Уязвимости протокола WEP и альтернативы улучшения безопасности с использованием EAP и WPA

Шитиков
Владимир
911гр.

1 Что такое WEP.
WEP (Wired Equivalent Privacy) протокол, призванный обеспечить защиту беспроводных сетей (WLAN) от несанкционированного доступа, путем шифрования трафика. Этот протокол также используется для устройств Bluetooth. Сразу три группы исследователей — из компании Intel, университетов Беркли (шт. Калифорния) и штата Мэриленд — подняли вопрос о способности WEP обеспечивать требуемый уровень защиты беспроводных коммуникаций.

Рассмотрим подробнее как осуществляется аутентификация в беспроводных сетях.

Сервисы аутентификации.

IEEE 802.11 определяет два подтипа сервиса аутентификации: Открытая система (Open system) и Распределенный ключ (Shared key). Использованный метод индицируется внутри управляющего кадра аутентификации (authentication management frame). Эти кадры отвечают за алгоритм аутентификации. Все управляющие фреймы аутентификации должны быть unicast кадрами, аутентификация проводится между двумя станциями (т.е. multicast аутентификация не допустима). Кадры деаунтификации могут быть и групповыми.

Open System Authentication.

Open System аутентификация это простейший из доступных методов аутентификации. В действительности он не является серьезным методом. Каждая станция, которая запрашивает данный метод, может быть аутентифицирована, если только на получателе dot11AuthenticationType установлен в Open System authentication. Этот метод не обязан закончиться успехом, так станция может отклонить аутентификацию какой-либо другой конкретной станции. Open System authentication это алгоритм, использующийся по умолчанию.

Open System аутентификация состоит из 2-шаговой-последовательности транзакций. 1-й шаг это подтверждение подлинности и запрос на аутентификацию. 2-й шаг это результат аутентификации. Если он успешный, то станции должны взаимно аутентифицироваться.

Open System authentication (1-й кадр)
— Message type: Management
— Message subtype: Authentication
— Information items:
• Authentication Algorithm Identification = “Open System”
• Station Identity Assertion (in SA field of header)
• Authentication transaction sequence number = 1
• Authentication algorithm dependent information (none)
— Direction of message: From authentication initiating STA to authenticating STA

Open System authentication (заключительный кадр)

— Message type: Management
— Message subtype: Authentication
— Information items:
• Authentication Algorithm Identification = “Open System”
• Authentication transaction sequence number = 2
• Authentication algorithm dependent information (none)
• The result of the requested authentication as defined in 7.3.1.9
— Direction of message: From authenticating STA to initiating STA

Shared Key authentication

Данный метод поддерживает аутентификацию станций, которые либо знают распределенный ключ, либо являются членом группы, которые не знают его. IEEE 802.11 Shared key authentication осуществляет это без посылки ключа открытым текстом, хотя для этого требуется использование шифрование WEP. Таким образом, эта схема доступна только в том случае, если есть возможность использовать WEP. Кроме того Shared Key authentication должна поддерживаться на всех станциях, где поддерживается WEP. Предполагается, что требуемый секретный распределенный ключ рассылается станциям по секретному каналу, который не зависит от протокола 802.11. Этот ключ содержится в доступном только для записи MIB-атрибуте через путь управления MAC. Этот атрибут доступен только для записи, поэтому ключ остается внутренним для MAC. Во время аутентификации ответ и зашифрованный ответ передаются. Это облегчает неавторизованное обнаружение псевдослучайной последовательности для пар ключ/IV в подпоследовательностях кадров, используемых при обмене. Станция не сможет инициировать аутентификацию пока ее dot11PrivacyOptionImplemented атрибут не установлен в true.

В последующем описании станция, инициирующая обмен названа как requester, и адресуемая станция как responder.

