Cisco Systems

White Paper (редакция 1.2)

Проблемы безопасности в беспроводных ЛВС IEEE 802.11 и решения Cisco Wireless Security Suite

Дмитрий Бугрименко
dbugrime@cisco.com

1. Введение

С момента ратификации стандарта IEEE 802.11b в 1999 году беспроводные ЛВС получили широкое распространение. Сегодня их можно встретить во многих офисах, конференц-залах, на промышленных складах, в школьных классах, кафе в деловой части мегаполиса.

Беспроводные ЛВС стандарта IEEE 802.11b представляют собой ряд новых проблем для администраторов сетей и систем безопасности. В отличие от проводных сетей Ethernet, беспроводные ЛВС стандарта IEEE 802.11b используют общедоступный радиоканал для связи с абонентами. Этот факт лежит в основе целого ряда новых сложных проблем, решение которых потребовало дополнений к стандарту IEEE 802.11.

Средства обеспечения безопасности, предусмотренные спецификацией IEEE 802.11 и применимые также к 802.11b, 802.11a, 802.11g подверглись тщательному анализу и серьёзной критике. Аналитиками были выявлены и продемонстрированы серьёзные уязвимости в определённых стандартом механизмах аутентификации (authentification), обеспечения конфиденциальности (privacy) и целостности (integrity) данных.

В настоящем документе:

- даётся обзор стандартизованных в Главе 8 спецификации IEEE 802.11 механизмов аутентификации, обеспечения конфиденциальности и целостности данных;
- описаны присущие этим механизмам проблемы уязвимости и управления;
- продемонстрированы способы их устранения с помощью ряда дополнений к стандартным механизмам IEEE 802.11;
- представлена архитектура Cisco Wireless Security Suite корпорации Cisco Systems для усиления режима безопасности в беспроводных ЛВС.
- описана технология контроля доступа на периметре сети IEEE 802.1X и её применение в беспроводной ЛВС.

2. Аутентификация в IEEE 802.11 и её уязвимость

Беспроводные ЛВС, ввиду их широковещательной природы, требуют реализации дополнительных механизмов для:

- *аутентификации абонентов* (user authentication) с целью предотвращения несанкционированного доступа к сетевым ресурсам;
- обеспечения *конфиденциальности данных* (data privacy) с целью обеспечения целостности и защиты при передаче по общедоступному радиоканалу.

Стандарт IEEE 802.11 предусматривает два механизма аутентификации беспроводных абонентов: *открытую аутентификацию* (open authentication) и *аутентификацию с общим ключом* (shared key authentication). Также широко используются два других механизма, а именно назначение *идентификатора беспроводной ЛВС* (Service Set Identifier, SSID) и *аутентификация абонента по его MAC-адресу* (MAC address authentication). Ниже рассмотрены перечисленные механизмы и присущие им недостатки.

Ключи шифрования WEP (Wired Equivalent Privacy) могут быть использованы в качестве своего рода механизма ограничения доступа, поскольку абонент, не обладающий корректным WEP-ключом не сможет ни принять, ни отправить данные в беспроводную ЛВС. Технология шифрования WEP стандарта IEEE 802.11 оперирует ключами длиной 40 либо 104 бита. Технология WEP и присущие ей недостатки рассмотрены в последующих разделах.

2.1. Идентификатор беспроводной ЛВС (Service Set Identificator, SSID)

SSID представляет собой атрибут беспроводной ЛВС, позволяющий логически отличать сети друг от друга. В общем случае, абонент беспроводной сети должен задать у себя соответствующий SSID для того, чтобы получить доступ к требуемой беспроводной ЛВС. SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по отношению к точке радиодоступа беспроводной ЛВС.

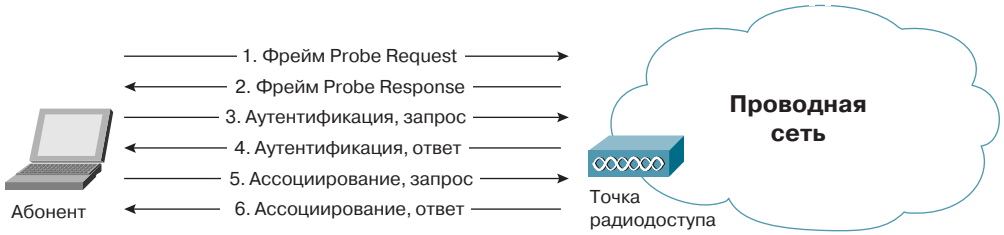
2.2. Аутентификация абонента в IEEE 802.11

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. Стардарт предусматривает два режима аутентификации: открытую и с общим ключом.

Процесс аутентификации абонента беспроводной ЛВС IEEE 802.11 состоит из следующих этапов (рис. 1):

1. Абонент (Client) посылает фрейм *probe request* во все радиоканалы.
2. Каждая точка радиодоступа (access point, AP), в зоне радиовидимости которой находится абонент, посылает в ответ фрейм *probe response*.
3. Абонент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию *(authentication request)*.
4. Точка радиодоступа посылает подтверждение аутентификации *(authentication reply)*.
5. В случае успешной аутентификации абонент посылает точке радиодоступа *association request*.
6. Точка радиодоступа посылает в ответ фрейм *association response*.
7. Абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

Рис. 1 Процесс аутентификации абонента IEEE 802.11



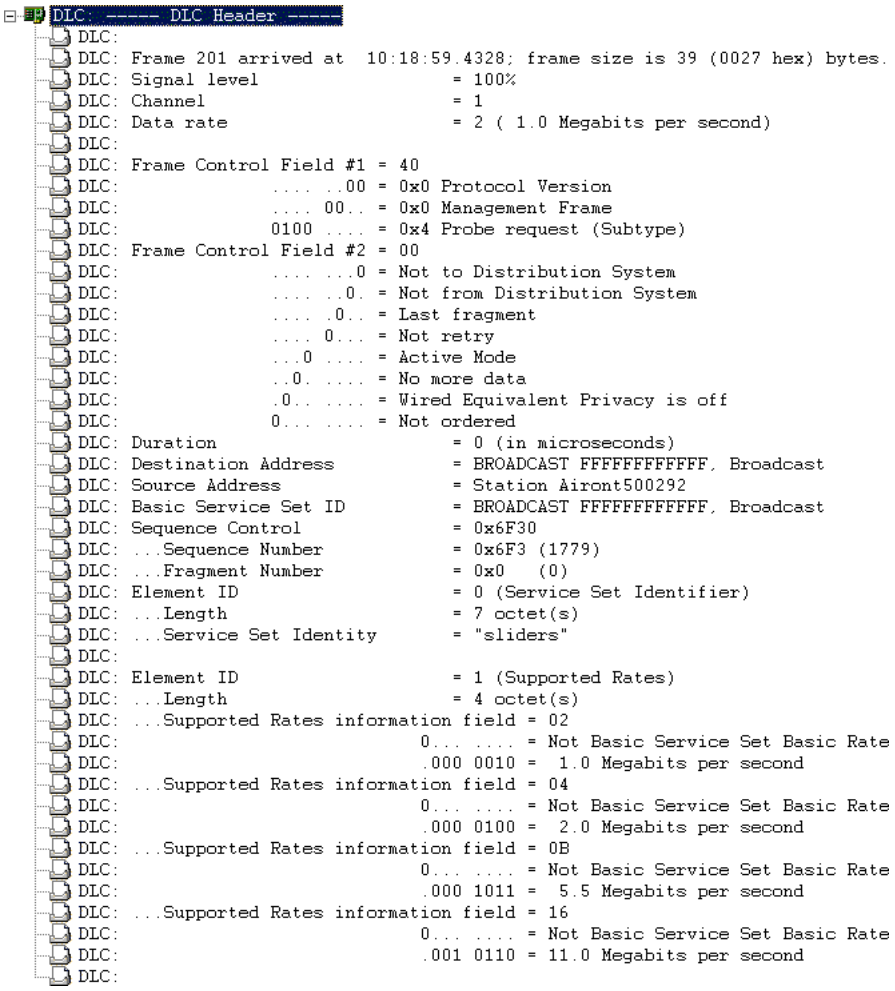
Ниже детально описаны процессы, происходящие на каждом из этапов.

2.2.1. Обмен фреймами Probe Requests, Probe Responses

При активизации беспроводной абонент начинает поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов probe request. Фреймы probe request посылаются в каждый из радиоканалов, поддерживаемых абонентским радиоинтерфейсом, в попытке найти все точки радиодоступа с требуемыми клиенту идентификатором SSID и поддерживаемыми скоростями радиообмена (рис. 2).

Каждая точка радиодоступа из находящихся в зоне радиовидимости абонента и удовлетворяющая запрашиваемым во фрейме probe request параметрам отвечает фреймом probe response, содержащем синхронизирующую информацию и данные о текущей загрузке точки радиодоступа. Абонент определяет, с какой точкой радиодоступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки. После того, как предпочтительная точка радиодоступа определена, абонент переходит в фазу аутентификации.

Рис. 2 Фрейм Probe Request



2.2.2. Открытая аутентификация (Open Authentication)

Открытая аутентификация по сути не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации. На первый взгляд, использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной ЛВС. В добавок к этому, многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т.п.), не имеющие достаточной процессорной мощности, требующейся для реализации сложных алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

- Запрос аутентификации (authentication request) (рис. 3)
- Подтверждение аутентификации (authentication response) (рис. 4)

Рис. 3 Запрос открытой аутентификации

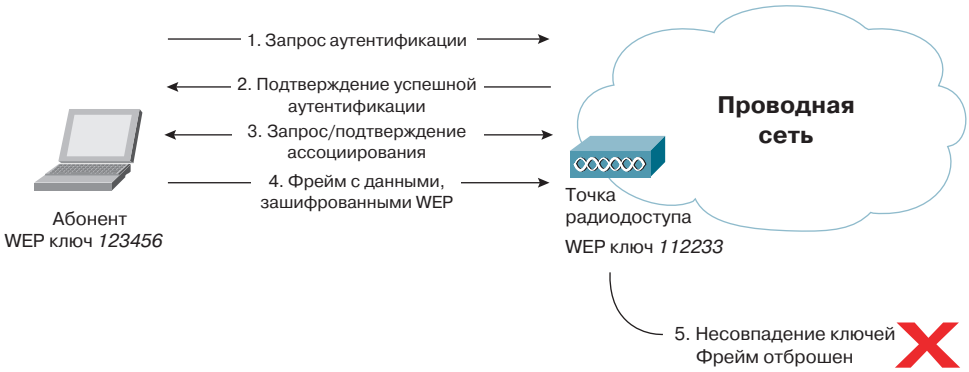
```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 95 arrived at  10:49:47.8255; frame size is 30 (001E hex) bytes.
DLC: Signal level                  = 100%
DLC: Channel                       = 1
DLC: Data rate                     = 2 ( 1.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = B0
DLC:               .... ..00 = 0x0 Protocol Version
DLC:               .... 00.. = 0x0 Management Frame
DLC:               1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:               .... ...0 = Not to Distribution System
DLC:               .... ..0. = Not from Distribution System
DLC:               .... .0.. = Last fragment
DLC:               .... 0... = Not retry
DLC:               ...0 .... = Active Mode
DLC:               ..0. .... = No more data
DLC:               .0.. .... = Wired Equivalent Privacy is off
DLC:               0... .... = Not ordered
DLC: Duration                      = 314 (in microseconds)
DLC: Destination Address           = Station Aironт31669C
DLC: Source Address                = Station Aironт500292
DLC: Basic Service Set ID          = Aironт31669C
DLC: Sequence Control              = 0x0A40
DLC: ...Sequence Number            = 0x0A4 (164)
DLC: ...Fragment Number            = 0x0   (0)
DLC: Authentication algorithm number = 0 (Open System)
DLC: Authentication transaction sequence number = 1
DLC: Status code                   = 0 (Reserved)
```

