информации (например, динамическая маршрутизация) и выдача результата сортировки по запросу

Учёт (Accounting)

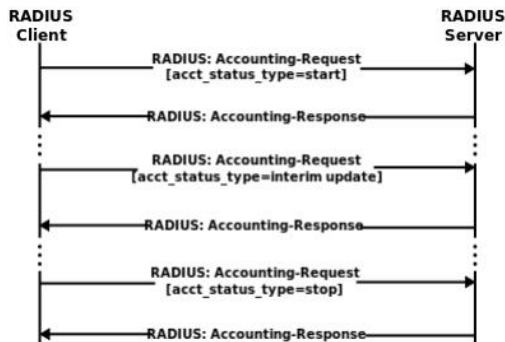


Рис. 9. Онлайн учёт через RADIUS-сервер

Онлайн учёт через RADIUS-сервер

- Онлайн-учёт средств абонента: уведомления о начале и конце сессии со стороны обслуживаемой системы
- Промежуточные сообщения о продолжении сессии (Interim-пакеты)
- Автоматическое принудительное завершение действия сессии на обслуживаемой системе в рамках услуги (packet of disconnection)
- BOOT message — специальный пакет, который отправляется телекоммуникационной системой на RADIUS-сервер при запуске (перезапуске) системы, с целью принудительного завершения всех сессий

В настоящее время протокол RADIUS используется для доступа к виртуальным частным сетям (VPN), точкам беспроводного (Wi-Fi) доступа, Ethernet коммутаторам, DSL и другим типам сетевого доступа. Благодаря открытости, простоте внедрения, постоянному усовершенствованию, протокол RADIUS сейчас является фактически стандартом для удаленной аутентификации.

Аутентификация и авторизация

Для выяснения работы RADIUS протокола рассмотрим рисунок, приведенный выше. Ноутбуки и IP телефон, представляют устройства пользователя, с которых необходимо выполнить аутентификации и авторизации на сетевых серверах доступа (NAS):

- точке Wi-Fi доступа,
- маршрутизаторе,
- VPN сервере и
- IP АТС.

Существуют и другие сетевые устройства доступа.

RADIUS протокол реализуется в виде интерфейса между NAS, который выступает как RADIUS клиент, и RADIUS сервером – программным обеспечением, которое может быть установлено на компьютере (сервере) или каком-то специализированном устройстве.

Таким образом, RADIUS сервер, как правило, не взаимодействует напрямую с устройством пользователя, а только через сетевой сервер доступа.

WPA: больше безопасности

Осознание проблем протокола [WEP](#) пришло не вчера, и еще в мае 2001 г. Группа IEEE Task Group I (TGi) начала работу над новым проектом IEEE 802.11i (MAC Enhancements for Enhanced Security), призванным обеспечить достаточную безопасность в беспроводных сетях. В ноябре 2003 г. состоялось последнее заседание группы, на котором была одобрена 7-я версия предварительного стандарта. Основные производители Wi-Fi-оборудования в лице организации WECA (Wireless Ethernet Compatibility Alliance), иначе именуемой Wi-Fi Alliance, устав ждать ратификацию стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию Wi-Fi Protected Access (WPA). WPA базируется на компонентах ожидаемого стандарта IEEE 802.11i, которые к настоящему времени уже стабильны и не подвергаются переработке, а также могут быть развернуты в существующих сетях 802.11 без внесения аппаратных изменений в

устройства. В WPA включены следующие компоненты IEEE 802.11i: протоколы IEEE 802.1x и TKIP (Temporal Key Integrity Protocol).

Протокол IEEE 802.1x, являющийся стандартом с августа 2001 г., обеспечивает контроль доступа на уровне портов. Основная его идея заключается в том, что разблокирование сетевого порта и обеспечение доступа клиента к сети происходит только после успешной аутентификации, которая выполняется на втором уровне модели OSI. 802.1x может использоваться совместно с протоколами более высоких уровней для генерации и управления ключами шифрования.

