Internet Engineering Task Force (IETF) Y. Sheffer
Request for Comments: 6989 Porticor
Updates: 5996 S. Fluhrer
Category: Standards Track Cisco
ISSN: 2070-1721 July 2013

Дополнительные тесты Diffie-Hellman для протокола IKEv2

Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)

Аннотация

Этот документ добавляет несколько обязательных тестов, требуемых для защищённой работы протокола обмена ключами IKE[1] версии 2 (IKEv2) с группами эллиптических кривых. Не требуется вносить какие-либо изменения в реализации IKE, использующие модульные экспоненциальные группы, отличающиеся от некоторых редко используемых групп DSA[2]. Этот документ служит обновлением спецификации протокола IKEv2, опубликованной в RFC 5996.

Статус документа

Этот документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[3] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[4]. Дополнительная информация о стандартах Internet приведена в разделе 2 RFC 5741.

Информацию о текущем состоянии данного документа, обнаруженных ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc6989.

Оглавление

[1] Internet Key Exchange Protocol.
[2] Digital Signature Algorithm - алгоритм цифровой подписи.
[3] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[4] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

IKEv2 [RFC5996] включает организацию общего секрета с использованием протокола Diffie-Hellman (DH) и последующей проверкой подлинности (аутентификацией) двух партнёров. Существующие реализации обычно применяют модульные экспоненциальные (MODP) группы DH, типа определённых в [RFC3526].

IKEv2 не требует выполнения каких-либо тестов партнёром, получившим открытый ключ DH от другого партнёра. Это очень хорошо для большинства групп MODP. Для других же групп DH, где партнёры неоднократно используют значения DH во множестве сессий IKE, отказ получателя от проверки может создавать потенциальные уязвимости (см. параграф 4.1). В частности, это относится к группам EC[1], использование которых становится все более популярным. В этом документе определены тесты для нескольких типов групп DH.

В дополнение к этому документ описывает другую возможную атаку, относящуюся к повторному использованию ключей DH - timing attack. Этот дополнительный материал заимствован из [RFC2412].

Данный документ обновляет [RFC5996] за счёт добавления требований безопасности, применимых ко многим реализациям протокола.

1.1. Используемые соглашения

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

2. Проверка принадлежности к группе

В этом разделе описаны тесты, которые должны выполняться партнёрами IKE при получении элементов данных KE[2]. Проверки **рекомендуются** для всех реализаций, но **требуются** только для тех, в которых многократно используются секретные ключи DH (см. определение в [RFC5996], параграф 2.12). Эти тесты относятся к получателям элементов данных KE и описывают как должны выполняться проверка полученных данных. Тесты описаны по группам DH.

2.1. Группы Sophie Germain Prime MODP

Эти группы в настоящее время являются наиболее широко применяемыми. Для всех таких групп значение (p-1)/2 также является простым числом. Приведённая здесь информация относится ко всем таким группам MODP. Каждый получатель **должен** удостовериться, что открытое значение партнёра r удовлетворяет условию (1 < r < p-1). Как указано в параграфе 2.2 работы [Menezes], после такой проверки ещё сохраняется возможность утечки одного бита секретного показателя при многократном использовании ключей DH. Такой размер потенциальной утечки считается несущественным.

Конкретные группы, входящие в это семейство, указаны в разделе 5.

2.2. Группы MODP с малыми подгруппами

В [RFC5114] определены модульные экспоненциальные группы с малыми подгруппами, каждая из которых имеет композит (p-1)/2. В параграфе 2.1 работы [Menezes] описаны некоторые утечки информации в результате атак на малые подгруппы при многократном использовании секретного значения DH.

Такие утечки можно предотвратить, если получатель выполняет проверку открытого значения партнёра., однако такая проверка требует ресурсов (приблизительно столько же, сколько экономится за счёт многократного использования секретных значений DH). Стандарт NIST ([NIST-800-56A], параграф 5.6.2.4) требует выполнения этой проверки, следовательно при желании соответствовать этому стандарту проверка должна выполняться.

С учётом отмеченного выше реализация IKE **должна** выбрать один из двух приведённых ниже вариантов.

- **Должна** проверяться принадлежность открытого значения партнёра. диапазону (1 < r < p-1) и выполнение условия $r^q = 1 \bmod p$ (q - размер подгруппы, указанный в определяющем ее документе RFC). После этого **можно** повторно использовать секретные значения DH. Этот вариант обеспечивает соответствие требованиям [NIST-800-56A].
- **Не допускается** многократное использование секретных значений DH (т. е., секретное значение DH для каждого обмена DH **должно** генерироваться из свежего вывода криптографически защищённого генератора случайных чисел) и **должна** проверяться принадлежность открытого значения партнёра. диапазону (1 < r < p-1). Этот вариант лучше подходит для тех случаев, когда соответствие [NIST-800-56A] не требуется.

Конкретные группы, входящие в это семейство, указаны в разделе 5.

2.3. Группы эллиптических кривых

IKEv2 может применяться с группами эллиптических кривых, определённых над полем GF(p) [RFC5903] [RFC5114]. Согласно параграфу 2.3 [Menezes], возможна некоторая утечка информации. Принимающая сторона **должна** убедиться в пригодности открытого ключа своего партнёра., т. е. параметры x и y из открытого ключа партнёра. должны удовлетворять уравнению кривой $y^2 = x^3 + ax + b \bmod p$ (где для групп 19, 20 и 21 значение a=-3 (mod p), а все остальные значения a, b и p для группы указаны в определяющем группу RFC).

Отметим, что дополнительная проверка того, что значение открытого ключа не является точкой на бесконечности, не требуется, поскольку IKE (см. раздел 7 в [RFC5903]) не позволяет закодировать такое значение.

Конкретные группы, входящие в это семейство, указаны в разделе 5.

[1]Elliptic Curve - эллиптическая кривая.
[2]Key Exchange - обмен ключами.

2.4. Обновление реализаций

Существующие реализации IKEv2 с группами ECDH[1] могут быть обновлены для включения описанных здесь тестов, даже если они не применяют многократно ключи DH. Тесты можно рассматривать, как проверку «здравомыслия», позволяющую предотвратить попытки обработки входных данных, которая не предусмотрена реализацией.

Реализации ECDH с возможностью повторного использования ключей DH **должны** включать описанные выше проверки.

2.5. Поведение протокола

Получатель открытого ключа DH, столкнувшийся с отказом при какой-либо из упомянутых выше проверок, предполагает, что отправитель является обманным или реализация на его стороне имеет ошибки. Описанное ниже поведение позволяет повысить устойчивость к атакам, пытающимся нарушить обмен IKE, а также помогает партнёрам с некорректными реализациями узнать о своих проблемах.

Если такая ошибка происходит в процессе обмена IKE_SA_INIT, получатель **должен** отбросить сообщение с непригодными данными KE и **недопустимо** использовать это сообщение при создании защищённой связи IKE (SA[2]).

Если в реализации поддерживается устойчивое к DoS поведение, предложенное в параграфе 2.4 [RFC5996], она может просто игнорировать ошибочные сообщения с запросами или откликами и продолжать ожидать следующего сообщения с действительными данными KE.

Если реализация не поддерживает устойчивое к DoS поведение и в запросе IKE_SA_INIT указаны непригодные данные KE, реализация **может** передать уведомление об ошибке INVALID_SYNTAX и удалить организуемую связь IKE SA. Если же непригодные данные KE были получены в отклике IKE_SA_INIT, реализация может просто удалить созданную наполовину IKE SA и заново инициировать обмен.

Если непригодные данные KE получены в процессе обмена CREATE_CHILD_SA (или любого другого обмена после организации IKE SA) и непригодные данные KE были в запросном сообщении, отвечающая сторона (Responder) **должна** передать уведомление об ошибке INVALID_SYNTAX и сбросить IKE SA. Если непригодные данные KE получены в отклике, принявший это сообщение инициатор (Initiator) **должен** незамедлительно удалить IKE SA путём отправки уведомления IKE SA Delete в качестве нового обмена. В таких случаях очевидно наличие ошибки в реализации отправителя и сброс IKE SA упрощает обнаружение такой ошибки.

3. Побочные каналы

В дополнение к атакам на малые подгруппы (small-subgroup) существует также возможность timing-атак на партнёров. IKE, которые повторно используют значения секретов Diffie-Hellman. Это атака с побочным каналом (side-channel), уязвимость к которой зависит от деталей реализации и модели угроз.

Оставшаяся часть этого параграфа заимствована из раздела 5 [RFC2412] с незначительными разъяснениями. Эта атака остаётся применимой к реализациям IKEv2, а также группам MODP и ECDH. Отметим также, что для представленных в проективной форме групп EC доступны более эффективные контрмеры, но их рассмотрение выходит за рамки этого документа.

Атаки с координацией (Timing), в которых может быть восстановлено значение показателя (exponent), использованного в расчётах Diffie-Hellman, описаны Paul Kocher [Kocher]. Для противодействия таким атакам в реализациях должны применяться меры сокрытия последовательности операций, вовлечённых в расчёты.

Одним из возможных методов борьбы с такими атаками является использование «фактора ослепления» (blinding factor). В этом методе элемент группы r выбирается случайным образом и рассчитывается его мультипликативная инверсия по модулю p (обозначим это r_inv). Значение r_inv можно рассчитать расширенным методом Эвклида (Extended Euclidean Method), используя r и p в качестве входных значений. Когда выбран показатель x, рассчитывается также значение r_inv^x. Затем, вычисляя $(g^y)^x$, реализация будет выполнять приведённую ниже последовательность расчётов.

$$A = r*g^y$$
$$B = A^x = (r*g^y)^x = (r^x)(g^{(xy)})$$
$$C = B*r\_inv^x = (r^x)(r^{(-1*x)})(g^{(xy)}) = g^{(xy)}$$

Фактор ослепления нужен лишь в тех случаях, когда показатель x применяется более 100 раз.

4. Вопросы безопасности

Этот документ целиком связан с протоколом защиты IKEv2 и необходимостью его усиления в некоторых случаях.

4.1. Повторное использование ключа DH и множество партнёров.

В этом параграфе описан вариант атаки, которую можно предотвратить с помощью описанных выше тестов.

Предположим, что IKE-партнер Alice поддерживает защищённые связи IKE с Bob и Eve. Alice использует один ключ ECDH для обеих SA, что разрешается с учётом некоторых ограничений. Если Alice не выполняет этих тестов, Eve получит возможность передать некорректно сформированный открытый ключ, с помощью которого она сможет определить секретный ключ Alice (как описано в разделе 2 [Menezes]). Поскольку ключ является общим для двух защищённых связей Eve сможет получить ключ IKE SA между Alice и Bob.

4.2. Многократное использование ключа DH - варианты

Секретные ключи DH могут повторно использоваться разными способами с различным влиянием на защиту. Ниже приведено несколько примеров.

[1] Elliptic Curve Diffie-Hellman.
[2] Security association.

1. Ключи DH используются для множества соединений (IKE SA) с одним партнёром и для соединений с другими партнёрами.
2. Ключи DH используются для множества соединений с одним партнёром (например, с партнёром, указанным его адресом IP), но не применяются для соединений с другими партнёрами.
3. Ключи DH используются повторно лишь в том случае, когда они не были применены в завершённом обмене (например, когда партнёр ответил уведомлением INVALID_KE_PAYLOAD).

Описанные в этом документе атаки small-subgroup и timing применимы по крайней мере к вариантам 1 и 2.

4.3. Группы, не охватываемые данным RFC

Существует множество типов групп, которые не были конкретно рассмотрены в данном RFC. Описывающие такие группы документы **должны** включать и описание требуемых для группы тестов.

Одним из типов являются чётно-характеристические эллиптические кривые (even-characteristic elliptic curve). Сейчас эти кривые имеют сомножители (cofactor) больше 1 и это ведёт к возможности утечки информации. Имеется несколько способов предотвращения такой утечки, включая выполнение тестов, аналогичных тесту из параграфа 2.2 или настройки операции ECDH для предотвращения утечки (типа ECC CDH[1], где общим секретом реально является hxyG). Поскольку подходящие тесты зависят от способа определения группы, описать из заранее невозможно.

4.4. Поведение при отказе теста

Рекомендованное в параграфе 2.5 поведение соответствует базовой обработке ошибок в процессе обмена IKE_SA_INIT, описанной в параграфе 2.21.1 [RFC5996]. Отправитель не обязан передавать уведомления об ошибках и получатель не может зависеть от таких уведомлений, поскольку его подлинность не проверена и фактически это могут быть попытки организации DoS-атаки на соединение. Таким образом, уведомления полезны лишь для поиска ошибок при отладке реализаций.

С другой стороны, уведомление об ошибке не угрожает безопасности, поскольку в нем не содержится секретной информации. Все группы Diffie-Hellman в IKEv2 открыты и ни один из определённых здесь тестов не зависит от секретного ключа. Фактически, все тесты могут быть проведены перехватчиком данных.

Ситуация с отказом при обмене CREATE_CHILD_SA иная, поскольку здесь все защищено IKE SA. Партнёры здесь аутентифицированы и могут полагаться на уведомления об ошибках. Более подробное описание обработки ошибок в таких случаях приведено в параграфе 2.21.3 [RFC5996].

5. Взаимодействие с IANA

Агентство IANA добавило колонку Recipient Tests (Тесты у получателя) в реестр Transform Type 4 - Diffie-Hellman Group Transform IDs для IKEv2 [IANA-IKEv2-Registry].

Включённые в эту колонку значения приведены в таблице.

Номер	**Тесты на стороне получателя**
1, 2, 5, 14, 15, 16, 17, 18	RFC 6989, параграф 2.1
22, 23, 24	RFC 6989, параграф 2.2
19, 20, 21, 25, 26, 27, 28, 29, 30	RFC 6989, параграф 2.3

Группы 27 - 30 определены в [RFC6954].

В будущих документах, определяющих группы DH для IKEv2, **потребуется** определение этой информации для каждой новой группы (возможно, путём ссылки на данный документ).

6. Благодарности

Авторы благодарят Dan Harkins, инициировавшего обсуждение этого вопроса в почтовой конференции IPsec. Спасибо Tero Kivinen и Rene Struik за полезные комментарии. Значительная часть текста в разделе 3 заимствована из [RFC2412] и мы признательны автору этого документа Hilarie Orman.

Документ был подготовлен с помощью программы lyx2rfc, созданной Nico Williams.

7. Литература

7.1. Нормативные документы

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

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996[2], September 2010.

7.2. Дополнительная литература

[IANA-IKEv2-Registry] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters/>.

[Kocher] Kocher, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", December 1996, <http://www.cryptography.com/timingattack/paper.html>.

[Menezes] Menezes, A. and B. Ustaoglu, "On Reusing Ephemeral Keys In Diffie-Hellman Key Agreement Protocols", December 2008, <http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-24.pdf>.

[1] Elliptic Curve Cryptography Cofactor Diffie-Hellman.

[2] Этот документ признан устаревшим и заменён RFC 7296. *Прим. перев.*

[NIST-800-56A] National Institute of Standards and Technology (NIST), "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)", NIST PUB 800-56A, March 2007.

[RFC2412] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

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

[RFC5114] Lepinski, M. and S. Kent, "Additional Diffie-Hellman Groups for Use with IETF Standards", RFC 5114, January 2008.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, June 2010.

[RFC6954] Merkle, J. and M. Lochter, "Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 6954, July 2013.

Адреса авторов

Yaron Sheffer

Porticor

EMail: yaronf.ietf@gmail.com

Scott Fluhrer

Cisco Systems

1414 Massachusetts Ave.

Boxborough, MA 01719

USA

EMail: sfluhrer@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru