Санкт–Петербургский государственный политехнический университет

Радиофизический факультет

**ИФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТЯХ Wi-Fi**

Выполнил: студент группы 6097

Хохлов А. С.

Санкт – Петербург

2005

# Оглавление

Оглавление

Безопасность беспроводных сетей

Обзор систем шифрования

Векторы инициализации

Режимы с обратной связью

Кодирование по стандарту 802.11

Механизмы аутентификации стандарта 802.11

Аутентификация с использованием МАС-адресов

Уязвимость системы защиты стандарта 802.11

Уязвимость открытой аутентификации

Уязвимость аутентификации с совместно используемым ключом

Уязвимость аутентификации с использованием МАС-адресов

Уязвимость WEP-шифрования

Проблемы управления статическими WEP-ключами

Защищенные LAN стандарта 802.11

Первая составляющая: базовая аутентификация

Вторая составляющая: алгоритм аутентификации

Третья составляющая: алгоритм защиты данных

Четвертая составляющая: целостность данных

Усовершенствованный механизм управления ключами

Шифрование по алгоритму AES

Резюме

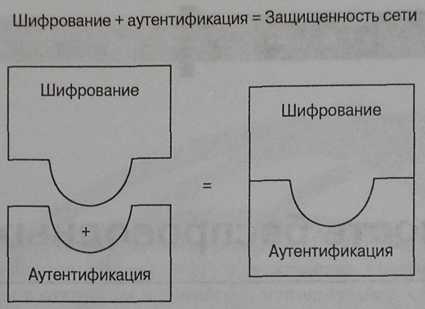
# Безопасность беспроводных сетей

Устройства стандарта 802.11 связываются друг с другом, используя в качестве переносчика данных сигналы, передаваемые в диапазоне радиочастот. Данные передаются по радио отправителем, полагающим, что приемник также работает в выбранном радиодиапазоне. Недостатком такого механизма является то, что любая другая станция, использующая этот диапазон, тоже способна принять эти данные.

Если не использовать какой-либо механизм защиты, любая станция стандарта 802.11 сможет обработать данные, посланные по беспроводной локальной сети, если только ее приемник работает в том же радиодиапазоне. Для обеспечения хотя бы минимального уровня безопасности необходимы следующие компоненты.

* Средства для принятия решения относительно того, кто или что может использовать беспроводную LAN. Это требование удовлетворяется за счет механизма аутентификации, обеспечивающего контроль доступа к LAN.
* Средства защиты информации, передаваемой через беспроводную среду. Это требование удовлетворяется за счет использования алгоритмов шифрования.

На рис.1 показано, что защита в беспроводных сетях обеспечивается как за счет аутентификации, так и благодаря шифрованию. Ни один из названных механизмов в отдельности не способен обеспечить защиту беспроводной сети.



*Рис. 1. Защита в беспроводных сетях обеспечива­ется за счет аутентификации и шифрования*

В спецификации стандарта 802.11 регламентировано применение механизма аутентификации устройств с открытым и с совместно используемым ключом и механизма WEP, обеспечивающего защищенность данных на уровне проводных сетей. Оба алгоритма аутентификации, с открытым и с совместно используемым ключом, основаны на WEP-шифровании и применении WEP-ключей для контроля доступа. Поскольку алгоритм WEP играет важную роль в обеспечении безопасности сетей стандарта 802.11, в следующем разделе будут рассмотрены основы шифрования и шифры.

# 

# Обзор систем шифрования

Механизмы шифрования основаны на алгоритмах, которые рандомизируют данные. Используются два вида шифров.

* Поточный (групповой) шифр.
* Блочный шифр.

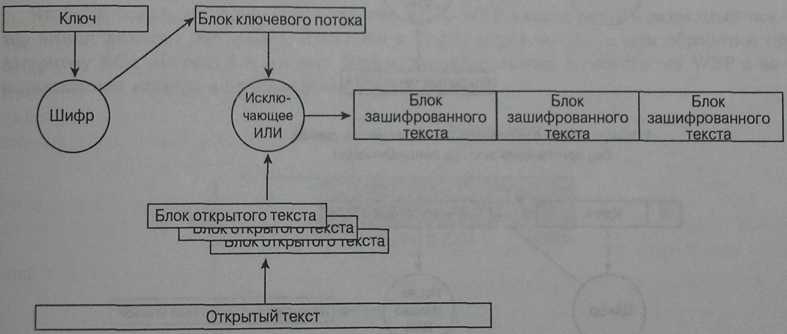
Шифры обоих типов работают, генерируя ключевой поток (key stream), получае­мый на основе значения секретного ключа. Ключевой поток смешивается с данными, или открытым текстом, в результате чего получается закодированный выходной сигнал, или зашифрованный текст. Названные два вида шифров отличаются по объему данных, с которыми они могут работать одновременно.

**Поточный шифр** генерирует непрерывный ключевой поток, основываясь на значении ключа. Например, поточный шифр может генерировать 15-разрядный ключевой поток для шифрования одного фрейма и 200-разрядный ключевой поток для шифрования другого. На рис. 2 проиллюстрирована работа поточного шифра. Поточные шифры — это небольшие и эффективные алгоритмы шифрования, благодаря которым нагрузка на центральный процессор оказывается небольшой. Наиболее распространенным является поточный шифр RC4, который и лежит в основе алгоритма WEP.

**Блочный шифр**, наоборот, генерирует единственный ключевой поток шифрования фиксированного размера. Открытый текст делится на блоки, и каждый блок смешивается с ключевым потоком независимо. Если блок открытого текста меньше, чем блок ключевого потока, первый дополняется с целью получения блока нужного размера. На рис. 3 проиллюстрирована работа блочного шифра. Процесс фрагментации, а также другие особенности шифрования с использованием блочного шифра вызывают повышенную, по сравнению с поточным шифрованием, нагрузку на центральный процессор. В результате производительность устройств, применяющих блочное шифрование, снижается.



*Рис. 2. Так осуществляется поточное шифрование*



*Рис. 3. Так осуществляется блочное шифрование*

Процесс шифрования, описанный нами для поточных и блочных шифров, называется *режим шифрования с помощью книги электронных кодов* (Electronic Code Book, ЕСВ). Режим шифрования ЕСВ характеризуется тем, что один и тот же открытый текст после шифрования преобразуется в один и тот же зашифрованный текст. Этот фактор потенциально представляет собой угрозу для безопасности, поскольку злоумышленники могут получать образцы зашифрованного текста и выдвигать какие-то предположения об исходном тексте.

Некоторые методы шифрования позволяют решить эту проблему.

* Векторы инициализации (initialization vectors, IV).
* Режимы с обратной связью (feedback modes).