802.1x использует протокол EAP (Extensible Authentication Protocol), изначально разрабатывавшийся для работы поверх PPP (Point-to-Point Protocol) для передачи сообщений между тремя участниками аутентификации в ЛВС-окружении. Этот вид инкапсуляции известен как EAP over LANs, или EAPOL. EAP нельзя назвать методом аутентификации. Он определяет основную протокольную структуру для выбора специфического метода аутентификации. При использовании EAP аутентификатору не требуется "понимать" детали различных методов аутентификации. В данном случае он выступает только как промежуточное звено, которое переупаковывает EAP-пакеты при их следовании между саппликантом (supplicant - объект на конце сегмента "точка-точка", которому необходима аутентификация: это может быть клиентское ПО на компьютере, PDA или другом беспроводном устройстве) и сервером аутентификации. Такая технология предоставляет разработчикам возможность выбора между разными видами аутентификации, что является несомненным преимуществом. Хотя протоколом EAP на сегодняшний день предусмотрено уже более десяти различных методов аутентификации, наиболее широкое распространение получили четыре:

- Message Digest 5 (MD5) - процедура односторонней аутентификации саппликанта сервером аутентификации, основанная на применении хэш-суммы MD5 имени пользователя и пароля как подтверждение для сервера RADIUS. Данный метод не поддерживает ни управления ключами, ни создания динамических ключей. Тем самым исключается его применение в стандарте 802.11i и WPA.

- Transport Layer Security (TLS) - процедура аутентификации, которая предполагает использование цифровых сертификатов X.509 в рамках инфраструктуры открытых ключей (Public Key Infrastructure -- PKI). EAP-TLS поддерживает динамическое создание ключей и взаимную аутентификацию между саппликантом и сервером аутентификации.
- Недостатком данного метода является необходимость поддержки инфраструктуры открытых ключей.
- Tunnelled TLS (TTLS) - EAP, разработанный компаниями Funk Software и Certicom и расширяющий возможности EAP-TLS. EAP-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между саппликантом и сервером аутентификации. В результате дальнейший процесс может производиться с помощью других протоколов аутентификации, например, таких, как: PAP, CHAP, MS-CHAP или MS-CHAP-V2. В связи с простотой применения и довольно высоким уровнем обеспечиваемой безопасности протокол EAP-TTLS, скорее всего, получит наибольшее распространение в Wi-Fi-сетях. В феврале 2002 г. EAP-TTLS был подан в качестве чернового стандарта на рассмотрение в IETF. IEEE 802.11x определяет три основных компонента в сетевом окружении:
- Саппликант.
- Сервер аутентификации (authentication server) - объект, обеспечивающий службы аутентификации. В стандарте четко не определено, что должно выступать в качестве сервера аутентификации, но, как правило, им является сервер RADIUS (Remote Access Dial In User Service).
- Аутентификатор (authenticator) - объект на конце сегмента "точка-точка" локальной вычислительной сети, который способствует аутентификации объектов. Другими словами - это устройство-посредник, располагаемое между сервером аутентификации и саппликантом. Обычно его роль выполняет беспроводная точка доступа.
- Аутентификация в 802.1x включает несколько шагов. Конкретная схема обмена EAP-кадрами зависит от выбранного способа

аутентификации. В одном из простейших вариантов (OTP - One Time Password) данный процесс выглядит следующим образом (Рис.10):

1. Салпликант инициирует соединение с аутентификатором (как правило, в соответствии со стандартом это может делать и аутентификатор).
2. Аутентификатор требует идентификационную информацию о салпликанте.
3. Салпликант отсылает идентификационную информацию аутентификатору, который отправляет ее серверу аутентификации.
4. Сервер аутентификации запрашивает у аутентификатора информацию, подтверждающую подлинность салпликанта. Аутентификатор пересылает запрос салпликанту.
5. Салпликант передает информацию, подтверждающую его подлинность, аутентификатору. Аутентификатор отправляет ее серверу аутентификации.
6. Сервер аутентификации проверяет информацию о подлинности салпликанта и в случае успешной аутентификации посылает специальное сообщение аутентификатору, который открывает порт для доступа салпликанту и отправляет ему сообщение о завершении процесса аутентификации.



