Network Working Group
Request for Comments: 4278
Category: Informational

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

January 2006

Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

The IETF Standards Process requires that all normative references for a document be at the same or higher level of standardization. RFC 2026 section 9.1 allows the IESG to grant a variance to the standard practices of the IETF. This document explains why the IESG is considering doing so for the revised version of the BGP-4 specification, which refers normatively to RFC 2385, "Protection of BGP Sessions via the TCP MD5 Signature Option". RFC 2385 will remain at the Proposed Standard level.

1. Introduction

The IETF Standards Process [RFC2026] requires that all normative references for a document be at the same or higher level of standardization. RFC 2026 section 9.1 allows the IESG to grant a variance to the standard practices of the IETF. Pursuant to that, it is considering publishing the updated BGP-4 specification [RFC4271] as Draft Standard, despite the normative reference to [RFC2385], "Protection of BGP Sessions via the TCP MD5 Signature Option". RFC 2385 will remain a Proposed Standard. (Note that although the title of [RFC2385] includes the word "signature", the technology described in it is commonly known as a Message Authentication Code or MAC, and should not be confused with digital signature technologies.)

[RFC2385], which is widely implemented, is the only transmission security mechanism defined for BGP-4. Other possible mechanisms, such as IPsec [RFC2401] and TLS [RFC2246], are rarely, if ever, used

for this purpose. Given the long-standing requirement for security features in protocols, it is not possible to advance BGP-4 without a mandated security mechanism.

The conflict of maturity levels between specifications would normally be resolved by advancing the specification being referred to along the standards track, to the level of maturity that the referring specification needs to achieve. However, in the particular case considered here, the IESG believes that [RFC2385], though adequate for BGP deployments at this moment, is not strong enough for general use, and thus should not be progressed along the standards track. In this situation, the IESG believes that variance procedure should be used to allow the updated BGP-4 specification to be published as Draft Standard.

The following sections of the document give detailed explanations of the statements above.

2. Draft Standard Requirements

The requirements for Proposed Standards and Draft Standards are given in [RFC2026]. For Proposed Standards, [RFC2026] warns that:

> Implementors should treat Proposed Standards as immature specifications. It is desirable to implement them in order to gain experience and to validate, test, and clarify the specification. However, since the content of Proposed Standards may be changed if problems are found or better solutions are identified, deploying implementations of such standards into a disruption-sensitive environment is not recommended.

In other words, it is considered reasonable for flaws to be discovered in Proposed Standards.

The requirements for Draft Standards are higher:

> A Draft Standard must be well-understood and known to be quite stable, both in its semantics and as a basis for developing an implementation.

In other words, any document that has known deficiencies should not be promoted to Draft Standard.

3. The TCP MD5 Signature Option

[RFC2385], despite its 1998 publication date, describes a Message Authentication Code (MAC) that is considerably older. It utilizes a technique known as a "keyed hash function", using MD5 [RFC1321] as the hash function. When the original code was developed, this was believed to be a reasonable technique, especially if the key was appended (rather than prepended) to the data being protected. But cryptographic hash functions were never intended for use as MACs, and later cryptanalytic results showed that the construct was not as strong as originally believed [PV1, PV2]. Worse yet, the underlying hash function, MD5, has shown signs of weakness [Dobbertin, Wang]. Accordingly, the IETF community has adopted Hashed Message Authentication Code (HMAC) [RFC2104], a scheme with provable security properties, as its standard MAC.

Beyond that, [RFC2385] does not include any sort of key management technique. Common practice is to use a password as a shared secret between pairs of sites, but this is not a good idea [RFC3562].

Other problems are documented in [RFC2385] itself, including the lack of a type code or version number, and the inability of systems using this scheme to accept certain TCP resets.

Despite the widespread deployment of [RFC2385] in BGP deployments, the IESG has thus concluded that it is not appropriate for use in other contexts. [RFC2385] is not suitable for advancement to Draft Standard.

4. Usage Patterns for RFC 2385

Given the above analysis, it is reasonable to ask why [RFC2385] is still used for BGP. The answer lies in the deployment patterns peculiar to BGP.

BGP connections inherently tend to travel over short paths. Indeed, most external BGP links are one hop. Although internal BGP sessions are usually multi-hop, the links involved are generally inhabited only by routers rather than general-purpose computers; general-purpose computers are easier for attackers to use as TCP hijacking tools [Joncheray].

Also, BGP peering associations tend to be long-lived and static. By contrast, many other security situations are more dynamic.

This is not to say that such attacks cannot happen. (If they couldn’t happen at all, there would be no point to any security measures.) Attackers could divert links at layers 1 or 2, or they

could (in some situations) use Address Resolution Protocol (ARP) spoofing at Ethernet-based exchange points. Still, on balance, BGP is employed in an environment that is less susceptible to this sort of attack.

There is another class of attack against which BGP is extremely vulnerable: false route advertisements from more than one autonomous system (AS) hop away. However, neither [RFC2385] nor any other transmission security mechanism can block such attacks. Rather, a scheme such as S-BGP [Kent] would be needed.

5. LDP

The Label Distribution Protocol (LDP) [RFC3036] also uses [RFC2385]. Deployment practices for LDP are very similar to those of BGP: LDP connections are usually confined within a single autonomous system and most frequently span a single link between two routers. This makes the LDP threat environment very similar to BGP's. Given this, and a considerable installed base of LDP in service provider networks, we are not deprecating [RFC2385] for use with LDP.

6. Security Considerations

The IESG believes that the variance described here will not adversely affect the security of the Internet.

7. Conclusions

Given the above analysis, the IESG is persuaded that waiving the prerequisite requirement is the appropriate thing to do. [RFC2385] is clearly not suitable for Draft Standard. Other existing mechanisms, such as IPsec, would do its job better. However, given the current operational practices in service provider networks at the moment -- and in particular the common use of long-lived standard keys, [RFC3562] notwithstanding -- the marginal benefit of such schemes in this situation would be low, and not worth the transition effort. We would prefer to wait for a security mechanism tailored to the major threat environment for BGP.

8. Informative References

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

[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, 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.

Authors' Addresses

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

Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

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 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.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).