Network Working Group
Request for Comments: 4635
Category: Standards Track

D. Eastlake 3rd
Motorola Laboratories

August 2006

Идентификаторы HMAC SHA алгоритма TSIG

HMAC SHA TSIG Algorithm Identifiers

Статус документа

В этом документе содержится спецификация стандарта для протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Аннотация

Использование записей DNS[1] TSIG требует спецификации кода криптографической аутентификации сообщений. В настоящее время спецификации имеются только для двух алгоритмов TSIG - HMAC MD5 (Hashed Message Authentication Code, Message Digest 5) и GSS (Generic Security Service). Данный документ стандартизует идентификаторы и требования к реализациям для дополнительных алгоритмов HMAC SHA (Secure Hash Algorithm), а также спецификацию и отсечку значений HMAC в TSIG.

Оглавление

1. Введение

[RFC2845] задаёт спецификацию записей о ресурсах TSIG RR[2], которые могут применяться для аутентификации запросов и откликов DNS (Domain Name System [STD13]). Запись RR содержит элемент данных с синтаксисом доменного имени, указывающий используемый алгоритм аутентификации. [RFC2845] определяет имя HMAC-MD5.SIG-ALG.REG.INT для кодов аутентификации, использующих алгоритм HMAC[3] [RFC2104] с хэшированием MD5[4] [RFC1321]. Агентство IANA также зарегистрировало gss-tsig в качестве идентификатора аутентификации TSIG, при которой криптографические операции делегируются службе GSS[5] [RFC3645].

Отметим, что использование TSIG предполагает предварительное соглашения между распознавателем (resolver) и сервером в части используемого алгоритма и ключа.

В разделе 2 данного документа указаны дополнительные имена алгоритмов аутентификации TSIG, основанных на алгоритмах US NIST SHA (United States, National Institute of Science and Technology, Secure Hash Algorithm) и HMAC, а также приведены требования к реализациям этих алгоритмов.

В разделе 3 рассмотрено влияние несовпадения выходного размера указанной хэш-функции и размера кода MAC[6] в TSIG RR. В частности, что избыточные по размеру значению усекаются, а малоразмерные приводят к ошибке.

В разделе 4 рассмотрены ограничения на отсечку и её влияние, а также указано, как код ошибки позволяет сообщить о недопустимо малом размере отсекаемого поля.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **возможно** (MAY), в данном документе интерпретируются в соответствии [RFC2119].

2. Алгоритмы и идентификаторы

Записи TSIG RR [RFC2845] используются для аутентификации запросов и откликов DNS. Они предназначены для обмена эффективными симметричными кодами аутентификации, создаваемые на основе общего секрета (могут применяться также асимметричные подписи с использованием SIG RR [RFC2931], в частности могут применяться

[1]Domain Name System - система доменных имён.
[2]Resource Record.
[3]Hashed Message Authentication Code - хэшированный код аутентификации сообщения.
[4]Message Digest 5 - подпись (дайджест) сообщения, вариант 5.
[5]Generic Security Service - базовый сервис защиты.
[6]Message Authentication Code - код аутентификации сообщения.

записи SIG(0) для подписи транзакций). При использовании строгой функцией хэширования HMAC [RFC2104] обеспечивает способ расчёта таких симметричных кодов аутентификации. Единственным алгоритмом TSIG на основе HMAC был указан HMAC-MD5.SIG-ALG.REG.INT, использующий функцию MD5 [RFC1321].

Использование алгоритма SHA-1 [FIPS180-2, RFC3174] с размером хэша 160 битов, в сравнении со 128 битами MD5, а также дополнительных алгоритмов хэширования из семейства SHA [FIPS180-2, RFC3874, RFC4634] с размерами хэша 224, 256, 384 и 512 битов в некоторых случаях может обеспечивать преимущества. Добавление этих алгоритмов обусловлено возможностью успешных криптоаналитических атак в случае применения более коротких значений.

Использование TSIG между распознавателем и сервером DNS согласовывается этими сторонами. Такое соглашение может включать поддержку дополнительных алгоритмов и критерии приемлемости алгоритмов и методов отсечки, к которым применимы ограничения и рекомендации разделов 3 и 4. Согласование ключей может выполняться с помощью механизма TKEY [RFC2930] или иным взаимоприемлемым методом.

Текущие идентификаторы HMAC-MD5.SIG-ALG.REG.INT и gss-tsig включены в приведённую ниже таблицу для удобства. Поддерживающие TSIG реализации **должны** поддерживать HMAC SHA1 и HMAC SHA256, а также **могут** поддерживать gss-tsig и другие перечисленные ниже алгоритмы.

Обязательный	HMAC-MD5.SIG-ALG.REG.INT
Необязательный	gss-tsig
Обязательный	hmac-sha1
Необязательный	hmac-sha224
Обязательный	hmac-sha256
Необязательный	hamc-sha384
Необязательный	hmac-sha512

Следует реализовать алгоритм SHA-1 с отсечкой до 96 битов (12 октетов).

3. Задание отсечки

Когда размер желательно сокращать и полной силы HMAC не требуется, разумно отсекать выход HMAC по размеру и применять для аутентификации сокращённое значение. Опция HMAC SHA-1 с отсечкой до 96 битов доступна для некоторых протоколов IETF, включая IPsec и TLS.

TSIG RR [RFC2845] включает поле размера кода аутентификации MAC size, которое указывает размер поля MAC в октетах. Однако [RFC2845] не задаёт поведения в ситуациях, когда размер поля MAC отличается от выходного размера конкретной функции HMAC. Отсечка выхода HMAC до размера поля MAC описана ниже.

3.1. Спецификация отсечки

Спецификация обработки TSIG изменяется в соответствии с приведёнными ниже описаниями.

1. Значение поля MAC size превышает выходной размер функции HMAC.

   Такая ситуация **недопустима** и при получении пакета с неполным полем MAC такой пакет **должен** отбрасываться с возвратом сообщения об ошибке RCODE 1 (FORMERR).

2. Значение поля MAC size совпадает с выходным размером функции HMAC.

   Выполняются операции, указанные в [RFC2845] с представлением полного результата HMAC.

3. Значение поля MAC size меньше выходного размера функции HMAC, но больше указанного ниже в п. 4.

   Такие пакеты передаются, когда подписывающий отсекает часть вывода HMAC до разрешённого размера, как описано в RFC 2104, принимая начальные октеты и отбрасывая конец вывода. Отсечка TSIG может выполняться только для целого числа октетов. При получении пакета с такой отсечкой рассчитанное локально значение MAC усекается таким же способом и результат сравнивается с полученным кодом для аутентификации. При расчёте TSIG MAC для отклика используется усечённый код MAC из запроса.

4. Значение поля MAC size меньше большего из двух чисел - 10 (октетов) и половина выходного размера хэш-функции.

   За исключением некоторых сообщений об ошибках TSIG, описанных в параграфе 3.2 RFC 2845, где допускается нулевое значение MAC,генерация таких пакетов **недопустима** и при получении они **должны** отбрасываться с возвратом ошибки RCODE 1 (FORMERR). В качестве предельного размера для этого случая может приниматься большее из значений половины выходного размера упоминаемых здесь хэш-функций (кроме MD5) и 10 октетов для MD5.

4. Политика отсечки TSIG и информирование об ошибках

Использование TSIG происходит по обоюдному согласию распознавателя и сервера имён. Предполагается, что параметрами такого «соглашения» являются приемлемость алгоритмов и ключей, а также, с учётом описанных здесь исключений, правил отсечки. Отметим, что для реализаций распознавателей и серверов имён. является общепринятой привязка секретного ключа TSIG или ключей, которые могут использоваться вместо него, к конкретному алгоритму. В результате такие реализации позволяют использовать тот или иной алгоритм только при наличии связанного с ним ключа. Получение неизвестного, нереализованного или запрещённого алгоритма обычно приводит к ошибке BADKEY.

Локальные правила **могут** требовать отказа от TSIG даже в случаях использования обязательного для реализации алгоритма.

Когда локальная политика разрешает принимать TSIG с конкретным алгоритмом и отличным от нуля значением параметра отсечки, ей **следует** разрешать также использование этого алгоритма с меньшей отсечкой (более длинный код MAC) или с полным выводом HMAC.

Независимо от заданного локальной политикой минимального допустимого размера усечённого кода MAC, отклик **следует** передавать с размером MAC не меньше полученного в соответствующем запросе, если запрос не указывает размер MAC, превышающий выходной размер HMAC.

Реализациям, поддерживающим множество приемлемых алгоритмов и/или размеров отсечки, **следует** поддерживать упорядочивание списка приемлемых параметров по предполагаемой степени защиты, а также **следует** разрешать трактовку разных параметров отсечки для одного алгоритма, как отдельных элементов такого списка. При реализации такого подхода **следует** разрешать использование алгоритмов и отсечек вплоть до минимального, допускаемого политикой, уровня защиты.

При получении TSIG с отсечкой, разрешённой разделом 3, но размером MAC, который слишком мал по требованиям локальной политики, **должна** возвращаться ошибка RCODE 22 (BADTRUNC).

5. Взаимодействие с IANA

Этот документ (1) регистрирует в IANA новые идентификаторы алгоритмов TSIG, указанные в разделе 2, и (2) выделяет код BADTRUNC RCODE 22, описанный в разделе 4 [RFC2845].

6. Вопросы безопасности

Для всех алгоритмов аутентификации сообщений, упомянутых в этом документе, более длинные значения кодов предполагаются более защищёнными. Хотя имеются аргументы в пользу того, что некоторое укорачивание MAC усиливает защиту за счёт сокращения доступной атакующему информации, однако избыточная отсечка явно ослабляет аутентификацию, за счёт уменьшения числа битов, которые атакующий должен попытаться угадать методом подбора (или грубой силы - brute force) [RFC2104].

В последнее время были достигнуты значительные успехи в криптоанализе используемых здесь функций, которые, в конечном итоге, основаны на устройстве алгоритма MD4. С учётом этого обстоятельства сделаны обязательными для реализации более сильные алгоритмы SHA-1 и SHA-256.

Прочтите раздел «Вопросы безопасности» в [RFC2845], а также одноимённый раздел [RFC2104], где рассматриваются ограничения для используемой в данном RFC отсечки.

7. Нормативные документы

[FIPS180-2] "Secure Hash Standard", (SHA-1/224/256/384/512) US Federal Information Processing Standard, with Change Notice 1, February 2004.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm ", RFC 1321, April 1992.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC3174] Eastlake 3rd, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

[RFC3874] Housley, R., "A 224-bit One-way Hash Function: SHA-224", RFC 3874, September 2004.

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA)", RFC 4634, July 2006.

[STD13] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.
Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

8. Дополнительная литература

[RFC2930] Eastlake 3rd, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

[RFC3645] Kwan, S., Garg, P., Gilroy, J., Esibov, L., Westhead, J., and R. Hall, "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS- TSIG)", RFC 3645, October 2003.

Адрес автора

Donald E. Eastlake 3rd
Motorola Laboratories
155 Beaver Street
Milford, MA 01757 USA
Phone: +1-508-786-7554 (w)
EMail: Donald.Eastlake@motorola.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).