Рис. 4 Подтверждение открытой аутентификации

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 97 arrived at  10:49:47.8279; frame size is 30 (001E hex) bytes.
DLC: Signal level                  = 81 %
DLC: Channel                       = 1
DLC: Data rate                     = 22 (11.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = B0
DLC:               .... ..00 = 0x0 Protocol Version
DLC:               .... 00.. = 0x0 Management Frame
DLC:               1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:               .... ...0 = Not to Distribution System
DLC:               .... ..0. = Not from Distribution System
DLC:               .... .0.. = Last fragment
DLC:               .... 0... = Not retry
DLC:               ...0 .... = Active Mode
DLC:               ..0. .... = No more data
DLC:               .0.. .... = Wired Equivalent Privacy is off
DLC:               0... .... = Not ordered
DLC: Duration                      = 258 (in microseconds)
DLC: Destination Address           = Station Aironт500292
DLC: Source Address                = Station Aironт31669C
DLC: Basic Service Set ID          = Aironт31669C
DLC: Sequence Control              = 0xED50
DLC: ...Sequence Number            = 0xED5 (3797)
DLC: ...Fragment Number            = 0x0   (0)
DLC: Authentication algorithm number = 0 (Open System)
DLC: Authentication transaction sequence number = 2
DLC: Status code                   = 0 (Successful)
```

Таким образом, при открытой аутентификации возможен доступ любого абонента к беспроводной ЛВС. Если в беспроводной ЛВС не используется шифрование, то любой абонент, знающий идентификатор SSID точки радиодоступа, получит доступ к сети. При использовании точками радиодоступа шифрования WEP сами ключи шифрования становятся средством контроля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку радиодоступа, ни расшифровывать данные, переданные точкой радиодоступа (рис. 5).

Рис. 5 Открытая аутентификация с несовпадающими WEP-ключами

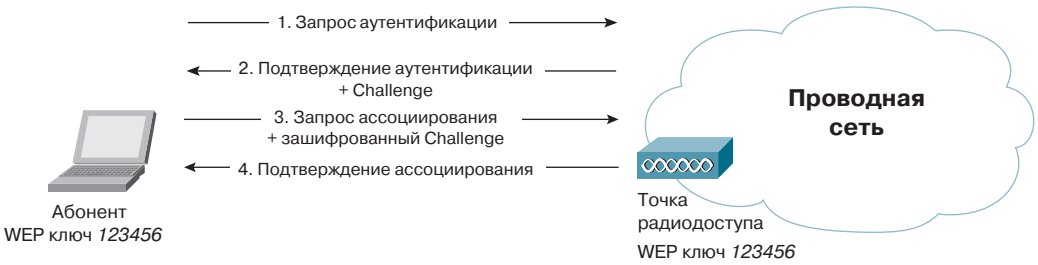


2.2.3. Аутентификация с общим ключом (Shared Key Authentication)

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации иллюстрирует рис. 6:

1. Абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.
2. Точка радиодоступа посылает подтверждение аутентификации , содержащее challenge text.
3. Абонент шифрует challenge text своим статическим WEP-ключом, и посылает точке радиодоступа запрос аутентификации.
4. Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем challenge text, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.

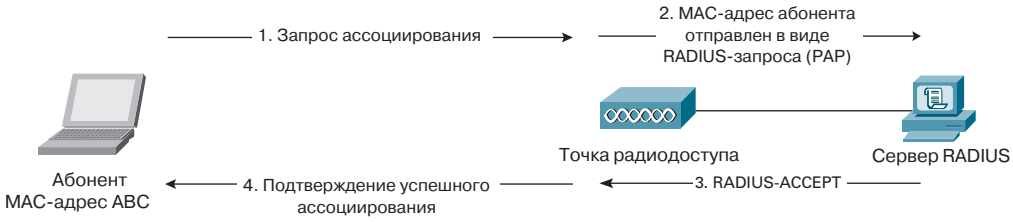
Рис. 6 Аутентификация с общим ключом



2.2.4. Аутентификация по MAC-адресу (MAC Address Authentication)

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных ЛВС, в том числе Cisco Systems. При аутентификация по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации (рис. 7). Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.

Рис. 7 Аутентификация по MAC-адресу



2.3. Уязвимость механизмов аутентификации

2.3.1. Проблемы идентификатора беспроводной ЛВС

Идентификатор SSID регулярно передается точками радиодоступа во фреймах beacon (рис. 8). Несмотря на то, то фреймы beacon играют чисто информационную роль в радиосети, т.е. совершенно "прозрачны" для абонента, сторонний наблюдатель в состоянии с легкостью определить SSID с помощью анализатора трафика протокола 802.11, например Sniffer Pro Wireless. Некоторые точки радиодоступа, в т.ч. Cisco Aironet, позволяют административно запретить широковещательную передачу SSID внутри фреймов beacon. Однако и в этом случае SSID можно легко определить путем захвата фреймов probe response, посылаемых точками радиодоступа (рис. 9).

Рис. 8 SSID в Beacon-фрейме точки радиодоступа

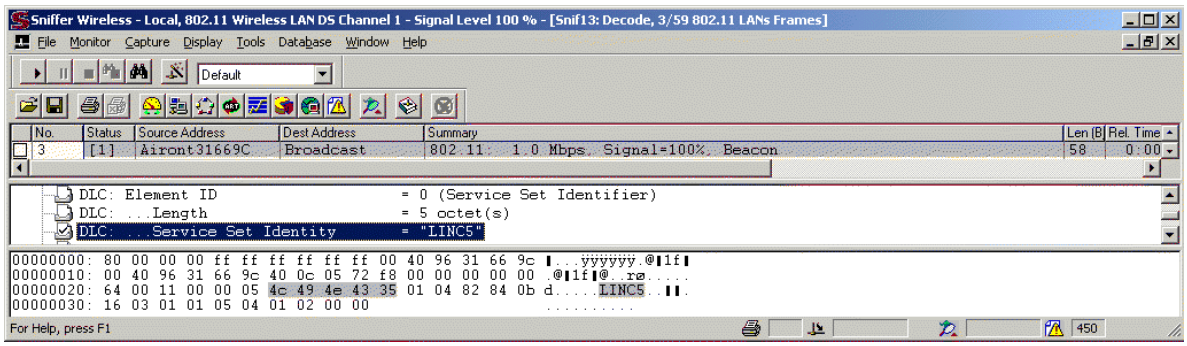
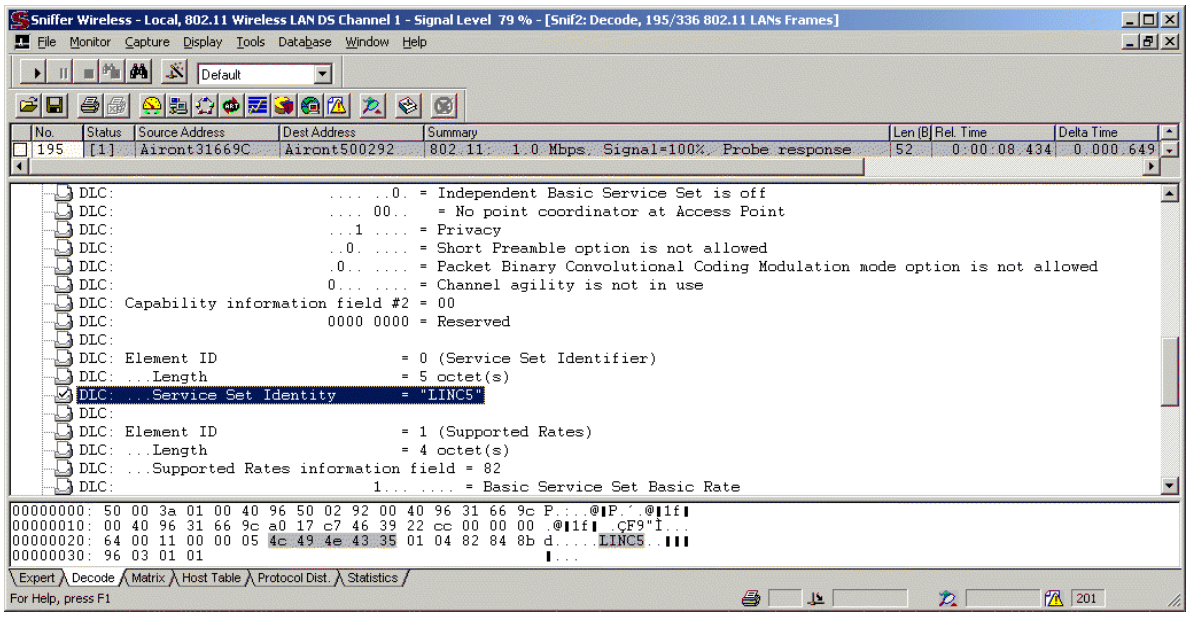


Рис. 9 SSID в фрейме Probe Response точки радиодоступа



Идентификатор SSID не разрабатывался для использования в качестве механизма обеспечения безопасности. В добавок к этому, отключение широковещательной передачи SSID точками радиодоступа может серьёзно отразиться на совместимости оборудования беспроводных ЛВС различных производителей при использовании в одной радиосети. Вследствие этого Cisco не рекомендует использование SSID в целях реализации режима безопасности.

2.3.2. Уязвимость открытой аутентификации

Открытая аутентификация не позволяет точке радиодоступа определить, является ли абонент легитимным или нет. Это становится серьезной брешью в системе безопасности в том случае, если в беспроводной ЛВС не используется шифрование WEP. Cisco не рекомендует эксплуатацию беспроводных ЛВС без шифрования WEP. В случаях, когда использование шифрования WEP не требуется или невозможно (например в беспроводных ЛВС публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством Cisco Service Selection Gateway (SSG).

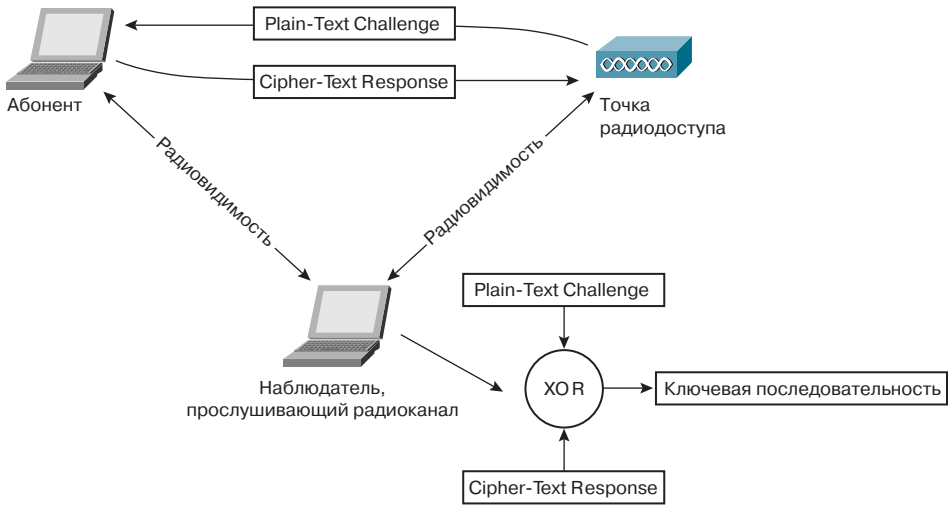
2.3.3. Уязвимость аутентификации с общим ключом

Аутентификация с общим ключом требует настройки у абонента статического WEP-ключа для шифрования challenge text, отправленного точкой радиодоступа. Точка радиодоступа аутентифицирует абонента посредством дешифрования его ответа на challenge и сравнения его с отправленным оригиналом.

Обмен фреймами, содержащими challenge text, происходит по открытому радиоканалу, а значит подвержен атакам со стороны стороннего наблюдателя (man-in-the-middle attack). Наблюдатель может принять как не-шифрованный challenge text, так и тот же challenge text, но уже в шифрованном виде (рис. 10). Шифрование WEP производится путем выполнения побитовой операции XOR над текстом сообщения и ключевой послкдо-вательностью (key stream), в результате чего получается зашифрованное сообщение (ciphertext). Важно понимать, что выполнение побитовой операции XOR над зашифрованным сообщением и ключевой

последовательностью имеет результатом текст исходного сообщения. Таким образом, наблюдатель может легко вычислить сегмент ключевой последовательности путем анализа фреймов в процессе аутентификации абонента.

Рис. 10 Уязвимость аутентификации с общим ключом



2.3.4. Уязвимость аутентификации по MAC-адресу

Стандарт IEEE 802.11 требует передачи MAC-адресов абонента и точки радиодоступа в открытом виде. В результате этого в беспроводной ЛВС, использующей аутентификацию по MAC-адресу, хакер может обмануть метод аутентификации путём подмены своего MAC-адреса на легитимный.

Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Хакер может воспользоваться анализатором трафика протокола IEEE 802.11 для выявления MAC-адресов легитимных абонентов.

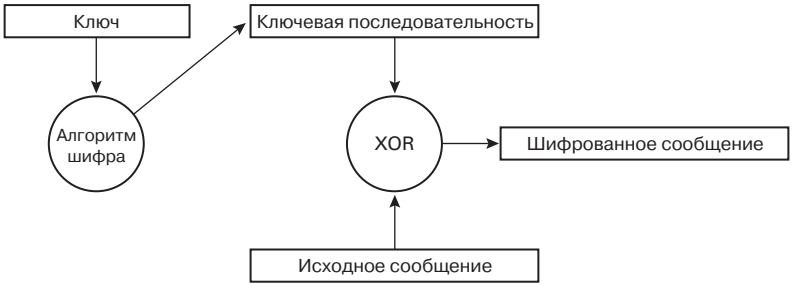
3. Уязвимость шифрования WEP

Шифрование WEP основано на алгоритме RC4, представляющем собой симметричное потоковое шифрование (symmetric key stream cipher). Как было отмечено ранее, для нормального обмена пользовательскими данными ключи шифрования у абонента и точки радиодоступа должны быть идентичными. Ниже рассматривается принципы работы алгоритмов потокового шифрования и проводится их сравнение с алгоритмами блочного шифрования.

3.1. Потоковое шифрование (Stream Cipher) и блочное шифрование (Block Ciphers)

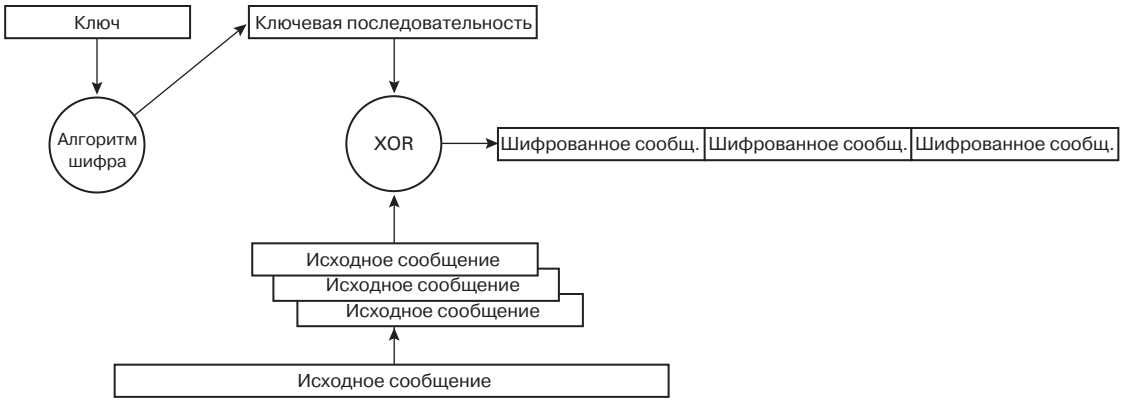
При потоковом шифровании выполняется побитовое сложение по модулю 2 (функция “исключающее ИЛИ“, XOR) ключевой последовательности, генерируемой алгоритмом шифрования на основе заранее заданного ключа, и исходного сообщения. Ключевая последовательность имеет длину, соответствующую длине исходного сообщения, подлежащего шифрованию (рис. 11).

Рис. 11 Потоковое шифрование



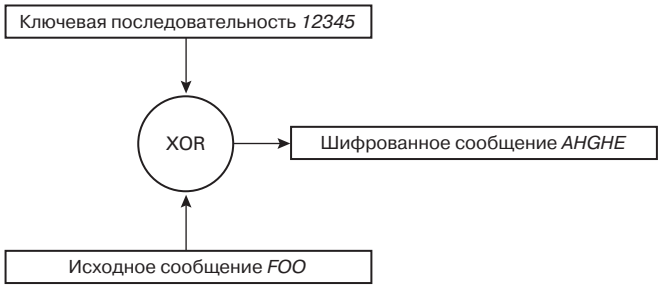
Блочное шифрование работает с блоками заранее определенной длины, не меняющейся в процессе шифрования. Исходное сообщение фрагментируется на блоки, и функция XOR вычисляется над ключевой последовательностью и каждым блоком. Размер блока фиксирован, а последний фрагмент исходного сообщения дополняется пустыми символами до длины нормального блока (рис. 12). Например, при блочном шифровании с 16-байтовыми блоками исходное сообщения длиной в 38 байтов фрагментируется на два блока длиной по 16 байтов и 1 блок длиной 6 байтов, который затем дополняется 10 байтами пустых символов до длины нормального блока.

Рис. 12 Блочное шифрование



Потоковое шифрование и блочное шифрование используют метод электронной кодовой книги (Electronic Code Book, ECB, encryption mode). Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе всегда порождает одно и то же защифрованное сообщение на выходе. Так на рис. 13 исходное сообщение "FOO" всегда преобразуется в одно и то же защифрованное сообщение “AHGHE”. Это представляет собой потенциальную брешь в системе безопасности, ибо сторонний наблюдатель, обнаружив повторяющиеся последовательности в защифрованном сообщении, в состоянии сделать обоснованные предположения относительно идентичности содержания исходного сообщения.

Рис. 13 Метод электронной кодовой книги



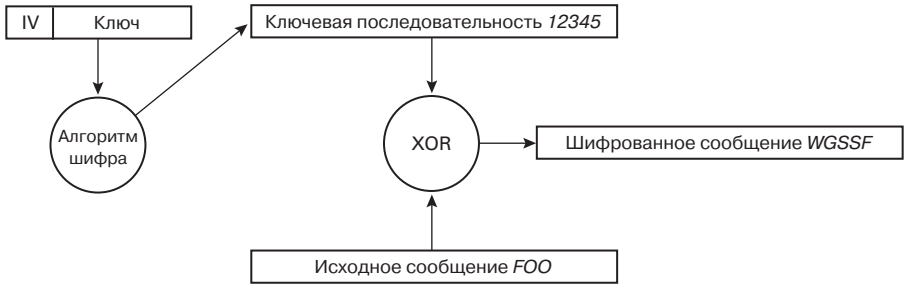
Для устранения указанной проблемы используют:

1. Векторы инициализации (Initialization Vectors, IVs)
2. Обратную связь (feedback modes)

3.1.1. Вектор инициализации (Initialization Vector, IV)

Вектор инициализации используется для модификации ключевой последовательности. При использовании вектора инициализации ключевая последовательность генерируется алгоритмом шифрования, на вход которого подаётся секретный ключ, конкатенированный с IV. При изменении вектора инициализации ключевая последовательность также меняется. На рис. 14 исходное сообщение "FOO" шифруется с использованием новой ключевой последовательности, сгенерированной алгоритмом шифрования после подачи на его вход комбинации из секретного ключа и вектора инициализации, что порождает на выходе шифрованное сообщение, отличное от рис. 13. Стандарт IEEE 802.11 рекомендует использование нового значения вектора инициализации для каждого нового фрейма, передаваемого в радиоканал. Таким образом, один и тот же нешифрованный фрейм, передаваемый многократно, каждый раз будет порождать уникальный шифрованный фрейм.

Рис. 14 Шифрование с использованием вектора инициализации



Вектор инициализации имеет длину 24 бита (рис. 15) и конкатенируется с 40- или 104-битовым базовым ключом шифрования WEP, таким образом на вход алгоритма шифрования подается 64- или 128-битовый ключ. Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале, с тем чтобы принимающая сторона могла успешно декодировать этот фрейм (рис. 16). Несмотря на то, что обычно говорят об использовании шифрования WEP с ключами длиной 64 или 128 битов, эффективная длина ключа составляет лишь 40 или 104 бита по причине передачи вектора инициализации в нешифрованном виде.

Рис. 15 Вектор инициализации в шифрованном фрейме

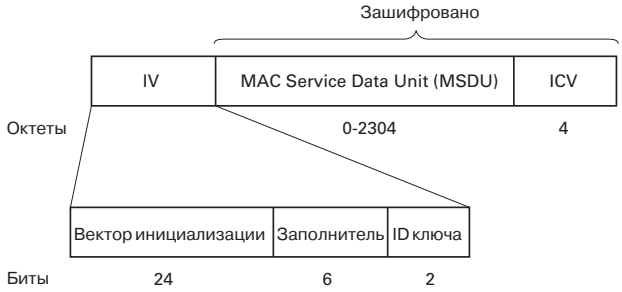


Рис. 16 Вектор инициализации в фрейме 802.11