## 

## Векторы инициализации

Вектор инициализации — это номер, добавляемый к ключу, конечным результатом этого является изменение информации ключевого потока. Вектор инициализации связывается с ключом до того, как начнется генерация ключевого потока. Вектор инициализации все время изменяется, то же самое происходит с ключевым потоком. На рис. 4 показаны два сценария. Первый относится к шифрованию с использова­нием поточного шифра без применения вектора инициализации. В этом случае открытый текст DATA после смешения с ключевым потоком 12345 всегда преобразуется в зашифрованный текст AHGHE. Второй сценарий показывает, как тот же открытый текст смешивается с ключевым потоком, дополненным вектором инициализации для получения другого зашифрованного текста. Обратите внимание на то, что зашифрованный текст во втором случае отличается от такового в первом. Стандарт 802.11 ре­комендует изменять вектор инициализации пофреймово (on a per-frame basis). Это означает, что если один и тот же фрейм будет передан дважды, весьма высокой окажется вероятность того, что зашифрованный текст будет разным.



1. Шифрование с использованием поточного шифра без применения вектора инициализации

1. Шифрование с использованием поточного шифра без применения вектора инициализации



2. Шифрование с использованием поточного шифра и вектора инициализации

*Рис. 4. Шифрование и векторы инициализации*

## 

## Режимы с обратной связью

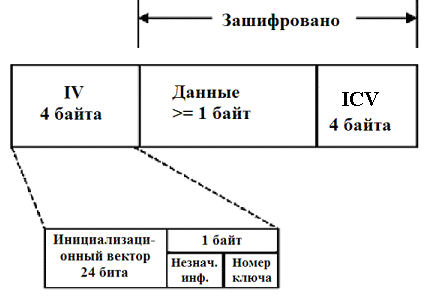
*Режимы с обратной связью* представляют собой модификации процесса шифрования, выполненные во избежание того, чтобы один и тот же открытый текст преобразовывался в ходе шифрования в одинаковый зашифрованный текст.

# 

# Кодирование по стандарту 802.11

Спецификация стандарта 802.11 предусматривает обеспечение защиты данных с использованием алгоритма WEP. Этот алгоритм основан на применении симметричного поточного шифра RC4. Симметричность RC4 означает, что согласованные WEP-ключи размером 40 или 104 бит статично конфигурируются на клиентских устройствах и в точках доступа. Алгоритм WEP был выбран главным образом потому, что он не требует объемных вычислений. Хотя персональные компьютеры с беспроводными сетевыми картами стандарта 802.11 сейчас широко распространены, в 1997 году ситуация была иной. Большинство из устройств, включаемых в беспроводные LAN, составляли специализированные устройства (application-specific devices, ASD). Примерами таких устройств могут служить считыватели штрих-кодов, планшетные ПК (tablet PC) и телефоны стан­дарта 802.11. Приложения, которые выполнялись этими специализированными устройствами, обычно не требовали большой вычислительной мощности, поэтому ASD оснащались слабенькими процессорами. WEP - простой в применении алгоритм, для записи которого в некоторых случаях достаточно 30 строк кода. Малые непроизводительные расходы, возникающие при применении этого алгоритма, делают его идеальным алгоритмом шифрования для специализированных устройств.

Чтобы избежать шифрования в режиме ЕСВ, WEP использует 24-разрядный вектор инициализации, который добавляется к ключу перед выполнением обработки по алгоритму RC4. На рис. 5 показан фрейм, зашифрованный по алгоритму WEP с использованием вектора инициализации.



*Рис. 5. Фрейм, зашифрованный по алгоритму WEP*

Вектор инициализации должен изменяться пофреймово во избежание IV-коллизий. Коллизии такого рода происходят, когда используются один и тот же вектор инициализации и один и тот же WEP-ключ, в результате чего для шифрования фрейма используется один и тот же ключевой поток. Такая коллизия предоставляет злоумышленникам большие возможности по разгадыванию данных открытого текста путем сопоставления подобных элементов. При использовании вектора инициализации важно предотвратить подобный сценарий, поэтому вектор инициализации часто меняют. Большинство про­изводителей предлагают пофреимовые векторы инициализации в своих устройствах для беспроводных LAN.

Спецификация стандарта 802.11 требует, чтобы одинаковые WEP-ключи были сконфигурированы как на клиентах, так и на устройствах, образующих инфраструктуру сети. Можно определять до четырех ключей на одно устройство, но одновременно для шифрования отправляемых фреймов используется только один из них.

WEP-шифрование используется только по отношению к фреймам данных и во время процедуры аутентификации с совместно используемым ключом. По алгоритму WEP шифруются следующие поля фрейма данных стандарта 802.11.

* Данные или полезная нагрузка (payload).
* Контрольный признак целостности (integrity check value, ICV).

Значения всех остальных полей передаются без шифрования. Вектор инициализации должен быть послан незашифрованным внутри фрейма, чтобы приемная станция могла получить его и использовать для корректной расшифровки полезной нагрузки и ICV. На рис. 6 схематично представлен процесс шифрования, передачи, приема и расшифровки фрейма данных в соответствии с алгоритмом WEP.

В дополнение к шифрованию данных спецификация стандарта 802.11 предлагает использовать 32-разрядное значение, функция которого — осуществлять контроль целостности. Этот контрольный признак целостности говорит приемнику о том, что фрейм был получен без повреждения в процессе передачи.

Контрольный признак целостности вычисляется по всем полям фрейма с использо­ванием 32-разрядной полиномиальной функции контроля и с помощью циклического избыточного кода (CRC-32). Станция-отправитель вычисляет это значение и помещает результат в поле ICV. Значение поля ICV включается в часть фрейма, шифруемую по алгоритму WEP, так что его не могут просто так "увидеть" злоумышленники. Получатель фрейма дешифрует его, вычисляет значение ICV и сравнивает результат со значе­нием поля ICV полученного фрейма. Если эти значения совпадают, фрейм считается подлинным, неподдельным. Если они не совпадают, такой фрейм отбрасывается. На рис. 7 представлена диаграмма функционирования механизма ICV.

Фрейм данных с открытым текстом

Фрагмент фрейма с

открытым текстом

Фрагмент фрейма с

открытым текстом и с ICV

Ключ

IV

Ключевой проток

Фрагмент фрейма с

зашифрованным текстом и с ICV

**Процесс шифрования**

Фрагмент фрейма с

открытым текстом

Фрагмент фрейма с

открытым текстом и с ICV

Ключ

IV

Ключевой проток

Фрагмент фрейма с

зашифрованным текстом и с ICV

**Процесс дешифрирования**

Отброшенный плохой ICV-фрейм

*Рис. 6. Процесс шифрования и дешифрования*

Фрагмент фрейма с открытым текстом

Фрагмент фрейма с открытым текстом

32-разрядный ICV

К механизму

шифрования WEP

*Рис. 7. Диаграмма функционирования механизма* ***ICV***

# 

# Механизмы аутентификации стандарта 802.11

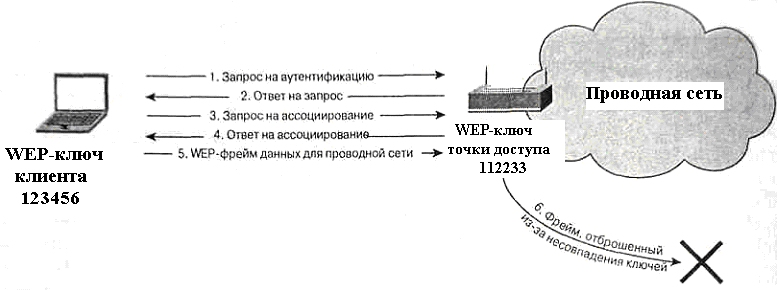
Спецификация стандарта 802.11 оговаривает два механизма, которые могут применяться для аутентификации клиентов WLAN.

* Открытая аутентификация (open authentication).
* Аутентификация с совместно используемым ключом (shared key authentication).

Открытая аутентификация по сути представляет собой алгоритм с нулевой аутентификацией (null authentication algorithm). Точка доступа принимает любой запрос на аутентификацию. Это может быть просто бессмысленный сигнал, используемый для указания на применение именно этого алгоритма аутентификации, тем не менее, открытая аутентификация играет определенную роль в сетях стандарта 802.11. Столь простые требования к аутентификации позволяют устройствам быстро получить доступ к сети.

Контроль доступа при открытой аутентификации осуществляется с использованием заранее сконфигурированного WEP-ключа в точке доступа и на клиентской станции. Эта станция и точка доступа должны иметь одинаковые ключи, тогда они могут связываться между собой. Если станция и точка доступа не поддерживают алгоритм WEP, в BSS невозможно обеспечить защиту. Любое устройство может подключиться к такому BSS, и все фреймы данных передаются незашифрованными.

После выполнения открытой аутентификации и завершения процесса ассоциирования клиент может начать передачу и прием данных. Если клиент сконфигурирован так, что его ключ отличается от ключа точки доступа, он не сможет правильно зашифровывать и расшифровывать фреймы, и такие фреймы будут отброшены как точкой доступа, так и клиентской станцией. Этот процесс предоставляет собой довольно-таки эффективное средство контроля доступа к BSS (рис. 8).



*Рис. 8. Процесс открытой аутентификации при различии WEP-ключей*

В отличие от открытой аутентификации, при аутентификации с совместно используемым ключом требуется, чтобы клиентская станция и точка доступа были способны поддерживать WEP и имели одинаковые WEP-ключи. Процесс аутентификации с совместно используемым ключом осуществляется следующим образом.

1. Клиент посылает точке доступа запрос на аутентификацию с совместно используемым ключом.

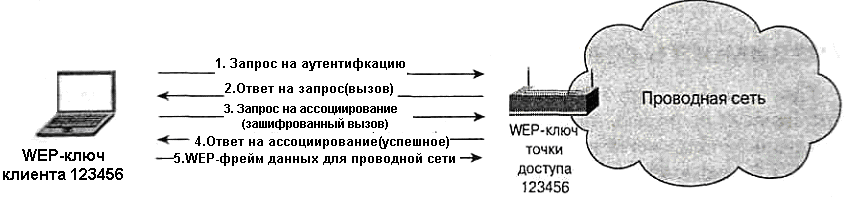
2. Точка доступа отвечает фреймом вызова (challenge frame), содержащим открытый текст.

3. Клиент шифрует вызов и посылает его обратно точке доступа.

4. Если точка доступа может правильно расшифровать этот фрейм и получить свой исходный вызов, клиенту посылается сообщение об успешной аутентификации.

5. Клиент получает доступ к WLAN.

Предпосылки, на которых основана аутентификация с совместно используемым ключом, точно такие же, как и те, которые предполагались при открытой аутентификации, использующей WEP-ключи в качестве средства контроля доступа. Разница между этими двумя схемами состоит в том, что клиент не может ассоциировать себя с точкой доступа при использовании механизма аутентификации с совместно используемым ключом, если его ключ не сконфигурирован должным образом. На рис. 9 схематично представлен процесс аутентификации с совместно используемым ключом.

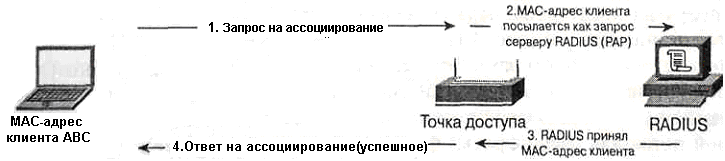


*Рис. 9. Процесс аутентификации с совместно используемым ключом*

# 

# Аутентификация с использованием МАС-адресов

Аутентификация с использованием МАС-адресов не специфицирована стандартом 802.11. но обеспечивается многими производителями. В ходе аутентификации с использованием МАС-адресов проверяется соответствие МАС-адреса клиента локально сконфигурированному списку разрешенных адресов или списку, хранящемуся на внешнем аутентификационном сервере (рис. 10). Аутентификация с использованием МАС-адресов усиливает действие открытой аутентификации и аутентификации с совместно используемым ключом, обеспечиваемыми стандартом 802.11, потенциально снижая тем самым вероятность того, что неавторизованные устройства получат доступ к сети. Например, администратор сети может пожелать ограничить доступ к определенной точке доступа для трех конкретных устройств. Если все станции и все точки доступа BSS используют одинаковые WEP-ключи, при использовании открытой аутентификации и аутентификации с совместно используемым ключом такой сценарий реализовать трудно. Чтобы усилить действие механизма аутентификации стандарта 802.11, он может применить аутентификацию с использованием МАС-адресов.



*Рис. 10. Процесс аутентификации с использованием МАС-адресов*

# 

# Уязвимость системы защиты стандарта 802.11

В предыдущем разделе рассказывалось о том, как осуществляются аутентификация и шифрование при использовании устройств стандарта 802.11. Не секрет, что система зашиты, специфицированная в стандарте 802.11, несовершенна. Вскоре после утверждения стандарта 802.11 появились статьи, в которых указывались слабые места механизма аутентификации стандарта 802.11 и шифрования по алгоритму WEP.

## 

## Уязвимость открытой аутентификации

При использовании механизма открытой аутентификации точка доступа не имеет возможности проверить правомочность клиента. Отсутствие такой возможности является недостатком системы защиты, если в беспроводной локальной сети не используется WEP-шифрование. Даже при использовании и клиентом, и точкой доступа статичного WEP механизм открытой аутентификации не предоставляет средств для определения того, кто использует устройство WLAN. Авторизованное устройство в руках неавторизованного пользователя — это угроза безопасности, равносильная полному отсутствию какой-либо защиты сети!

