МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т H.235.5

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2005)

СЕРИЯ H: АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

Инфраструктура аудиовизуальных услуг – Системные аспекты

Безопасность H.323: Структура надежной аутентификации в RAS с использованием слабых общих секретов

Рекомендация МСЭ-Т H.235.5

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ H

АУДИОВИЗУАЛЬНЫЕ И МУЛЬТИМЕДИЙНЫЕ СИСТЕМЫ

ХАРАКТЕРИСТИКИ ВИДЕОТЕЛЕФОННЫХ СИСТЕМ	H.100–H.199
ИНФРАСТРУКТУРА АУДИОВИЗУАЛЬНЫХ УСЛУГ	
Общие положения	H.200–H.219
Мультиплексирование и синхронизация при передаче	H.220–H.229
Системные аспекты	**H.230–H.239**
Процедуры связи	H.240–H.259
Кодирование движущихся видеоизображений	H.260–H.279
Сопутствующие системные аспекты	H.280–H.299
Системы и оконечное оборудование для аудиовизуальных услуг	H.300–H.349
Архитектура услуг справочника для аудиовизуальных и мультимедийных услуг	H.350–H.359
Качество архитектуры обслуживания для аудиовизуальных и мультимедийных услуг	H.360–H.369
Дополнительные услуги для мультимедиа	H.450–H.499
ПРОЦЕДУРЫ МОБИЛЬНОСТИ И СОВМЕСТНОЙ РАБОТЫ	
Обзор мобильности и совместной работы, определений, протоколов и процедур	H.500–H.509
Мобильность для мультимедийных систем и услуг серии H	H.510–H.519
Приложения и услуги мобильной мультимедийной совместной работы	H.520–H.529
Защита мобильных мультимедийных систем и услуг	H.530–H.539
Защита приложений и услуг мобильной мультимедийной совместной работы	H.540–H.549
Процедуры мобильного взаимодействия	H.550–H.559
Процедуры взаимодействия мобильной мультимедийной совместной работы	H.560–H.569
ШИРОКОПОЛОСНЫЕ И МУЛЬТИМЕДИЙНЫЕ TRIPLE-PLAY УСЛУГИ	
Предоставление широкополосных мультимедийных услуг по VDSL	H.610–H.619

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т H.235.5

Безопасность H.323: Структура надежной аутентификации в RAS с использованием слабых общих секретов

Резюме

В данной Рекомендации представлена структура для двусторонней аутентификации во время обменов RAS H.225.0. Описанные методы "проверки собственности" делают возможным надежное использование общих секретов, таких как пароли, которые, если их использовать сами по себе, не обеспечивают достаточной защищенности.

Также описаны улучшения в инфраструктуре, делающие возможными одновременное согласование параметров защиты транспортного уровня для защиты последующего вызова канала сигнализации.

В предыдущих версиях Рекомендаций МСЭ-Т подсерии H.235 данный профиль содержался в Приложении H к основной части Рекомендации МСЭ-Т H.235. В Дополнениях IV, V, VI к Рекомендации МСЭ-Т H.235.0 показано полное соответствие между пунктами, рисунками и таблицами версий 3 и 4 Рекомендации МСЭ-Т H.235.

Источник

МСЭ-Т Рекомендация H.235.0 утверждена 13 сентября 2005 года 16-й Исследовательской комиссией МСЭ-Т (2005−2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

Ключевые слова

Аутентификация, пароли, безопасность.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Во многих приложениях конечная точка (или ее пользователь) и ее привратник могут разделять только "малый" секрет, такой как пароль или "персональный идентификационный номер" (PIN). Такой секрет (который мы должны будем называть в последующем "паролем"), и любой ключ шифрования, полученный из него, является криптографически слабым. Аутентификационные схемы запроса/ответа, как описывается в пункте 10, предоставляют образцы обычного текста и соответствующего зашифрованного текста, а, следовательно, могут подвергаться атаке прямым перебором от наблюдателя транзакции, когда аутентификации снабжаются ключом при помощи простых паролей. Таким образом, наблюдатель может обнаружить пароль или PIN и затем выдать за конечную точку, чтобы получить услугу.

Семейство протоколов под общим заголовком "Обмен зашифрованным ключом" использует общий секрет, чтобы "скрыть" обмен ключом Диффи-Хеллмана таким способом, что атакующий должен решить ряд конечных логарифмических задач, чтобы осуществить атаку прямым перебором на общий секрет. В обмене зашифрованного ключа (EKE) по Белловину и Мериту [B&M] общий секрет используется, чтобы зашифровать открытые ключи Диффи-Хеллмана в соответствии с симметричным алгоритмом. В методе SPEKE (простой обмен экспоненциальным ключом) Джаблона [Jab] общий секрет используется, чтобы выбрать другой генератор группы Диффи-Хеллмана. В этих протоколах сочетаются защита обмена сильного ключа Диффи-Хеллмана с использованием общего секрета таким способом, что атакующий не может получить известный простой текст для применения в атаке прямым перебором против общего секрета без решения конечных логарифмических задач Диффи-Хеллмана. Преимуществом таких протоколов является то, что они умножают силу задачи Диффи-Хеллмана на силу шифрования секретного ключа (или наоборот). Возможный недостаток заключается в том, что они, как правило, являются предметом патентной защиты.

Рекомендация МСЭ-Т H.235.5

БезопасностьH.323: Структура надежной аутентификации в RAS с использованием слабых общих секретов

1 Сфера применения

Данная Рекомендация может предназначаться для любого привратника или конечной точки с использованием протоколов RAS H.225.0.

2 Справочные документы

2.1 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования, действовали указанные редакции документов. Все Рекомендации и другая справочная литература являются предметом корректировки, в связи с чем пользователям данной Рекомендации настоятельно рекомендуется изыскать возможность для использования самых последних изданий Рекомендации и справочной литературы, перечисленной ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему, как отдельному документу, статуса рекомендации.

– Рекомендация МСЭ-Т H.225.0 (2003 г.), *Протоколы сигнализации о соединении и пакетирование потоков носителей для мультимедийных систем связи на основе пакетов*.

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– Federal Information Processing Standard FIPS PUB 180-2, *Secure Hash Standard*, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.

– NIST Special Publication 800-38A 2001, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*. http://www.csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

2.2 Информативные справочные документы

[AES] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security*.

