Internet Engineering Task Force (IETF)
Request for Comments: 6194
Category: Informational
ISSN: 2070-1721

T. Polk
L. Chen
NIST
S. Turner
IECA
P. Hoffman
VPN Consortium

March 2011

Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms

Вопросы безопасности для алгоритмов цифровой подписи SHA-0 и SHA-1

Аннотация

Этот документ рассматривает вопросы безопасности для алгоритмов цифровой подписи SHA-0 и SHA-1.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется с информационными целями.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Не все документы, одобренные IESG, претендуют на статус стандартов Internet, см. раздел 2 в RFC 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc6194.

1. Введение

Безопасные алгоритмы хэширования (Secure Hash Algorithm) заданы в [SHS]. В предыдущей версии [SHS] был также задан SHA-0. Алгоритм SHA-0 опубликован в 1993 г., SHA-1 - в 1996 г. и оба являются алгоритмами создания дайджестов сообщений, иногда их называют хэш-функциями или алгоритмами хэширования. Они принимают на входе сообщение произвольной длины и дают 160-битовый оттиск (fingerprint) или дайджест сообщения. Опубликованные атаки на эти алгоритмы показывают, что их неразумно применять там, где требуется устойчивость к коллизиям.

В [HASH-Attack] приведена сводка применения хэширования в протоколах Internet и рассматривается влияние атак на свойства необратимости и отсутствия коллизий на протоколы. Предполагается знакомство читателя с [HASH-Attack].

Могут оказаться полезными рекомендации по размеру ключей и стойкости алгоритмов в [SP800-57] и [SP800-131].

2. Вопросы безопасности SHA-0

Ниже приведены краткие сведения о недавних атаках на стойкость к конфликтам (коллизиям) SHA-0, поиск прообраза и второго прообраза. Кроме того, обсуждаются атаки на SHA-0 при хэшировании с ключом (HMAC-SHA-0).

Национальный институт стандартов и технологии США (U.S. National Institute of Standards and Technology или NIST) отозвал SHA-0 в 1996 г., SHA-0 больше не считается пригодным для использования в каких-либо транзакциях, связанных с криптографией, в федеральных правительственных органах США для защиты конфиденциальной, но не засекреченной информации. Обсуждение SHA-0 здесь приводится лишь для полноиы.

Настоятельно не рекомендуется применять SHA-0 для каких-либо целей. Анализ SHA-0 подолжается, поскольку многие считают его ослабленной версией SHA-1.

2.1. Стойкость к конфликтам

Первая атака на SHA-0 была опубликована в 1998 г. [CHJO1998] и показала, что конфликты могут быть найдены за 2^61 операций. В 2006 г. была продемонстрирована усовершенствованная атака [NSSYK2006] с обнаружением коллизий за 2^36 операций. Известные результаты показывают, что алгоритм SHA-0 не так устойчив к конфликтам, как предполагалось. Стойкость к конфликтам значительно ниже значения для идеальной хэш-функции (2^36 против 2^80).

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

2.2. Стойкость прообраза и второго прообраза

Опубликованные сведения об атаках на прообраз и второй прообраз для сокращённой версии SHA-0 (меньше 80 раундов) показывают что запаса безопасности SHA-0 достаточно для таких атак. В [deCARE2008] показана атака на прообраз в 49 из 80 раундов со сложностью 2^159, а в [AOSA2009] - в 52 из 80 раундов со сложностью 2^156.

2.3. HMAC-SHA-0

Существующие векторы атак на HMAC можно классифицировать как атаки с разделением, атаки с подделками и атаки с восстановлением ключей, из которых последние на сегодняшний день являются наиболее серьёзными.

Атаки на хэш-функции можно выполнять атономно, поскольку атакующий может сам генерировать неограниченное число пар «сообщение-хэш».