Shared Key authentication (первый кадр)
— Message type: Management
— Message subtype: Authentication
— Information Items: (Информационные поля)
• Station Identity Assertion (in SA field of header)
• Authentication Algorithm Identification = “Shared Key” (Используемый алгоритм)
• Authentication transaction sequence number = 1
• Authentication algorithm dependent information (none) (пусто)
— Direction of message: From requester to responder

Shared Key authentication (второй кадр)
Перед отсылкой второго кадра в данной последовательности, responder должен использовать WEP для генерации строки из октетов, которые должны быть использованы как ответный текст при аутентификации.
— Message type: Management
— Message subtype: Authentication
— Information Items:
• Authentication Algorithm Identification = “Shared Key”
• Authentication transaction sequence number = 2 (номер кадра)
• Authentication algorithm dependent information = the authentication result. (информация, которая зависит от использованного алгоритма)
• The result of the requested authentication

Если код возврата – неуспех, то это заключительный кадр в последовательности. В этом случае содержимое поля challenge text не специфицируется.

Если код возврата – успех, то следующие дополнительные поля должны иметь Определенное содержание.

—Authentication algorithm dependent information = challenge text.

Это поле должно быть фиксированной длины.128 октет. Оно должно быть заполнено октетами сгенерированными WEP генератором псевдослучайной последовательности PRNG. Точное значение неважно, но значение не должно быть статическим. Ключ и IV неспецифицированы, так как они не открыты и не могут конфликтовать из-за взаимодействия между сетями.

— Direction of message: From responder to requester

Shared Key authentication (third frame)

Requester должен скопировать challenge text из второго кадра в третий. Третий кадр должен быть зашифрован, при помощи WEP, используя shared secret key.
— Message type: Management
— Message subtype: Authentication
— Information Items:
• Authentication Algorithm Identification = “Shared Key”
• Authentication transaction sequence number = 3
• Authentication algorithm dependent information = challenge text from sequence two frame
— Direction of message: From requester to responder
—
Этот кадр должен быть зашифрован.

Shared Key authentication (заключительный кадр)

Ответчик responder должен попытаться расшифровать содержимое третьего кадра в аутентификационной последовательности как описано ранее. Если проверка WEP IV прошла успешно, ответчик должен сравнить расшифрованные составляющие Challenge text с теми что, были посланы в кадре 2 . Если они одинаковы, то отсылается статус успеха. Если проверка не прошла, то ответчик должен отослать код unsuccessful в кадре 4 последовательности как описано ранее.

— Message type: Management
— Message subtype: Authentication
— Information Items:
• Authentication Algorithm Identification = “Shared Key”
• Authentication transaction sequence number = 4
• Authentication algorithm dependent information = the authentication result
Результат аутентификации.
Фиксированное поле “successful” and “unsuccessful.”
— Direction of message: From responder to requester (Направление)

Итак, 802.11 поддерживает 2 типа аутентификации один из которых вообще не препятствует доступу, и любой запросивший сервис его получает. Второй хоть и

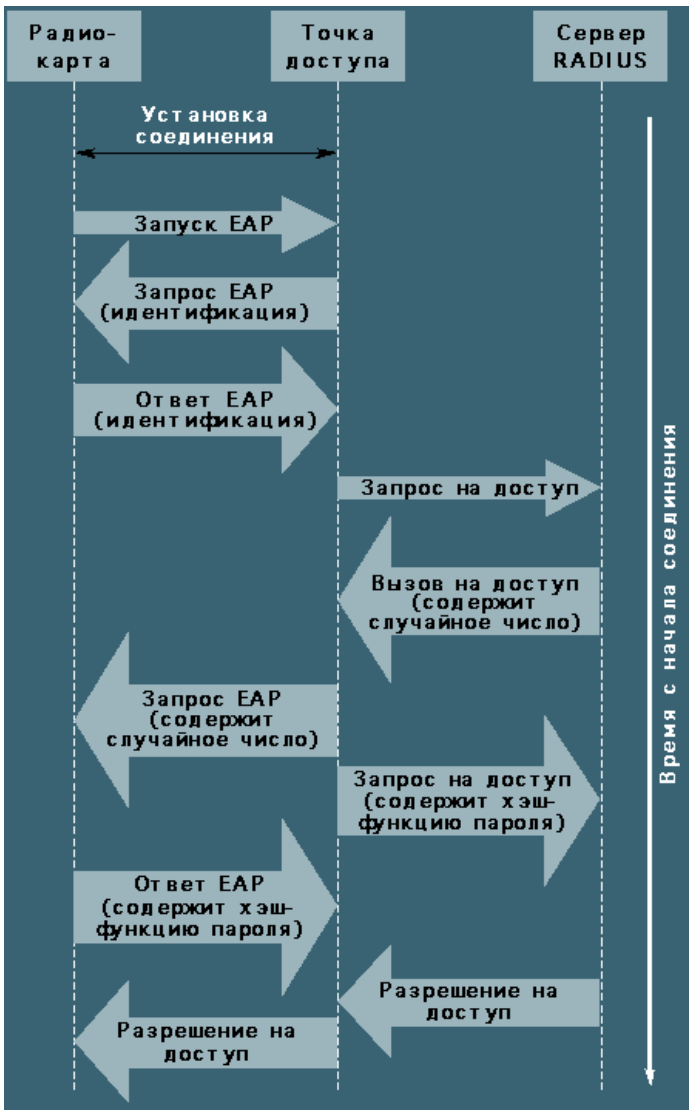
использует шифрование WEP, но длина ключа составляет 40 бит и он должен быть известен всем, поэтому ключи являются статическими.