[B&M] BELLOVIN (S.), MERRITT (M.): U.S. Patent 5,241,599, August 31, 1993, originally assigned to AT&T Bell Laboratories, now assigned to Lucent Technologies.

[Jab] JABLON (D.): Strong Password-Only Authenticated Key Exchange, *Computer Communication Review*, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-26, October 1996.

[NIST SP 800-57] NIST Draft Special Publication 800-57 (2005), *Recommendation for Key Management, Part 1: General Guideline*. http://www.csrc.nist.gov/publications/drafts/draft-800-57-Part1-April2005.pdf

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[RFC2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[RFC3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

3 Определения

Отсутствуют.

4 Сокращения

В данной Рекомендации используются следующие символы и сокращения:

ACF	Admission Confirm	Подтверждение доступа
AES	Advanced Encryption Standard	Улучшенный стандарт шифрования (AES)
ARJ	Admission Reject	Отклонение допуска
ARQ	Admission Request	Запрос допуска
CBC	Cipher Block Chaining	Сцепление блоков шифротекста
CTR	Counter Mode (see NIST SP 800-38A)	Режим счетчика (см. SP 800-38A NIST)
D-H	Diffie-Hellman	Алгоритм Диффи-Хеллмана
EKE	Encrypted Key Exchange	Обмен зашифрованного ключа
GCF	Gatekeeper Confirm	Подтверждение привратника
GK	Gatekeeper	Привратник
GRJ	Gatekeeper Reject	Отклонение привратника
GRQ	Gatekeeper Request	Запрос привратника
HMAC	Hashed Message Authentication Code	Код аутентификации сообщения, использующий хэш-функцию
ICV	Integrity Check Value	Значение проверки целостности
ID	Identifier	Идентификатор
LCF	Location Confirm	Подтверждение местонахождения
LRJ	Location Reject	Отклонение местонахождения
LRQ	Location Request	Запрос местонахождения
MIM	Man-in-the-middle	Посредник
OID	Object Identifier	Идентификатор объекта
PIN	Personal Identification Number	Персональный идентификационный номер
PRF	Pseudo-Random Function	Псевдослучайная функция
RAS	Registration, Admission and Status	Регистрация, допуск, статус
RCF	Registration Confirm	Подтверждение регистрации
RFC	Request for Comments	Запрос о комментариях
RRJ	Registration Reject	Отклонение регистрации
RRQ	Registration Request	Запрос регистрации
SHA1	Secure Hash Algorithm 1	Алгоритм безопасного хеширования версии 1

SPEKE	Simple Password Exponential Key Exchange	Простой обмен экспоненциальным ключом, подтвержденный паролем
TLS	Transport Layer Security	Защита транспортного уровня
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя

5 Соглашения по терминам

В данной Рекомендации используются следующие соглашения:

– "должен" означает обязательное требование.

– "следует" означает предлагаемый, но не обязательный ход действий.

– "может" означает скорее необязательный ход действий, чем рекомендацию о том, что что-либо должно иметь место.

Для информации о дальнейших соглашениях обращайтесь к пункту 5/H.235.0.

6 Основная структура

6.1 Улучшенные возможности согласования в H.235.0

В Рекомендации МСЭ-Т H.235.0 обеспечивается поддержка для данной структуры безопасности посредством включения следующего общего элемента в **ClearToken**:

• **profileInfo –** это последовательность зависящих от профиля элементов, каждый из которых идентифицирован собственным целочисленным значением, как определено специфическим профилем, OID которого содержится в **ClearToken.tokenOID**.

В последующем описании, некоторые элементы переходят в **profileInfo**; каждому из этих элементов будет дано имя, отличное от идентификационной величины, для удобства обсуждения.

6.2 Использование между конечной точкой и привратником

Основная структура (в которой запросчик является конечной точкой, желающей получить регистрацию у привратника, и отвечающая сторона – это тот самый привратник) действует прямым способом. В дальнейшем неявно предполагается, что каждый упомянутый **ClearToken** идентифицируется с **tokenOID** профиля аутентификации. Предполагается, что **ClearToken** должен быть расширен. Элементы **random** и/или **random2** могут использоваться профилем в обоих случаях: они могут быть включены в расчет ключа аутентификации, и/или они могут быть включены в профиль **ClearToken** в каждом последующем сообщении RAS (например, RRQ/RCF) чтобы предотвратить атаку замещением оригинала. Регистрационный обмен конечной точки осуществляется следующим образом:

1) Конечная точка заявляет о своем желании участвовать в одном или более согласованиях ключа и схемах аутентификации посредством включения соответствующего объекта ID для желаемого профиля в элементы **authenticationMechanism.keyExch** элемента **authenticationCapability** запроса привратника. Предполагается, что каждый специфический OID полностью определяет процедуру аутентификации в показателях системы открытого ключа (например, Диффи-Хеллман или Эллиптическая кривая) и специфическую группу (например, одна из группы OAKLEY из RFC 2412), алгоритмы симметричного шифрования (например, AES-128-CBC с захватом зашифрованного текста), функцию получения ключа (например, с помощью псевдослучайной функции пункта 10/H.235.0), код аутентификации сообщения (например, HMAC-SHA1-96 [RFC2104]), и последовательность, в которой они используются. Конечная точка также включает один или более профилей **ClearToken** в GRQ, каждый из которых несет OID для предложенного специфического профиля и необходимый (зашифрованный) материал открытого ключа в следующей форме:

   a) **tokenOID** несет профиль OID как предложенный в **authenticationCapability** инкапсулирующего GRQ.

b) **timeStamp** может использоваться, чтобы обеспечить продолжительность и защитить от атаки замещением оригинала.

c) **password** не должен использоваться как действительный пароль.

d) **dhkey** несет параметры ключа Диффи-Хеллмана, если используется. Вложенный элемент **halfkey** закодирован, как указано выбранным профилем.

e) **challenge** не требуется.

f) **random** предоставляется инициирующей стороной и используется для предотвращения атак замещением оригинала.

g) **certificate** может использоваться, если обмен сертификата является частью профиля.

h) **generalID** может использоваться, если требуется профилем.

i) **eckasdhkey** несет параметры ключа Эллиптической кривой**,** если используется профилем. Вложенный элемент **public-key** должен быть закодирован, как указано профилем.

j) **sendersID** может использоваться, как указано профилем.