Рис. 10. Схема аутентификации пользователя в соответствии со стандартом 801.1x

Temporal Key Integrity Protocol (TKIP) - второй протокол, предусмотренный спецификацией WPA. TKIP предназначен для решения основных проблем WEP в области шифрования данных. Для совместимости с существующим аппаратным обеспечением

TKIP использует тот же алгоритм шифрования, что и WEP - RC4. TKIP подразумевает несколько способов повышения защищенности беспроводных сетей: динамические ключи, измененный метод генерации ключей, более надежный механизм проверки целостности сообщений, увеличенный по длине вектор инициализации, нумерация пакетов.



Рис. 11. Структура пакета при использовании протокола TKIP

В отличие от WEP, где для контроля целостности передаваемых данных использовалась CRC-32, TKIP применяет так называемый Message Integrity Code (MIC), обеспечивающий криптографическую контрольную сумму от нескольких полей (адрес источника, адрес назначения и поля данных). Так как классические MIC-алгоритмы (например, HMAC-MD5 или HMAC-SHA1) для существующего беспроводного оборудования являлись очень "тяжелыми" и требовали больших вычислительных затрат, то специально для использования в беспроводных сетях Нильсом Фергюсоном (Niels Ferguson) был разработан алгоритм Michael. Для шифрования он применяет 64-битный ключ и выполняет действия над 32-битными блоками данных. MIC включается в зашифрованную часть фрейма между полем данных и полем ICV.

Для обеспечения целостности данных в протоколе TKIP, помимо механизма MIC, предусмотрена еще одна функция, отсутствовавшая в WEP, - нумерация пакетов. В качестве номера используется IV, который теперь называется TKIP Sequence Counter (TSC) и имеет длину 48 бит, в отличие от 24 бит в WEP (рис. 3). Увеличение длины IV до 48

бит позволяет избежать коллизии векторов и гарантирует, что они не повторятся на протяжении более тысячи лет.

Основным и самым важным отличием TKIP от WEP является механизм управления ключами, позволяющий периодически изменять ключи и производить обмен ими между всеми участниками сетевого взаимодействия: саппликантом, аутентификатором и сервером аутентификации. В процессе работы и аутентификации на разных этапах взаимодействия и для различных целей генерируются специализированные ключи. При аутентификации с помощью протокола IEEE 802.1x на основе заранее predetermined информации, известной саппликанту и серверу аутентификации (например, сертификат, имя пользователя, пароль и т. д. - зависит от способа аутентификации), генерируется мастер-ключ (Master Key - МК), посредством которого они производят взаимную аутентификацию. Далее на основании МК саппликант и сервер аутентификации генерируют парный МК (Pairwise Master Key -- РМК), а затем сервер аутентификации передает (не копирует) его аутентификатору. Получение аутентификатором РМК является последним этапом в процессе EAP-аутентификации, после чего сервер аутентификации посылает аутентификатору пакет "ответ/принято" (RADIUS/Accept), а аутентификатор саппликанту -- "успешно" (EAP/Success). РМК не используется для операции непосредственного шифрования и дешифрования данных, он применяется для генерации целой группы ключей.

После получения саппликантом и аутентификатором РМК они производят взаимную аутентификацию и генерацию парного временного ключа (Pairwise Transient Key - РТК).