```
DLC: WEP (Wired Equivalent Privacy) Header
DLC:   Initialization Vector #(1-3)= D200F8
DLC: ...Initialization Vector #4    = C0
DLC:                          11.. .... = 3 (Key ID 4)
DLC:                          ..00 0000 = Pad
DLC: ...[68 byte(s) of encrypted MSDU]
DLC: ...Encrypted Integrity Check Value = F9E3F873
```

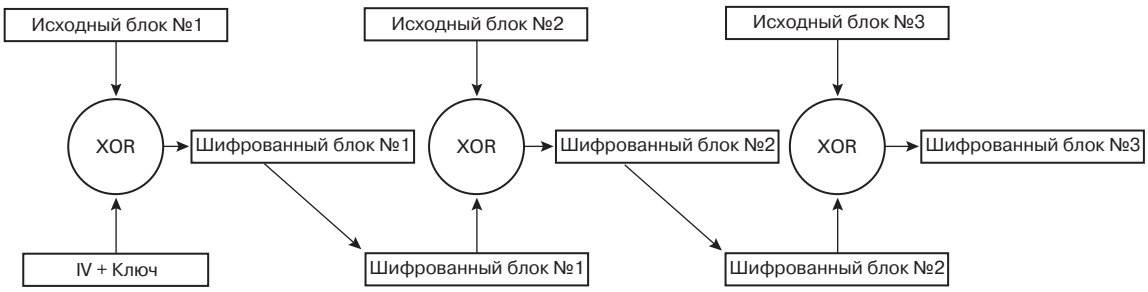
3.1.2. Обратная связь

Обратная связь модифицируют процесс шифрования и предотвращают порождение одним и тем же исходным сообщением одного и того же шифрованного сообщения. Обратная связь обычно используется при блочном шифровании. Наиболее часто встречается тип обратной связи, известный как цепочка шифрованных блоков (cipher block chaining, CBC, mode).

В основе использования цепочки шифрованных блоков лежит идея вычисления двоичной функции XOR между блоком исходного сообщения и предшествовавшим ему блоком шифрованного сообщением. Поскольку самый первый блок не имеет предшественника, для модификации ключевой последовательности используют вектор инициализации. Работу цепочки шифрованных блоков иллюстрирует рис. 17.

Существуют и другие типы обратной связи, некоторые их них будут обсуждаться впоследствии.

Рис. 17 Цепочка шифрованных блоков



3.2. Пассивные сетевые атаки—статистический метод вычисления ключа

В августе 2001 года криптоаналитики Fluhrer, Mantin, и Shamir установили, что секретный ключ шифрования WEP может быть вычислен с использованием определенных фреймов (interesting frames), пассивно собранных в беспроводной ЛВС. Причиной уязвимости послужила реализация в WEP метода планирования ключей (key scheduling algorithm, KSA) алгоритма потокового шифрования RC4. Некоторые векторы инициализации (так называемые “слабые” векторы) дают возможность установить побайтовый состав секретного ключа, применяя статистический анализ. Исследователями из AT&T/Rice University и авторами программы AirSnort была продемонстрорована возможность определения секретного ключа длиной 40 и 128 битов после анализа всего лишь 4 миллионов фреймов. Для загруженной беспроводной ЛВС это эквивалентно приблизительно 4 часам работы, после чего ключ шифрования станет известен пассивному наблюдателю.

Подобная уязвимость делает шифрование с использованием WEP неэффективным, лишая его криптографической стойкости. Использование динамических секретных ключей шифрования WEP рещает проблему лишь частично, для полного устранения уязвимости требуется способ усиления самого ключа.

3.3. Активные сетевые атаки—индуктивное вычисление ключа

Индуктивное вычисление секретного ключа шифрования WEP представляет собой процесс воздействия на беспроводную ЛВС для получения определённой информации и относится к классу активных сетевых атак. Как было сказано ранее, при потоковом шифровании выполняется двоичное сложение по модулю 2 исходного сообщения с ключевой последовательностью с целью получения шифрованного сообщения. Этот факт лёг основу данной атаки.

Высокая эффективность атаки индуктивного вычисления ключа, предпринимаемой сторонним наблюдателем в беспроводной ЛВС IEEE 802.11 объясняется отсутствием действенных средств контроля целостности сообщений (message intgrity check, MIC). Принимающая сторона не в состоянии распознать факт модификации содержимого фрейма в процессе передачи по общедоступному радиоканалу. Более того, значение Integrity Check Value (ICV), предусмотренное стандартом для контроля целостности сообщений, вычисляется с помощью функции CRC32, которая подвержена атакам с манипуляцией битами. Таким образом, в отсутствии механизмов контроля целостности сообщений беспроводные ЛВС подвержены активным атакам с манипуляцией битами (bit-flipping) и поторным использованием вектора инициализации (IV replay).

3.3.1. Повторное использование вектора инициализации (Initialization Vector Replay Attacks)

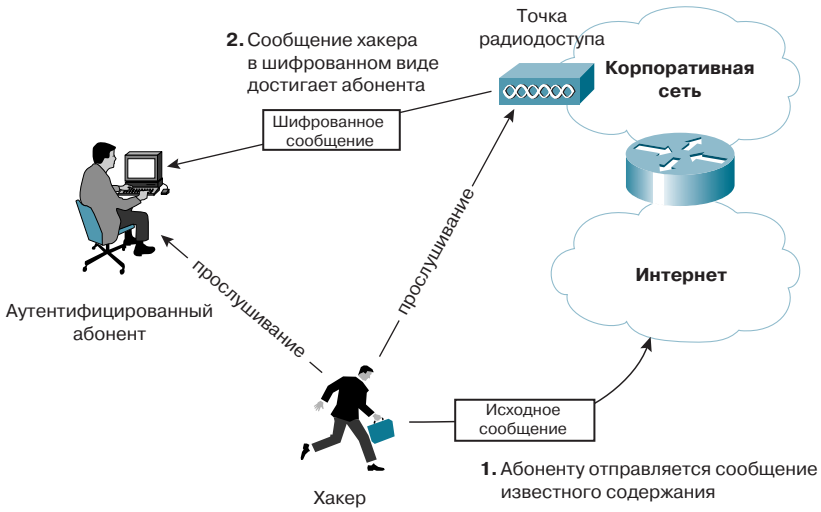
IV replay представляет собой разработанную теоретически и реализованную практически активную сетевую атаку в беспроводной ЛВС, существующую в нескольких разновидностях, одна из которых описана ниже и проиллюстрирована на рис. 18:

1. Хакер многократно отправляется абоненту беспроводной ЛВС по проводной сети сообщение известного содержания (например, IP пакет, письмо электронной почты, и т.п.)
2. Хакер пассивно прослушивает радиоканал связи абонента с точкой радиодоступа и собирает фреймы, предположительно содержащие шифрованное сообщение.
3. Хакер вычисляет ключевую последовательность, применяя функцию XOR к предполагаемому шифрованному и известному нешифрованному сообщениям.

4. Хакер “выращивает“ ключевую последовательность для пары вектора инициализации и секретного ключа, породившей ключевую последовательность, вычисленную на предыдущем шаге.

В основе атаки лежит знание того, что пара вектора инициализации и секретного ключа шифрования, а значит и порождаемая ими ключевая последовательность, может быть повторно использована для воссоздания ключевой последовательности достаточной длины для нарушения конфиденциальности в беспроводной ЛВС в условиях использования шифрования WEP.

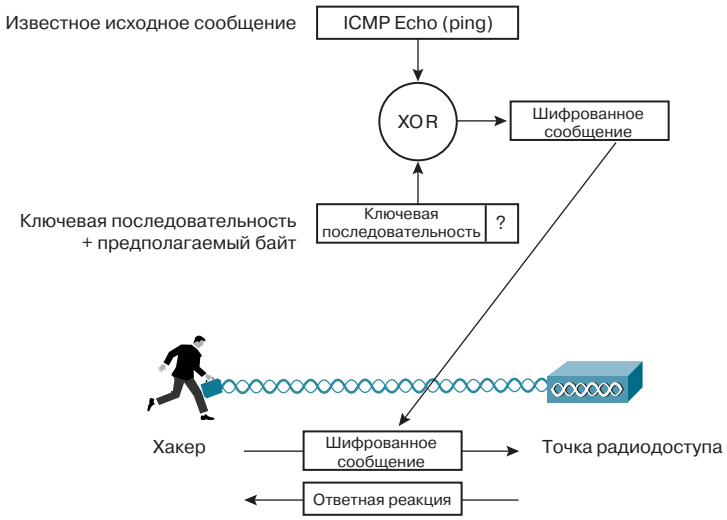
Рис. 18 Повторное использование вектора инициализации



После того, как ключевая последовательность вычислена для фреймов некоторой длины, она может быть “выращена“ до любого требуемого размера, как описано ниже и проиллюстрировано на рис. 19:

1. Хакер создает фрейм на один байт длинее, чем длина уже известной ключевой последовательности. Пакеты ICMP echo request (ping) идеальны для этих целей, ибо точка радиодоступа вынуждена на них отвечать.
2. Хакер увеличивает длину ключевой последовательности на один байт.
3. Значение дополнительного байта выбирается случайным образом из 256 возможных.
4. Если предполагаемое значение дополнительного байта ключевой последовательности верно, то будет получен ожидаемый ответ от точки радиодоступа, в данном примере это ICMP echo reply.
5. Процесс повторяется до тех пор, пока не будет подобрана ключевая последовательность требуемой длины.

Рис. 19 "Выращивание" ключевой последовательности



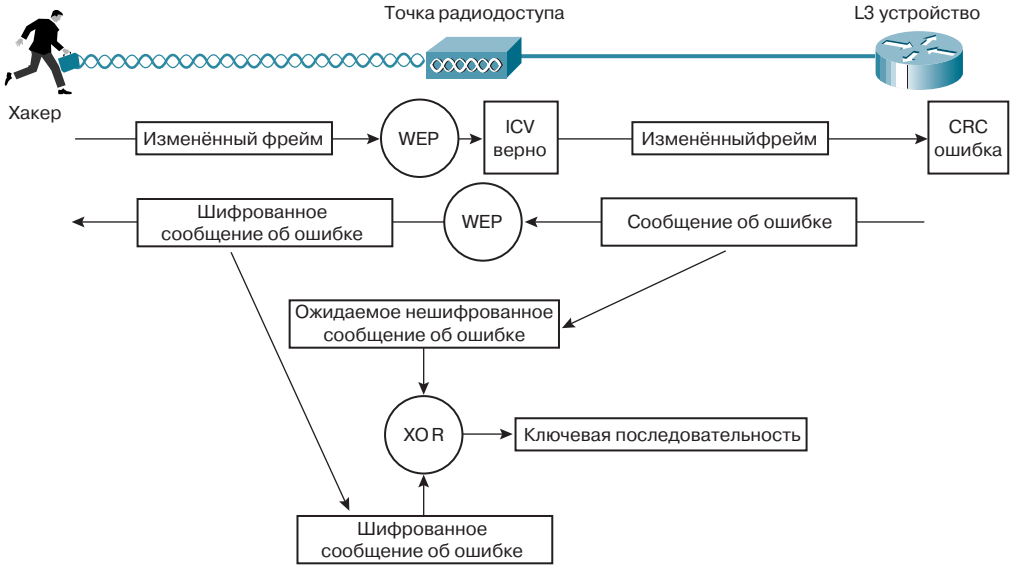
3.3.2. Манипуляция битами (Bit-Flipping Attacks)

Манипуляция битами преследует ту же цель, что и повторное использование вектора инициализации, и опирается на уязвимость вектора контроля целостности фрейма ICV. Пользовательские данные могут различаться от фрейма к фрейму, в то же самое время многие служебные поля и их положение внутри фрейма остаются неизменными. Хакер манипулирует битами пользовательских данных внутри L2-фрейма с целью искажения L3-пакета. Процесс манипуляции проиллюстрирован на рис. 20:

1. Хакер пассивно наблюдает фреймы беспроводной ЛВС с помощью средств анализа трафика протокола 802.11.
2. Хакер захватывает фрейм и произвольно изменяет биты в поле данных протокола 3-го уровня.
3. Хакер модифицирует значение вектора контроля целостности фрейма ICV (как именно будет описано ниже).
4. Хакер передаёт модифицированный фрейм в беспроводную ЛВС.
5. Принимающая сторона (абонент либо точка радиодоступа) вычисляет значение вектора контроля целостности фрейма ICV для полученного модифицированного фрейма.
6. Принимающая сторона сравнивает вычисленное значение вектора ICV с имеющимся в полученном модифицированном фрейме.
7. Значения векторов совпадают, фрейм считается неискажённым и не отбрасывается.
8. Принимающая сторона деинкапсулирует содержимое фрейма и обрабатывает пакет сетевого уровня.
9. Поскольку манипуляция битами происходила на канальном уровне, контрольная сумма пакета сетевого уровня оказывается неверной.
10. Стек протокола сетевого уровня на принимающей стороне генерирует предсказуемое сообщение об ошибке.
11. Хакер наблюдает за беспроводной ЛВС в ожидании зашифрованного фрейма с сообщением об ошибке.

12. Хакер захватывает фрейм, содержащий зашифрованное сообщение об ошибке и вычисляет ключевую последовательность, как это было описано ранее для атаки с повторным использованием вектора инициализации на стр. 13.

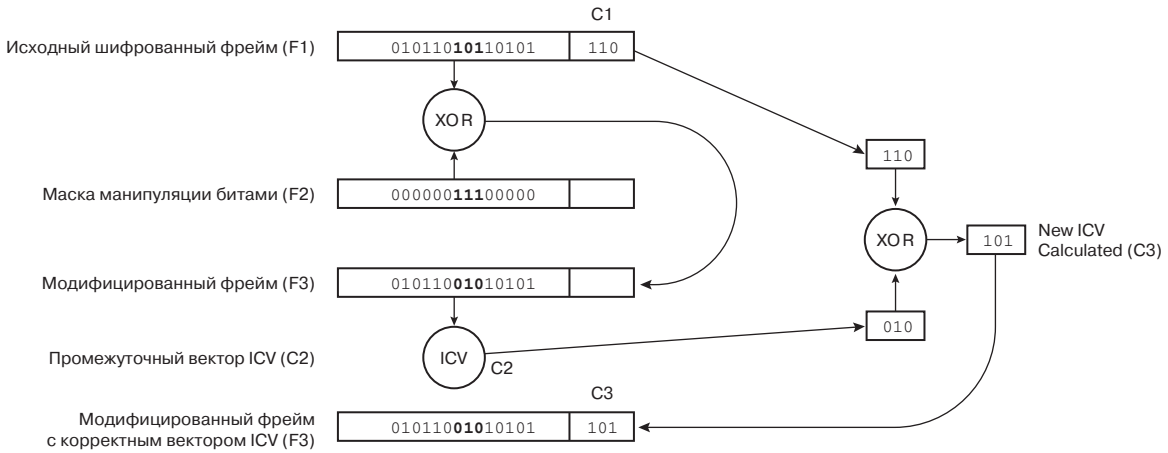
Рис. 20 Атака с манипуляцией битами



Вектор ICV находится в шифрованной части фрейма. С помощью следующей процедуры хакер манипулирует битами шифрованного вектора ICV и таким образом обеспечивает корректность самого вектора для нового, модифицированного фрейма (рис. 21):

1. Исходный фрейм F1 имеет вектор C1.
2. Создаётся фрейм F2 таклй же длины, что и F1, служащий маской для модификации битов фрейма F1.
3. Создаётся фрейм F3 путём выполнения двоичной функции XOR над фреймами F1 и F2.
4. Вычисляется промежуточный вектор C2 для фрейма F3.
5. Вектор C3 для фрейма F3 вычисляется путём выполнения двоичной функции XOR над C1 и C2.

Рис. 21 Уязвимость ICV



3.4. Проблемы управления статическими WEP-ключами

Стандартом IEEE 802.11 не предусмотрены какие либо механизмы управления ключами шифрования. По определению, алгоритм WEP поддерживает лишь статические ключи, которые заранее распространяются тем или иным способом между абонентами и точками радиодоступа беспроводной ЛВС. Поскольку IEEE 802.11 аутентифицирует физическое устройство, а не его пользователя, утрата абонентского адаптера, точки радиодоступа или собственно секретного ключа представляют опасность для системы безопасности беспроводной ЛВС. В результате при каждом подобном инциденте администратор сети будет вынужден вручную произвести смену ключей у всех абонентов и в точках доступа.

Эти административные действия приемлемы для небольшой беспроводной ЛВС, но совершенно неприемлимы для сетей, в которых абоненты исчисляются сотнями и тысячами, и/или распределены территориально. В условиях отсутствия механизмов генерации и распространения ключей администратор вынужден пристально охранять абонентские адаптеры и оборудование инфраструктуры сети.

4. Cisco Wireless Security Suite для обеспечения безопасности в беспроводной ЛВС

Cisco Systems отчётливо осознаёт многочисленные уязвимости механизмов аутентификации, конфиденциальности и целостности в IEEE 802.11. Чтобы обеспечить возможность создания безопасных, при этом масштабируемых и управляемых беспроводных ЛВС, Cisco Systems разработала набор дополнений и улучшений механизмов аутентификации и шифрования IEEE 802.11, получивший название Cisco Wireless Security Suite.

Некоторые специалисты ошибочно считают WEP единственным компонентом системы безопасности беспроводной ЛВС, однако в действительности таких компонентов три:

1. Архитектура аутентификации.
2. Механизм аутентификации.
3. Механизм обеспечения конфиденциальности и целостности данных.

Все указанные компоненты присутствуют в составе Cisco Wireless Security Suite:

- Архитектура аутентификации IEEE 802.1X — стандарт IEEE 802.1X описывает единую архитектуру контроля доступа к портам с использованием разнообразных методов аутентификации абонентов.
- Алгоритм аутентификации Cisco Lightweight Extensible Authentication Protocol (LEAP) — поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной ЛВС и её пользователей с возможностью динамической генерации ключей шифрования.
- Протокол Temporal Key Integrity Protocol (TKIP) — разработанные Cisco Systems средства усиления алгоритма шифрования WEP:
  - проверка целостности сообщений (Message Integrity Check, MIC) — обеспечивает аутентичность данных, предотвращает возможность манипуляции сообщениями сторонними лицами;
