Network Working Group
Request for Comments: 4307
Category: Standards Track

J. Schiller
Massachusetts Institute of Technology

December 2005

Криптографические алгоритмы для использования с IKEv2

Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

Статус документа

В этом документе описан предлагаемый стандарт протокола для сообщества Internet; документ служит приглашением к дискуссии в целях развития протокола. Информацию о текущем состоянии стандартизации протокола можно найти в документе Internet Official Protocol Standards (STD 1). Данный документ может распространяться свободно.

Авторские права

Аннотация

Группа протоколов IPsec использует различные криптографические алгоритмы для обеспечения защиты информации. Протоколы IKE[1] (RFC 2409) и IKEv2 обеспечивают механизм согласования алгоритма, который должен использоваться для данного соединения (association). Однако для обеспечения взаимодействия между независимыми реализациями необходимо задать набор обязательных для реализации алгоритмов, чтобы по крайней мере один алгоритм поддерживался всеми реализациями. В этом документе определяется набор алгоритмов, являющихся обязательными для реализации, как часть IKEv2, а также алгоритмы, которые следует реализовать потому, что они могут стать обязательными в будущем.

1. Введение

Протокол IKE обеспечивает согласование криптографических алгоритмов между конечными точками криптографической ассоциации[2]. Различные реализации IPsec и IKE могут поддерживать разные алгоритмы. Однако IETF желает обеспечить между всеми реализациями тот или иной вариант взаимодействия. В частности, требуется, чтобы протокол IKE определял набор обязательных для реализации алгоритмов, поскольку сам протокол IKE использует такие алгоритмы как часть процесса согласования. По этой причине некий набор алгоритмов требуется задать в качестве обязательного для реализации в IKE.

В криптографии постоянно появляются новые алгоритмы, а существующие подвергаются непрерывным атакам. Алгоритм, представляющийся сегодня достаточно сильным, может завтра обнаружить свою слабость. По этой причине выбор обязательных для реализации алгоритмов должен быть достаточно осторожным, чтобы снизить вероятность компрометации выбранных алгоритмов в течение короткого времени. Следует также принимать во внимание производительность, поскольку многие используют IPsec в средах, где производительность имеет большое значение.

Наконец, следует принимать во внимание, что обязательные для реализации алгоритмы могут изменяться с течением времени для адаптации к меняющимся условиям. По этой причине выбор обязательных для реализации алгоритмов был удалён из спецификации протокола IKEv2 и помещён в данный документ. При изменении набора обязательных алгоритмов требуется обновить лишь данный документ.

В идеальном варианте алгоритмы, обязательные завтра для реализации, уже доступны сегодня в большинстве реализаций IPsec. Для достижения этой цели мы попытаемся идентифицировать такие алгоритмы (известные сегодня) в этом документе. Нет никакой гарантии, что алгоритмы, которые мы предполагаем обязательными в будущем, станут таковыми на самом деле. Все алгоритмы, известные сегодня, являются объектами криптографических атак и могут быть отвергнуты в будущем.

2. Уровни 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 перейдёт в число обязательных (MUST).

SHOULD- Этот термин обозначает то же, что и SHOULD. Однако, алгоритм, помеченный как SHOULD-, может перейти на уровень разрешённых (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-.

[1] Internet Key Exchange – обмен ключами в Internet.
[2] Шифрованное соединение. *Прим. перев.*

3. Выбор алгоритма

3.1. Выбор алгоритма IKEv2

3.1.1. Алгоритмы шифрования данных

Шифрование данных IKEv2 требует как алгоритма обеспечения конфиденциальности, так и алгоритма обеспечения целостности. Для обеспечения конфиденциальности реализация **должна** (MUST-) поддерживать 3DES-CBC и **следует** (SHOULD+0 также поддерживать AES-128-CBC. Для обеспечения целостности **должен** поддерживаться алгоритм HMAC-SHA1.

3.1.2. Группы Diffie-Hellman

Существует несколько групп MODP[1], определённых для использования в IKEv2. Эти группы определены как в базовом документе [IKEv2], так и в документе, посвящённом расширениям MODP. Группы идентифицируются номерами. Все группы, не указанные здесь, рассматриваются как **возможные** для реализации.

Номер группы	*Длина в битах*	*Статус*	*Документ*
2	1024	MUST-	[RFC2409]
14	2048	SHOULD+	[RFC3526]

3.1.3. Алгоритмы преобразования IKEv2 типа 1

IKEv2 определяет несколько алгоритмов для Transfer Type 1 (шифрование). Ниже эти алгоритмы перечислены с указанием статуса для каждого.

Имя	*Номер*	*Документ*	*Статус*
Резерв	0		
ENCR_3DES	3	[RFC2451]	MUST-
ENCR_NULL	11	[RFC2410]	MAY
ENCR_AES_CBC	12	[AES-CBC]	SHOULD+
ENCR_AES_CTR	13	[AES-CTR]	SHOULD

3.1.4. Алгоритмы преобразования IKEv2 типа 2

Алгоритмы Transfer Type 2 являются псевдослучайными функциями для генерации случайных значений.

Имя	*Номер*	*Документ*	*Статус*
Резерв	0		
PRF_HMAC_MD5	1	[RFC2104]	MAY
PRF_HMAC_SHA1	2	[RFC2104]	MUST
PRF_AES128_CBC	4	[AESPRF]	SHOULD+

3.1.5. Алгоритмы преобразования IKEv2 типа 3

Алгоритмы Transfer Type 3 служат для обеспечения целостности и защищают данные от подделки.

Имя	*Номер*	*Документ*	*Статус*
NONE	0		
AUTH_HMAC_MD5_96	1	[RFC2403]	MAY
AUTH_HMAC_SHA1_96	2	[RFC2404]	MUST
AUTH_AES_XCBC_96	5	[AES-MAC]	SHOULD+

4. Вопросы безопасности

Безопасность криптографических систем зависит как от силы выбранных криптоалгоритмов, так и от качества используемых этими алгоритмами ключей. Безопасность также зависит от устройства протокола, используемого системой для предотвращения использования не использующих криптографии путей обхода защиты системы в целом.

Этот документ посвящён выбору криптографических алгоритмов для использования с IKEv2, а именно - выбору алгоритмов, обязательных для реализации. Алгоритмы, для которых указано MUST (**необходимо**) и SHOULD (**следует**), приняты к считаются безопасными в настоящее время и криптографические исследования позволяют надеяться на то, что они останутся безопасными в обозримом будущем. Однако это предположение может не оправдаться. Следовательно, в будущем могут появляться пересмотренные варианты этого документа, отражающие накопленный опыт.

5. Нормативные документы

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

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

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

[RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

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

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

[1] Modular Exponential – модульная экспоненциальная.

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

[AESPRF] Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 3664, January 2004.

[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.

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

Адрес автора

Jeffrey I. Schiller

Massachusetts Institute of Technology

Room W92-190

77 Massachusetts Avenue

Cambridge, MA 02139-4307

USA

Phone: +1 (617) 253-0161

EMail: jis@mit.edu

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.