Генерация РТК происходит в четыре этапа:

1. В первом сообщении аутентификатор посылает саппликанту случайные данные, называемые nonce. Саппликант объединяет nonce аутентификатора (Anonce) со своим собственным (Snonce) и применяет эти данные для генерации РТК. Далее саппликант подсчитывает значение Message Integrity Check (MIC) от тела второго сообщения и первых 128 бит ключа РТК.

2. Во втором сообщении саппликант посылает Snonce и MIC аутентификатору, который также генерирует РТК и затем использует его для проверки значения MIC, полученного во втором сообщении.
3. Если ошибок не обнаружено, аутентификатор отправляет саппликанту сообщение о применении РТК.
4. В четвертом сообщении саппликант подтверждает аутентификатору использование данного ключа.

РТК является составным. Биты с 0 по 127 представляют собой ключ подтверждения ключа (Key Confirmation Key - КСК), применяемого для шифрования нового сессионного ключа (РМК) при его следующей смене. Биты со 128 по 255 отводятся для ключа шифрования ключа (Key Encryption Key - КЕК), который используется для распространения группового временного ключа (Group Transient Key - GTK). Биты с 256-го и выше могут иметь специфическую структуру, зависящую от метода шифрования, и представляют собой временный ключ (Temporal Key - ТК), применяемый для шифрования данных.

GTK - это ключ, используемый для шифрования группового (multicast) и широковещательного (broadcast) трафика. Он генерируется из группового МК (Group Master Key -- GMK), который, в свою очередь, является производным МК. Распространение GTK происходит в два этапа, в отличие от четырех в случае с РТК, так как его доставка выполняется через безопасное соединение после того, как переданы все парные ключи, и аутентификация в данном случае не требуется. При отключении одного из клиентов от сети осуществляются генерация нового ключа GTK и его распространение оставшимся клиентам. ТК также может быть составным, и его часть или он полностью вместе с MAC-адресом источника (Transmitter Address - ТА) и вектором инициализации (IV) являются входными данными для двухфазовой функции микширования, генерирующей пакетные ключи (Per-packet Key - РК) длиной 128 бит (Рис. 12). Введение в функцию микширования такого параметра, как ТА, позволяет избежать атак с использованием подставных объектов.

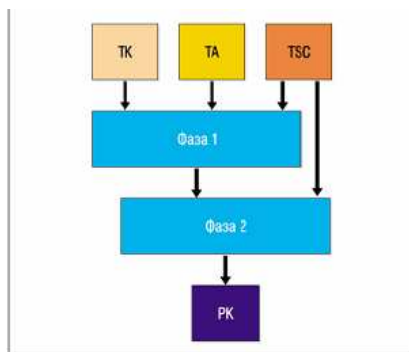


Рис. 12. Процесс формирования пакетного ключа

Для домашнего применения и небольших офисов, где, как правило, отсутствует сервер аутентификации, спецификация WPA предусматривает режим использования общего ключа (Pre-Shared Key -- PSK). В этом случае PMK вводится вручную на саппликанте и аутентификаторе. В остальном процедура генерации ключей прежняя.

Настройка безопасности распределённой беспроводной сети

Итак, если первоначальное тестирование созданной распределённой беспроводной сети прошло успешно, можно переходить ко второму этапу – настройке безопасности сети для предотвращения несанкционированного доступа в свою сеть хотя бы со стороны соседей.

В случае, если беспроводная сеть является одноранговой, то есть все компьютеры этой сети равноправны и отсутствует выделенный сервер, регламентирующий работу сети, полагаться на политику системной безопасности в такой сети бессмысленно, поскольку подобной политики там просто нет. Поэтому настройку безопасности беспроводной сети необходимо проводить на уровне точек доступа.