  - попакетная смена ключа шифрования (Per-Packet Keying) — обеспечивает уникальность ключа для каждого пакета, делает безуспешными пассивные и активные атаки, направленные на вычисление ключа;
  - динамическая смена ключей шифрования широковещательного трафика (Broadcast Key Rotation).

4.1. Компоненты Cisco Wireless Security Suite

4.1.1. Архитектура аутентификации 802.1X

В основе Cisco Wireless Security Suite лежит архитектура контроля доступа к ЛВС IEEE 802.1X. Подробная информация о IEEE 802.1X представлена в разделе “Контроль доступа к сети в стандарте IEEE 802.1X” на стр. 22.

4.1.2. LEAP – алгоритм аутентификации EAP от Cisco

Cisco Systems разработала алгоритм LEAP в 2001 году для обеспечения сильной аутентификации, не требующей при этом трудоёмкого администрирования. LEAP, как и другие разновидности алгоритмов аутентификации в классе EAP, функционирует в рамках архитектуры 802.1X. Причина популярности алгоритма кроется в его обширных возможностях.

4.1.2.1. Взаимная аутентификация (Mutual Authentication)

В беспроводныой ЛВС абонент должен быть уверен в том, что работает с легитимными элементами инфраструктуры. Ввиду отсутствия физического подключения к сети абоненту необходимо аутентифицировать сеть, равно как аутентифицироваться самому по отношению к сети. Cisco LEAP поддерживает взаимную аутентификацию.

4.1.2.2. Аутентификация конечного пользователя (User-Based Authentication)

Стандарт IEEE 802.11 предусматривает аутентификацию физических устройств, а конечный пользователь беспроводного оборудования остаётся невидим для процесса аутентификации, поэтому неавторизованный пользователь одновременно с получением доступа к физическому устройству автоматически получает беспрепятственный доступ к беспроводной ЛВС. В частности, угрозу системе безопасности представляют портативные компьютеры, оснащенные интерфейсами 802.11 и использующие статические ключи WEP для обеспечения конфиденциальности и аутентификации, которые могут быть утеряны или похищены. В случае утраты такого оборудования администраторы вынуждены в кратчайшие сроки произвести смену WEP-ключей во всей беспроводной ЛВС.

Описанный сценарий встречается крайне часто и является одним из главных препятствий для развёртывания беспроводных ЛВС. Cisco LEAP поддерживает аутентификацию пользователя в дополнение к аутентификации физического устройства.

4.1.2.3. Динамические WEP-ключи

Несмотря на то, что взаимная аутентификация пользователя и беспроводной сети обеспечивает очень высокий уровень безопасности при минимальном и полностью централизованном администрировании, тем не менее необходимы механизмы эффективного управления WEP-ключами. Cisco LEAP поддерживает динамическую генерацию уникальных сессионных ключей для каждого абонента беспроводной ЛВС.

802.1X предусматривает использование таймаута для периодической реаутентификации абонентов. Процесс реаутентификации прозрачен для абонента, периодически генерирует новые ключи по истечении административно заданного интервала времени. Эта технология позволяет предотвратить атаки, направленные на статистическое вычисление ключа WEP, и является существенной частью усовершенствований Cisco для WEP.

4.1.3. Обеспечение конфиденциальности данных посредством TKIP

В предыдущих разделах были рассмотрены разнообразные сетевые атаки на беспроводные ЛВС 802.11 и продемонстрирована неэффективность WEP для обеспечения конфиденциальности и целостности данных. Cisco Systems разработала ряд предстандартных усовершенствований технологии WEP, исключающих перечисленные выше уязвимости. Этот набор усовершенствований получил название Temporal Key Integrity Protocol (TKIP), и был принят в качестве основы рабочей группой IEEE 802.11 Task Group i.

В TKIP входят следующие улучшения технологии WEP:

1. Контроль целостности данных (message integrity check, MIC) шифрованных фреймов.
2. Попакетная смена ключа шифрования (Per-Packet Keying).
3. Периодическая смена широковещательного ключа (broadcast key rotation) (эта возможность в настоящее время не входит в предварительные спецификации IEEE 802.11 Task Group i).

4.1.3.1. Контроль целостности данных (message integrity check, MIC)

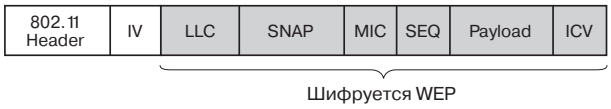
MIC повышает эффективность стандартной функции контроля целостности данных ICV в 802.11. MIC позволяет исключить следующие уязвимости:

- Повторное использование вектора инициализации и базового ключа—MIC добавляет к фрейму поле с порядковым номером (sequence number), а точка беспроводного доступа отбрасывает все фреймы с нарушенным порядком следования.
- Манипуляция битов—MIC добавляет к фрейму поле контроля целостности данных, не имеющее проблем, присущих вектору ICV.

На рис. 22 приведен формат стандартного фрейма, а на рис. 23–фрейма, использующего контроль целостности данных MIC.

Рис. 22 Формат WEP-фрейма

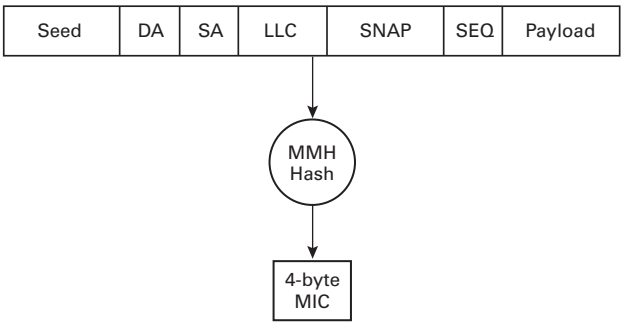
Рис. 23 Формат WEP-фрейма с полем контроля целостности MIC



Поле порядкового номера sequence number представляет собой счетчик, инкрементируемый на единицу для каждого вновь передаваемого фрейма индивидуально для каждой пары абонент–точка радиодоступа. Точка радиодоступа отбрасывает фреймы с нарушенным порядком следования.

Поле контроля целостности данных MIC вычисляется для составных частей фрейма, как показано на рис. 24.

Рис. 24 Вычисление поля контроля целостности MIC



Изменение содержимого фрейма в процессе передачи приведёт к расхождению значений MIC, содержащегося во фрейме и вычисленного на принимающей стороне. В результате получатель (точка радиодоступа либо абонент) отбросит модифицированный фрейм.

На настоящий момент такая реализация MIC является предстандартной. Несмотря на то, что она входит в предварительные спецификации IEEE 802.11 Task Group i, не все производители оборудования для беспроводных ЛВС её поддерживают. Таким образом, использование MIC требует наличия точки радиодоступа Cisco Aironet.

4.1.3.2. Попакетная смена ключа шифрования (Per-Packet Keying)

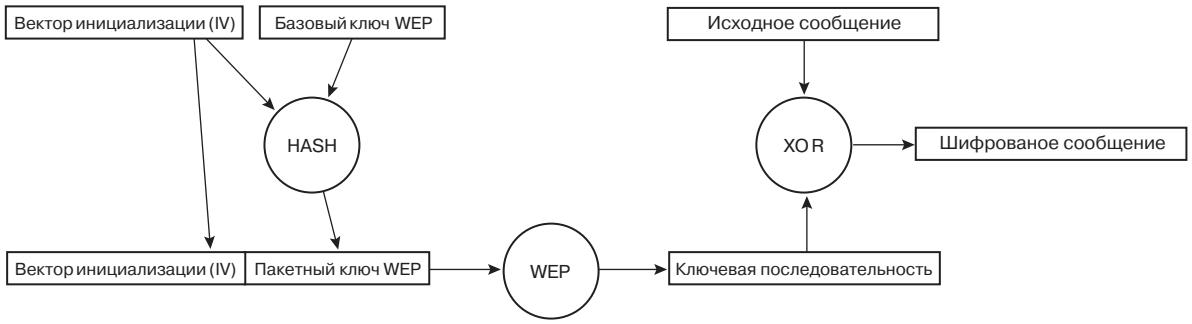
Уязвимости, обнаруженные криптоаналитиками Fluhrer, Mantin, и Shamir, и обыгранные в программе AirSnort, сделали протокол WEP неэффективным для обеспечения конфиденциальности и целостности данных. Периодическая смена ключей в процессе реаутентификации смягчает, но полностью не устраняет проблему.

IEEE 802.11 Task Group i включила механизм попакетной смены ключей в предварительную спецификацию стандарта. Cisco Systems была инициатором этого усовершенствования, и реализовала его в абонентском оборудовании и точках радиодоступа.

В реализации Cisco Systems алгоритма WEP векторы инициализации IV генерируются случайным образом, затем конкатенируются с базовым ключом и подаются на вход алгоритма шифрования для генерации ключевой последовательности, которая затем посредством двоичной функции XOR шифрует исходное сообщение.

В реализации Cisco Systems алгоритма попакетной смены ключа усиление криптографической стойкости происходит путём хеширования базового WEP-ключа и вектора инициализации IV, а затем использовании результата в качестве нового базового ключа шифрования. Оригинальный вектор инициализации конкатенируется с новым ключом и подаётся на вход алгоритма шифрования обычным образом (рис. 25).

Рис. 25 Попакетная смена ключа шифрования.



Для эффективного использования пространства 24-битовых векторов инициализации Cisco Systems выбрала метод sequencing. Абонент и точка радиодоступа реализуют метод sequencing путём создания 24-битового счетчика, инкрементирования его на единицу для каждого нового фрейма и использования значения в качестве вектора инициализации IV. Если абонент и точка радиодоступа одновременно инициализируют счетчик IV нулевым значением, это приведёт к к подаче одинаковых комбинаций вектора инициализации IV и базового ключа WEP на вход хэш-алгоритма и генерации одинаковых ключей шифрования. Для предотвращения подобного эффекта метод sequencing наделён свойством направленности, а именно фреймы абонента могут использовать чётные значения векторов IV, фреймы точки радиодоступа—нечётные.

При попакетной смене ключи шифрования будут уникальными до тех пор, пока будут уникальными пары вектора инициализации IV и базового WEP-ключа. В случае со статическими базовыми ключами существуют лишь 2^{24} уникальных ключа шифрования, ибо после исчерпания всех возможных значений IV начнётся их повторное использование. Значит, смена базового ключа WEP должна произойти до того, как будет исчерпано всё пространство IV. Для выполнения этого требования в Cisco LEAP реализованы таймеры. После автоматической смены базового ключа новые уникальные пары вектора IV и базового ключа подаются на вход алгоритма шифрования.

4.1.3.3. Периодическая смена широковещательного ключа (broadcast key rotation)

Типы аутентификации IEEE 802.1X, поддерживающие индивидуальные абонентские WEP-ключи, обеспечивают ключи только для unicast-трафика. Для обеспечения конфиденциальности broadcast- и multicast-трафика в Cisco Wireless Security Suite предусмотрены следующие возможности:

- Использование статического broadcast-ключа, административно настроенного на точке радиодоступа.
- Автоматическая периодическая смена broadcast-ключа.

Статический broadcast-ключ для клиентов 802.1X настраивается администратором на точке радиодоступа. В беспроводных ЛВС, использующих Cisco TKIP, статический broadcast-ключ подвергается попакетной смене, что уменьшает вероятность статистического вычисления ключа шифрования. Однако, поскольку базовый

ключ статичен, а пространство векторов IV мало и к тому же используется многократно, ключевая последовательность будет повторяться. В результате статистические атаки хотя и потребуют существенно большего времени, но тем не менее по-прежнему могут быть успешно осуществимы.

В некоторых случаях требуется использование статичаского broadcast-ключа. При этом broadcast-ключ отправляется абоненту точкой доступа, зашифрованный с помощью уникального unicast-ключа абонента. Поскольку broadcast-ключи распространяются после успешного завершения аутентификации, нет необходимости настраивать одинаковые ключи на всех точках радиодоступа.

Cisco рекомендует активировать периодическую смену broadcast-ключа на точках радиодоступа. Точка радиодоступа генерирует broadcast-ключ, использую генератор псевдослучайных чисел алгоритма RC4, каждый раз по истечению административно настроенного таймера. В большинстве случаев значение таймера берется из опций RADIUS по реаутентификации абонента.

Поскольку периодическая смена broadcast-ключа разработана для абонентов с поддержкой 802.1X, её использование в точках радиодоступа, также обслуживающих традиционных абонентов со статическими broadcast-ключами, вызовет проблемы нарушения связи. Cisco Systems рекомендует активировать механизм периодической смены broadcast-ключа в точках доступа, ориентированных на облуживание лишь абонентов с поддержкой 802.1X.

5. Контроль доступа к сети в стандарте IEEE 802.1X

5.1. Предпосылки появления технологии контроля доступа к сети IEEE 802.1X

Проводные и беспроводные ЛВС IEEE 802 в большинстве случаев реализуются с возможностью неконтролируемого физического подключения неавторизованных устройств к инфраструктуре сети и/или доступа к ЛВС неавторизованных пользователей через уже подключенные устройства. Наглядным примером могут служить корпоративные ЛВС с портами в доступных широкому кругу лиц помещениях, либо обслуживающие сторонние организации в деловых центрах или арендуемых офисах, а также сети с беспроводным доступом.