Рассмотрим подробнее WEP.

В WEP используется симметричная схема шифрования с 40-битным ключом, построенная на алгоритме RC4. Согласно стандарту IEEE 802.11, который определяет механизм шифрования пакетов данных, передаваемых по беспроводным каналам, WEP состоит из пяти элементов.

- Секретный ключ (WEP-ключ — распространяется среди всех абонентов сети).
- Алгоритмы шифрования и дешифровки, которые используют поточную схему кодирования на основе алгоритма RC4.
- Вектор инициализации длиной 24 бит. Он объединяется с WEP-ключом, в результате чего получается входная последовательность (длиной 64 или 128 бит) алгоритма RC4. При этом WEP случайным образом выбирает для любого передаваемого пакета уникальный вектор инициализации (в ряде вариантов для каждого последующего пакета его значение изменяется на единицу).
- Инкапсуляция — передача вектора инициализации и закодированного сообщения от отправителя к адресату.
- Проверка целостности. Ее результаты шифруются вместе с открытым текстом и передаются адресату в составе закодированного сообщения.

Однако столь простая система защиты трафика (назовем ее «WEP со статическими ключами») недостаточно устойчива к некоторым вариантам атак, на что и обратили внимание авторы вышеупомянутых исследований. Система защиты беспроводной сети, основанная на WEP со статическими ключами и аутентификацией по MAC-адресу устройства, не удовлетворяет практическим условиям безопасной эксплуатации. Все это послужило стимулом к усовершенствованию процедур аутентификации и работы WEP. Одним из наиболее значимых достижений последнего времени стал переход на применение протокола EAP (Extended Authentication Protocol)при выполнении процедуры взаимной аутентификации пользователя и точки доступа.



Протокол EAP устанавливает стандартную последовательность действий при проведении аутентификации и авторизации абонента сети (рис). Сеанс связи начинается с установления соединения между клиентской частью системы, снабженной радиокартой, и точкой доступа. Передаваемая часть трафика является открытой (то есть не содержит конфиденциальной информации). Точка доступа блокирует любые попытки клиентской части войти в сеть до успешного завершения аутентификации и авторизации. Далее пользователь вводит свои имя и пароль. Имя служит идентификатором, без которого невозможны учет и контроль использования ресурсов сети. Пароль, наоборот, представляет собой закрытое сообщение, которое хранится в базе данных сервера и не должно передаваться в открытом виде по радиоканалам, даже если весь остальной трафик будет открытым. Для шифрования пароля применяется односторонняя хэш-функция, работающая по алгоритму MD5. Ее аргументом является пароль пользователя и случайное число, переданное радиокарте сервером на предыдущем этапе. В результате получается дайджест сообщения длиной 128 бит, по которому невозможно вычислить аргумент хэш-функции за разумное время (число вычислений хэш-функции, необходимых для такого определения, равно примерно 2V64). Кроме того, данный дайджест нельзя задействовать для следующей аутентификации, поскольку изменится значение случайного числа, полученного от сервера.

Указанный дайджест вместе с именем пользователя и идентификатором передается на точку доступа и далее на сервер RADIUS. Сервер находит имя потребителя в своей базе данных, извлекает из нее пароль пользователя, присоединяет к нему идентификатор и выполняет хэш-преобразование. Если новый дайджест совпадает с тем, который поступил из точки доступа, сервер принимает положительное решение об аутентификации. Сообщение о положительной аутентификации направляется к точке доступа и дополняется атрибутами, определяющими права данного пользователя при обращении к сетевым ресурсам и содержащимися в той же базе данных сервера RADIUS. Таким образом, процедура авторизации совмещена во времени с процессом аутентификации. Получив это сообщение, точка доступа посылает радиокарте сообщение об успешной аутентификации. Затем радиокарта, применяя ту же самую последовательность, проводит аутентификацию сервера. Данная последовательность действий исключает возможность атаки на сеть путем создания злоумышленником «ложной» точки доступа.

На следующем этапе сервер и радиокарта определяют индивидуальный WEP-ключ, который принадлежит конкретному потребителю в конкретной сессии связи. Сервер RADIUS включает в сообщение об успешной аутентификации специальный атрибут — случайное число. Это число и пароль пользователя служат для формирования WEP-ключа, которое осуществляется с помощью специальной процедуры определения ключа (ПОК), выполняемой программным обеспечением радиокарты и сервера. После успешной взаимной аутентификации радиокарта и сервер независимо друг от друга вычисляют один и тот же сессионный ключ, применяя ПОК. Потом сервер посылает сессионный ключ на точку доступа, которая загружает его для шифрования и дешифровки трафика данного пользователя. Следующий шаг: сервер вычисляет (формирует) WEP-ключ для широковещательных сообщений и передает его на точку доступа, которая зашифровывает этот ключ сессионным ключом и посылает радиокарте.

Такая схема распределения ключей называется динамическим WEP. Ее достоинство состоит в том, что промежуточная точка связи (точка доступа) не располагает какими-либо долговременными секретами (например, паролем пользователя). Кроме того, секретная информация не передается по радиоканалу. Все эти особенности работы оборудования, соответствующего стандарту IEEE 802.1x, делают невозможными атаки, которые были рассмотрены исследователями из Беркли и Массачусетса, либо заставляют злоумышленника задействовать гигантские вычислительные ресурсы.

Итак, применение стандарта IEEE 802.1x в радиосетях позволяет добиться существенного повышения уровня безопасности радиосетей, что выражается в минимизации рисков, связанных с утратой и подделкой оборудования, с эмуляцией хакерами «фальшивого» узла для внедрения в сеть. Другими преимуществами (реализуемыми с помощью динамического алгоритма WEP) являются простота и легкость распределения ключей среди пользователей, повышение стойкости передаваемого трафика к криптоанализу. Использование сервера RADIUS дает возможность управления допуском всех клиентов к сетевым ресурсам из единого центра.

Также специалистами был анонсирован новый протокол WPA, который также призван устранить недостатки, присущие WEP. Сети, работающие по этому протоколу, называются сетями Wi-Fi. Тестирование на совместимость различных решений с WPA и их сертификация начались в феврале 2003 г.

В заключение необходимо отметить, что ни одна система обеспечения безопасности не дает абсолютной гарантии. Рассмотренный нами механизм, реализованный в продуктах Cisco AiroNet 350, является естественным продолжением мер, предпринимаемых для

защиты локальных сетей, и предоставляет беспроводному сегменту такую же защиту, которая характерна для проводного сегмента. Используемые в данном случае протоколы полностью совместимы с обычно применяемыми программными и аппаратными средствами, что позволяет рассматривать проводные и беспроводные сегменты как равноправные. Это открывает перспективы для включения беспроводных сегментов в более крупные защищенные сети (например, в составе VPN). Но в целом для организации полноценной защиты сетей связи недостаточно лишь средств канального и физического уровней — требуется поддержка и на более высоких уровнях (в частности, использование протоколов IPSec). Все сказанное относится и к продуктам других компаний (Lucent Technologies, 3Com и др.), внедряющих новый перспективный стандарт IEEE 802.1x.