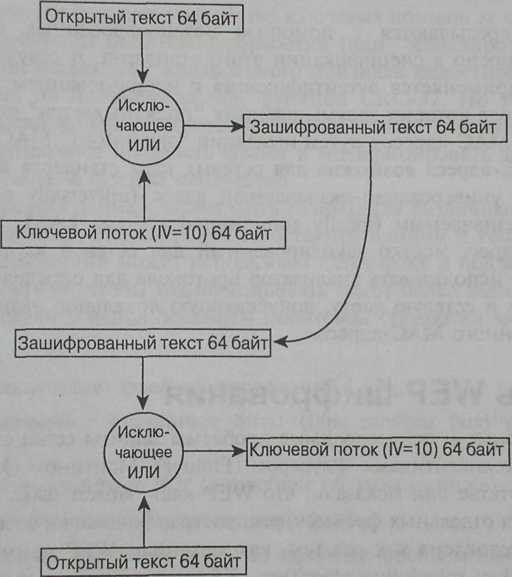
## 

## Уязвимость аутентификации с совместно используемым ключом

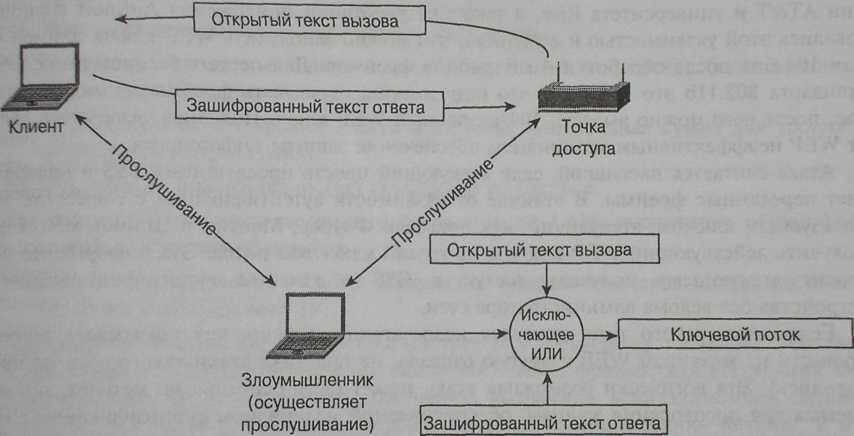
В случае аутентификации с совместно используемым ключом необходимо, чтобы клиент использовал заранее выделенный для совместного использования ключ и шифровал текст вызова, полученного от точки доступа. Точка доступа аутентифицирует клиента путем расшифровки зашифрованного с помощью совместно используемого ключа ответа и проверки того, что полученный текст вызова полностью соответствует отправленному.

Процесс обмена текстом вызова осуществляется по беспроводному каналу связи и является уязвимым для атаки, возможной при знании открытого текста. Эта уязвимость в случае аутентификации с совместно используемым ключом обусловлена математическими методами, лежащими в основе шифрования. Ранее в этой главе говорилось о том, что процесс кодирования состоит в перемешивании открытого текста с ключевым потоком и получении в результате зашифрованного текста. Процесс пе­ремешивания представляет собой выполнение двоичной математической операции, которая называется "исключающее ИЛИ" (XOR). Если открытый текст перемешать с соответствующим зашифрованным текстом, в результате выполнения этой операции будет получена следующая пара: ключевой поток, используемый для WEP-ключа, и вектор инициализации (рис. 11).

Злоумышленник может захватить как открытый, так и зашифрованный текст ответа. Выполнив над этими значениями операцию "исключающее ИЛИ", он может получить действующий ключевой поток. Затем злоумышленник может использовать этот ключевой поток для расшифровки фреймов, имеющих такой же размер, как и ключевой поток, поскольку вектор инициализации, используемый для получения ключевого потока, такой же, как и у расшифрованного фрейма. На рис. 12 показано, как атакующий сеть злоумышленник может проследить процесс аутентификации с совместно используемым ключом и заполучить ключевой поток.



*Рис. 11. Извлечение ключевого потока*



*Рис. 12. Уязвимость механизма аутентификации с совместно используемым ключом*

## 

## Уязвимость аутентификации с использованием МАС-адресов

МАС-адреса пересылаются с помощью незашифрованных фреймов стандарта 802.11, как и оговорено в спецификации этого стандарта. В результате беспроводные LAN. в которых применяется аутентификация с использованием МАС-адресов, уязвимы для атак, в ходе которых злоумышленник "подкапывается" под аутентификацию с использованием МАС-адресов путем имитации "законного" МАС-адреса.

Имитация МАС-адреса возможна для сетевых карт стандарта 802.11, которые позволяют заменять универсально-назначаемый адрес (universally administered address, UAA) локально-назначаемым (locally administered address, LAA). Универсальный адрес — это МАС-адрес, жестко закодированный для сетевой карты производителем. Атакующий может использовать анализатор протокола для определения разрешенного в BSS МАС-адреса и сетевую карту, допускающую локальное назначение адреса, для имитации разрешенного МАС-адреса.

## 

## Уязвимость WEP-шифрования

Наиболее серьезные и непреодолимые проблемы защиты сетей стандарта 802.11 были выявлены криптоаналитиками Флурером (Fluhrer), Мантином (Mantin) и Шамиром (Shamir). В своей статье они показали, что WEP-ключ может быть получен путем пассивного накопления отдельных фреймов, распространяющихся в беспроводной LAN.

Уязвимость обусловлена как раз тем, как механизм WEP применяет алгоритм составления ключа (key scheduling algorithm, KSA) на основе поточного шифра RC4. Часть векторов инициализации (их называют слабые IV — weak IV) могут раскрыть биты ключа в результате проведения статистического анализа. Исследователи компании AT&T и университета Rice воспользовались этой уязвимостью и выяснили, что можно заполучить WEP-ключи длиной 40 или 104 бит после обработки 4 миллионов фреймов. Для первых беспроводных LAN стандарта 802.11b это означает, что они должны передавать фреймы примерно один час, после чего можно вывести 104-разрядный WEP-ключ. Подобная уязвимость делает WEP неэффективным механизмом обеспечения защиты информации.

Атака считается пассивной, если атакующий просто прослушивает BSS и накапливает переданные фреймы. В отличие от уязвимости аутентификации с совместно ис­пользуемым ключом, атакующий, как показали Флурер, Мантин и Шамир, может заполучить действующий WEP-ключ, а не только ключевой поток. Эта информация позволит атакующему получить доступ к BSS в качестве аутентифицированного устройства без ведома администратора сети.

Если атаки такого типа окажется недостаточно, можно, как показывает теория, провести на механизм WEP и другую (правда, на практике атаки такого рода не проводились). Эта логически возможная атака может быть основана на методах, применяемых для преодоления защиты, обеспечиваемой механизмом аутентификации с совместно используемым ключом: для получения ключевого потока используются открытый текст и соответствующий ему зашифрованный текст.

Как уже говорилось, выведенный ключевой поток можно использовать для дешифровки фреймов для пары "вектор инициализации —WEP-ключ" и для определенной длины. Умозрительно можно предположить, что атакующий будет прослушивать сеть с целью накопления как можно большего числа таких ключевых потоков, чтобы создать базу данных ключ поток, взломать сеть и получить возможность расшифровывать фреймы. В беспроводной LAN, в которой не используется аутентификация с совместно используемым ключом, атака с применением побитовой обработки фрейма позволяет злоумышленнику вывести большое количество ключевых потоков за короткое время.

Атаки с использованием побитовой обработки (или "жонглирования битами", bit flipping) основаны на уязвимости контрольного признака целостности (ICV). Данный механизм базируется на полиномиальной функции CRC-32. Но эта функция неэффективна как средство контроля целостности сообщения. Математические свойства функции CRC-32 позволяют подделать фрейм и модифицировать значение ICV, даже если исходное содержимое фрейма неизвестно.

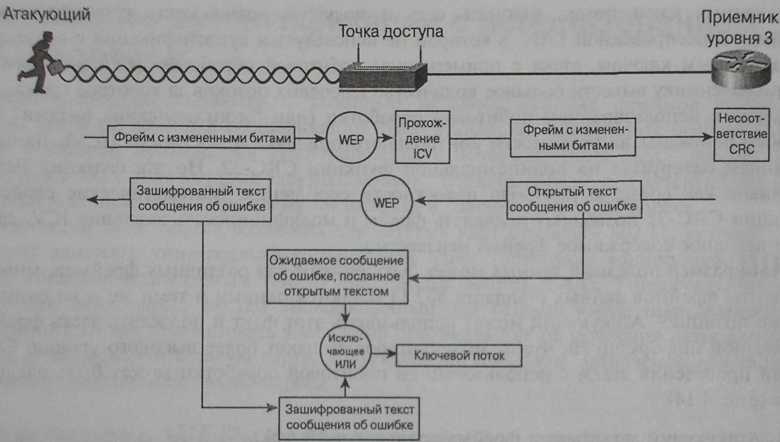
Хотя размер полезных данных может быть разным для различных фреймов, многие элементы фреймов данных стандарта 802.11 остаются одними и теми же и на одних и тех же позициях. Атакующий может использовать этот факт и подделать часть фрейма с полезной информацией, чтобы модифицировать пакет более высокого уровня. Сценарий проведения атаки с использованием побитовой обработки может быть следующим (рис. 13).

1. Атакующий захватывает фрейм беспроводной LAN.
2. Атакующий изменяет случайные биты (flips random bits) полезной нагрузки фрейма.
3. Атакующий модифицирует ICV (подробнее об этом — ниже).
4. Атакующий передает модифицированный фрейм.
5. Приемник (клиент или точка доступа) получает фрейм и вычисляет ICV по содержимому фрейма.
6. Приемник сравнивает вычисленный ICV со значением, хранящимся в поле ICV фрейма.
7. Приемник принимает модифицированный фрейм.
8. Приемник передает модифицированный фрейм на устройство более высокого уровня (повторитель или хост-компьютер).
9. Поскольку в пакете уровня 3 биты изменены, контрольная сумма для уровня 3 оказывается неправильной.
10. Протокол IP приемника выдаст сообщение об ошибке.
11. Атакующий получает сведения о беспроводной LAN, анализируя незашифро­ванное сообщение об ошибке.
12. Получая сообщение об ошибке, атакующий выводит ключевой поток, как в случае атаки с повторением IV.

Основой такой атаки является несоответствие ICV требуемому значению. Значение ICV находится в зашифрованной с помощью WEP части фрейма; как атакующий может изменить ее, чтобы согласовать изменения, вызванные жонглированием битами, с фреймом? На рис. 14 проиллюстрирован процесс "жонглирования битами" и изменения ICV.

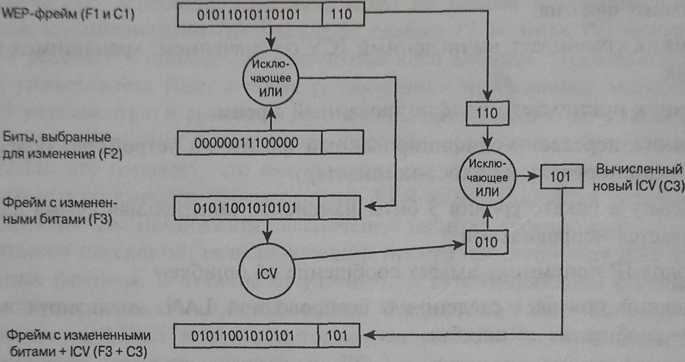
1. Пусть фрейм (F1) имеет ICV, значение которого равно С1.

2. Генерируется новый фрейм (F2) той же длины, какую имеет набор битов фрейма F1.



*Рис. 13. Атака с использованием побитовой обработки*

1. С помощью операции "исключающее ИЛИ" над F1 и F2 создается фрейм F3.
2. Вычисляется ICV для F3 (С2).
3. Посредством операции "исключающее ИЛИ" над С1 и С2 генерируется ICV СЗ.



*Рис. 14. Модифицирование ICV за счет побитовой обработки*

## 

## Проблемы управления статическими WEP-ключами

В спецификации стандарта 802.11 не указан конкретный механизм управления ключами. WEP по определению поддерживает только статические ключи, заранее предназначенные для совместного использования. Поскольку в процессе аутентифи­кации по стандарту 802.11 аутентифицируется устройство, а не пользователь этого устройства, утеря или кража беспроводного адаптера немедленно приводит к возникновению проблемы, связанной с защитой сети. Для ее решения администратору сети придется долго вручную изменять ключи всех беспроводных устройств сети, если имеющийся ключ "скомпрометирован" из-за утери или кражи адаптера.

Такой риск может оказаться приемлемым для небольших сетей, когда управление пользовательскими устройствами — несложная задача. Но подобная перспектива не­приемлема для крупных сетей, когда счет беспроводных пользовательских устройств идет на тысячи. Без механизма распределения или генерации ключей администратору придется дневать и ночевать там, где развернута беспроводная сеть.

# 

# Защищенные LAN стандарта 802.11

Промышленность преодолела слабые места в механизмах аутентификации и защиты сетей стандарта 802.11. Чтобы предоставить пользователям решения, обеспечивающие защищенность, масштабируемость и управляемость сетей, IEEE повысил защищенность сетей стандарта 802.11, разработав улучшенный механизм аутентификации и шифрования. Эти изменения были введены в проект стандарта 802.11i. На сегодняшний день проект 802.11i не утвержден как стандарт, поэтому Альянс Wi-Fi (Wi-Fi Alliance) собрал поднабор компонентов, соответствующих стандарту 802.11i, который получил название "защищенный доступ к Wi-Fi" (Wi-Fi Protected Access, WPA). В данном разделе подробно описаны стандарт 802.11i и компоненты WPA.

Многие ошибочно полагают, что WEP — это единственный компонент, обеспечивающий защиту беспроводных **LAN.** На самом деле защита беспроводных сетей имеет четыре составляющие.

* **Базовая аутентификация** (authentication framework). Представляет собой механизм, который усиливает действие алгоритма аутентификации путем организации защищенного обмена сообщениями между клиентом, точкой доступа и сервером аутентификации.
* **Алгоритм аутентификации.** Представляет собой алгоритм, посредством которого подтверждаются полномочия пользователя.
* **Алгоритм защиты данных.** Обеспечивает защиту при передаче через беспровод­ную среду фреймов данных.
* **Алгоритм обеспечения целостности данных** (data integrity algorithm). Обеспечивает целостность данных при передаче их через беспроводную среду, позволяя приемнику убедиться в том, что данные не были подменены.

## Первая составляющая: базовая аутентификация

Основой аутентификации стандарта 802.11 является служебный фрейм аутентификации стандарта 802.11. Этот служебный фрейм помогает реализовать алгоритмы открытой аутентификации и аутентификации с совместно используемым ключом, хотя сам по себе фрейм не обладает способностью аутентифицировать клиента. Поскольку о недостатках аутентификации стандарта 802.11 мы уже говорили, попробуем разобраться в том, что необходимо сделать для того, чтобы обеспечить проведение защи­щенной аутентификации в беспроводных LAN.

В стандарте 802.11 не определены основные компоненты, способные обеспечить эффективную аутентификацию (они перечислены ниже).

* Централизованная аутентификация, ориентированная на пользователя.
* Динамично шифруемые ключи.
* Управление зашифрованными ключами.
* Взаимная аутентификация.

Аутентификация, ориентированная на пользователя, чрезвычайно важна для обеспечения защиты сети. Аутентификация, ориентированная на устройства, подобная открытой аутентификации и аутентификации с совместно используемым ключом, не способна воспрепятствовать неавторизованным пользователям воспользоваться авторизованным устройством. Из этого следует, что при потере или краже такого устройства или по окончании работы по найму администратор сети будет вынужден вручную изменять ключи всех точек доступа и клиентов сети стандарта 802.11. При централизованном, ориентированном на пользователя управлении через сервер аутентификации, авторизации и учета (authentication, authorization, and accounting, AAA), такой как. RADIUS, администратор может запретить доступ к сети отдельным пользователям, а не их устройствам.

Требование проводить аутентификацию, ориентированную на пользователя, имеет положительный побочный эффект: наличие отдельных ключей шифрования для каждого пользователя. Разновидности аутентификации, которые поддерживают создание динамических ключей шифрования, хорошо подходят для улучшения защиты беспроводных LAN и модели управления ими. Динамические ключи, индивидуальные для каждого пользователя, освобождают администратора сети от необходимости использо­вания статически управляемых ключей. Ключи шифрования динамически назначаются и аннулируются, когда пользователь проходит процедуру аутентификации или выходит из сети. Для того чтобы удалить какого-либо пользователя из сети, достаточно аннулировать его учетную запись, и он потеряет возможность доступа к сети.

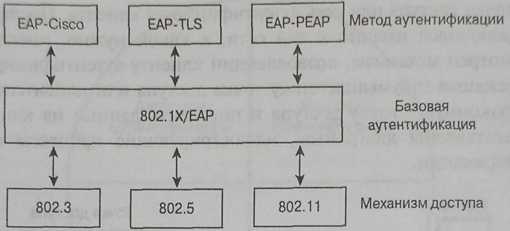
**Взаимная аутентификация** — это аутентификация двухсторонняя. Ее "двухсторонняя" природа обусловлена тем, что не только сеть аутентифицирует клиента, но и клиент аутентифицирует сеть. При открытой аутентификации и аутентификации с совместно используемым ключом точка доступа или сеть аутентифицирует клиента. Последний не знает наверняка, что подключился именно к той сети, к какой нужно, поскольку в стандарте 802.11 не предусмотрен механизм, позволяющий клиенту аутентифицировать сеть. В результате принадлежащая злоумышленнику точка доступа или клиентская станция может выдать себя за "законную" точку доступа и повредить данные на клиентской машине. На рис. 15 представлены диаграммы, иллюстрирующие процессы односторонней и взаимной аутентификации.



*Рис. 15. Односторонняя и взаимная аутентификация*

Поставщики сетей стандарта 802.11 и IEEE осознают необходимость усиления и замены существующих механизмов обеспечения защиты — и аутентификации, и шифрования. Исследовательская группа I рабочей группы стандарта 802.11 сейчас работает над этим, и после того как изменения будут полностью подготовлены, спецификации по защите будут утверждены как спецификации стандарта 802.11i.

IEEЕ начал борьбу с дефектами механизма аутентификации стандарта 802.11 с принятия базовой аутентификации, соответствующей стандарту 802.1X. Стандарт 802.1X представляет собой стандарт IEEE, который относится ко всем топологиям канального уровня серии стандартов 802 и позволяет наращивать его механизмы аутентификации до таковых, обычно реализуемых на более высоких уровнях. Стандарт 802.1X основан на принципах аутентификации, характерных для протокола типа "точка-точка" (Point-to-Point Protocol, PPP), и называется *расширяемый протокол аутентификации* (Extensible Authentication Protocol, EAP). Попросту говоря, стандарт 802.1X инкапсулирует сообщения для использования их на уровне 2. Стандарт 802.11i включает базовую аутентификацию стандарта 802.1X, требуя, чтобы она применялась для аутентификации пользователей. На рис. 16 представлен стандарт 802.1X в части алгоритма аутентификации и топо­логий канального уровня серии стандартов 802.



*Рис. 16. Стандарт 802.1X и топологии канального уровня*

Протокол ЕАР (RFC 2284) и стандарт 802.1X не регламентируют использование особого алгоритма аутентификации. Администратор сети может применять соответствующую протоколу ЕАР разновидность аутентификации — или 802.1X, или ЕАР. Единственное требование — чтобы как клиент стандарта 802.11 (здесь он называется *просителем* (supplicant)), так и сервер аутентификации поддерживали алгоритм ЕАР-аутентификации. Такая открытая и расширяемая архитектура позволяет использовать базовую аутентификацию в различных условиях, и в каждой ситуации можно приме­нять подходящую разновидность аутентификации.

Ниже приведены примеры типов ЕАР-аутентификации.

* **ЕАР защиты транспортного уровня** (EAP-transport layer security, EAP-PEAP). Работает аналогично протоколу защищенных сокетов (secure sockets layer, SSL). Взаимная аутентификация выполняется с использованием цифровых сертификатов на стороне сервера для создания SSL-туннеля для клиента, осуществляющего защищенную аутентификацию в сети.
* **EAP-Message Digest 5 (EAP-MD5).** Аналогично протоколу аутентификации с предварительным согласованием вызова (challenge handshake authentication protocol, CHAP), EAP-MD5 обеспечивает работу алгоритма односторонней аутентификации с использованием пароля.
* **EAP-Cisco**. ЕАР-аутентификация типа EAP-Cisco, которую называют также LEAP, была первой, определенной для применения специально в беспроводных LAN. EAP-Cisco — это алгоритм взаимной аутентификации с использованием пароля.

Аутентификация по стандарту 802.1X требует наличия трех составляющих.

* Проситель. Размещается на стороне клиента беспроводной LAN.
* Аутентификатор (authenticator). Размещается в точке доступа.
* Сервер аутентификации. Размещается на сервере RADIUS.

Эти составляющие представляют собой программные компоненты, устанавливае­мые на устройствах сети. С точки зрения стандарта 802.11 аутентификатор создает логический порт для устройства клиента, основанный на идентификаторе ассоциации (AID). Этот логический порт имеет два тракта прохождения данных: неконтролируе­мый и контролируемый. Неконтролируемый тракт прохождения данных позволяет проходить через сеть всему трафику аутентификации стандарта 802.1X. Контролируемый тракт прохождения данных блокирует обычный трафик сети до тех пор, пока не будет осуществлена успешная аутентификация клиента. На рис. 17 показаны логические порты аутентификатора стандарта 802.1X



*Рис. 17. Логические порты аутентификатора стандарта 802. 1X*

## 

## Вторая составляющая: алгоритм аутентификации

Стандарт 802.11i и WPA обеспечивают механизм, поддерживающий работу алгоритма аутентификации с целью обеспечения связи между клиентом, точкой доступа и сервером аутентификации с использованием механизма базовой аутентификации стандарта 802.1X.

Ни стандарт 802.11i, ни WPA не регламентируют применение особого алгоритма аутентификации, но оба рекомендуют использовать алгоритм, который поддерживал бы взаимную аутентификацию, генерацию динамических ключей шифрования и аутентификацию пользователя. Примером такого алгоритма является алгоритм EAP-Cisco. Этот алгоритм, более известный как Cisco LEAP, представляет собой простой и эффективный алгоритм, разработанныйспециально для использования в беспроводных LAN.

Алгоритм EAP-Cisco является патентованным алгоритмом, который работает по­верх алгоритма базовой открытой аутентификации. По этой причине детали алгоритма EAP-Cisco, касающиеся содержимого генерируемых вызова и ответа на вызов, а также распределения ключей шифрования, не могут быть разглашены. Алгоритм EAP-Cisco перевыполняет требования, предъявляемые к защищенной аутентификации пользователя в беспроводной LAN, за счет применения следующих мер.

* + Аутентификация, ориентированная на пользователя.
  + Взаимная аутентификация.
  + Динамические ключи шифрования.

Если какому-либо пользователю нужно запретить доступ к сети, достаточно удалить его учетную запись на централизованном сервере аутентификации. В результате пользователь не сможет успешно пройти процесс аутентификации, а его устройство — сгенерировать правильный динамический ключ шифрования.

## 

## Третья составляющая: алгоритм защиты данных

Уязвимость шифрования в WEP поставила производителей сетей стандарта 802.11 и исследователей IEEE в затруднительное положение. Как можно улучшить систему шифрования стандарта 802.11, не прибегая к замене всех точек доступа и сетевых карт клиентов?

IEEE ответил на этот вопрос, предложив являющийся частью стандарта 802.11i (и WPA) *временный протокол целостности ключа* (temporal key integrity protocol, TKIP).

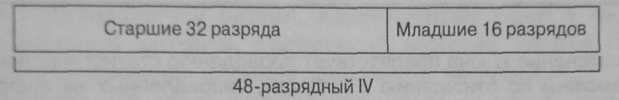
Этот протокол использует многие основные функции WEP, чтобы оправдать инвестиции, сделанные клиентами в оборудование и инфраструктуру стандарта 802.11, но ликвидирует несколько слабых мест последнего, обеспечивая эффективное шифрование фреймов данных. Основные усовершенствования, внесенные протоколом TKIP, таковы.

* Пофреймовое изменение ключей шифрования. WEP-ключ быстро изменяется, и для каждого фрейма он другой.
* Контроль целостности сообщения (message integrity check, MIC). Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов.

Атаки, использующие уязвимость слабых IV, основаны на накоплении нескольких фреймов данных, содержащих информацию, зашифрованную с использованием слабых IV. Простейшим способом сдерживания таких атак является изменение WEP-ключа, используемого при обмене фреймами между клиентом и точкой доступа, до того как атакующий успеет на­копить фреймы в количестве, достаточном для вывода битов ключа.

IEEE адаптировала схему, известную как *пофреймовое изменение ключа* (per-frame keying). (Ее также называют *изменение ключа для каждого пакета* (per-packet keying) и *частое изменение ключа пакета* (fast packet keying).) Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, МАС-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешива­ния. Результат применения этой функции соответствует стандартному 104-разрядному WEP-ключу и 24-разрядному IV.

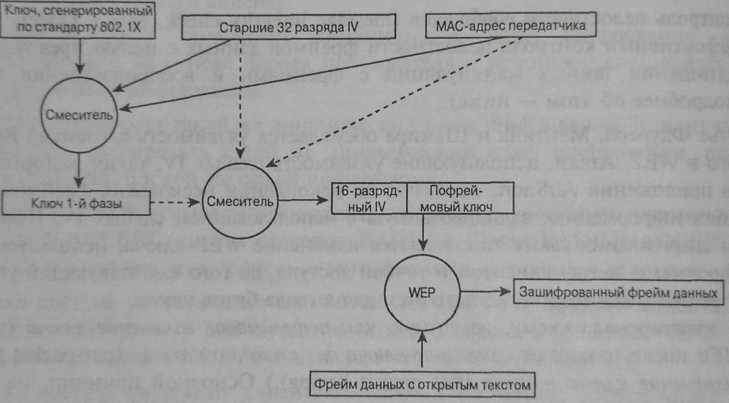
IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV. В нижеследующих разделах объясняется, почему необходимо такое расширение IV. На рис. 18 представлен образец 48-разрядного IV и показано, как этот IV разбивается на части для использования при пофреймовом изменении ключа.



*Рис. 18. Разбиение на части IV для использования при пофреймовом изменении ключа*

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

1. Базовый WEP-ключ (полученный в процессе аутентификации по стандарту 802.1X) перемешивается со старшими 32 разрядами 48-разрядного IV (32-разрядные числа могут принимать значения 0-4 294 967 295) и МАС-адресом передатчика. Результат этого действия называется *ключ 1-й фазы* (phase 1 key). Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ (рис. 19).
2. Ключ 1-й фазы снова перемешивается с IV и МАС-адресом передатчика (ТА) для выработки значения пофреймового ключа.
3. Вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0-65 535). Оставшиеся 8 бит представляют фиксированное значение, используемое как заполнитель.
4. Пофреймовый ключ используется для WEP-шифрования фрейма данных.
5. Когда 16-битовое пространство IVоказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1. (Если значение IV первой фазы было равно 12, оно увеличивается до 13.)
6. Значение Пофреймового ключа вычисляется заново, как на этапе 2.



*Рис. 19. Процесс Пофреймового изменения ключа*

Пофреймово изменяемый ключ имеет силу только тогда, когда 16-разрядные значения IV не используются повторно. Если 16-разрядные значения IV используются дважды, происходит коллизия, в результате чего появляется возможность провести атаку и вывести ключевой поток. Чтобы избежать коллизий IV, значение ключа 1-й фазы вычисляется заново путем увеличения старших 32 разрядов IV на 1 и повторного вычисления пофреймового ключа.

Этот алгоритм усиливает WEP до такой степени, что почти все известные сейчас возможности атак устраняются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью залатать бреши в системе аутентификации WEP и стандарта 802.11. Он жертвует слабыми алгоритмами, вместо того чтобы заменять оборудование. Следующее поколение оборудования стандарта 802.11 должно поддерживать TKIP, но WEP/TKIP будет постепенно свертываться в пользу алгоритма с большими возможностями шифрования, такого как усовершенствованный стандарт шифрования (advanced encryption standard, AES).

## 

## Четвертая составляющая: целостность данных

В будущем для усиления малоэффективного механизма, основанного на использо­вании контрольного признака целостности (ICV) стандарта 802.11, будет применяться контроль целостности сообщения (MIC). Благодаря MIC могут быть ликвидированы слабые места защиты, способствующие проведению атак с использованием поддельных фреймов и жонглированием битами, рассмотренные ранее в. IEEE предложила специальный алгоритм, получивший название *Michael* (Майкл), чтобы усилить роль ICV в шифровании фреймов данных стандарта 802.11.

MIC имеет уникальный ключ, который отличается от ключа, используемого для шифрования фреймов данных. Этот уникальный ключ перемешивается с назначенным МАС-адресом и исходным МАС-адресом фрейма, а также со всей незашифрованной частью фрейма, несущей полезную нагрузку.

Меры противодействия MIC состоят в выполнении приемником следующих задач.

1. Приемник удаляет существующий ключ на ассоциирование.
2. Приемник регистрирует проблему как относящуюся к безопасности сети.
3. Ассоциированный клиент, от которого был получен ложный фрейм, не может быть ассоциирован и аутентифицирован в течение 60 секунд, чтобы замедлить атаку.
4. Если клиент получил ложный фрейм, то он отбрасывает все фреймы, не соответствующие стандарту 802.1X.
5. Такой клиент также запрашивает новый ключ.

Наше рассмотрение пофреймового назначения ключей и MIC касалось в основном ключа шифрования и ключа MIC. Но мы ничего не говорили о том, как ключи генерируются и пересылаются от клиента к точке доступа и наоборот. В следующем разделе мы и рассмотрим предлагаемый стандартом 802.11 механизм управления ключами.

## 

## Усовершенствованный механизм управления ключами

Алгоритмы аутентификации стандарта 802.11 и ЕАР могут обеспечить сервер RADIUS и клиента динамическими, ориентированными на пользователя ключами. Но тот ключ, который создается в процессе аутентификации, не является ключом, используемым для шифрования фреймов или проверки целостности сообщений. В стандарте 802.11i WPA для получения всех ключей используется так называемый *мастер-ключ* (master key). Клиент и точка доступа устанавливают динамический ключ (он называется *парный мастер-ключ,* или РМК, от англ. pairwise master key), полученный в процессе аутентификации по стандарту 802.1X. На основе этого ключа, а также МАС-адресов клиента и точки доступа генерируется парный переходный ключ (painvise transient key, PTK), на основе которого получают ключи для шифрования фреймов и проверки целостности сообщений.

Парный мастер-ключ (РМК) и парный переходный ключ (РТК) являются одноадресатными по своей природе. Они только шифруют и дешифруют одноадресатные фреймы, и предназначены для единственного пользователя. Широковещательные фреймы требуют отдельной иерархии ключей, потому что использование с этой целью одноадресатных ключей приведет к резкому возрастанию трафика сети. Точке доступа (единственному объекту BSS, имеющему право на рассылку широковещательных или многоадресатных сообщений) пришлось бы посылать один и тот же широковещательный или многоадресатный фрейм, зашифрованный соответствующими пофреймовыми ключами, каждому пользователю.

Широковещательные или многоадресатные фреймы используют иерархию групповых ключей. Групповой мастер-ключ (group master key, GMK) находится на вершине этой иерархии и выводится в точке доступа.

Групповой мастер-ключ, текстовая строка, МАС-адрес точки доступа и Gnonce (значение, которое берется из счетчика ключа точки доступа) объединяются и обрабатываются с помощью генератора ПСП, в результате чего получается 256-разрядный групповой переходный ключ (group transient key, GTK). GTK делится на 128-разрядный ключ шифрования широковещательных/многоадресатных фреймов, 64-разрядный ключ переда­чи MIC (transmit MIC key) и 64-разрядный ключ приема MIC (MIC receive key).

С помощью этих ключей широковещательные и многоадресатные фреймы шифруются и дешифруются точно так же, как с помощью одноадресатных ключей, полученных на основе парного мастер-ключа (РМК).

Групповые ключи удаляются и регенерируются каждый раз, когда какая-нибудь станция диассоциируется или деаутентнфицируется в BSS. Если происходит ошибка MIC, одной из мер противодействия также является удаление всех ключей с имеющей отношение к ошибке приемной станции, включая групповые ключи.

# 

# Шифрование по алгоритму AES

Известно, что шифрование и аутентификация, проводимые в соответствии со стандартом 802.11, имеют слабые стороны. IEEE и WPA усилили алгоритм WEP протоколом TKIP и предлагают сильный механизм аутентификации по стандарту 802.11i, обеспечивающий защиту беспроводных LAN стандарта 802.11. В то же время IEEE рассматривает возможность усиления механизма шифрования. С этой целью IEEE адаптировал алгоритм AES для применения его по отношению к разделу, касающемуся защищаемых данных предлагаемого стандарта 802.11i. Компоненты WPA не обеспечивают поддержку шифрования по алгоритму AES. Однако последние версии WPA, возможно, будут реализованы в соответствии со стандартом 802.11i и для обеспечения взаимодействия будут поддерживать шифрование по алгоритму AES.

Алгоритм AES представляет собой следующее поколение средств шифрования, одобренное Национальным институтом стандартов и технологий (NIST) США. IEEE разработал режим AES, предназначенный специально для применения в беспроводных LAN. Этот режим называется *режим счета сцеплений блоков шифра* (Cipher Block Chaining Counter Mode, CBC-CTR) с контролем аутентичности сообщений о сцеплениях блоков шифра (Cipher Block Chaining Message Authenticity Check, CBC-MAC), все вместе это обозначается аббревиатурой AES-CCM. Режим ССМ представляет собой комбинацию режима шифрования CBC-CTR и алгоритма контроля аутентичности сообщений СВС-МАС. Эти функции скомбинированы для обеспечения шифрования и проверки целостности сообщений в одном решении.

Алгоритм шифрования CBC-CTR работает с использованием счетчика для пополнения ключевого потока. Значение этого счетчика увеличивается на единицу после шифрования каждого блока. Такой процесс обеспечивает получение уникального ключевого потока для каждого блока. Фрейм с открытым текстом делится на 16-байтовые блоки. После шифрования каждого блока значение счетчика увеличивается на единицу, и так до тех пор, пока не будут зашифрованы все блоки. Для каждого нового фрейма счетчик переустанавливается.

Алгоритм шифрования СВС-МАС выполняется с использованием результата шифрования СВС по отношению ко всему фрейму, к адресу назначения, адресу источника и данным. Результирующий 128-разрядный выход усекается до 64 бит для использования в передаваемом фрейме.

СВС-МАС работает с известными криптографическими функциями, но имеет издержки, связанные с выполнением двух операций для шифрования и целостности сообщений. Этот процесс требует серьезных вычислительных затрат и значительно увеличивает "накладные расходы" шифрования.

# Резюме

Алгоритмы аутентификации и шифрования, определенные в стандарте 802.11 разработки 1997 года, имеют множество недостатков. Система аутентификации, так же как алгоритм WEP-шифрования, могут быть взломаны за короткое время. Протокол TKIP обещает ликвидировать недостатки WEP-шифрования и системы аутентификации в краткосрочной перспективе, а стандарт 802.1X и AES предоставят долговременное решение проблемы безопасности беспроводных сетей.