Такие сети имеют, как минимум, три существенные уязвимости, относящиеся как к работе пользователей и приложений, так и к обмену управляющей сетевой информацией между элементами сети:

- *Подмена личности (identity theft)*—злоумышленник получает доступ к защищённым ресурсам сети, выдавая себя за легитимного пользователя или элемент сети.
- *Подслушивание (eavesdropping)*—злоумышленник прослушивает обмен информацией между легитимными пользователями.
- *Man-in-the-Middle*—злоумышленник вмешивается в обмен информацией и модифицирует данные, в крайних случаях полностью подменяет собой участника обмена.

Для защиты от перечисленных проблем традиционно ограничивают доступ к сервисам кругом имеющих соответствующие полномочия пользователей и устройств. Эффективная стратегия обеспечения безопасности должна предусматривать подобные меры на на всех уровнях взаимодействия модели OSI.

Технология контроля доступа к портам в IEEE 802.1X использует свойства канального уровня ЛВС для аутентификации и авторизации устройств, подключаемых соединениями точка-точка, и предотвращения доступа к порту сети в случае безуспешной аутентификации и авторизации. Примерами портов, для которых

желательно использование аутентификации, являются порты коммутаторов доступа, порты подключения серверов или маршрутизаторов в проводной ЛВС, логическая ассоциация между абонентом и точкой радиодоступа в беспроводной ЛВС IEEE 802.11.

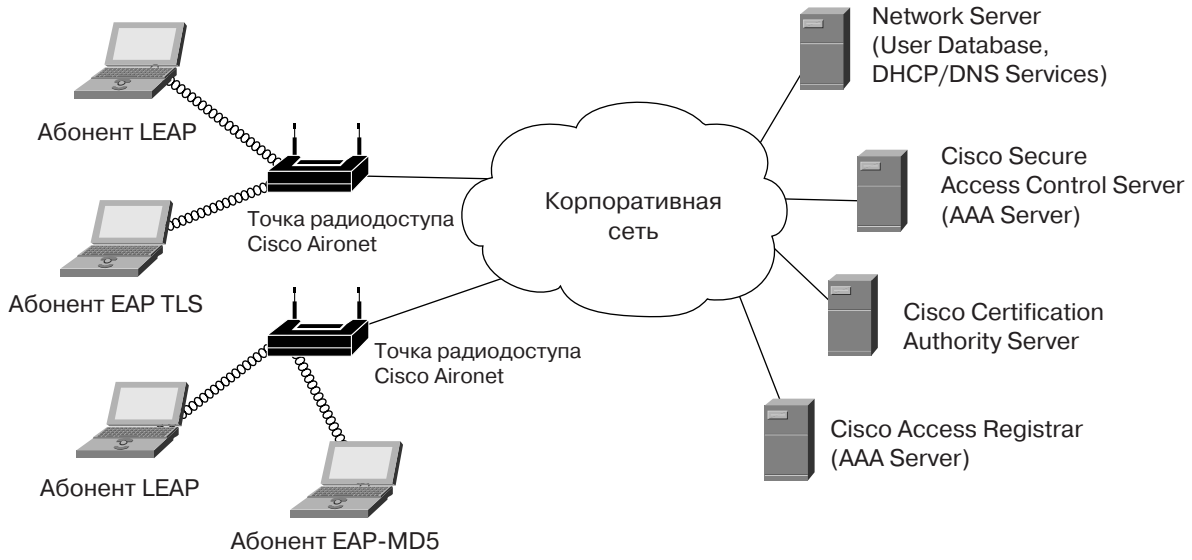
5.2. Содержание стандарта IEEE 802.1X

Для обеспечения совместимости механизмов аутентификации и авторизации между объединёнными в ЛВС устройствами в стандарте IEEE 802.1X разработаны обобщённые методы контроля доступа к портам и определены:

- Архитектура, в рамках которой происходит централизованная аутентификация и генерация и распространение ключей шифрования;
- Принципы работы механизмов управления доступом;
- Необходимые уровни доступа и поведение порта в плане передачи и приёма фреймов для каждого из них;
- Требования к протоколу обмена между устройством, требующим аутентификации, и устройством, подключаемым к его портам, и RADIUS-сервером;
- Механизмы и процедуры реализации управления доступом посредством использования протоколов аутентификации и авторизации;
- Формат фреймов, используемых при транспортировке трафика обобщённого протокола аутентификации EAP с “вложенным” в него тем или иным методом аутентификации;
- Способы управления по SNMP.

Поскольку IEEE 802.1X определяет архитектуру контроля доступа и функционирование обобщённого протокола аутентификации EAP, возможно использование различных методов аутентификации в соответствие с типом абонентов и решаемыми задачами (рис. 26).

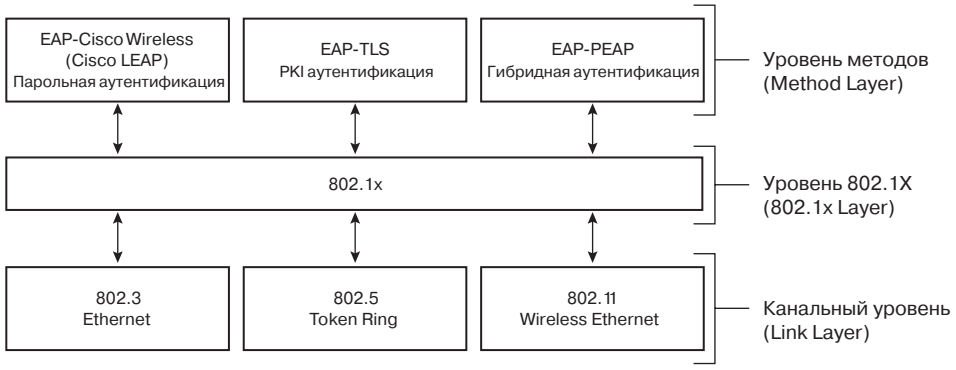
Рис. 26 Сосуществование различных механизмов аутентификации в беспроводной ЛВС с 802.1X



5.3. Архитектура IEEE 802.1X

Архитектура IEEE 802.1X является основой спецификации улучшенных средств безопасности канального уровня IEEE 802.11, разрабатывающейся в рамках рабочей группы IEEE 802.11 Task Group i (TGi). Архитектура IEEE 802.1X наделяет канальный протокол проводных и беспроводных ЛВС развитой аутентификацией, традиционно свойственной верхним уровням модели OSI (рис. 27).

Рис. 27 Уровни архитектуры 802.1X



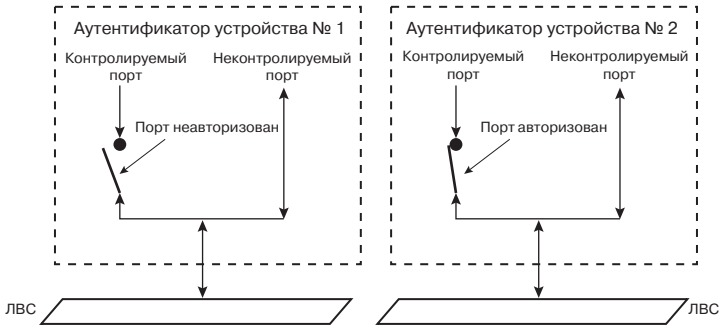
Архитектура IEEE 802.1X включат в себя следующие обязательные логические элементы:

- Клиент (Supplicant)—находится в операционной системе абонента.
- Аутентификатор (Authenticator)—находится в программном обеспечении точки радиодоступа (или коммутатора в случае проводной ЛВС).
- Сервер аутентификации (Authentication Server)—находится на RADIUS-сервере.

IEEE 802.1X предоставляет абоненту беспроводной ЛВС лишь средства передачи атрибутов (Credentials) серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка требуемых политикой сетевой безопасностью методов аутентификации. В последующих разделах подробно рассмотрены методы аутентификации Cisco LEAP, EAP-TLS, EAP-SIM.

Аутентификатор, находясь в точке радиодоступа, создаёт логический порт для каждого клиента на основе его идентификатора ассоциирования (Association ID). Логический порт имеет два канала для обмена данными. Неконтролируемый канал беспрепятственно пропускает трафик из беспроводного сегмента в проводной и обратно, в то время как контролируемый канал требует успешной аутентификации для беспрепятственного прохождения фреймов (рис. 28).

Рис. 28 Порты в 802.1X

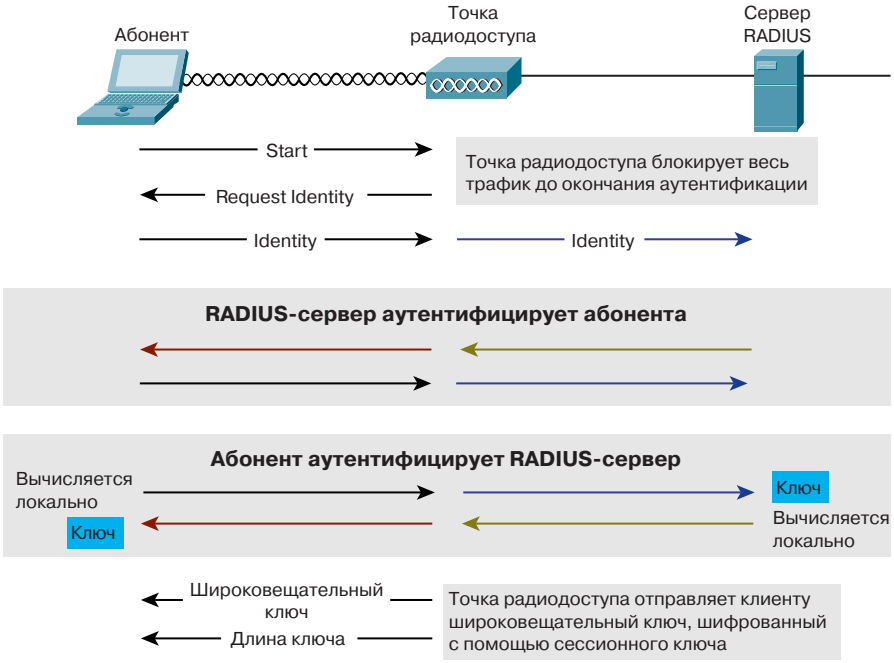


Клиент активизируется и ассоциируется с точкой радиодоступа (или физически подключается к сегменту в случае проводной ЛВС). Аутентификатор распознаёт факт подключения и активизирует логический порт для клиента, сразу переводя его в состояние “неавторизован“. В результате этого через клиентский порт возможен обмен лишь трафиком протокола IEEE 802.1X, для всего остального трафика порт заблокирован. Клиент также может (но не обязан) отправить сообщение EAP Start (рис. 29) для запуска процесса аутентификации.

Аутентификатор отправляет сообщение EAP Request Identity и ожидает от клиента его имя (Identity). Ответное сообщение клиента EAP Response, содержащее атрибуты, перенапрявляется серверу аутентификации.

После завершения аутентификации сервер отправляет сообщение RADIUS-ACCEPT или RADIUS-REJECT аутентификатору (в случае беспроводной ЛВС–точке радиодоступа). При получении сообщения RADIUS-ACCEPT аутентификатор переводит порт клиента в состояние “авторизован“, и начинается передача всего трафика абонента.

Рис. 29 Обмен сообщениями в 802.1X/EAP



5.4. Протокол EAP

5.4.1. Общие принципы

Extensible Authentication Protocol (EAP) является “обобщённым“ протоколом в системе аутентификации, авторизации и учёта (authentication, authorization, and accounting, AAA), обеспечивающим работу разнообразных методов аутентификаци. AAA-клиент (сервер доступа в терминологии AAA, в беспроводной ЛВС представлен точкой радиодоступа), поддерживающий EAP, может не понимать конкретных методов, используемых абонентом и сетью в процессе аутентификации. Сервер доступа туннелирует сообщения протокола аутентификации, циркулирующие между абонентом и сервером аутентификации (напр. Cisco Secure ACS). Сервер доступа интересует лишь факт начала и окончания процесса аутентификации.

Будучи обобщённым протоколом, EAP позволяет использовать разнообразные методы аутентификации. Ряд методов, в т.ч. MD5, Kerberos, Public Key, One Time Passwords (OTP), смарт-карты, решают задачу аутентификации абонента по отношению к AAA-серверу. В беспроводных ЛВС и в ряде других случаев желательна взаимная аутентификация, а для алгоритмов шифрования, предполагающих наличие сессионных ключей (в т.ч. IEEE 802.11 WEP) – поддержка их динамической генерации и распространения. Поскольку разработка протоколов безопасного управления ключами является сама по себе нетривиальной задачей, EAP позволяет использовать существующие возможности протокола TLS по согласованию параметров защищённой связи, управлению ключами и взаимной аутентификации.

В табл. 1 и 00000 представлены основные характеристики наиболее распространённых методов аутентификации.

Табл. 1 Основные характеристики распространённых методов аутентификации

	Совместимость с 802.1X/EAP	Взаимная аутентификация	Поддержка динамических WEP-ключей	Поддержка операционных систем
Cisco EAP (LEAP)	Да	Да	Да	Windows XP, 2000, 98, 95, ME, NT, Windows CE, Linux, DOS, Mac OS
Protected EAP (PEAP)	Да	Да	Да	Windows XP, 2000, 98, 95, ME, NT
EAP-TLS	Да	Да	Да	Windows XP[1]
EAP-MD5	Да	Нет	Нет	Windows XP[1]

1. Корпорация Microsoft анонсировала планы по поддержке EAP в операционных системах Windows 2000, Windows NT 4, Windows 98, Windows 98 Second Edition, Windows ME. На момент написания настоящего документа такая поддержка отсутствовала. Существует программное обеспечение ряда компаний, поддерживающее EAP-TLS и другие механизмы аутентификации в разнообразных операционных системах, напр. EAP supplicant компании Meetinghouse Data Communications (www.mtghouse.com).

Табл. 2 Сравнение распространённых методов аутентификации

	LEAP	PEAP	EAP-TLS
Возможность единой регистрации в Windows	Да	Нет	Да
Статические пароли	Да	Да	Нет
Динамические ключи и взаимная аутентификация	Да	Да	Да
Базы пользователей Microsoft	Да	Да	Да
Базы пользователей не-Microsoft (LDAP, NDS, проч.)	Нет	Да	Только LDAP
Возможность смены пароля через Windows	Нет	Да	Нет
Поддержка однократных паролей (OTP)	Нет	Да	Нет
Требуется серверный цифровой сертификат	Нет	Да	Да
Требуется клиентский цифровой сертификат	Нет	Нет	Да
Совместимость с Layer 3 роумингом	Да	Да	Да
Предотвращение атак типа Man-in-the-middle	Да	Да	Да
Простота обновления ПО клиента	Да	Нет	Нет

5.4.2. Основные стандарты Интернет (RFC) для протокола EAP

В табл. 3 перечислены основные действующие стандарты Интернет для протокола EAP.

Табл. 3 Основные стандарты Интернет (RFC) для протокола EAP

Интернет-стандарт	Содержание
RFC 2865	Сервис аутентификации абонентов при удалённом доступе (RADIUS)
RFC 2869	Расширения протокола RADUIS
RFC 2284	Расширяемый протокол аутентификации EAP для PPP
RFC 2716	Протокол аутентификации EAP-TLS для PPP
RFC 2246	Протокол TLS
RFC 2459	Инфраструктура PKI, часть 1: Сертификаты X.509 и реестр отозванных сертификатов CRL

5.5. Инфраструктура криптографии с открытыми ключами (Public Key Infrastructure, PKI)

5.5.1. Взаимосвязь между PKI и EAP-TLS

Метод аутентификации EAP-TLS использует протокол TLS 1.0 (RFC 2246), основанный на спецификации Secure Socket Layer (SSL) 3.0 компании Netscape. Различия между TLS и SSL минимальны, однако достаточны для несовместимости TLS 1.0 и SSL 3.0.

Протоколы TLS и SSL используют ряд элементов инфраструктуры PKI:

- Абонент должен иметь действующий сертификат для аутентификации по отношению к сети.
- AAA-сервер должен иметь действующий сертификат для аутентификации по отношению абоненту.
- Орган сертификации с сопутствующей инфраструктурой управляет сертификатами субъектов PKI.

Далее кратко описана архитектура PKI и концепция цифровых сертификатов.

5.5.2. Основные стандарты Интернет (RFC) для инфраструктуры PKI

В табл. 4 перечислены основные действующие стандарты Интернет для протокола PKI.

Табл. 4 Основные стандарты Интернет (RFC) для инфраструктуры PKI

Интернет-стандарт	Содержание
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2511	Internet X.509 Certificate Request Message Format
RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 2528	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP
RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema

5.5.3. Обзор PKI

Использование PKI позволяет упростить управление безопасностью путём автоматизации, усилить режим безопасности благодаря значительной сложности компрометации цифровых ертификатов, усовершенствовать и интегрировать управление защитой, усилить контроль защищенного доступа к бизнес-ресурсам.

PKI представляет собой иерархическую архитектуру управления атрибутами безопасности пользователей, участвующих в защищённом обмене информацией. Помимо живых людей в PKI также могут участвовать элементы инфраструктуры сети–межсетевые экраны, концентраторы виртуальных частных сетей, маршрутизаторы, защищенные серверы приложений и другие программно-аппаратные комплексы, нуждающиеся в проверке подлинности и шифровании.

