Network Working Group
Request for Comments: 4278
Category: Informational

S. Bellovin
AT&T Labs Research
A. Zinin
Alcatel

January 2006

Отход от стандартных требования для опции TCP MD5 Signature (RFC 2385) и спецификации BGP-4

Standards Maturity Variance Regarding the TCP MD5 Signature Option

(RFC 2385) and the BGP-4 Specification

Статус документа

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

Тезисы

Процедура стандартизации IETF[1] требует, чтобы все ссылки на нормативные документы (normative reference) имели такой же или более высокий уровень стандартизации, как и ссылающийся на них документ. Параграф 9.1 RFC 2026 позволяет IESG предоставлять возможность отхода от стандартной практики IETF. Данный документ объясняет, как IESG делает это в отношении пересмотренной версии спецификации BGP-4, которая содержит ссылку на нормативный документ RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option[2]. Документ RFC 2385 продолжает сохранять статус Proposed Standard[3].

1. Введение

Процедура стандартизации IETF [RFC2026] требует, чтобы все ссылки на нормативные документы (normative reference) имели такой же или более высокий уровень стандартизации, как и ссылающийся на них документ. Параграф 9.1 RFC 2026 позволяет IESG предоставлять возможность отхода от стандартной практики IETF. В соответствии с такой возможностью рассматривается вопрос публикации обновленной спецификации BGP-4 [RFC4271] как предварительного стандарта (Draft Standard), несмотря на то, что в ней имеется ссылка в разделе “Нормативные документы” на [RFC2385] Защита сеансов BGP и использованием сигнатур MD5. Документ RFC 2385 продолжает сохранять статус Proposed Standard (отметим, что несмотря на наличие в названии документа [RFC2385] слова «сигнатура», описанная в нем технология более известна как MAC[4] и ее не следует путать с технологиями цифровых подписей).

Широко реализованный алгоритм [RFC2385] для протокола BGP-4 представляет собой только механизм защиты на транспортном уровне. Другие возможные механизмы типа IPsec [RFC2401] и TLS [RFC2246] используются для этой задачи весьма редко, если не сказать никогда. С учетом долгосрочных требований по обеспечению защиты протокола невозможно продвигать BGP-4 без обязательного механизма защиты.

Конфликт уровней завершенности стандартизации разных спецификаций обычно разрешается путем продвижения спецификации, на которую имеется нормативная ссылка до уровня завершенности ссылающегося документа. Однако в рассматриваемом случае IESG полагает, что алгоритм [RFC2385], вполне подходящий для BGP, не является достаточно надежным для задач общего назначения и его не следует стандартизовать. В этой ситуации IESG полагает, что следует использовать изменение процедуры, чтобы позволить публикацию обновленной спецификации BGP-4 со статусом Draft Standard.

В следующих параграфах документа приводится детальное обоснование необходимости изменения процедуры.

2. Требования к предварительным стандартам

Требования к уровням Proposed Standard (предложенный стандарт) и Draft Standard (предварительный стандарт) изложены в [RFC2026]. Для Proposed Standards [RFC2026] указывает:

> «Разработчикам следует трактовать уровень Proposed Standards как незавершенную спецификацию. Желательно реализовать ее для приобретения опыта и проверки, тестирования и прояснения спецификации. Однако, поскольку спецификация уровня Proposed Standards может быть изменена в результате обнаружения проблем или появления более эффективного решения, развертывание реализаций таких стандартов в чувствительной к повреждениям среде не рекомендуется.»

Иными словами, считается разумным предполагать наличие недоработок в спецификациях со статусом Proposed Standards.

---

[1] IETF Standards Process.
[2] Защита сеансов BGP и использованием сигнатур MD5. Перевод документа имеется на сайте www.protocols.ru. *Прим. перев.*
[3] Предложенный стандарт.
[4] Message Authentication Code – код аутентификации сообщения.

Требования для Draft Standards более жестки:

> Предварительный стандарт (Draft Standard) должен быть понятным и для него должна быть достоверная информация о достаточном уровне стабильности, а также должна присутствовать база для разработки реализаций.

Иными словами, документы, которые имеют известные недостатки, не следует продвигать в качестве Draft Standard.

3. Опция TCP MD5 Signature

[RFC2385], несмотря на публикация в 1998 г., описывает существенно более старый алгоритм MAC (Message Authentication Code). Алгоритм основан на методе keyed hash function, использующем MD5 [RFC1321] в качестве функции хэширования. На момент разработки оригинального кода этот метод представлялся подходящим, особенно для тех случаев, когда ключ добавлялся в конце (append), а не в начале (prepend) защищаемых данных. Но криптографические хэш-функции не были предназначены для использования в качестве MAC и результаты последующего криптоанализа показали, что конструкция не столь сильна, как представлялось поначалу [PV1, PV2]. Хуже того, в используемой методом функции MD5, были найдены существенные недостатки [Dobbertin, Wang]. С учетом этого было принято решение IETF об адаптации алгоритма HMAC (Hashed Message Authentication Code) [RFC2104] с подтвержденными защитными свойствами в качестве стандартного MAC.

Кроме того, [RFC2385] не включает никакого механизма управления ключами. Общепринятой практикой является использование пароля в качестве открытого ключа (shared secret) для пары сайтов, но это не является хорошей идеей [RFC3562].

Другая проблема указана непосредственно в [RFC2385] и связана отсутствием кода типа или номера версии, а также с неспособностью использующих эту схему систем воспринимать некоторые пакеты TCP reset.

Несмотря на широкое использование [RFC2385] в системах BGP, IESG считает, что этот алгоритм не подходит для использования в ином контексте. [RFC2385] не удовлетворяет требованиям к уровню Draft Standard.

4. Картина использования RFC 2385

С учетом сказанного выше возникает резонный вопрос, почему [RFC2385] продолжает использоваться для BGP. Ответом на этот вопрос является практика развертывания, присущая исключительно BGP.

Соединения BGP обычно являются очень короткими. На практике протяженность внешних соединений BGP обычно составляет 1 интервал[1] (hop). Хотя внутренние соединения BGP обычно бывают более длинными, они, как правило, включают в себя только маршрутизаторы (а не компьютеры общего назначения, которые более подходят атакующим для использования в качестве средств перехвата TCP [Joncheray]).

Кроме того, партнерские отношения BGP обычно бывают долговременными и стабильными. В отличии от них многие другие задачи защиты являются более динамичными.

Сказанное выше не отрицает возможности организации атак (если бы атаки не были возможны, не возникало бы задачи обеспечения защиты). Атакующие могут перехватывать соединения на уровнях 1 и 2 или использовать (в некоторых случаях) подставные пакеты[2] ARP[3] в точках обмена на основе технологий Ethernet. Тем не менее, в целом протокол BGP используется в средах, которые менее подвержены этому типу атак.

Существует другой тип атак, по отношению к которым протокол BGP весьма уязвим – фиктивные анонсы маршрутов из автономных систем, находящихся на расстоянии более одного интервала. Однако ни [RFC2385], ни другие механизмы защиты на транспортном уровне, не могут блокировать такие атаки. Для решения этой проблемы требуются иные схемы типа S-BGP [Kent].

5. Протокол LDP

Протокол LDP[4] [RFC3036] также использует [RFC2385]. Практика развертывания LDP очень похожа на среду работы BGP - соединения LDP обычно существуют внутри одной автономной системы и чаще всего представляют собой прямые соединения между маршрутизаторами. Это делает среду LDP очень похожей (с точки зрения угроз) на среду BGP. Учитывая это обстоятельство и достаточно широкое использование LDP в сетях сервис-провайдеров мы не запрещаем использование [RFC2385] с протоколом LDP.

6. Вопросы безопасности

IESG полагает, что описанная здесь процедура не будет оказывать негативного влияния на безопасность Internet.

7. Заключение

Проведенный выше анализ убеждает IESG в том, что в данном случае допустимо отклонение от предусмотренных требований. [RFC2385] явно не подходит для статуса Draft Standard. Другие существующие механизмы (например, IPsec) будут делать эту работу лучше. Однако имеющийся опыт эксплуатации в сетях сервис-провайдеров (и, в частности, использование стандартных ключей с большим сроком жизни, вопреки [RFC3562]) говорит, что преимущества от использования таких схем в описанной ситуации достаточно малы и не покроют издержек, связанных с переходом. Мы предпочитаем дождаться появления механизма защиты, приспособленного для основных угроз в среде BGP.

8. Литература

[Dobbertin] H. Dobbertin, "The Status of MD5 After a Recent Attack"[5], RSA Labs' CryptoBytes, Vol. 2 No. 2, Summer 1996.

---

[1] Т. е., между маршрутизаторами-партнерами BGP обычно нет других маршрутизаторов. *Прим. перев.*

[2] ARP spoofing

[3] Address Resolution Protocol – протокол преобразования адресов.

[4] Label Distribution Protocol – протокол распределения меток.

[5] Эта статья доступна на сайте http://www.rsa.com/rsalabs/pubs/cryptobytes.html. *Прим. перев.*

[Joncheray] Joncheray, L. "A Simple Active Attack Against TCP." Proceedings of the Fifth Usenix Unix Security Symposium, 1995.

[Kent] Kent, S., C. Lynn, and K. Seo. "Secure Border Gateway Protocol (Secure-BGP)." IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, April, 2000, pp. 582-592.

[RFC3562] Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.

[PV1] B. Preneel and P. van Oorschot, "MD-x MAC and building fast MACs from hash functions," Advances in Cryptology --- Crypto 95 Proceedings, Lecture Notes in Computer Science Vol. 963, D. Coppersmith, ed., Springer-Verlag, 1995.

[PV2] B. Preneel and P. van Oorschot, "On the security of two MAC algorithms," Advances in Cryptology --- Eurocrypt 96 Proceedings, Lecture Notes in Computer Science, U. Maurer, ed., Springer-Verlag, 1996.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm ", RFC 1321, April 1992.

[RFC2026] Bradner, S., "The Internet Standards Process – Revision 3", BCP 9, RFC 2026, October 1996.

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

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

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

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401[1], November 1998.

[RFC3036] Andersson, L., Doolan, P., Feldman, N., Fredette, A., and B. Thomas, "LDP Specification", RFC 3036, January 2001.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, Eds., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[Wang] Wang, X. and H. Yu, "How to Break MD5 and Other Hash Functions." Proceedings of Eurocrypt '05, 2005.

Адреса авторов

Steven M. Bellovin

Department of Computer Science

Columbia University

1214 Amsterdam Avenue, M.C. 0401

New York, NY 10027-7003

Phone: +1 212-939-7149

EMail: bellovin@acm.org

Alex Zinin

Alcatel

701 E Middlefield Rd

Mountain View, CA 94043

EMail: zinin@psg.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

Полное заявление авторских прав

Интеллектуальная собственность

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license

[1]Этот документ устарел и земенен RFC 4301. *Прим. перев.*

under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено IETF Administrative Support Activity (IASA).