Network Working Group
Request for Comments: 4305
Obsoletes: 2404, 2406
Category: Standards Track

D. Eastlake 3rd
Motorola Laboratories

December 2005

Требования к реализациям криптографических алгоритмов для ESP и AH

Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

Статус документа

Это документ содержит проект стандарта протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации и статус протокола[1] можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Допускается свободное распространение документа.

Аннотация

В серии протоколов IPsec используются различные криптографические алгоритмы для защиты передаваемых через сеть данных. Протоколы ESP[2] и AH[3] обеспечивают два механизма защиты данных при передаче через защищенные связи IPsec SA[4]. Для обеспечения совместимости разнородных реализаций требуется задать набор обязательных для реализации алгоритмов, чтобы всем реализациям был доступен по крайней мере один алгоритм. В этом документе определен текущий вариант набора обязательных для реализаций ESP и AH алгоритмов, а также указаны алгоритмы, которые следует реализовать, поскольку они могут стать обязательными в будущем.

Оглавление

1. Введение

Протоколы ESP и AH обеспечивают два механизма защиты данных при передаче через защищенные связи IPsec SA [IPsec, ESP, AH]. Для обеспечения совместимости разнородных реализаций требуется задать набор обязательных для реализации алгоритмов, чтобы всем реализациям был доступен по крайней мере один алгоритм. В этом документе определен текущий вариант набора обязательных для реализаций ESP и AH алгоритмов, а также указаны алгоритмы, которые следует реализовать, поскольку они могут стать обязательными в будущем.

По самой природе криптографии пространство новых алгоритмов и существующие алгоритмы подвергаются непрерывным атакам. Алгоритмы, считающиеся достаточно сильными сегодня, могут завтра обнаружить свои уязвимости. С учетом этого выбирать обязательные для реализации алгоритмы следует достаточно консервативно чтобы снизить вероятность быстрой компрометации выбранных алгоритмов. Следует также принимать во внимание вопросы производительности, поскольку многие приложения IPsec будут использоваться в средах, где производительность важна.

Наконец, следует признать, что обязательные для реализации алгоритмы нужно менять время от времени с учетом происходящих в мире изменений. По этой причине выбор обязательных для реализации алгоритмов не включен в основные спецификации IPsec, ESP и AH. Вместо этого был создан настоящий документ. При смене алгоритмов достаточно будет обновить только один документ.

В идеальном случае алгоритмам, которые будут внесены в число обязательных для реализации завтра, уже следует присутствовать в большинстве реализаций IPsec на момент придания им статуса обязательных. Для облегчения этого мы будем пытаться идентифицировать такие алгоритмы (поскольку они уже известны) в данном документе. Не существует гарантий того, что указанные алгоритмы станут в будущем обязательными, но они могут ими стать. Все известные алгоритмы являются объектами атак и использование любого из них может быть прекращено в будущем.

---

[1] В настоящее время этот документ заменен RFC 4835. *Прим. перев.*
[2] Encapsulating Security Payload - инкапсуляция защищенных данных.
[3] Authentication Header - заголовок аутентификации.
[4] Security Association - защищенная связь.

2. Обозначения уровня требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [RFC2119].

В этом документе определены также дополнительные уровни требований:

SHOULD+ Этот термин обозначает то же, что и SHOULD. Однако, алгоритм, помеченный как SHOULD+, в будущем перейдет в число обязательных (MUST).

SHOULD- Этот термин обозначает то же, что и SHOULD. Однако, алгоритм, помеченный как SHOULD-, может перейти на уровень разрешенных (MAY) в будущих версиях этого документа.

MUST- Этот термин обозначает то же, что и MUST. Однако мы предполагаем, что в какой-то момент этот алгоритм перестанет быть обязательным и может перейти на уровень SHOULD или SHOULD-.

3. Выбор алгоритма

Для обеспечения совместимости реализаций IPsec требуется поддержка по крайней мере одного общего алгоритма защиты. В этом разделе приведены требования по реализации алгоритмов защиты для соответствующих спецификации реализаций протоколов ESP и AH. Алгоритмы защиты, реально используемые любой конкретной защищенной связью ESP или AH, определяются механизмом согласования (таким, как IKE[1] [RFC2409, IKEv2]) или задаются при организации соединения.

Естественно, допускается реализация дополнительных (стандартных или фирменных) алгоритмов, не упомянутых в этом документе.

3.1. Протокол ESP

Требования в поддержке алгоритмов защиты для соответствующих спецификации реализаций протокола ESP приведены ниже. Определения уровней требований содержатся в разделе 2.

3.1.1. Алгоритмы шифрования и аутентификации для ESP

В приведенных ниже таблицах указаны требования к алгоритмам шифрования и аутентификации для протокола IPsec ESP.

Требования	Алгоритм шифрования
MUST - **обязательно**	NULL[2]
MUST- - **обязательно**, но может утратить статус	TripleDES-CBC [RFC2451]
SHOULD+ - **следует**, но может стать **обязательным**	AES-CBC с ключами размером 128 битов [RFC3602]
SHOULD - **следует**	AES-CTR [RFC3686]
SHOULD NOT - **не следует**	DES-CBC [RFC2405][3]

Требования	Алгоритм аутентификации
MUST - **обязательно**	HMAC-SHA1-96 [RFC2404]
MUST - **обязательно**	NULL[2]
SHOULD+ - **следует**, но может стать **обязательным**	AES-XCBC-MAC-96 [RFC3566]
MAY - **возможно**	HMAC-MD5-96 [RFC2403][4]

3.1.2. Комбинированные алгоритмы для ESP

Как указано в [ESP], протокол поддерживает использование комбинированных алгоритмов, которые обеспечивают услуги конфиденциальности и аутентификации. Поддержка таких алгоритмов требует соответствующего структурирования реализации ESP. Во многих ситуациях комбинированные алгоритмы обеспечивают значительные преимущества в части эффективности и пропускной способности. Хотя в настоящее время не указывается предлагаемых или обязательных к реализации комбинированных алгоритмов, предполагается, что в ближайшем будущем представит интерес алгоритм AES-CCM [CCM], адаптированный в качестве предпочтительного для IEEE 802.11 [802.11i].

3.2. Протокол AH

Ниже приведены требования к реализации алгоритмов защиты в соответствующих спецификации реализациях протокола AH. Определения уровней требований приведены в разделе 2. Как вы понимаете, все перечисленные алгоритмы относятся к числу алгоритмов аутентификации.

---

[1] Internet Key Exchange - обмен ключами в Internet.

[2] Поскольку шифрование и аутентификация в ESP являются необязательными, поддержка двух «пустых» алгоритмов NULL обязательна для обеспечения совместимости со способом согласования используемых услуг. Отметим, что алгоритмы шифрования и аутентификации по отдельности могут принимать значения NULL, но **недопустимо**, чтобы значение NULL имели оба алгоритма сразу.

[3] Алгоритм DES с его малым размером ключей и публично показанной открытой аппаратурой для взлома, является сомнительным средством защиты общего пользования.

[4] Алгоритм MD5 достаточно слаб, однако эта слабость не проявляется при использовании MD5 с HMAC.

Требования	Алгоритм аутентификации
MUST - **обязательно**	HMAC-SHA1-96 [RFC2404]
SHOULD+ - **следует**, но может стать обязательным	AES-XCBC-MAC-96 [RFC3566]
MAY - **возможно**	HMAC-MD5-96 [RFC2403][5]

4. Вопросы безопасности

Безопасность криптографически защищенных систем зависит от стойкости выбранных криптографических алгоритмов и используемых этими алгоритмами ключей. Кроме того, безопасность зависит также от устройства и администрирования протокола, используемого для предотвращения обхода криптосистемы.

Этот документ посвящен выбору криптографических алгоритмов для использования с протоколами ESP и AH и, в частности, обязательных для реализации алгоритмов. Алгоритмы, которые в соответствии с этой спецификацией **требуется** (MUST) или **следует** (SHOULD) реализовать, не имеют в данный момент известных фактов взлома и выполненные криптографические исследования позволяют надеяться, что эти алгоритмы останутся безопасными в обозримом будущем. Однако, такое положение дел не обязательно сохранится. Мы, следовательно, предполагаем появление новых версий этого документа, отражающих накопленный в сфере защиты опыт.

5. Благодарности

Значительная часть приведенного здесь текста была заимствована из RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2, автором которого является Jeffrey I. Schiller.

6. Отличия от RFC 2402 и 2406

[RFC2402] и [RFC2406] определяли протоколы IPsec AH и IPsec ESP. Каждый из этих документов содержал требования к криптографическим алгоритмам для соответствующего протокола. В настоящее время эти спецификации заменены документами [AH] и [ESP], которые не содержат требований к реализации криптографических алгоритмов. В данном документе указаны такие требования для обоих протоколов - [AH] и [ESP].

Сравнение требований приведено ниже.

Старое требование	Старый RFC	Новое требование	Алгоритм
MUST - **требуется**	2406	SHOULD NOT - **не следует**	DES-CBC [RFC2405][1]
MUST - **требуется**	2402, 2406	MAY - **возможно**	HMAC-MD5-96 [RFC2403]
MUST - **требуется**	2402, 2406	MUST - **требуется**	HMAC-SHA1-96 [RFC2404]

7. Нормативные документы

[AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[IPsec] Kent, S., "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

[RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

8. Дополнительная литература

[802.11i] LAN/MAN Specific Requirements Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i, June 2004.

[JIS] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

---

[5]Алгоритм MD5 достаточно слаб, однако эта слабость не проявляется при использовании MD5 с HMAC.

[1]IETF запрещает самостоятельное использование DES уже много лет и не включает этот алгоритм в новые стандарты в течение достаточного времени (см. комментарий IESG на первой странице [RFC2407]). Но этот документ является первым проектом стандарта, в котором указано, что реализациям **не следует** использовать алгоритм DES самостоятельно (не в комбинации с другими, *прим. перев.)*. Институт стандартов и технологий США (NIST) формально признал слабость DES при самостоятельном использовании в документе, опубликованном 26 июля 2004 в Федеральном правительственном реестре США (Docket No. 040602169-4169-01), призывая прекратить использование этого алгоритма в качестве Государственного стандарта США. Алгоритм Triple DES по прежнему признается как IETF, так и NIST.

[CCM] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

Адрес автора

Donald E. Eastlake 3rd

Motorola Laboratories

155 Beaver Street

Milford, MA 01757 USA

Phone: +1-508-786-7554 (w)

+1-508-634-2066 (h)

EMail: Donald.Eastlake@Motorola.com

Перевод на русский язык
Николай Малых
nmalykh@protokols.ru

Полное заявление авторских прав

Интеллектуальная собственность

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.