PKI обеспечивает элементы защиты, перечисленных в табл. 5.

Табл. 5 Элементы защиты, обеспечиваемые с помощью PKI

Аутентификация "личности"	Цифровые сертификаты, эмитированые в рамках PKI, позволяют индивидуальным пользователям, организациям и приложениям в сети с уверенностью подтверждать личность каждого участника транзакции через сети общего пользования.
Контроль целостности	Цифровой сертификат позволяет гарантированно подтвердить или опровергнуть факт того, что подписанное им сообщение не было изменено или искажено в процессе передачи.
Гарантия конфиденциальности	Использование цифровоых сертификатов обеспечивает невозможность перехвата сообщений при передаче через сети общего пользования.
Авторизация доступа	Цифровые сертификаты заменяют собой имена и пароли пользователей, которые во многих случаях могут быть подобраны путём перебора, теряются либо разглашаются. В результате упрощается подключение пользователей к сети и сокращаются расходы на контроль доступа к приложениям.
Авторизация транзакций	Инфраструктура PKI предоставляет средства наделения пользователя привилегиями и полномочиями для требующих того транзакций, и контроля их использования.
Невозможность отрицания транзакции	Цифровые сертификаты подтверждают личность их обладателей, делая практически невозможным отрицать либо оспаривать впоследствии "подписанную" транзакцию, напр. покупку в Интернет-магазине.

Примечание: EAP-TLS использует аутентификацию "личности", как будет показано ниже.

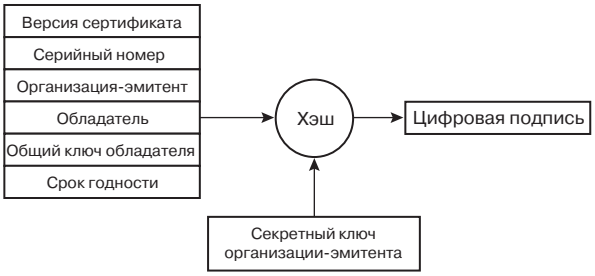
5.5.4. Цифровые сертификаты и цифровые подписи

Каждый субъект PKI имеет цифровой сертификат, эмитируемый, отзываемый и подписанный органом сертификации. Сертификат представляет собой упорядоченную структуру данных, связывающую общий ключ с его обладателем, и содержит набор элементов, используемых субъектами при установлении защищённых соединений:

- Версия сертификата (Certificate version)
- Серийный номер сертификата (Serial number)
- Эмитент сертификата (Certificate issuer)
- Обладатель сертификата (User)
- Общий ключ обладателя сертификата (User's public key)
- Срок годности сертификата (Validity period)
- Дополнительные параметры (Optional extensions)
- Тип алгоритма цифровой подписи (Signature algorithm)
- Цифровая подпись органа сертификации (Signature)

При вычислении цифровой подписи сертификата органом сертификации в качестве входных данных используются версия сертификата, его серийный номер, имя органа сертификации, имя обладателя и его общий ключ, срок годности сертификата, которые подаются на вход хэш-функции вместе с секретным ключом органа сертификации (рис. 30).

Рис. 30 Цифровая подпись сертификата



5.5.5. Криптография с открытыми ключами и несимметричное шифрование

При несимметричном шифровании для обеспечения конфиденциальности сообщений используется пара ключей–открытый и секретный. Сообщение, зашифрованное открытым ключом, может быть расшифровано секретным ключом, и наоборот. Однако сообщение, будучи зашифровано открытым ключом, не может быть расшифровано тем же открытым ключом. В основе данного факта лежит непреодолимая на настоящий момент сложность факторизации (разложения на простые множители) больших чисел. Тем самым предотвращается возможность искажения и подмены сообщения даже при овладении открытыми ключами путём прослушивания обмена сертификатами. Субъекты PKI, нуждающиеся в конфиденциальной связи, обмениваются открытыми ключами, содержащимися в их сертификатах, не разглашая свои секретные ключи. Отправитель шифрует сообщение открытым ключом получателя и затем пересылает ему шифрограмму. Получатель успешно использует свой секретный ключ для расшифровки отправленной ему шифрограммы.

5.5.6. Элементы PKI и их взаимодействие.

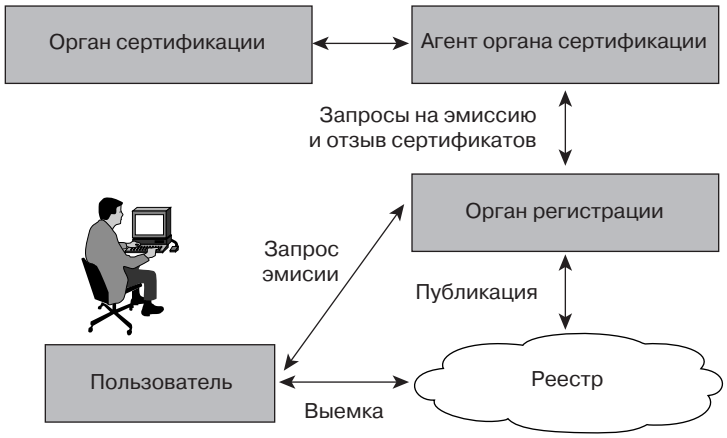
Инфраструктура PKI состоит, как минимум, из пяти элементов, перечисленных в табл. 6.

Табл. 6 Элементы инфраструктуры PKI

Орган регистрации (Registration authority, RA)	Орган регистрации обеспечивает глобальную координацию всех действий по управлению безопасностью, полное и целостностное представление конфигурации режима безопасности. В части управления ключами он регистрирует пользователей, нуждающихся в ключах и сертификатах, собирает информацию, необходимую для подачи запросов на выдачу или отзыв сертификатов, и обеспечивает взаимодействие между органами сертификации.
Орган сертификации (Certification authority, CA)	Орган сертификации выпускает и отзывает сертификаты в соответствии с политикой сертификации. В общем, орган сертификации является специализированным компонентом, работающим в режиме оффлайн, которым управляет оператор сертификации в соответствии с политикой сертификации.
Агент органа сертификации (Certification authority agent, CAA)	Агент органа сертификации является точкой взаимодействия внешнего мира в оперативном режиме с органом сертификации.
Пользователь (End entity, EE)	Пользователем может быть обладатель сертификата, могущий использовать его для подписи цифровых документов, либо пользователь, запрашивающий подтверждение подлинности цифровых подписей и их цепочку сертификации через доверенные органы сертификации.
Реестр (Repository)	В реестре хранятся и из него извлекаются по мере необходимости сертификаты и списки отзывов (Revocation Lists).

На рис. 31 представлена базовая модель архитектуры PKI и взаимодействие между её элементами.

Рис. 31 Модель архитектуры PKI



Механизмы безопасного распространения ключей и сертификатов между различными элементами PKI поддерживают выполнение следующих операций:

- Распространение открытых ключей CA/RA (CA/RA Public Key Distribution)
- Эмиссия сертификата (Certificate Enrollment)
- Отзыв сертификата (Certificate Revocation)
- Запрос сертификата (Certificate Query)
- Запрос списка отозванных сертификатов (CRL Query)

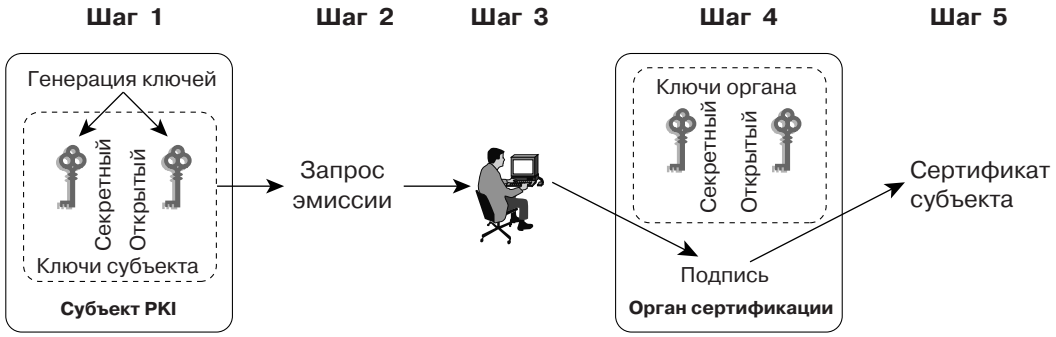
Обмен запросами и сертификатами между пользователями, CA, и RA в рамках PKI происходит в соответствии с разработанными RSA Laboratories пятнадцатью стандартами Public Key Cryptography Standards (PKCS).

Распространение открытых ключей и сертификатов CA/RA происходит в открытом виде. Пользователь при их получении вычисляет "отпечаток" (односторонний хэш) и по другим каналам (телефон, электронная почта, т.д.) сравнивает с "отпечатком", имеющимся у оператора CA/RA.

После получения аутентичных открытых ключей CA/RA пользователь обращается за своим сертификатом, инициируя механизм *эмиссии сертификата*. Пользователь, участвующий в PKI, получает сертификат для представления его другой стороне, с которой будет вступать в безопасную связь. Эмиссия сертификата происходит следующим образом (рис. 32):

1. Пользователь генерирует свою пару секретный ключ–открытый ключ.
2. Пользователь заполняет запрос на эмиссию сертификата (Enrollment Request), добавляет к нему парольную фразу (Challenge Password), шифрует открытым ключом CA/RA и отправляет в адрес CA/RA. Парольная фраза служит дополнительным методом аутентификации при эмиссии сертификата и проверке действий пользователя по другим каналам.
3. CA/RA засшифровывает запрос на эмиссию своим секретным ключом, затем автоматически или вручную с участием оператора одобряет или отклоняет запрос на эмиссию сертификата.
4. После одобрения CA/RA подписывает запрос на эмиссию сертификата, используя свой секретный ключ, и возвращает пользователю полностью готовый сертификат.
5. Получив сертификат, пользователь сохраняет его для последующего предъявления по требованию.

Рис. 32 Эмиссия сертификата



Отзыв сертификата происходит в случае компрометации секретного ключа пользователя, или в иных случаях, когда дальнейшее использование сертификата невозможно или нежелательно. Для отзыва сертификата пользователь связывается с оператором CA/RA и сообщает свою парольную фразу, которая известна обеим сторонам, поскольку была передан на этапе эмиссии сертификата. Убедившись в корректности

парольной фразы, оператор CA/RA следует процедуре конкретного CA/RA по отзыву пользовательского сертификата, после чего отозванный сертификат будет опубликован в списке отозванных сертификатов (Certificate Revocation List, CRL).

При отсутствии у пользователя возможности по хранению собственного сертификата он может использовать функцию *запроса сертификата* для его получения от CA. Пользователь должен знать серийный номер сертификата и использованное при эмиссии имя Fully Qualified Domain Name (FQDN).

Когда пользователь получает от кого-либо сертификат при вступлении в безопасную связь, он извлекает из него URL центра распространения списков отозванных сертификатов (CRL Distribution Point), и затем пытается *запросить список отозванных сертификатов* для выяснения актуальности представленного сертификата.

5.5.7. Роль органов сертификации (CA) и регистрации (RA)

Архитектура PKI допускает наличие иерархии, вследствие чего эмиссию сертификатов может производить как главный орган сертификации (root CA), так и подчиненный ему (subordinate CA). В инфраструктуре PKI возможно существование дополнительных компонентов – органов регистрации RA – для обработки запросов на эмиссию сертификатов и снижения нагрузки на CA в рамках системы, обрабатывающей значительное количество транзакций, либо для поддержания работоспособности инфраструктуры в случае временной недоступности CA.

Орган сертификации–центральная “точка доверия“ в инфраструктуре PKI. Все субъекты организации доверяют CA как авторитетному источнику информации об аутентичности субъектов. Когда CA эмитирует сертификат, его цифровая подпись служит признаком того, что обладатель является частью инфраструктуры PKI.

В более сложных реализациях орган регистрации RA может выполнять операции по установлению подлинности личности пользователя и паролей для транзакций по управления сертификатами, размещению запросов на эмиссию в орган сертификации CA, а также другие разнообразные операции, напр. отзыв сертификатов и проч.

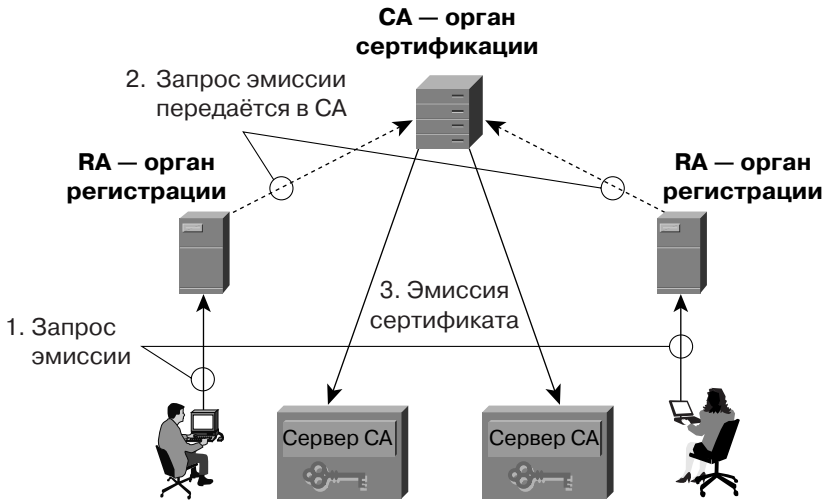
Орган регистрации RA обладает лишь полномочиями по приёму запросов эмиссии и передаче их органу сертификации CA. Орган регистрации RA не имеет права эмисси сертификатов или публикации реестра отозванных сертификатов–за эти функции также отвечает орган сертификации CA. На рис. 33 показан порядок взаимодействия:

Шаг 1. Субъект представляет запрос на эмиссию сертификата в орган регистрации RA.

Шаг 2. Орган регистрации RA дополняет запрос специфической информацией, запрос одобряется в соответствии с политикой организации и передаётся в орган сертификации CA.

Шаг 3. Орган сертификации CA подписывает сертификат и возвращает его субъекту.

Рис. 33 Взаимосвязь между CA и RA



5.5.8. Структура PKI

Простейшая инфрастуктура PKI состоит из одного органа сертификации CA, объединяющего функциональность регистрации и LDAP-сервера, обслуживающего функции центра распространения списков отозванных сертификатов (CRL Distribution Point, CDP). Подобная простейшая инфраструктура имеет ограниченные возможности по масштабированию, не обладает отказоустойчивостью и сложна в управлении в рамках организации с множеством самостоятельных административных единиц (подразделений). К решению этих проблем традиционно подходят путём распределения инфраструктуры PKI внутри организации по географическому и/или функциональному признакам.

На крупном предприятии, подразделения которого нуждаются в чётком контроле за безопасностью на основе “личности“ субъекта, может быть развёрнута иерархическая инфраструктура PKI, состоящая из нескольких органов CA и RA. В этом случае пользователю A будет эмитирован сертификат органом регистрации CA_A в соответствующем подразделении. При установлении защищённой связи с пользователем B, сертификат которого эмитирован органом сертификации CA_B в рамках той же инфраструктуры PKI, пользователь A проверит, подписывает ли его “родной“ CA (CA_A) сертификаты других CA. Если нет, то пользователь переходит на следующий уровень иерархии до тех пор, пока не будет найден общий CA для обеих ветвей PKI, вплоть то главного органа сертификации CA_ROOT.

5.5.9. Проверка годности сертификата (certificant validation)

После того как субъектам эмитированы сертификаты, они готовы для вступления в безопасную связь друг с другом. В большинстве случаев участники обмена вначале контактируют друг с другом посредством протокола прикладног уровня, напр. ISAKMP для IPSec или HTTP для SSL. В конце концов участники обмениваются своими сертификатами для взаимной аутентификации.

На рис. 34 проиллюстрированы шаги при проверке действительности сертификатов. Субъекты проводят проверку сертификатов на предмет того, что:

- Срок действия представленного сертификата не истёк;
- Орган сертификации CA, подписавший сертификат, является частью соответствующей инфраструктуры PKI;
- Сертификат отсутствует в реестре отозванных сертификатов.

Рис. 34 Проверка действительности сертификата

Если сертификат соответствует всем перечисленным критериям годности, субъекты могут использовать открытые ключи для установления IPsec Security Associations (SA). Все данные, отправляемые через SA, шифруются открытым ключом получателя, и расшифровываются на принимающей стороне секретным ключом. В IPSec SA обычно используют периодическую смену ключей по прошествию наперёд заданного интервала времени или по завершению передачи определённого интервала времени.

6. Метод аутентификации EAP-TLS

В настоящем разделе подробно рассмотрен метод аутентификации EAP-TLS. EAP-TLS основан на протоколе SSL v3.0. В случае EAP-TLS квитирование протокола SSL происходит через протокол EAP, в то время как в случае с SSL в Интернет-браузере для этих целей используется протокол TCP.

Поскольку EAP-TLS выполняет взаимную аутентификацию в рамках SSL, этот метод требует наличия сертификатов и у пользователя, и у аутентификатора (т.е. RADIUS-сервера). При взаимной аутентификации каждая сторона должна подтвердить свою “личность” другой стороне, используя при этом свои сертификат и секретный ключ.

6.1. Процесс аутентификации в TLS

Аутентификация в TLS происходит посредством протокола квитирования:

1. SSL-клиент устанавливает соединение с сервером и посылает запрос аутентификации.
2. Сервер посылает клиенту свой цифровой сертификат.
3. Клиент проверяет действительность сертификата и его цифровую подпись.

4. Сервер запрашивает аутентификацию клиента.
5. Клиент посылает серверу свой цифровой сертификат.
6. Сервер проверяет действительность сертификата клиента и его цифровую подпись.
7. Сервер и клиент согласуют алгоритмы шифрования и контроля целостности сообщения.

После этого происходит обмен пользовательскими данными через шифрованный туннель посредством протокола обмена данными.

6.2. Как работает EAP с TLS

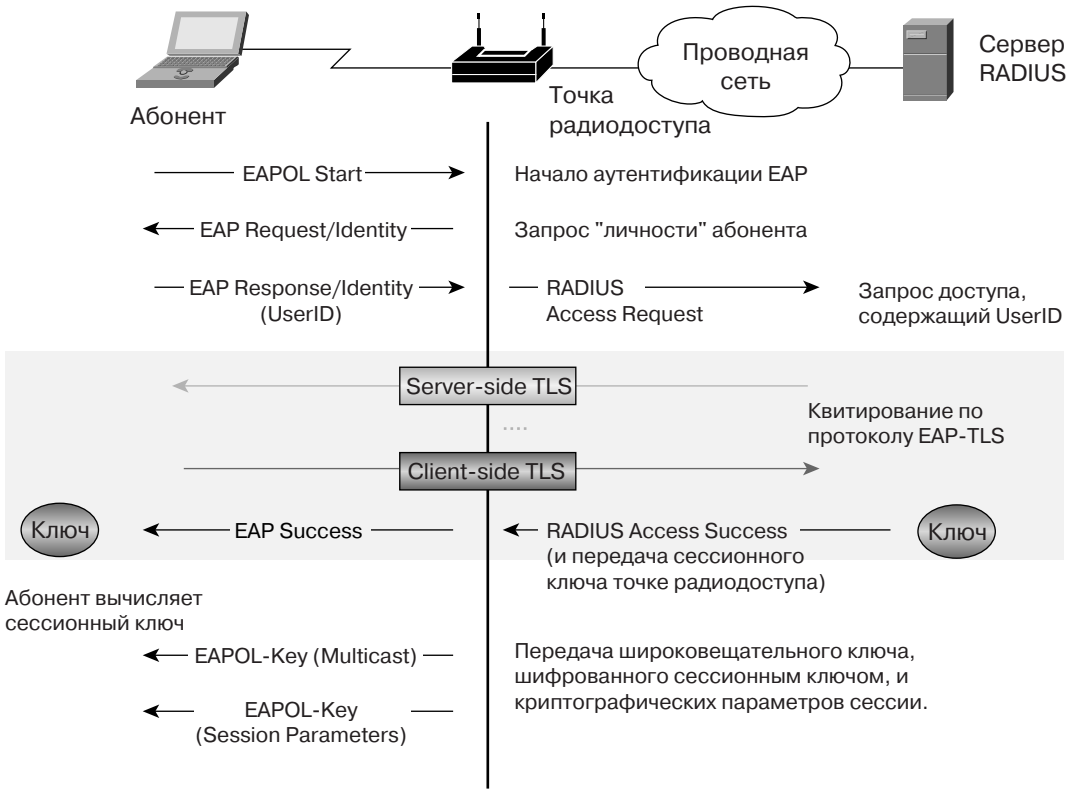
Как было упомянуто выше, метод аутентификации EAP-TLS опирается на архитектуру 802.1x/EAP, подразумевающую наличие следующих компонентов: *клиента* (компонент операционной системы абонентского оборудования), *аутентификато*ра (точка радиодоступа) и *сервера аутентификации* (RADIUS-сервер). Клиент и RADIUS-сервер должны поддерживать метод аутентификации EAP-TLS. Точка радиодоступа должна поддерживать процесс аутентификации в рамках 802.1x/EAP, хотя может и не знать деталей конкретного метода аутентификации.

На рис. 35 показан полный процесс аутентификации 802.1x/EAP в беспроводной ЛВС с использованием протокола EAP-TLS:

1. Абонент посылает сообщение EAP Start точке радиодоступа.
2. Точка радиодоступа отвечает сообщением EAP Request Identity.
3. Абонент посылает точке радиодоступа сообщение EAP Response со своим идентификатором доступа к сети (network access identifier, NAI), представляющем собой имя пользователя.
4. Точка радиодоступа пересылает NAI RADIUS-серверу, инкапсулируя его в сообщение RADIUS Access Request.
5. RADIUS-сервер посылает абоненту свой цифровой сертификат.
6. Абонент проверяет действительность сертификата RADIUS-сервера.
7. Абонент посылает RADIUS-серверу свой цифровой сертификат.
8. RADIUS-сервер сверяет атрибуты абонента с его цифровым сертификатом.
9. Абонент и RADIUS-сервер генерируют сессионные ключи шифрования.
10. RADIUS-сервер посылает точке радиодоступа сообщение RADIUS Accept и сессионный WEP-ключ, тем самым сигнализирую об успешной аутентификации.
11. Точка радиодоступа посылает абоненту сообщение EAP Success.
12. Точка радиодоступа посылает абоненту широковещательный WEP-ключ и его длину, шифрованные сессионным WEP-ключом этого абонента.

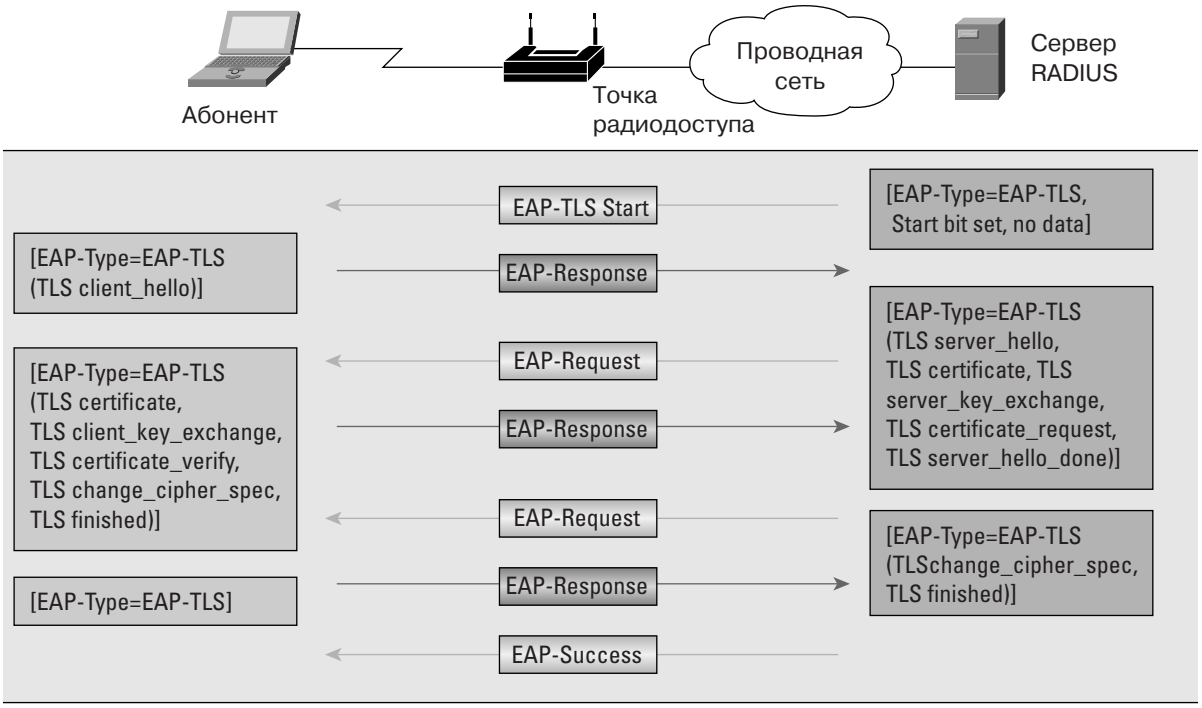
Схема верна в том числе и для методов LEAP и EAP-MD5.

Рис. 35 EAP-TLS в общем



Подробности квитирования EAP-TLS проиллюстрированы на рис. 36. Так в рамках запроса EAP-Request RADIUS-сервер предоставляет клиенту свой сертификат и запрашивает его сертификат. Клиент проверяет годность серверного сертификата и отвечает сообщением EAP-Response, содержащим его сертификат, и инициирует согласование криптографических параметров (алгоритмов шифрования и компрессии). После успешной проверки годности клиентского сертификата RADIUS-сервер передаёт криптографические параметры сессии.

Рис. 36 EAP-TLS в деталях



6.3. Генерация ключей в EAP-TLS

Процесс генерации сессионных ключей шифрования по окончанию успешной аутентификации EAP-TLS иллюстрирует рис. 37.

В процессе квитирования TLS-клиент либо генерирует premaster secret и непосредственно отправляет его RADIUS-серверу, зашифровав общим или временным RSA-ключом сервера, либо обменивается с RADIUS-сервером параметрами метода обмена ключами Diffie-Hellman, DH_RSA или DH_DSS, для локального вычисления premaster secret обеими сторонами. Затем генерируется сессионный master secret, задающий энтропию генерируемых ключей, путём подачи на вход генератора псевдослучайных чисел (Pseudo-Random Function, PRF), определённого в спецификации TLS RFC 2246, последовательностит из:

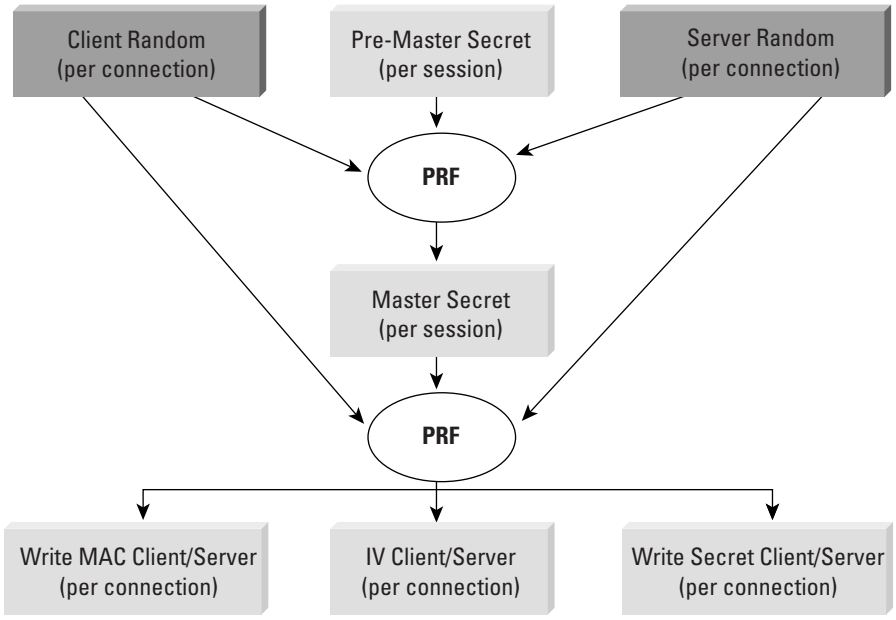
- значения premaster secret,
- ASCII-строки “master secret”,
- конкатенированных случайных чисел ClientHello.random и ServerHello.random.

Спецификация EAP-TLS RFC 2716 определяет способ генерации сессионного ключа. Генератору случайных чисел подают на вход:

- значение master secret,
- ASCII-строку “client EAP encryption”.
- конкатенированные случайные числа ClientHello.random и ServerHello.random.

На выходе появляются сессионный ключ, ключи Message Authentication Code (MAC), векторы инициализации (для блочного шифрования). Длина сессионного ключа определяется аутентификатором (точкой радиодоступа), и затем посредством сообщения EAPOL Key Message передаётся клиенту (рис. 35).

Рис. 37 Генерация сессионного ключа при аутентификации методом EAP-TLS.



7. Тип аутентификации PEAP (Protected EAP)

Тип аутентификации Protected EAP разработан с целью сделать возможной гибридную аутентификацию. PEAP использует инфраструктуру и технологии PKI для аутентификации RADIUS-сервера, для аутентификация клиента используется любой другой тип. Поскольку PEAP устанавливает защищённый туннель посредством аутентификации RADIUS-сервера, не являющиеся взаимными методы аутентификации EAP могут без опасений применяться для аутентификации клиента. К таким методам относятся, в частности, EAP generic token card (GTC) для однократных паролей (one-time passwords, OTP) и EAP-MD5 для аутентификации по паролю (password based authentication).

Тот факт, что PEAP основан на аутентификации сервера, позволяет решить проблемы управления и масштабирования EAP-TLS. Предприятие, организация или учреждение могут избежать проблем, связанных с установкой цифровых сертификатов на каждую клиентскую систему, как того требует EAP-TLS, и выбрать наиболее подходящий для них метод аутентификации клиентов.

Тип аутентификации PEAP разработан компаниями Cisco Systems, Microsoft, RSA Security, и подан в виде предварительного стандарта в IETF. Ведущим разработчиком спецификации является Glen Zorn, сотрудник Cisco Systems.

7.1. Процесс аутентификации в PEAP

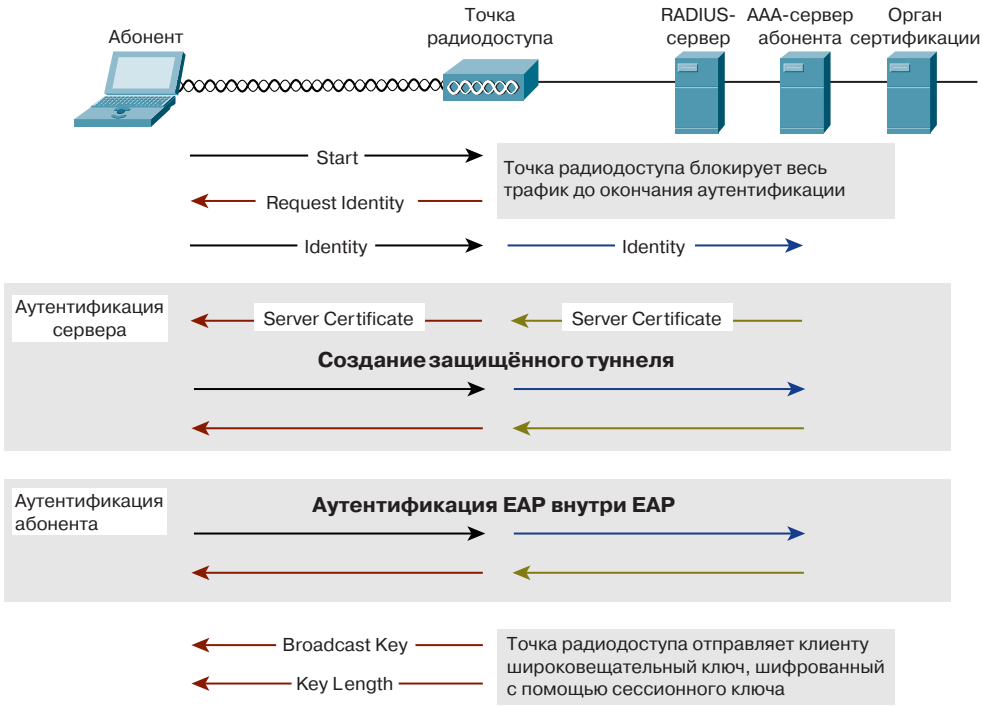
Процесс аутентификации в PEAP иллюстрирует рис. 38. Начало аутентификации в точности повторяет EAP-TLS:

1. Абонент посылает сообщение EAP Start точке радиодоступа.
2. Точка радиодоступа отвечает сообщением EAP Request Identity.
3. Абонент посылает точке радиодоступа сообщение EAP Response со своим идентификатором доступа к сети (network access identifier, NAI), представляющем собой имя пользователя.
4. Точка радиодоступа пересылает NAI RADIUS-серверу, инкапсулируя его в сообщение RADIUS Access Request.
5. RADIUS-сервер посылает абоненту свой цифровой сертификат.
6. Абонент проверяет действительность сертификата RADIUS-сервера.

Дальнейшие шаги специфичны для PEAP:

7. Абонент и RADIUS-сервер создают защищённые туннель, обеспечивающие конфиденциальность обмена данными для аутентификации абонента.
8. Посредством протокола TLS Record Protocol RADIUS-сервер инициирует ещё одну аутентификацию EAP.
9. Происходят транзакции используемого для аутентификации абонента типа протокола EAP.
10. RADIUS-сервер посылает точке радиодоступа сообщение RADIUS Accept и сессионный WEP-ключ, тем самым сигнализирую об успешной аутентификации.

Рис. 38 Процесс аутентификации в PEAP.



7.2. Особенности реализации PEAP у Cisco и Microsoft

PEAP позволяет проводить аутентификацию, используя для этого разнообразные службы каталогов (directory services), включая доступные по LDAP, Novell NDS и базы однократных паролей (OTP databases). Клиентское программное обеспечение PEAP от Cisco и Microsoft различается поддерживаемыми методами аутентификации клиента через TLS-туннель. Microsoft поддерживает лишь аутентификацию клиента с использованием MS-CHAP Version 2, что ограничивает выбор базы атрибутов пользователей системами Windows NT Domains и Active Directory. Cisco поддерживает аутентификацию клиента с использованием однократных и logon-паролей, тем самым открывая возможность выбора OTP-базы и базы logon-паролей пользователей от различных производителей, включая RSA Security, Secure Computing Corporation, Novell, Microsoft и другие. Дополнительно, клиентское ПО Cisco позволяет скрыть имена пользователей до момента создания защищённого TLS-туннеля, т.е. не пересылать их по сети на этапе аутентификации, что обеспечивает дополнительную конфиденциальность.

8. Метод аутентификации Cisco LEAP

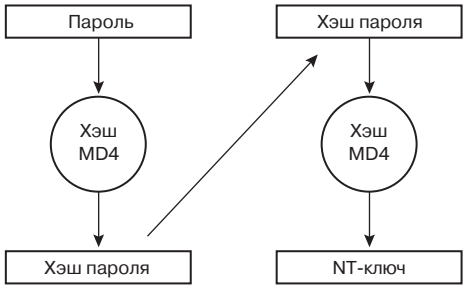
Cisco LEAP обеспечивает взаимную аутентификацию пользователей в беспроводной ЛВС 802.11, а также исходные данные алгоритма генерации ключей шифрования для абонента и RADIUS-сервера. В этом разделе рассматривается алгоритм LEAP, начиная с формата сообщений и заканчивая практическими рекомендациями по его применению на RADIUS-серверах, в точках радиодоступа и у абонентов.

