Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 2, 2011

A. Kukec
University of Zagreb
S. Krishnan
Ericsson
S. Jiang
Huawei Technologies Co., Ltd
March 7, 2011

SEND Hash Threat Analysis
draft-ietf-csi-hash-threat-12

Abstract

This document analyzes the use of hashes in Secure Neighbor Discovery (SEND), the possible threats to these hashes and the impact of recent attacks on hash functions used by SEND. The SEND specification currently uses the SHA-1 hash algorithm [SHA1] and PKIX certificates and does not provide support for hash algorithm agility. This document provides an analysis of possible threats to the hash algorithms used in SEND.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 2, 2011.

Copyright Notice

Table of Contents

1. Introduction 3
2. Impact of collision attacks on SEND 3
2.1. Attacks against CGAs used in SEND 3
2.2. Attacks against PKIX certificates in Authorization Delegation Discovery process 3
2.3. Attacks against the Digital Signature in the SEND RSA Signature option 4
2.4. Attacks against the Key Hash field of the SEND RSA Signature option 4
3. Conclusion 4
4. IANA Considerations 5
5. Security Considerations 5
6. Acknowledgements 5
7. References 5
7.1. Normative References 5
7.2. Informative References 5
Authors' Addresses 6

1. Introduction

SEND [RFC3971] uses the SHA-1 hash algorithm to generate the contents of the Key Hash field and the Digital Signature field of the RSA Signature option. It also indirectly uses a hash algorithm (SHA-1, MD5, etc.) in the PKIX certificates [RFC5280] used for router authorization in the Authorization Delegation Discovery(ADD) process. Recently there have been demonstrated attacks against the collision free property of such hash functions [SHA1-COLL], and attacks on the PKIX X.509 certificates that use the MD5 hash algorithm [X509-COLL]. The document analyzes the impacts of these attacks on SEND and it recommends mechanisms to make SEND resistant to such attacks.

2. Impact of collision attacks on SEND

[RFC4270] performed a study to assess the threat of the aforementioned attacks on the use of cryptographic hashes in Internet protocols. This document analyzes the hash usage in SEND following the approach recommended by [RFC4270] and [NEW-HASHES].

The following sections discuss the various aspects of hash usage in SEND and determine whether they are affected by the attacks on the underlying hash functions.

2.1. Attacks against CGAs used in SEND

Cryptographically Generated Addresses (CGAs) are defined in [RFC3972] and are used to securely associate a cryptographic public key with an IPv6 address in the SEND protocol. Impacts of collision attacks on current uses of CGAs are analyzed in [RFC4982]. The basic idea behind collision attacks, as described in Section 4 of [RFC4270], is on the non-repudiation feature of hash algorithms. However, CGAs do not provide non-repudiation features. Therefore, as [RFC4982] points out CGA based protocols, including SEND, are not affected by collision attacks on hash functions. If pre-image attacks were to

become feasible, an attacker can find new CGA Parameters that can generate the same CGA as the victim. This class of attacks could be potentially dangerous since the security of SEND messages relies on the strength of the CGA.

2.2. Attacks against PKIX certificates in Authorization Delegation Discovery process

To protect Router Discovery, SEND requires that routers be authorized to act as routers. Routers are authorized by provisioning them with certificates from a trust anchor, and the hosts are configured with the trust anchor(s) used to authorize routers. Researchers

demonstrated attacks against PKIX certificates with MD5 signatures in 2005 [NEW-HASHES], in 2007 [X509-COLL] [STEV2007], and in 2009 [SSALMOdeW2009] [SLdeW2009]. An attacker can take advantage of these vulnerabilities to obtain an certificate with a different identity and use the certificate to impersonate a router. For this attack to succeed the attacker needs to predict the content of all fields (some of them are human-readable) appearing before the public key including the serial number and validity periods. Even though a relying party cannot verify the content of these fields, the CA can identify the forged certificate, if necessary.

2.3. Attacks against the Digital Signature in the SEND RSA Signature option

The digital signature in the RSA Signature option is produced by signing, with the sender's private key, the SHA-1 hash over certain fields in the Neighbor Discovery message as described in Section 5.2 of [RFC3971]. It is possible for an attacker to come up with two different Neighbor Discovery messages m and m' that result in the same value in the Digital Signature field. Since the structure of the Neighbor Discovery messages is well defined, it is not practical to use this vulnerability in real world attacks.

2.4. Attacks against the Key Hash field of the SEND RSA Signature option

The SEND RSA signature option described in Section 5.2 of [RFC3971] defines a Key Hash field. This field contains a SHA-1 hash of the public key that was used to generate the CGA. To use a collision

attack on this field, the attacker needs to come up with another public key (k') that produces the same hash as the real key (k). But the real key (k) is already authorized through a parallel mechanism (either CGAs or router certificates). Hence collision attacks are not possible on the Key Hash field. Pre-image attacks on the Key Hash field are not useful for the same reason (any other key that hashes into the same Key Hash value will be detected due to a mismatch with the CGA or the router certificate).

3. Conclusion

Current attacks on hash functions do not constitute any practical threat to the digital signatures used in SEND (both in the RSA signature option and in the X.509 certificates). Attacks on CGAs, as described in [RFC4982], will compromise the security of SEND and they need to be addressed by encoding the hash algorithm information into the CGA as specified in [RFC4982].

4. IANA Considerations

5. Security Considerations

This document analyzes the impact that the attacks against hash functions hash attacks have on SEND. It concludes that the only practical attack on SEND stems from a successful attack on an underlying CGA. It does not add any new vulnerabilities to SEND.

6. Acknowledgements

The authors would like to thank Lars Eggert, Pete McCann, Julien Laganier, Jari Arkko, Paul Hoffman, Pasi Eronen, Adrian Farrel, Dan Romascanu, Tim Pol, Richard Woundy, Marcelo Bagnulo and Barry Leiba for reviewing earlier versions of this document and providing comments to make it better.

7. References

7.1. Normative References

[NEW-HASHES] Bellovin, S. and E. Rescorla, "Deploying a New Hash Algorithm", November 2005.

[RFC4270] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

[RFC4982] Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, July 2007.

7.2. Informative References

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[SHA1] NIST, FIBS PUB 180-1, "Secure Hash Standard", April 1995.

[SHA1-COLL] Wang, X., Yin, L., and H. Yu, "Finding Collisions in the Full SHA-1. CRYPTO 2005: 17-36", 2005.

[SLdeW2009] Stevens, M., Lenstra, A., de Weger, B., "Chosen-prefix Collisions for MD5 and Applications, Journal of Cryptology, 2009.", 2009, <http://deweger.xs4all.nl/papers/%5B42%5DStLedW-MD5-JCryp%5B2009%5D.pdf>.

[SSALMOdeW2009] Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D., and B. de Weger., "Short chosen-

prefix collisions for MD5 and the creation of a rogue CA certificate, Crypto 2009", 2009.

[STEV2007]
Stevens, M., "On Collisions for MD5", <http://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf>.

[X509-COLL]
Stevens, M., Lenstra, A., and B. Weger, "Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities. EUROCRYPT 2007: 1-22", 2007.

Authors' Addresses

Ana Kukec
University of Zagreb
Unska 3
Zagreb
Croatia

Email: ana.kukec@fer.hr

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Email: suresh.krishnan@ericsson.com

Sheng Jiang
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xinxi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing
P.R. China

Email: jiangsheng@huawei.com