k) элемент **profileInfo**, **initVect**, может поставляться вместе с (зашифрованным) материалом открытого ключа (**dhkey** или **eckasdhkey**), если профилем запрашивается вектор инициализации для расшифровывания.

l) Если инициатор желает использовать материал ключа, полученный из обмена который был ранее, он должен включить элемент **profileInfo**, отмеченный как **sessionID**, содержащий идентификатор, присвоенный во время раннего обмена. В таком случае **dhkey**, **eckasdhkey** и/или **initVect** не должны включаться.

m) Если инициатор желает установить сеанс TLS для соединения сигнализации вызова, он может включать один и более элементов **profileInfo**, содержащих наборы шифрования TLS; сообщение должно содержать только один набор шифрования (ранее согласованный) при наличии **sessionID**.

n) Если инициатор желает установить сеанс TLS для сигнализации вызова, он может включать элемент **profileInfo**, содержащий список методов сжатия; только один метод сжатия (ранее согласованный) должен быть включен при наличии **sessionID**.

o) Больше элементов **profileInfo** могут использоваться для любых дополнительных параметров, требуемых для процедур профиля.

2) При получении GRQ, привратник выбирает профиль **AuthenticationMechanism** из предложенного списка, создает подходящий частный (секретный) ключ, вычисляет соответствующий открытый ключ, вектор инициализации, если это необходимо для симметричного шифрования с использованием пароля, зашифровывает открытый ключ, создает уникальный ID сеанса и создает случайную величину, и все это кодируется в **ClearToken**. В зависимости от профиля, последующее применение выполняется из элементов ClearToken:

a) **tokenOID** несет профиль OID, как выбрано из **authenticationMethod** инкапсулирующего GCF.

b) **timeStamp** может использоваться, чтобы обеспечить продолжительность и защитить от атаки замещением оригинала.

c) **password** не должен использоваться как действительный пароль.

d) **dhkey** несет параметры ключа Диффи-Хеллмана, если используется. Вложенный элемент **halfkey** закодирован, как указано выбранным профилем.

e) **challenge** используется для переноса вектора инициализации, если требуется для шифрования ключа, как указано профилем, или может использоваться, чтобы нести случайную строку, которая должна возвращаться конечной точкой для предотвращения атак замещением оригинала.

f) **random** может содержать непредсказуемое, исключительное значение, предоставляемое запросчиком для предотвращения атак замещением оригинала.

g) **certificate** может использоваться, если обмен сертификата является частью профиля.

h) **generalID** может использоваться, если требуется профилем.

i) **eckasdhkey** несет параметры ключа Эллиптической кривой, если используется профилем. Вложенный элемент **public-key** должен быть закодирован, как указано профилем.

j) **sendersID** может использоваться, как указано профилем.

k) **random** (или добавочный элемент **profileInfo**, обозначаемый как **random2**, если профиль запрашивает оба случайных числа чтобы остаться в сообщении) должен содержать непредсказуемую, исключительную величину, подаваемую ответчиком чтобы избежать атаки замещением оригинала.

l) **initVect** предоставляется вместе с (зашифрованным) материалом открытого ключа (**dhkey** или **eckasdhkey**), если профиль запрашивает вектор инициализации для раскодирования.

m) **sessionID** – исключительный (для привратника) идентификатор, используемый для идентификации данного сеанса регистрации. При определенных профилях, может быть также использован как ID сеанса TLS для быстрой установки защищенного TLS канала сигнализации вызова.

n) **profileInfo** может использоваться для любых дополнительных параметров, требуемых для процедур профиля.

Привратник затем вычисляет общий секрет или главный ключ, используя их частный ключ и (расшифрованный) открытый ключ из GCF, и извлекает из главного ключа необходимые ключи шифрования, ключи аутентификации или другой материал в соответствии с профилем. Вышеописанный **ClearToken** помещается внутри сообщения **G**atekeeper**C**on**F**irm. GCF должен быть проверен на целостность/аутентифицирован, с применением полученного ключа аутентификации, затем отправлен к конечной точке. Аутентификация/проверка целостности может быть возвращена одним из нескольких способов, как указано профилем: через зависящий от профиля элемент **profileInfo** или посредством одной из процедур, указанной в Рекомендации МСЭ-Т H.235.1.

3) Конечная точка исследует выбранный **authenticationMechanism.keyExch** из GCF и извлекает параметры из **ClearToken**, идентифицированного соответствующим **tokenOID**. Конечная точка затем выбирает свой частный ключ, вычисляет соответствующий открытый ключ и выбирает какие-либо другие параметры, требуемые профилем. Конечная точка затем вычисляет общий секрет или главный ключ, используя свой частный ключ и (расшифрованный) открытый ключ из GCF, и извлекает оттуда необходимые ключи шифрования, ключи аутентификации или другой материал, в соответствии с профилем. Конечная точка затем должна проверить целостность GCF. Если GCF сделал проверку неверно, конечная точка должна отклонить его вместе со всем полученным из него ключевым материалом, и продолжить ожидать верного сообщения GRQ. Стандартное восстановление RAS приведет к повторной передаче GRQ и, предположительно, к получению неповрежденного GCF. Если через несколько повторных передач не удалось получить удачный ответ, конечная точка должна прекратить попытки зарегистрироваться и сообщить своему пользователю, что что-то неверно. Отметим, что каждый отправленный GRQ предоставляет самозваному гостю шлюза еще одну попытку угадать пароль пользователя и подтвердить правильность этой догадки принятием GRQ. Если проверка целостности GCF удается, конечная точка должна удостоверить привратника, и может продолжать регистрацию и, в процессе, аутентифицировать себя у привратника.

4) Конечная точка затем заполняет **ClearToken** профилем **tokenOID** способом, схожим со способом привратника, как описывалось выше. Все поля из ClearToken GCF, определенные профилем как проблемные, должны быть включены в **ClearToken**. Если указано профилем для предотвращения атаки замещением оригинала, **ClearToken** должен включать **random** и **random2** из полученного выше GCF. **ClearToken** затем помещается в **R**egistration **ReQ**uest, чтобы быть отправленным привратнику. Конечная точка затем должна аутентифицировать полное сообщение RRQ и отправить его привратнику. С этого момента, далее, конечная точка не должна ни принимать, ни отправлять сообщения RAS, которые не аутентифицированы согласованным профилем, с использованием ключа аутентификации, полученного из материала общего ключа.

5) Привратник получает RRQ и должен использовать материал общего ключа, чтобы проверить целостность RRQ по отношению к включенной аутентификации и проверке целостности. Если проверка целостности не удается, привратник должен игнорировать полученный RRQ и ждать поддающегося проверке RRQ. Если ничего не приходит, конечная точка в итоге окончательно оставит попытку регистрации и возвратится к поиску привратника. Если проверка целостности удается, привратник подготовит сообщение Registration ConFirm, чтобы отправить его обратно к конечной точке. В зависимости от профиля, этот RCF может содержать **ClearToken**, который включает **random**, **random2**, и/или элементы **challenge** из профиля аутентификации **ClearToken,** представленного в RRQ. RCF и все последующие сообщения RAS, должен содержать достоверную аутентификацию и проверку целостности, вычисленные с использованием согласованного ключа аутентификации и алгоритма.

6) Когда конечная точка получает сообщение RCF, она проверяет целостность посредством включенной аутентификации и элемента проверки целостности. Если проверка не пройдена, RCF должен быть отклонен; если не получено никакого действительного RCF, даже после того, как PRQ передан повторно, сеанс должен быть остановлен и конечная точка должна вернуться к поискам нового привратника. Если RCF проверен, ID сеанс и выбранный набор шифрования, при наличии, может быть извлечен из **ClearToken** для дальнейшего использования при установке безопасного канала сигнализации вызова.

6.3 Использование профиля между привратниками

Главным образом, та же процедура может использоваться между привратниками в обмене LRQ/LCF. В такой ситуации невозможен точный выбор профиля; создаваемый привратник должен предлагать один и более профилей при включении соответствующих **ClearToken**, как описывалось выше для сообщения GRQ. Отвечающий привратник может выбрать предложенный профиль и должен возвратить соответствующий **ClearToken**, как описывалось выше для сообщения GCF. Отметим, что в таком случае вызывающий привратник не аутентифицирует себя отвечающему привратнику до тех пор, пока он не установит канал сигнализации вызова с этим привратником.

Эта процедура может применяться в многоадресном режиме, если группа привратников делает общим один секрет для использования его с этой целью. Многоадресный LRQ будет основываться на этом секрете; те привратники, которые отвечают с LCF, будут использовать этот ключ, чтобы расшифровать предложенный открытый ключ Диффи-Хеллмана, и каждый будет выбирать собственное значение, используемое только однажды (nonce) и частный ключ Диффи-Хеллмана для своего ответа. Итоговые ключи сеанса будут исключительными для последней пары привратников.

6.4 Шифрование сигнализации канала и аутентификация

Если маршрутизация привратника поддерживается привратником, вновь согласованный материал главного ключа и идентифицированные криптографические параметры могут использоваться для аутентификации и защиты канала сигнализации вызова, например, путем установления сеанса TLS для сигнализации вызова. Если должен использоваться TLS, привратник должен включать выбранный **cipherSuite** и элементы **compress** в возвращаемом профиле **ClearToken**.

7 Специфический профиль защиты (SP1)

В данном пункте содержится стандартный профиль защиты, предполагающий обеспечение общего секрета, оцениваемого как эквивалентный 80-битовому случайному числу (см [NIST SP 800-57]). Профиль состоит из следующего:

- ID объекта для данного профиля (обозначенный "SP1") будет {рекомендация (0) мсэ-t (0) h (8) 235 версии (0) 3 60}.
- Согласование главного ключа, K_m: обмен ключа Диффи-Хеллмана с использованием хорошо известной группы 2 OAKLEY [RFC 2412], за которой следует снижение хеша секрета Диффи-Хеллмана SHA1 [FIPS PUB 180-1]: K_m = SHA1 (общий секрет Диффи-Хеллмана).
- Алгоритм симметричного шифрования: должен быть AES-128 в сегментированном режиме счетчика 2-октетной, D, 12-октетный вектор инициализации, IV, и 2-октетное поле счетчика, C, этот счетчик = D || IV || C, и C = 0 первоначально. См [NIST SP 800-38A] для описания режима CTR. Дискриминатор группы, D, устанавливается в 0x3636, когда IV генерируется

группой, которая выдала GRQ/RRQ, или LRQ, и устанавливается в 0x5c5c, когда IV генерируется группой, которая отвечает на GCF/RCF, или LCF. Каждая группа должна убедиться, что каждый IV, которого она генерирует, − исключительный; она может использовать свой собственный метод чтобы убедиться в этой исключительности.

- Ключ шифрования Диффи-Хеллмана: должен использовать сегментированный режим счетчика AES-128, чтобы зашифровать открытый ключ Диффи-Хеллмана (представленный как октетная строка в сетевом порядке байтов); вектор инициализации должен нести **ClearToken.initVect**, а 16-октетный ключ, K_p, должен быть создан как 128 битов высокого порядка хэша SHA1 пароля пользователя: K_p = Trunc (SHA1(пароль пользователя), 16), где Trunc(x,y) отсекает октетную строку от x до y октетов. Отметим, что это обычно считается слабым ключом.
- Защита от атаки замещением оригинала: каждая группа должна обеспечивать 32-битовое "случайное" число (которое может содержать поле счетчика для обеспечения исключительности); случайные числа явно используются в вычислении извлекаемых ключей, значит, каждый из них должен быть передан только один раз.
- Вывод ключа аутентификации, K_a: применение PRF, описанного в пункте 10/H.235.0, который мы обозначаем как PRF (*in_key*, *label*, *outkey_len*) с *in_key* = K_m, и *label* = "auth_key" || R_e || R_g, где R_e есть значение, используемое только однажды, полученное из **ProfileElement** GRQ и R_g − значение, используемое только однажды**,** полученное из **ProfileElement** GCF, и *outkey_len* = 128.
- Функция аутентификации и целостности сообщений: применяя **ClearToken** с **tokenOID**, установленным в значение "SP1", и **ProfileElement.octets**, установленные в значение HMAC-SHA1-96, значение хэша, вычисляемое для всего сообщения, как описывалось в Рек. МСЭ-Т H.225.0; эта процедура должна быть применена ко всем сообщениям RAS и сигнализации вызова (за исключением GRQ или LRQ, которые не содержат **sessionID**).
- Ключ шифрования элемента, K_e: выбранные элементы сообщений сигнализации вызова (или элементы, туннелированные в них) могут быть зашифрованы с использованием AES-128 в сегментированном режиме счетчика с применением ключа K_e = PRF(K_m, "encrypt_key" || R_e || R_g, 128). Например, этот ключ может использоваться, чтобы зашифровать ключи сеанса медиа для распространения в элементы **h235Key**, как используется в быстром соединении и /или H.245. При таком использовании "SP1" применяется как OID алгоритма шифрования.

Данный профиль составляет использование **ProfileElement**s, определенных в таблице 1. Эти элементы содержатся в последовательности элементов **ClearToken.profileInfo**, как описано в Рек. МСЭ-Т H.235.0.

Таблица 1/H.235.5 – Элементы профиля

Название элемента (используемое в тексте)	**Значение ElementID**	**Выбор элемента (длина)**	**Описание элемента**
initVect	1	Октеты (12)	Вектор инициализации для шифрования EKE
nonce	2	Октеты (любая)	Непредсказуемое, исключительное значение
cipherSuite	3	Октеты (2)	Набор шифрования TLS
compression	4	Октеты (1)	Алгоритм сжатия TLS
sessionID	5	Октеты (1..)	Исключительный, может сочетаться с ID сеанса TLS
integrityCheck	6	Октеты (12)	Контрольное число с ключом

Последовательность регистрации должна состоять из:

– Конечная точка должна отправить GRQ с элементом **authenticationCapability**, содержащим **AuthenticationMechanism.keyExch**, который включает OID "SP1" и соответствующий **ClearToken** с **tokenID** = "SP1" и **dhkey**, включающий 1024-битовый открытый ключ, зашифрованный с использованием **initVect** в качестве IV и ключа, выведенного из пароля пользователя, и значение, используемое только однажды = 32-битовое случайное число, выбранное конечной точкой.

– Привратник должен отправить в ответ GCF с элементом **authenticationMode**, равным **AuthenticationMechanism.keyExch**, содержащим OID "SP1", и **ClearToken** с **tokenID** = "SP1" и **dhkey**, содержащим расшифрованный 1024-битовый открытый ключ, и значение, используемое только однажды = 32-битовому случайному числу, выбранного привратником, вместе с **integrityCheck**, содержащим значение хэша аутентификации, вычисленное при использовании выведенного ключа аутентификации, K_a. Отметим, что нет необходимости для привратника зашифровывать свою половину ключа Диффи-Хеллмана в GCF в этом профиле, потому что это первая сторона, которая аутентифицирует себя, демонстрируя свою способность аутентифицировать GCF, используя выведенный ключ аутентификации. Этот режим разрешает привратнику заново использовать свои ключи Диффи-Хеллмана с более чем одной конечной точкой. См. пункт 10.5.

– Конечная точка должна отправить в ответ RRQ со значением аутентификации и проверки целостности в **ProfileElement** с **elementID**, установленным в значение **integrityCheck**, и **element**, установленный в значение, вычисленное с использованием выведенного ключа аутентификации, K_a.

– Последующие сообщения RAS, включающие RCF, должны быть аутентифицированы и проверены на целостность, используя ту же самую процедуру и ключ. Сообщения сигнализации вызова H.225.0 (и туннелированные сообщения H.245, при наличии) должны быть аутентифицированы, используя **ClearToken**, с **tokenOID**, установленным на "SP1", содержащий **profileInfo ProfileElement** с **elementID**, установленным на **integrityCheck** и **element**, установленный на вычисленное значение.

– Ключ шифрования, K_e, и алгоритм шифрования AES-128 в сегментированном режиме счетчика может использоваться привратником и конечной точкой, чтобы зашифровать выбранную информацию, передаваемую через RAS, сигнализацию вызова и/или H.245. Например, привратник может распространить шифрованные ключи медиа, сохраняемые под K_e и алгоритмом шифрования профиля.

– Если конечной точке требуется перерегистрироваться и она сохраняет ID первоначального сеанса и главный секрет, она должна попытаться перерегистрироваться, используя ID первоначального сеанса и главный секрет, включая ID сеанса явно в GRQ (и не включая половину ключа Диффи-Хеллмана) в свой GRQ.

– Этот профиль должен быть пригоден к использованию между привратниками (см. 6.3).

8 Улучшенный профиль защиты (SP2)

В данном пункте описывается новый профиль защиты, основывающийся на первоначальном профиле, SP1. Неофициально он определен как SP2 и официально с OID – {рекомендация (0) мсэ-t (0) h (8) 235 версия (0) 4 62}. Данный профиль идентичен SP1, за исключением указанного в следующих подпунктах. Особые улучшения по сравнению с SP1 включают:

– Улучшения в порядковой нумерации сообщений сигнализации вызова для противодействия атакам замещением оригинала.

– Расширение генерации ключа шифрования на основе пароля с использованием псевдонима конечной точки для противодействия атакам перебором словаря.

– Размер значения, используемого только однажды, увеличен и стал переменным.

– Выводится расширение ключа для использования с вектором инициализации шифрования.

– Предоставлена более эффективная передача профиля **ClearToken**, с использованием **genericData**.

SP2 использует элементы профиля таблицы 1, а также дополнительные элементы профиля, описанные в таблице 2:

Таблица 2/H.235.5 – Дополнительные элементы профиля для SP2

Название элемента (использованное в тексте)	Значение ElementID	Выбор элемента (длина)	Описание элемента
seqNumber	7	Октеты (4)	32-битовый порядковый номер в сетевом порядке байтов
connectID	8	Октеты (2)	Идентификатор соединения сигнализации. (Необязательный, по умолчанию = 0)
endpointID	9	Октеты (переменная)	ASN.1-зашифрованный псевдоадрес, связанный с конечной точкой и ее паролем. (Необязательный)

8.1 Порядковый номер сигнализации вызова

В сообщениях сигнализации вызова H.225.0 не содержится порядковый номер, потому что они транспортируются через надежное соединение (TCP), которое несет ответственность за установление последовательности. Тем не менее, отсутствие исключительного идентификатора сообщения на уровне приложения подвергает сигнализацию вызова атакам замещением оригинала и отражения. Эта проблема может быть решена посредством добавления порядкового номера и добавочного идентификатора соединения к каждому сообщению сигнализации вызова. Отметим, что этот прием не полностью предотвращает атаки замещением оригинала и отражения, но значительно сокращает шансы атакующих на успех.

Порядковые номера должны быть исключительными в каждом направлении для предотвращения отражения. Это может быть выполнено, в практических пределах, при запросе сообщения от запросчика GRQ (конечная точка) или LRQ (привратник) о начале порядкового номера передачи сигнализации вызова со значения 0 (ноль) и о достижении им порядкового номера 2^{31}, с соответствующим поведением принимающего привратника. Таким образом обеспечивается очень большой промежуток времени, перед тем как может произойти какое-либо наложение (почти 600 часов при достаточно необычной скорости, равной одному сообщению в миллисекунду). Последующие вызовы с тем же самым SessionID должны передавать со следующим неиспользованным порядковым номером в каждом направлении. (Чтобы учесть потерянные сообщения во время неудавшихся соединений, получатель должен принимать сообщения внутри маленького окна (например, 5-10), следующего за последним порядковым номером, и продолжать с него). Устройства, которые поддерживают множественные одновременные соединения сигнализации вызова под одним и тем же ID сеанса, могут использовать дополнительное **connectID,** чтобы выявлять отдельные пропуски порядковых номеров для вызовов. Если не указано иное, то **connectID** предполагается равным 0 (нулю).

8.2 Генерация слабого ключа шифрования из пароля

Для предотвращения атак перебором словаря, при которых угадывается PIN, используемый для шифрования открытого ключа D-H, а затем последовательно применяется ко всем известным псевдонимам конечной точки, желательно "расширить" ключ шифрования непосредственно псевдонимом. В частности, ключ на основе пароля, K_p, должен быть вычислен из объединения пароля и предоставляемого **endpointID**:

$$K_p = \text{Trunc}(\text{SHA1}(\text{пароль пользователя} \,||\, \textbf{endpointID}), 16)$$

Как правило, **AliasAddress** в **endpointID** будет одним из псевдонимов, включенных в элемент GRQ **endpointAlias**, но это необязательно. Например, **endpointID** может идентифицировать шлюз, поддерживающий многие конечные точки, чьи псевдонимы занесены в **endpointType**.

8.3 Размер значения, используемого только однажды

Профиль защиты 1 требует, чтобы каждая сторона предоставила 4-октетное (32-битовое) значение, используемое только однажды как часть протокола согласования ключа. При предоставлении в

течение начального согласования ключа 32 битов, возможно, достаточно, чтобы обеспечить новизну в тех случаях, в которых отвечающий привратник заново использует открытый ключ Диффи-Хеллмана, но запросчик генерирует новый ключ. Однако, во время согласования ключа нового сеанса из согласованного ранее главного ключа, все 64 исключительных бита не могут обеспечить достаточную разницу между каждым набором выведенных ключей. Предполагается, что размер значения, используемого только однажды, будет переменным, минимум 4 октета, и максимум 16 октетов.

8.4 Расширение вектора инициализации

Как добавочный показатель затемнения, 112-битовый расширяющий ключ сеанса K_s, выведен из согласованного главного ключа следующим образом:

$K_s = PRF(K_m, "расширяющий ключ" || R_e || R_g, 112)$.

Создание начального счетчика AES-128-CM для шифрования и расшифровывания выполняется следующим образом:

Счетчик = (K_s ^ (D || IV)) || C, где C – 16-битовое поле счетчика, изначально нуль.

8.5 Шифрование ClearToken

Профиль защиты 1 использует последовательность **clearToken** для хранения параметров профиля. Каждое сообщение H.225.0 содержит последовательность **ClearToken**s, за исключением выбора **empty h323-message-body**; все сообщения содержат **genericData**. Структура процедур SP1 делает возможной скорее регулярную структуру для **ClearToken**, которая позволяет ей быть преждевременно кодированной ASN.1, и переносящей в качестве параметра **raw** с **id.standard**, установленным в значение 1 в элементе **GenericData**, выявляемом OID SP2. Данная форма делает возможной идентификацию **clearToken** "нулевым" OID {0,0}. Что наиболее важно, она упрощает расположение маркера и проверку значения в нем, потому что шифрованная форма **ClearToken** сама по себе становится доступной как часть обычного процесса шифрования и расшифровывания. Таким образом, расположить элемент integrityCheck внутри шифрованного чистого маркера быстрее, чем внутри целого шифрованного сообщения.

9 Расширения к структуре (информативно)

Следующие элементы могут быть объединены в профиль защиты, описанный в данной структуре.

9.1 Использование главного ключа для защиты канала сигнализации вызова через TLS

Материал ключа, согласованный во время обмена RAS, может быть использован также, чтобы вывести ключи сеанса для защиты канала сигнализации вызова в соответствии транспортным протоколом TLS ([RFC 2246], [RFC 3546]). В сущности, согласование RAS заменяет исходный протокол квитирования TLS. Это, естественно, имеет смысл, только если сигнализация вызова будет маршрутизирована привратником. Это особенно полезно для аутентификации и сигнализации между привратниками при использовании обмена LRQ/LCF. В этом случае, нет третьего сообщения RAS, по которому запрашивающий привратник может аутентифицировать себя к вызываемому привратнику, используя материал согласованного ключа, но запросчик может быть полностью аутентифицирован своей способностью устанавливать канал сигнализации вызова с верными параметрами сеанса TLS. На рис. 1 проиллюстрирован поток используемой информации: для согласования главного ключа сеанса используется RAS, ID сеанса и соответствующий предварительный главный секрет распределяются в программное обеспечение TLS, и ID сеанса используется уровнем сигнализации вызова для установления канала сигнализации вызова через TLS. Средства, с помощью которых выполняется передача секрета, зависят от реализации и выходят за границы области применения данной Рекомендации. Отметим, что в данной Рекомендации порт 1300 указан как прослушивающий порт TLS по умолчанию для сигнализации вызова. Конечная точка должна, тем не менее, использовать один из адресов транспортировки сигнализации вызова, поставляемых привратником.

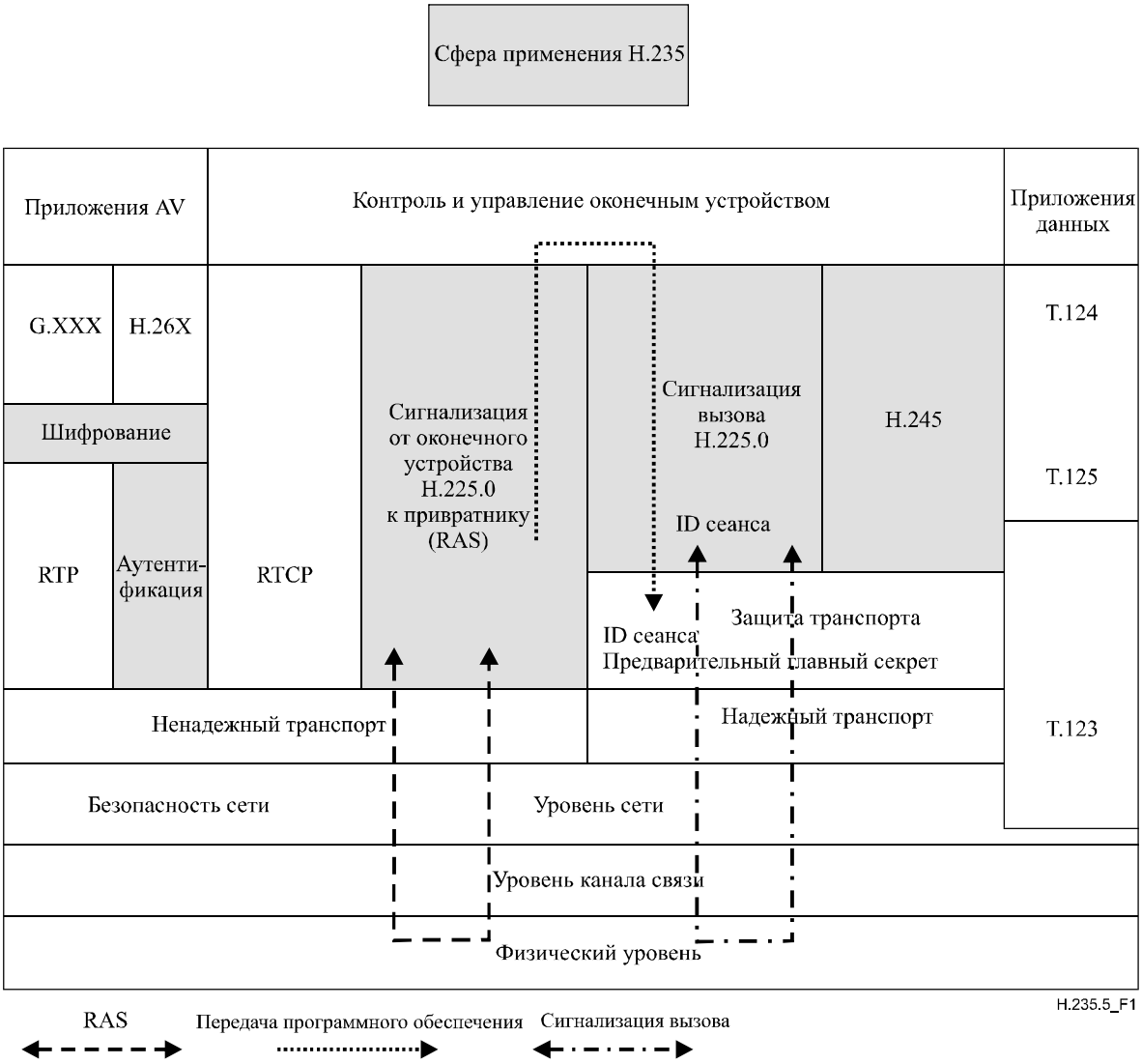

Рисунок 1/H.235.5 –Поток информации для профиля защиты и TLS

Следующее описание опирается на этапы основной структуры на рис. 1.

9.1.1 Регистрация конечной точки

Конечная точка может проверить возможность привратника поддерживать защищенную TLS сигнализацию вызова, включая один или более элементов **cipherSuite** и один или более элементов **compression** в профиль **ClearToken** в сообщении GRQ, отправленного на этапе 1, выше. Если конечная точка желает использовать ранее согласованный сеанс, она также должна включить **sessionID** в **ClearToken** (и должна указать только один набор шифрования и один метод сжатия, которые согласуются с запрашиваемым сеансом). Если согласование должно основываться на существующем сеансе TLS, никакого другого криптографического материала помимо значения, используемого только однажды, в профиле **ClearToken** не запрашивается.

Если запрашиваемый сеанс не существует, привратник должен выбрать другой профиль аутентификации (если предлагается) или должен возвратить GRJ с **GatekeeperRejectReason.resourceUnavailable**. Если запрашиваемый сеанс существует, материал главного ключа извлекается из сеанса TLS и используется (совместно с **random2** из GRQ и генерируемым привратником **random2**) для вычисления ключа аутентификации для обмена RAS. **SessionID**, **cipherSuite**, метод **compress** и значение привратника, используемое только однажды, должны быть возвращены в профиль **ClearToken** GCF.

Если привратник может поддерживать согласование сеанса TLS, он должен вычислить материал главного ключа, как указано профилем, присвоит ID нового сеанса и возвратит его **ClearToken**

профиля в **sessionID**. **ClearToken** профиля также должен содержать требуемые параметры безопасности этапа 2, выше, вместе с одним выбранным **cipherSuite**, одним выбранным методом **compress** и не равным нулю **sessionID**. Отметим, что метод обмена ключа выбранного набора шифрования является несущественным. Если привратник соглашается с защитой TLS сигнализации вызова, все адреса транспортировки сигнализации вызова, обмененные в последующих сообщениях RRQ/RCF или ARQ/ACF, должны поддерживать TLS.

Если согласование TLS и/или маршрутизация привратника не поддерживаются привратником, тогда параметры TLS не должны быть возвращены, но процедуры аутентификации могут продолжиться с этапа 3, как описывалось выше. Конечная точка должна определить, готова ли она продолжать без защиты TLS сигнализации вызова; она может сделать выбор в пользу продолжения и продолжать использовать профиль аутентификации. По успешном завершении последовательности регистрации, сеанс TLS доступен для использования при быстрой установке одного и более соединений сигнализации вызова к привратнику без необходимости пересогласования ключевого материала посредством методов открытого ключа.

Сеансы TLS имеют ограниченное время. Поэтому, для конечной точки может быть необходимым пересогласовать параметры сеанса и получить ID нового сеанса. Это может быть выполнено при обмене необходимыми элементами **ClearToken**, как описывалось выше в облегченной ("вспомогательной") последовательности регистрации. Эта последовательность не должна повлиять на ключ аутентификации RAS.

9.2 Использование сертификатов для аутентификации привратника

Хотя может быть непрактичным обменивать поддающиеся проверке цепочки сертификата в RAS (в соответствии с ограничениями размера пакета UDP), возможно, что сервер аутентифицирует себя к конечной точке, если конечная точка сможет получить доверенную копию открытого ключа сервера при помощи некоторых других средств. Сервер может просто включить в сообщение GCF **CryptoH323Token.cryptoGKCert** с **ClearToken.tokenOID**, установленным на выбранный OID профиля защиты.

9.3 Использование альтернативных механизмов защиты сигнализации

Параметры, согласованные как часть профиля защиты в соответствии с этой Рекомендацией, могут быть применены в механизмах защиты на уровне транспортировки и/или применения, как определенные заданным профилем. Последовательность **profileInfo**, добавленная к **ClearToken** H.235, предоставлялась в таком случае при необходимости.

10 Угрозы (информативно)

10.1 Пассивная атака

В настоящее время схема, описанная выше, неуязвима для пассивной атаки, при условии обеспечения того, что согласование по процессу Диффи-Хеллмана неуязвимо к пассивной атаке.

10.2 Атаки "отказ от обслуживания"

Эта схема является предметом активной атаки "отказ от обслуживания", в которых третья сторона отвечает на исходный GRQ ложным GRJ. Этот тип атаки может быть опознаваемым, а может и не быть: если отвергающий привратник является легальным и знает общий секрет (например, привратник – это привратник конечной точки, а **rejectReason** – это **resourceUnavailable**), тогда привратник может завершить согласование ключа и аутентифицировать GRJ посредством возвращения в GRJ тех же самых элементов, описанных для GCF (за исключением того, что OID, возвращенный в **authenticationMode** GCF, должен быть возвращен в элемент **ClearToken.profileInfo** GRJ). Это оставлено как часть определения заданного профиля.

Если GRJ не аутентифицирован, он может исходить от атакующего. Перед действиями в GRJ (например, при поиске альтернативного привратника), конечная точка должна дождаться возможного получения другого GRJ или аутентифицированного GCF от истинного привратника. В противном случае, конечная точка должна проверять каждый привратник, предполагаемый в любой **altGKInfo**,

получаемой во всех GRJ (один из которых, возможно, легальный). В любом случае, только истинный привратник (который знает общий секрет) может возвратить GCF аутентификации.

10.3 Атаки через посредника

Заманчиво рассматривать обмен с использованием обмена незашифрованного ключа Диффи-Хеллмана, за которым следует использование пароля или PIN, чтобы получить ключи сеанса из секрета Диффи-Хеллмана. Однако, эта форма обмена является предметом атаки через посредника, которая может использоваться для обнаружения "малого" общего секрета при помощи атаки прямым перебором с использованием значения проверки целостности, предоставленного легальным привратником в сообщении GCF.

Любой посредник, конечно, может воздействовать на любое аутентифицированное сообщение RAS, для того чтобы обеспечивать то, что сообщение будет отвергнуто из-за неудачной проверки целостности. Если возможно воздействие на все сообщения, в обслуживании может быть отказано.

10.4 Атаки угадыванием

Атакующий может принимать вид любой легальной конечной точки, легального привратника или обоих сразу (посредник), и пытаться угадать общий секрет методом проб и ошибок. Например, атакующий (которому предположительно известны детали профиля аутентификации, но не общий секрет) может угадать общий секрет и попытаться зарегистрироваться, отправляя GRQ, используя эту догадку. Как правило, привратник отправит в ответ на эту попытку GCF, содержащий открытый ключ GK (зашифрованный с использованием настоящего общего секрета), и ICV, вычисленный с использованием выведенного ключа, который зависит от расшифровывания GK зашифрованного открытого ключа атакующего. Атакующий может использовать эту информацию, чтобы проверить свое предположение касательно общего секрета. Если догадка подтверждает ICV GCF, тогда вероятно, что оно равно настоящему общему секрету; это может быть подтверждено продолжением последовательности регистрации. Если предположение не может использоваться, чтобы воспроизвести ICV GCF, тогда атакующий должен сделать другое предположение и попытаться снова. С малым ключевым пространством для общего секрета число предположений для поиска прямым перебором может не быть беспредельно высоким. Эта атака требует активного участия привратника (или конечной точки, если атакующий представляет себя как привратник). Традиционный способ противостояния такой атаке заключается в отслеживании количества неуспешных попыток и когда достигается определенный порог, все последующие попытки необходимо рассматривать как неверные (по крайней мере, на определенный период) и поднять тревогу, но такие процедуры зависят от способа реализации.

10.5 Незашифрованная половина ключа привратника

Как упоминалось выше, обмен EKE может оставаться безопасным ввиду некоторых условий, если отвечающий привратник не шифрует свою половину ключа Диффи-Хеллмана. В частности, привратник должен быть первой стороной, доказывающей свое знание общего секрета (PIN) через ICV. Если это не тот случай, тогда привратник (или объект, представляющийся привратником) может просто испытать все возможные PIN, чтобы расшифровать половину ключа Диффи-Хеллмана конечной точки, вычислить итоговый общий секрет Диффи-Хеллмана, получить ключ аутентификации и проверить его на ICV, предоставляемый конечной точкой. Это невозможно, если конечная точка может проверить ICV, предоставляемый привратником, и отказать в продолжении регистрации, если ICV окажется не таким, как ожидалось.

Использование незашифрованной половины ключа является преимущественным для привратника потому, что он может заново использовать соответствующий частый ключ со многими конечными точками. Это было бы невозможным, если бы один и тот же ключ распространялся шифрованным при многочисленных общих секретах или PIN. Наблюдатель третьей стороны может собрать примеры половин ключей, зашифрованных под двумя разными PIN, например, затем может искать через возможные сочетания двух PIN, чтобы определить какая пара дает такую же половину ключа при расшифровывании. Если существует, например, 10^8 возможных PIN, тогда есть только 10^{16} возможных сочетаний для пробы. Это представляет собой проблему, эквивалентную поиску 54-битового случайного числа, что отнюдь не является невыполнимым. Даже если найдется более одного возможного решения, правильное можно быстро определить при использовании третьего наблюдения.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	**Аудиовизуальные и мультимедийные системы**
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.