8.1. Процесс аутентификации в Cisco LEAP

Cisco LEAP представляет собой алгоритм аутентификации пользователей и обладает криптографической стойкостью, достаточной для применения во враждебной среде беспроводной ЛВС. Учитывая требования по безопасности к беспроводной ЛВС и необходимость единого подключения (single-sign-on, SSO), Cisco реализовала алгоритм LEAP на принципах протокола аутентификации Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

Алгоритм LEAP основан на использовании секретного пароля пользователя/абонента, и обеспечивает его целостность в процессе аутентификации в беспроводной среде посредством преобразования пароля в некий секретный ключ, в результате чего сторонний наблюдатель не может получить пароль путём захвата и дешифрации фреймов. Секретный ключ вычисляется с помощью односторонней хэш-функции, обратное преобразование для однозначного вычисления подаваемого на вход хэш-функции пароля невозможно. LEAP использует секретный ключ в формате NT-ключа (Microsoft NT key), представляющего собой дважды применённую к паролю пользователя/абонента хэш-функцию Message Digest Algorithm 4 (MD4) (рис. 39).

Рис. 39 NT-ключ Windows



Использование NT-ключа позволяет алгоритму LEAP интегрироваться с существующими хранилищами атрибутов пользователей/абонентов в Windows NT Domain Services и Windows 2000 Active Directory. Также возможна интеграция по протоколу Open Database Connectivity (ODBC) с любыми хранилищами данных, поддерживающими пароли формата MS-CHAP.

Cisco Sytems разработала драйверы для большинства разновидностей Microsoft Windows (Windows 95, 98, ME, 2000, NT and XP) и использует Windows logon для Cisco LEAP logon. Программный код встраивается в Windows logon и передает имя пользователя и пароль в драйвер Cisco Aironet. Драйвер преобразует пароль в NT-ключ и передаёт его вместе с именем пользователя адаптеру беспроводной ЛВС. Адаптер выполняет необходимые процедуры 802.1X с точкой радиодоступа и RADIUS-сервером.

Внимание: Ни пароль, ни хэш пароля пользователя/абонента никогда не передаются через радиоканал.

8.2. Внедрение беспроводных ЛВС с Cisco LEAP

LEAP разрабатывался для усиления безопасности в беспроводной ЛВС, с одновременным облегчением ввода в эксплуатацию и минимизацией администрирования. Cisco поддерживает беспроводные адаптеры и RADIUS-серверы других производителей, что позволяет потребителю сохранить уже сделанные инвестиции в инфраструктуру, программное обеспечиние, средства мониторинга и управления, обучение персонала. Инженеры-консультанты Cisco разработали ряд практических рекомендаций для облегчения быстрого развёртывания беспроводных решений Cisco Aironet, в том числе с поддержкой алгоритма LEAP.

8.2.1. Интеграция с решениями других производителей

Cisco Systems поддерживает LEAP на следующих RADIUS-серверах собственного производства:

- Cisco Secure Access Control Server (ACS) 2.6 и выше
- Cisco Access Registrar v1.7 и выше

Cisco Systems поддерживает LEAP на следующих RADIUS-серверах других производителей:

- Funk Steel Belted RADIUS v3.0
- Interlink Networks Merit v5.1

Алгоритм LEAP реализован также в беспроводных адаптерах AirPort компании Apple Computers.

8.2.2. Практические рекомендации по внедрению Cisco LEAP

Инженеры-консультанты Cisco разработали и протестировали ряд практических рекомендаций для беспроводных ЛВС в рамках архитектуры безопасности Cisco SAFE для корпоративных клиентов. Брошюра “SAFE: Wireless Security in Depth“ находится здесь:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

Ниже кратко перечислены основные рекомендации для проектировщиков и администраторов беспроводных ЛВС.

8.2.2.1. Использование “правильных“ паролей для аутентификации LEAP

Алгоритм LEAP оперирует пользовательскими паролями. Для минимизации вероятности успешной атаки с подбором по словарю используйте “правильные” пароли, которые трудно угадать. “Правильный” пароль обладает, как минимум, следующими характеристиками:

- минимальная длина—6 символов;
- содержит как строчные, так и прописные буквы;
- содержит как буквы, так и цифры;
- не совпадает с именем пользователя;
- не содержит слов, встречающихся в каких-либо языках.

Вот несколько примеров “правильных” паролей:

- cnw84Fri, от фразы “cannot wait for Friday”
- !crE8vpw, от фразы “not creative password”
- G8tSm^rt, от фразы “get smart”

8.2.2.2. Разные протоколы аутентификации на одном RADIUS-сервере

В беспроводных ЛВС с RADIUS-сервером Cisco Secure ACS, аутентифицирующем абонентов как по MAC-адресам по запросу точек радиодоступа в процессе аутентификации 802.11 (открытой или с общим ключём), так и по протоколу LEAP, убедитесь в наличии “правильного” пароля CHAP/MS-CHAP в учётной записи физического устройства (т.е. MAC-адреса).

Cisco Secure ACS использует пароли в учётной записи пользователя следующим образом:

- CiscoSecure CHAP—для протоколов аутентификации CHAP, MS-CHAP и ARAP.
- CiscoSecure PAP—для протокола аутентификации PAP; также используется для протоколов аутентификации CHAP, MS-CHAP и ARAP, если пароль CiscoSecure CHAP не явно указан (его настройка опциональна).

Для аутентификации абонента беспроводной ЛВС по MAC-адресу на сервере Cisco Secure ACS создаётся учётная запись для физического устройства абонента, в качестве пароля в которой указываются 12 символов представления MAC-адреса в коде ASCII. Если в этой же учётной записи не указан отдельный пароль CHAP/MS-CHAP, хакер может предпринять спуфинг MAC-адреса легитимного абонента для ассоциирования с точкой радиодоступа, а затем использовать этот MAC-адрес в качестве имени и пароля для аутентификации по протоколу LEAP.

Подробные инструкции по настройке Cisco Wireless Security Suite приведены здесь:

http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wrsec_an.htm

8.2.2.3. Использование таймера реаутентификации для автоматической смены ключей

Протоклы Cisco LEAP и EAP Transport Layer Security (TLS) поддерживают автоматическую периодическую реаутентификацию, используя в качестве таймера RADIUS Option 27 (RADIUS session timeout option). Реаутентификация необходима для генерации нового ключа до того, как будут использованы все возможные векторы инициализации IV.

В худшем случае, таймер реаутентификации при максимально возможной скорости обмена фреймами в радиоканале 1000 фреймов в секунду составляет

$$\frac{2^{24}\ \text{фреймов}}{1000\ \text{фреймов в секунду}} = \frac{16777216}{1000} \approx 16777\ \text{секунд} = 4\ \text{часа}\ 40\ \text{минут}$$

В реальной жизни скорость передачи фреймов будет меньше, однако приведённый пример наглядно иллюстрирует порядок величины таймера реаутентификации.

8.2.2.4. Виртуальные сети для абонентов с различными способами аутентификации

Поместив абонентов, использующих LEAP, в отдельную виртуальную сеть в рамках корпоративной ЛВС, администратор получает возможность использовать пакетную фильтрацию на сетевом уровне (Layer 3 ACL) для контроля их доступа к проводным сегментам. Более того, трафик в/из беспроводной ЛВС можно будет подвергнуть мониторингу системой обнаружения вторжений (intrusion-detection system, IDS) и межсетевыми экранами (firewall).

9. Заключение

Беспроводных ЛВС в наибольшей степени, по сравнению с другими типами сетей, подвержены атакам, а значит должны быть соответствующим образом защищены. Стандарт IEEE 802.11 предоставляет крайне слабые средства обеспечения безопасности, подверженные многочисленным сетевым атакам. В настоящем документе описаны наиболее существенные уязвимости беспроводных ЛВС и показано, каким образом использование Cisco Wireless Security Suite позволяет дополнить и укрепить стандартные средства обеспечения безопасности для полноценной защиты беспроводных ЛВС.

Некоторые из улучшений и дополнений Cisco являются предстандартными, что в некоторых случаях может представлять трудности при реазизации беспроводных ЛВС, например при использовании специализированных устройств сбора данных, радиотелефонов и т.д. с поддержкой лишь статических WEP-ключей, или при использовании оборудования различных производителей. В этих случаях крайне важно, чтобы проектировщик и администратор понимали потенциальные угрозы беспроводной ЛВС.

Cisco Systems видит своей задачей информирование потребителей о своих решениях для беспроводных ЛВС, и предлагает практические рекомендации по проектированию и реализации сетей, позволяя потребителю сделать обоснованный и наилучший выбор с учётом специфики конкретной задачи.

Cisco Systems рекомендует использование Cisco Wireless Security Suite для создание наиболее безопасной среды для абонентов беспроводных ЛВС, отказываясь от унаследованных слабых методов аутентификации и шифрования в пользу современных полноценных разработок.

Cisco Systems прилагает максимум усилий по обеспечению совместимости в беспроводных ЛВС. Cisco Wireless Security Suite содержит набор предстандартных средств безопасности, которые будут программно обновляться по мере ратификации соответствующих стандартов. Такой подход даёт возможность развёртывания безопасных беспроводных ЛВС сегодня с созможностью обеспечения полной совместимости в будущем.

10. Дополнительные источники информации

Положение "О порядке использования на территории Российской Федерации внутриофисных систем передачи данных в полосе частот 2400-2483,5 МГц"

http://www.minsvyaz.ru/site.shtml?parent=462&id=486#2

Cisco Wireless LAN Security Web site

http://www.cisco.com/go/aironet/security

Cisco Aironet Wireless LAN Security Overview

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

SAFE: Wireless LAN Security in Depth

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

Intercepting Mobile Communications: The Insecurity of 802.11

http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Your 802.11 Wireless Network Has No Clothes

http://www.cs.umd.edu/%7Ewaa/wireless.pdf

Cisco response to Your 802.11 Wireless Network Has No Clothes

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm

An Initial Security Analysis of the IEEE 802.1x Standard

http://www.cs.umd.edu/~waa/1x.pdf

Cisco response to An Initial Security Analysis of the IEEE 802.1x Standard

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP

http://www.cs.rice.edu/~astubble/wep/

Cisco Wireless LAN Security Bulletin

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

Authentication with 802.1x and EAP Across Congested WAN Links

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.htm

Configuring the Cisco Wireless Security Suite

http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wrsec_an.htm

OCB mode

http://www.cs.ucdavis.edu/~rogaway/ocb/ocb.htm

IEEE 802.11 Working Group Web site

http://grouper.ieee.org/groups/802/11/

Understanding PKI: Concepts, Standards, and Deployment Considerations, 2nd Edition
Adams, Carlisle and Steve Lloyd, ISBN: 0672323915, Publisher: Pearson Education, May 2002

http://btobsearch.barnesandnoble.com/booksearch/isbnInquiry.asp?btob=Y&isbn=0672323915

IETF Public-Key Infrastructure Working Group:

http://www.ietf.org/html.charters/pkix-charter.html

Discussion of Simple Certificate Enrollment Protocol:

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm

RSA Public Key Cryptography Standards:

http://www.rsasecurity.com/rsalabs/pkcs/

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe