Network Working Group
Request for Comments: 4304
Category: Standards Track

S. Kent
BBN Technologies

December 2005

Добавление расширенных порядковых номеров (ESN) в области интерпретации IPsec (DOI) для протокола управления защитными связями и ключами (ISAKMP)

Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)

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 можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Допускается свободное распространение документа.

Аннотация

Протоколы AH[1] и ESP[2] используют порядковые номера для детектирования попыток повторного использования пакетов. В этом документе описано расширение области интерпретации (DOI[3]) для протокола управления защищёнными связями и ключами (ISAKMP[4]). Это расширение поддерживает согласование использования традиционных 32-битовых порядковых номеров или расширенных (64 бита) порядковых номеров (ESN[5]) для конкретной защищённой связи AH или ESP.

1. Введение

Спецификации протоколов AH [AH] и ESP [ESP] описывают опцию использования расширенных (64 бита) порядковых номеров. Эта опция обеспечивает возможность передачи очень больших объемов данных с высокмими скоростями через защищенные связи (SA) без сменя ключей, связанной с исчерпанием пространства порядковых номеров. В этом документе описано дополнение к IPsec DOI для ISAKMP [DOI], которое требуется для поддержки согласования опции ESN.

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 RFC 2119 [Bra97].

2. Атрибут SA

Описанный здесь атрибут SA используется во второй фазе (Phase II) согласования протокола IKE[6]. Атрибут относится к базовому типу - Basic (B). Кодирование этого атрибута определено в базовой спецификации ISAKMP [ISAKMP]. Атрибуты, описанные в качестве базовых, **недопустимо** кодировать, как переменные. Более подробное описание кодирования атрибута в IPsec DOI приведено в документе [IKE]. Все ограничения, перечисленные в [IKE], применимы к IPsec DOI и настоящему дополнению.

Тип атрибута

Класс	Значение	Тип
Extended (64-bit) Sequence Number	11	B

Значения класса

Этот класс показывает, что защищенная связь SA будет использовать 64-битовые порядковые номера (описание расширенных порядковых номеров содержится в документах [AH] и [ESP]).

Резерв	0
64-битовый порядковый номер	1

3. Согласование атрибута

Если реализация получает определенный атрибут IPsec DOI (или значение атрибута), который не поддерживается, **следует** передать сигнал ATTRIBUTES-NOT-SUPPORT, а организация защищенной связи **должна** быть прервана.

---

[1]Authentication Header - заголовок аутентификации.
[2]Encapsulating Security Payload - инкапсуляция защищенных данных.
[3]Internet IP Security Domain of Interpretation - область интерпретации защиты IP.
[4]Internet Security Association and Key Management Protocol - протокол управления защищенными связями и ключами в Internet.
[5]Extended Sequence Number.
[6]Internet Key Exchange - протокол обмена ключами.

Если реализация получает любое значение атрибута, отличное от значений для 64-битовой нумерации, организация защищенной связи **должна** быть прервана.

4. Вопросы безопасности

Этот документ связан с протоколом обмена ключами [IKE], который объединяет ISAKMP [ISAKMP] и Окли [OAKLEY] для распространения криптографических ключей с обеспечением защиты и идентификации сторон. Обсуждение различных протоколов защиты и преобразований, описанных в этом документе, можно найти в упомянутых ниже базовых документах и документах по шифрованию.

Добавление атрибута ESN не меняет параметров безопасности IKE. При использовании ESN с протоколом ESP важно выбрать режим шифрования, который обеспечит достаточную защиту при шифровании очень большого объема данных с использованием одного ключа. В этом смысле такие алгоритмы, как DES[1] в режиме CBC[2] **не** подходит для использования с ESN, поскольку с использованием одного ключа DES не следует шифровать более 2^{32} блоков в таком режиме. Аналогично, с протоколами ESP и AH следует использовать алгоритмы контроля целостности, обеспечивающие должную защиту при больших объемах передаваемой информации. Во избежание возможных проблем с защитой, порождаемых ограничениями алгоритмов, время жизни SA можно ограничивать по объему информации, защищаемой с использованием одного ключа, до того, как будет достигнут предел ESN в 2^{64} пакетов.

5. Согласование с IANA

В этом документе задано «магическое» число, поддерживаемое IANA. Для этого атрибута не выделяется дополнительных значений. Агентство IANA выделило значение IPsec Security Attribute для Attribute Type (тип атрибута). Это значение указано в колонке «Значение» таблицы раздела 2.

Благодарности

Автор благодарит членов рабочей группы IPsec. Автор также признателен Karen Seo за помощь при редактировании этой спецификации.

Нормативные документы

[Bra97] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

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

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

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

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

[ISAKMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

Дополнительная литература

[OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

Адрес автора

Stephen Kent

BBN Technologies

10 Moulton Street

Cambridge, MA 02138

USA

Phone: +1 (617) 873-3988

EMail: kent@bbn.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1] Data Encryption Standard - стандарт шифрования данных.
[2] Cipher Block Chaining - сцепка шифрованных блоков.

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 Internet Society.