Настройка шифрования

Любая точка доступа и тем более беспроводной маршрутизатор предоставляют в распоряжение пользователей возможность настраивать шифрование сетевого трафика при его передаче по открытой среде. Первым стандартом, который использовался для шифрования данных в беспроводных сетях, был стандарт WEP. В соответствии с этим стандартом шифрование осуществляется с помощью 40- или 104- битного ключа, а сам ключ представляет собой набор ASCII-символов длиной 5 (для 40-битного) или 13 (для 104-битного ключа) символов. Набор этих символов переводится в последовательность шестнадцатеричных цифр, которые и являются ключом. Допустимо также вместо набора ASCII-символов напрямую использовать шестнадцатеричные значения (той же длины).

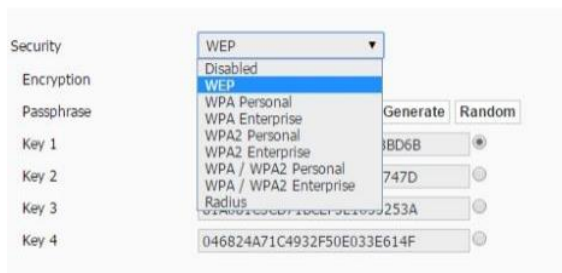


Рис. 13. Выбор режима шифрования и аутентификации

Как правило, в утилитах настройки беспроводного оборудования указываются не 40- или 104-битные ключи, а 64- или 128-битные. Дело в том, что 40 или 104 бита – это статическая часть ключа, к которой добавляется 24-битный вектор инициализации, необходимый для рандомизации статической части ключа. В результате с учетом вектора инициализации общая длина ключа получается равной 64 (40+24) или 128 (104+24) битам. Протокол [WEP-шифрования](#), даже со 128-битным ключом, считается не очень стойким, поэтому в устройствах стандарта 802.11g поддерживается улучшенный алгоритм шифрования WPA – Wi-Fi Protected Access. Однако при использовании WDS-технологии поддерживается только WEP-шифрование на основе статических

ключей. Поэтому в данном случае это единственная реализуемая возможность.

При настройке точек доступа для использования WEP-шифрования следует ввести ключ (в нашем примере используется ключ в шестнадцатеричном формате). Всего возможно задать до четырёх значений ключа, и, если задано несколько ключей, необходимо указать, какой именно из них используется по умолчанию (Рис. 14). Далее требуется реализовать настройки на беспроводных адаптерах сетевых клиентов. Они будут идентичны описанным настройкам.

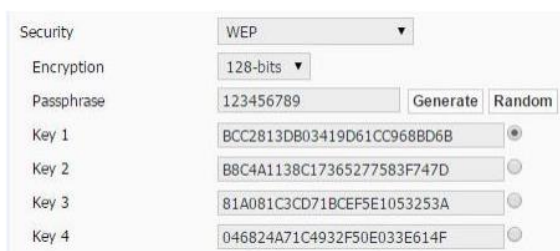
The image shows a configuration window for WEP security. It has a 'Security' dropdown set to 'WEP'. Below it, 'Encryption' is set to '128-bits'. A 'Passphrase' field contains '123456789', with 'Generate' and 'Random' buttons to its right. There are four 'Key' fields, each with a radio button. Key 1 is selected and contains 'BCC2813DB03419D61CC968BD6B'. Key 2 contains 'B8C4A1138C17365277583F747D'. Key 3 contains '81A081C3CD71BCEF5E1053253A'. Key 4 contains '046824A71C4932F50E033E614F'.

Рис. 14. Настройка точки доступа для использования WEP-шифрования

При настройке точек доступа для использования WPA-шифрования следует ввести ключ, либо нажав Random, получить сгенерированный ключ. Далее требуется реализовать настройки на беспроводных адаптерах сетевых клиентов.

The image shows a configuration window for WPA security. It has a 'Security' dropdown set to 'WPA / WPA2 Personal'. 'Encryption' is set to 'AES'. A 'Shared Key' field is highlighted in yellow and contains eight asterisks, with a 'Random' button to its right. A 'Group Key Renewal' field is set to '3600' with '(seconds)' in parentheses.

Рис. 15. Настройка точки доступа для использования WPA-шифрования

Заключение

Все описанные выше механизмы существуют уже сегодня в продуктах многих производителей или появятся в скором будущем путем замены прошивок или драйверов устройств, так как разрабатывались они с целью повышения безопасности уже развернутых сетей без необходимости замены установленного оборудования. Что же нас ждет в будущем?

В ближайшее время нас ожидает неоднократно откладываемая ратификация стандарта IEEE 802.11i, иначе называемого WPA2, который предусматривает новые, более надежные механизмы обеспечения целостности и конфиденциальности данных:

- Протокол CCMP (Counter-Mode-CBC-MAC Protocol), основанный на режиме Counter Cipher-Block Chaining Mode (CCM) алгоритма шифрования Advanced Encryption Standard (AES). CCM объединяет два механизма: Counter (CTR) для обеспечения конфиденциальности и Cipher Block Chaining Message Authentication Code (CBC-MAC) для аутентификации.
- Протокол WRAP (Wireless Robust Authentication Protocol), основанный на режиме Offset Codebook (OCB) алгоритма шифрования AES.
- Протокол TKIP для обеспечения обратной совместимости с ранее выпущенным оборудованием.
- Взаимная аутентификация и доставка ключей на основе протоколов IEEE 802.1x/EAP.
- Безопасный Independent Basic Service Set (IBSS) для повышения безопасности в сетях Ad-Hoc.
- Поддержка роуминга.

Ожидается, что протокол CCMP будет обязательным для реализации, а WRAP и TKIP-опциональными. Использование механизмов шифрования и аутентификации, определенных в стандарте IEEE 802.11i, потребует от устройств более высокой вычислительной мощности и применения специализированных микросхем, которые будут решать возлагаемые на них задачи. Поэтому, скорее всего, после ратификации стандарта появятся принципиально новые устройства.

Кроме описанных выше способов обеспечения безопасности в беспроводных сетях, существуют и другие - например, контроль доступа на основе MAC-адресов и отключение режима широковещательной рассылки параметра Service Set Identifier (SSID).

К сожалению, их нельзя считать относительно надежными средствами обеспечения безопасности, поскольку с помощью простейших сетевых анализаторов можно отследить MAC-адреса устройств сети и значение SSID, которое передается в открытом виде в каждом пакете, а драйверы практически всех сетевых адаптеров позволяют изменить их MAC-адрес.

Рассмотренные выше способы обеспечения безопасности беспроводных сетей предусмотрены стандартами или спецификациями, относящимися к беспроводным сетям и являющимися частью функциональных возможностей данного оборудования. Но для создания необходимого уровня безопасности могут применяться и другие классические способы, в частности построение VPN-туннеля поверх беспроводной сети с помощью хорошо себя зарекомендовавших протоколов более высоких уровней - например IPSec.

Кроме этого, беспроводной сегмент или сеть можно выделить как отдельную зону с низким уровнем доверия на межсетевом экране (firewall) и настроить правила ограничения и контроля трафика между этой зоной и остальной сетью предприятия.

Также возможно ввести дополнительную аутентификацию пользователей на каком-либо пограничном ресурсе, устанавливаемом между беспроводной и корпоративной сетями.

Осознавая проблемы защиты информации в беспроводных сетях, а также учитывая специфику их развертывания и поддержки, ряд производителей начали выпускать на рынок устройства, которые сами по себе не являются беспроводным оборудованием (т. е. у них отсутствуют радиомодуль и другие радиоатрибуты), но выполняют ряд сервисных функций, позволяющих повысить уровень защиты беспроводных сетей и предоставить пользователям и администраторам дополнительные возможности, облегчающие их развертывание, настройку, эксплуатацию и контроль над такими сетями. Подобные

устройства называются по-разному (беспроводные шлюзы, беспроводные коммутаторы), но обычно они устанавливаются в качестве пограничных между точками доступа и корпоративной сетью и играют роль брандмауэров, служб аутентификации, могут терминировать на себе туннели VPN и решают другие специфические задачи, например, тарификацию работы беспроводных клиентов и др.

Используя вышеперечисленные методы в том или ином их сочетании, сегодня возможно обеспечить необходимую и достаточную безопасность беспроводных сетей. Естественно, внедрение всех или некоторых из приведенных мер приводит к удорожанию системы и повышению затрат на ее эксплуатацию, таким образом возрастает совокупная стоимость владения (TCO) системы. В этом случае мы сталкиваемся со следующей дилеммой: что обойдется дороже - стоимость внедрения системы и затраты, связанные с ее эксплуатацией, или потери, вызванные утечкой информации. Но это уже отдельный вопрос.

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Настроить точки доступа на использование в режиме WDS, AP, AP+WDS, Wireless Client, Wireless Ethernet Brige. Подключиться через web-интерфейс к каждой точке доступа и настроить поочередно все возможные варианты шифрование.
2. Проверить работоспособность созданной сетевой конфигурации.
3. Сделать выводы.
4. Все действия подробно согласовать с преподавателем в письменном виде.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

1. Изложите краткую характеристику первого стандарта шифрования в беспроводных сетях.
2. Опишите тип аутентификации, используемый в WEP-шифровании.
3. Изложите тип шифрования, поддерживающий режим WDS.
4. Изложите на базе какого протокола основано шифрование WPA.
5. Опишите этапы работы протокола TKIP.
6. Изложите какой стандарт шифрования используется в протоколе WPA помимо TKIP.
7. Опишите для чего необходим протокол MIC.
8. Дайте определение термину WPA-PSK.
9. Раскройте роль RADIUS-сервера.

ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

На выполнение лабораторной работы отводится 2 занятия (4 академических часа: 3 часа на выполнение и сдачу лабораторной работы и 1 час на подготовку отчета).

Отчет на защиту предоставляется в печатном виде.

Структура отчета (на отдельном листе(-ах)): титульный лист, формулировка задания (вариант), этапы выполнения работы (со скриншотами), результаты выполнения работы. выводы.

ОСНОВНАЯ ЛИТЕРАТУРА

1. Смелянский Р.Л. Компьютерные сети. 2 т. Т.1. Системы передачи данных [Текст] / Р.Л. Смелянский. –М.: Изд. Центр «Академия», 2011.- 304 с.
2. Смелянский Р.Л. Компьютерные сети. В 2 т. Т.2. Сети ЭВМ [Текст]: учебник для вузов / Р.Л. Смелянский. –М.: Изд. Центр «Академия», 2011.- 240 с.
3. Власов Ю.В. Администрирование сетей на платформе MS Windows Server [Электронный ресурс] / Ю.В. Власов, Т.И. Рицкова. —М.: Интернет-Университет Информационных технологий (ИНТУИТ), 2016. — 622 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52219.html>

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Технологии коммутации и маршрутизации в локальных компьютерных сетях. [Текст]: учеб. пособие для вузов / Е.В. Смирнова, А.В. Пролетарский [и др.]; под. ред. А.В. Пролетарского. -М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. - 389 с.: ил.
5. Таненбаум Э. Компьютерные сети [Текст] / Э. Таненбаум. – 4-е изд. – СПб.: Питер, 2010. — 992 с.
6. Ачилов Р.Н. Построение защищенных корпоративных сетей [Электронный ресурс]: учеб. пособие / Р.Н. Ачилов. — Москва: ДМК Пресс, 2013. — 250 с. — 2227-8397. — Режим доступа: <http://e.lanbook.com/book/66472>

Электронные ресурсы:

7. Электронно-библиотечная система «Лань»
8. Электронно-библиотечная система «Университетская библиотека ONLINE»
9. Электронно-библиотечная система «IPRbooks»
10. Электронно-библиотечная система «Юрайт»