Network Working Group M. Leech
Request for Comments: 3562 Nortel Networks
Category:Informational July 2003

Управление ключами при использовании опции TCP MD5 Signature

Key Management Considerations for
the TCP MD5 Signature Option

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задает каких-либо стандартов Internet. Допускается свободное распространение документа.

Авторские права

Тезисы

Опция TCP MD5 Signature (RFC 2385), используемая преимущественно протоколом BGP, достаточно широко реализована в критически важных областях инфраструктуры Internet. Обеспечиваемый этой опцией уровень защиты определяется качеством ключей, используемых для расчета сигнатур MD5. В данном документе рассматриваются требования безопасности для таких ключей.

1. Введение

Безопасность различных криптографических функций зависит от функции, как таковой, к различного рода атакам, а также (возможно в большей степени) от используемого функциями ключевого материала. Хотя теоретически атаки на простую конструкцию MAC, используемую в RFC 2385, вполне возможны [MDXMAC], число пар текст-MAC, требуемых для подделки, делает атаки против RFC 2385 на основе предсказания ключей значительно более вероятными.

Мы покажем количественный метод определения требований безопасности к ключам, используемым с [RFC2385].

- Размер ключа **следует** поддерживать в диапазоне от 12 до 24 байтов, поскольку дополнительное увеличение размеров ключа практически не увеличивает сложность его вычисления.
- Совместное использование ключей **следует** ограничивать, чтобы один ключ не использовался множеством партнерских пар BGP.
- Кличи **следует** менять по крайней мере каждые 90 дней.

1.1. Уровни требований

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

2. Оценка производительности

Наиболее свежим исследованием производительности MD5, найденным автором этого документа, была работа J. Touch из ISI. Результаты этого исследования были опубликованы в [RFC1810]. На момент проведения этого исследования наилучшая **программная** реализация MD5 обеспечивала производительность 87 Мбит/с. Предполагается, что к этой оценке применим закон Мура. Экстраполяция этого значения на время подготовки данного документа (2002 год) дает значение около 2,1 Гбит/с.

Для упрощения мы будем предполагать, что при попытках подбора ключа атакующий будет использовать только короткие пакеты. Возможным типом таких пакетов будут отклики ACK, не содержащие данных. Это ведет к необходимости расчета MD5 примерно для 40 байтов данных вместе с некоторым разумным максимальным числом байтов ключа. MD5 дополняет входные данные для выравнивания по границе 512 битов (64 байта)[1]. Это означает, что минимальный “блок” MD5 имеет размер 64 байта и с учетом экстраполированной для 2002 г. производительности 2,1 Гбит/с мы получим для однопроцессороной системы производительность MD5 около $4.1*e^6$ одноблоковых операций MD5 в секунду.

Эти значения основаны на предположении, что занимающийся подбором ключей, ограничен ресурсами одного процессора. На практике распределенные криптографические атаки с подбором ключей в недавнем прошлом достаточно часто завершались успехом.

Может оказаться поучительным анализ недавних эпидемий «червей» в Internet в целях определения максимального числа хостов, которые могут быть тайком вовлечены в организацию атаки MD5 путем подбора ключей. В отчете CAIDA [CAIDA2001] указывается, что червь Code Red смог заразить более 350 000 хостов Internet за первые 14 часов своей деятельности. Представляется разумным предположение, что червь, содержащий незаметный механизм для участия в

[1] На практике все происходит несколько более сложно, но это не имеет существенного значения для нашего анализа.

атаке с подбором ключей (возможно использующий периоды бездействия CPU на зараженном хосте) будет по крайней мере столь же эффективным, как Code Red. Если предположить, что такой червь будет максимально скрытным, в установившемся состоянии размер его популляции может достигнуть миллиона хостов или более того. Это позволит увеличить производительность операций подбора (на однопроцессорной системе около $4.1*e^6$ операций в секунду) до $1.0e^{11}$ - $1.0e^{13}$ операций MD5 в секунду.

В 1997 г. John Gilmore и Electronic Frontier Foundation [EFF98] разработали машину специального назначения для проведения исследований стоимостью приблизительно $250000. Эта машина была способна организовать атаку с подбором ключей против алгоритма DES и рассчитывала один ключ в неделю. На основе закона Мура можно предположить, что за те же деньги сегодня можно создать машину, способную работать примерно в 8 раз быстрее. Разумно предположить, что подобное оборудование может использоваться для подбора ключей MD5 и при таком же размере ключей, как в DES, оно будет незначительно уступать в производительности (производительность аппаратной реализации MD5 в 2-3 раза уступает производительности DES).

3. Время жизни ключей

Опыт практического использования RFC 2385 говорит, что ключи, используемые с этой опцией могут иметь время жизни порядка нескольких месяцев. Представляет разумным выбирать минимальный размер ключей, который будет гарантировать, что продолжительность подбора ключа будет в несколько раз больше интервала замены ключей с учетом наилучшей (с точки зрения атакующего) производительности подбора ключей.

Ключи, используемые с RFC 2385, предназначены только для аутентификации и не используются в целях обеспечения конфиденциальности. Следовательно, возможность подобрать ключ с использованием собранных ранее данных (трафик, собранный до смены ключей) не рассматривается как угроза.

3. Энтропия ключей

Если мы предположим, что интервал замены ключей составляет 90 дней а разумное значение верхней границы производительности программных атак составляет $1.0*e^{13}$ операций MD5 в секунду, минимальная допустимая энтропия ключей составит приблизительно 68 битов. Разумно округлить это значение до 80 битов (10 байтов). Если предполагается возможность аппаратных атак с использованием оборудования типа EFF но с бюджетом небольшой страны, минимальный размер ключа увеличится примерно до 83 битов или 11 байтов. Поскольку число 11 достаточно неудобно, будет разумным округлить размер ключа до 12 байтов.

Для достижения достаточно большой энтропии с ключами на основе английского языка следует помнить, что энтропия этого языка составляет приблизительно 1,3 бита/символ. Другие языки человеческого общения имеют близки значения энтропии. Это означает, что ключи, полученные из языка человеческого общения, должны иметь размер приблизительно 61 байт для созданий энтропии в 80 битов и 73 байта для энтропии в 96 битов.

В документе [RFC1750] описываются более подходящие методы получения высококачественных случайных ключей размером 96 и более битов.

Ранее было отмечено, что атакующий скорей всего будет пытаться использовать для организации атаки короткие пакеты, поскольку в этом случае повышается производительность подбора ключей. Было также отмечено, что операции MD5 в таких случаях будут выполняться для блоков размером 64 байта. Принимая во внимание, что пакет будет включать 40 байтов заголовков IP и TCP, оставшиеся 24 байта блока MD5 могут использоваться в качестве ключевого материала без увеличения нагрузки на процессор маршрутизатора, но со значительным ростом нагрузки на атакующего. Хотя такой подход будет увеличивать нагрузку на CPU для случая обычных коротких пакетов BGP (поскольку это будет заставлять расчет MD5 переходить во второй блок MD5) в настоящее время это не представляется существенным увеличением нагрузки на машину маршрутизации BGP.

На практике наиболее разумно выбрать наибольший возможный ключ, размер которого меньше 25 байтов, но не менее 12 байтов.

Некоторые реализации ограничивают набор ключей строками символов ASCII (подобно простым паролям) размером 8 байтов или меньше. Это создает реальный риск подбора ключа в результате описанных выше атак. Наихудшим вариантом будет использование ключа/пароля из символов ASCII, содержащего слово из языка человеческого общения или псевдослово. Такие ключи/пароли содержат не более 12 битов энтропии. В таких случаях атаки с использованием словаря могут привести к сокращению времени подбора во много раз. Таким реализациям **следует** позволять пользователям напрямую вводить двоичные ключи с использованием командного интерфейса. Одним из вариантов может служить соглашение о том, что ключи ASCII, начинающиеся с префикса "0x", интерпретируются как строки байтов, представленных в шестнадцатеричной записи. В идеальном случае такие строки следует создавать на основе случайных данных, как описано в [RFC1750]. Реализациям **не следует** без необходимости ограничивать размер ключей и **следует** разрешать ключи размером по крайней мере 16 байтов, чтобы противостоять неизбежным по закону Мура угрозам.

4. Практика управления ключами

В современной практике ключи TCP MD5 Signature [RFC2385] могут совместно использоваться большим числом систем. Здравый смысл и опыт в сфере криптографии и защиты говорят, что такое совместное использование повышает вероятность случайного или преднамеренного раскрытия ключей. Чем более часто происходят манипуляции с такими ключами, тем выше вероятность случайного раскрытия ключей посторонним лицам.

Поскольку любой обладатель ключа может создавать обманные пакеты, как будто они исходят от любого другого владельца ключа, наиболее подходящим вариантом защиты является ограничение использования ключей только парой взаимодействующих сторон. В современных реализациях это может вызвать затруднения, однако такой подход обеспечивает наибольшую безопасность при достаточно продолжительном сроке жизни ключей. Сокращение срока жизни ключей в системах с их совместным использованием может частично решить проблему за счет сокращения временных рамок, в которых может действовать нелегитимный владелец ключа.

Ключи являются критически важной компонентой обеспечения безопасности и поэтому обращаться с ними нужно осторожно. При электронной транспортировке ключей (включая настройку конфигурации элементов сети типа

маршрутизаторов) **должны** использоваться безопасные методы работы с ключами. Для защиты передаваемых ключей по возможности **следует** использовать протоколы типа S/MIME [RFC2633], TLS [RFC2246], Secure Shell (SSH).

5. Вопросы безопасности

Этот документ целиком посвящен вопросам безопасности ключей, используемых механизмом RFC 2385.

Документ не показывает новых угроз безопасности.

6. Благодарности

Steve Bellovin, Ran Atkinson и Randy Bush внесли значимые комментарии при подготовке этого документа.

7. Литература

[RFC1771] Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771[1], March 1995.

[RFC1810] Touch, J., "Report on MD5 Performance", RFC 1810, June 1995.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385[2], August 1998.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119[2], March 1997.

[MDXMAC] Van Oorschot, P. and B. Preneel, "MDx-MAC and Building Fast MACs from Hash Functions". Proceedings Crypto '95, Springer-Verlag LNCS, August 1995.

[RFC1750] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[EFF98] "Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design". Electronic Frontier Foundation, 1998.

[RFC2633] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[CAIDA2001] "CAIDA Analysis of Code Red" http://www.caida.org/analysis/security/code-red/

8. Адрес автора

Marcus D. Leech

Nortel Networks

P.O. Box 3511, Station C

Ottawa, ON

Canada, K1Y 4H7

Phone: +1 613-763-9145

EMail: mleech@nortelnetworks.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

9. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечивается Internet Society.

[1]Этот документ устарел и заменен RFC 4271. Перевод имеется на сайте http://www.protocols.ru. *Прим. перев.*
[2]Перевод этого документа имеется на сайте http://www.protocols.ru. *Прим. перев.*