Атаки на HMAC должны выполняться в режиме online, поскольку для вывода ключа требуется большое число значений HMAC. Наилучшие результаты атак с частичным восстановлением ключа для HMAC-SHA-0 были опубликованы на Asiacrypt 2006 с 2^84 запросами и 2^60 расчётами SHA-0 [COYI2006].

3. Вопросы безопасности SHA-1

Далее рассматриваются атаки на стойкость SHA-1 к коллизиям, а также поиску прообраза и второго прообраза. Рассмотрены также атаки на SHA-1 при хэшировании с ключом (HMAC-SHA-1).

Следует отметить, что NIST рекомендует не применять SHA-1 для создания цифровых подписей после 31 декабря 2010 г. и указывает, что алгоритм не будет использоваться для создания цифровых подписей федеральными правительственными органами США «для защиты конфиденциальной, но незасекреченной информации» после 31 декабря 2013 г. [SP800-131].

3.1. Стойкость к конфликтам

Первая атака на SHA-1 была опубликована в начале 2005 г. [RIOS2005]. Описана теоретическая атака на SHA-1, сокращённый до 53 раундов. В следующем месяце были продемонстрированы коллизии [WLY2005] во всех 80 раундах за 2^69 операций. С тех пор было разработано много новых методов для усовершенствования атаки, представленной в [WLY2005]. Однако результатов, превосходящих опубликованные в [WLY2005], не было получено. В [Man2008/469] (электронная версия International Association for Cryptologic Research или IACR) [Man2009] заявлено, что с помощью представленного в статье метода были найдены конфликты в полном SHA-1 за 2^51 вызовов хэш-функции. Однако это заявление отсутствует в печатных материалах конференции [Man2009].

В любом случае, известные результаты исследований показывают, что стойкость SHA-1 к коллизиям ниже, чем ожидалось и значительно ниже значения для идеальной хэш-функции (2^69 против 2^80).

3.2. Стойкость прообраза и второго прообраза

Не существует известных атак на поиск прообраза или второго прообраза для полного варианта SHA-1. В [KeSch] обнаружен общий результат для всех хэш-функций Merkle-Damgaard с узким каналом (включают SHA-1) - поиск второго прообраза требует менее 2^n расчетов. При n = 160, как в случае SHA-1, для поиска второго прообраза в 60-байтовом сообщении потребуется 2^106 расчетов.

В отсутствие атак при полном числе раундов криптографы рассматривают атаки на сокращённые варианты, как способ оценки стойкости алгоритма. Атаки при незначительно сокращённом числе раундов не показывают связи с атаками на полный алгоритм. Однако лучшая атака с сокращённым числом раундов указывает определённый запас безопасности. Например, если наилучшая атака выполняется в 60 из 80 раундов, алгоритм имеет ещё 20 раундов для противодействия усовершенствованным атакам. Однако связь между числом раундов при атаке и числом раундов в алгоритме не является линейной и не даёт математического доказательства. Иными словами, атаки с сокращённым числом раундов показывают стойкость алгоритма к определённой атаке, а не близость атаки к достижению взлома. Поэтому приведённые ниже сведения об атаках с сокращённым числом раундов служат лишь для полноты.

Опубликованные атаки на прообраз и второй прообраз для сокращенных версий SHA-1 (меньше 80 раундов) показывают, что SHA-1 сохраняет запас безопасности против таких атак. В [AOSA2009] показана атака на прообраз в 48 из 80 раундов со сложностью 2^159.

3.3. HMAC-SHA-1

На сегодняшний день нет признаков распространения атак на SHA-1 применительно к HMAC-SHA-1.

4. Заключение

Стойкость SHA-1 к коллизиям оказалась меньше ожидаемой и было показано, что эта стойкость влияет на некоторые (но не все) приложения, использующие цифровые подписи. Разработчикам протоколов IETF, в которых применяются цифровые подписи, следует серьёзно отнестись к выбору алгоритма хэширования с большей по сравнению с SHA-1 стойкостью к конфликтам. И, конечно, не следует использовать SHA-0 ни в одном из протоколов IETF.

> Примечание. Разработчикам протоколов следует изучить текущее состояние дел, чтобы убедиться в достаточной безопасности выбираемых алгоритмов хэширования. На момент публикации документа наиболее часто применялся алгоритм SHA-256 [SHS]. Известные атаки на стойкость к коллизиям SHA-256 (с сокращённым числом раундов) показывают существенный запас безопасности, а более длинный дайджест повышает строгость хэширования.

Почти во всх протоколах IETF, использующих подписи, предполагается наличие инфраструктуры открытых ключей и SHA-1 по-прежнему применяется в подписях почти повсеместно. Поэтому нецелесообразно строго запрещать использование SHA-1 в алгоритмах подписи. В протоколах, разрешающих применять цифровые подписи на основе SHA-1 как опцию, следует всерьёз рассмотреть упоминание этого документа при рассмотрении вопросов безопасности.

Разработчики протоколов могут рассматривать использование SHA-1 с рандомизированным хэшированием, как указано в [SP800-107]. Отметим, что такое хэширование увеличивает размер подписи и требует от протокола передачи информации, которая сегодня не нужна. HMAC-SHA-1 остаётся безопасным и является предпочтительным алгоритмом хэширования с ключом для протоколов IETF.

5. Вопросы безопасности

Документ целиком посвящён вопросам безопасности.

6. Благодарности

Спасибо Ran Atkinson и Sheila Frankel за комментарии и предложения.

7. Нормативные документы

[AOSA2009] Aoki, K., and K. Saski, "Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1", Crypto 2009.

[deCARE2008] De Canniere, C., and C. Rechberger, "Preimages for Reduced SHA-0 and SHA-1", Crypto 2008.

[CHJO1998] Chaubad, F., and A. Joux, "Differential Collisions in SHA-0", Crypto 1998.

[COYI2006] Contini, S., and Y. Lin, "Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions", Asiacrypt 2006.

[HASH-Attack] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

[KeSch] Kelsey, J., and B. Schneier, "Second Preimages on n-Bit Hash Functions for Much Less than 2n Work", In Cramer, R., ed.: Eurocrypt 2005. Volume 3494 of Lecture Notes in Computer Science, Springer (2005) 474-490.

[Man2008/469] Manuell, S., "Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1", http://eprint.iacr.org/2008/469.pdf.

[Man2009] Manuell, S., "Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1", International Workshop on Coding and Cryptography, 2009, Norway.

[NSSYK2006] Naito, Y., Sasaki, Y., Shimoyama, T., Yajima, J., Kunihiro, N., and K. Ohta, "Improved Collision Search for SHA-0", Asiacrypt 2006.

[RIOS2005] Rijmen, V., and E. Oswald, "Update on SHA-1", CT-RSA 2005, Lecture Notes in Computer Science, vol. 3376, pp. 58-71.

[SHS] National Institute of Standards and Technology (NIST), FIPS Publication 180-3: Secure Hash Standard, October 2008.

[SP800-57] National Institute of Standards and Technology (NIST), Special Publication 800-57: Recommendation for Key Management - Part 1 (Revised), March 2007.

[SP800-107] National Institute of Standards and Technology (NIST), Special Publication 800-107: Recommendation for Applications using Approved Hash Algorithms, February 2009.

[SP800-131] National Institute of Standards and Technology (NIST), Special Publication 800-131A: Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes, January 2011.

[WLY2005] Wang, X., Yin, Y., and H. Yu., "Finding Collisions in the Full SHA-1", Crypto 2005.

Адреса авторов

Tim Polk
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA
EMail: tim.polk@nist.gov

Lily Chen
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA
EMail: lily.chen@nist.gov

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA
EMail: turners@ieca.com

Paul Hoffman
VPN Consortium
EMail: paul.hoffman@vpnc.org

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru