Network Working Group
Internet-Draft
Expires: December 6, 2008

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

June 4, 2008

SeND Hash Threat Analysis
draft-kukec-csi-hash-threat-00

Status of this Memo

Abstract

This document analysis the use of hashes in SeND, possible threats and the impact of recent attacks on hash functions used by SeND. Current SeND specification [rfc3971] uses SHA-1 [sha-1] hash algorithm and PKIX certificates [rfc3280] and does not provide support for the hash algorithm agility. Based on previous analysis, this document suggests multiple hash support that should be included in the SeND update specification.

Table of Contents

1. Introduction

The most common uses of hash functions are non-repudiable digital signatures on messages and digital signatures on certificates. Both are affected by recent collision attacks and both are used in SeND [rfc4270]. SeND uses SHA-1 hash algorithm to produce contents of the RSA Signature option in ND message (Digital Signature field and Key Hash field). PKIX certificates are used for the router authorization in Authorization Delegation Discovery (ADD) process. Hash functions are also used in the statless autoconfiguration process that is based on CGAs.

Theoretically, all mentioned uses of hash functions are affected by recent collision attacks. According to our analysis in this document, none of these attacks are currently doable. But we have to take into account that future attacks will be improved and provide a support for multiple hash algorithms.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [rfc2119].

3. Impact of collision attacks on SeND

"Hash algorithms are used by cryptographers in a variety of security protocols, for a variety of purposes, at all levels of the Internet protocol stack. They are used because they have two security properties: to be one way and collision free." "The recent attacks have demonstrated that one of those security properties is not true."[rfc4270] Following the approach recommended by [rfc4270] and [new-hashes], we will analyze the impact of these attacks on SeND case by case in this section. Through our analysis, whether we should support hash agility on SeND is also discussed.

Up to date, all demonstrated attacks are attacks against a collision-free property. Attacks against the one-way property are not yet feasible [rfc4270].

3.1. Attacks against CGAs in stateless autoconfiguration

Hash functions are used in the stateless autoconfiguration process that is based on CGAs. Impacts of collision attacks on current uses of CGAs are analyzed in the update of CGA specification [rfc4982], which also enables CGAs to support hash agility. CGAs provide proof-

of-ownership of the private key corresponding to the public key used to generate CGA, and they don't deal with the non-repudiation feature, while collision attacks are mainly about affecting non-repudiation feature. While SeND is CGA based protocol, we are sure that the node that signes the message is the same as the node that creates the message and associated hash. So, as [rfc4982] points out CGA based protocols, including SeND, are not affected by the recent collision attacks.

3.2. Attacks against PKIX certificates in ADD process

The second use of hash functions is for router auhtorization in ADD process. Router sends to host a certification path, which is a path between a router and hosts's trust anchor and consists of PKIX certificates. Researchers demonstrated attack against PKIX certificates with MD5 signature. They succeded to construct the original and the false certificate that had the same identity data and digital signature, but different public key [new-hashes]. The problem for the attacker is that two certificates with the same identity are not very useful in real-world scenarios, while Certification Authority is not allowed to provide such two certificates. Additionally, most certificate parts are not in danger because human-readable certificate fields are not affected by the collision attacks. However, implementations SHOULD use human-readable certificate extensions only if SeND certificate profile demands. We also have to take into account that attacker could

produce such false certificate only if he could predict context-useful certificate data. So, although collision attacks against PKIX certificates are theoretically possible, they can hardly be performed in practice.

However, if attacker succeeds to perform attack, once in future when attacks will be improved, the most dangerous will be attacks against middle-certificates in the certification path, where for the cost of one false certificate, attacker launches attack on multiple routers. In such scenarios, We will be at least safe from attacks against Trust Anchor's certificate because it is not exchanged in SeND messages. If attacker, for example, will manage to produce a false certificate with changed IP prefixes in IP subjectAltName extension (which is currently just theoretically possible), IP prefixes range will be broadened at maximum to the range from the Trust Anchor's

certificate.

3.3. Attacks against Digital Signature in RSA Signature option

Digital signature in RSA Signature option is produced as the SHA-1 hash of IPv6 addresses, ICMPv6 header and ND message and is signed with the sender's private key, which corresponds to the public key from the CGA parameters structure and is authorized usually through CGAs. The possible attack on such explicit digital signature is typical non-repudiation attack. Attacker could generate a false message with the same hash and sign that false hashed message with authorized private key. However, the problem for the attacker is that they are very hard to predict the useful input data. It minimizes the possibility for a real-world collision attack and the fact that in order to perform a succesfull real-world attack he can not change a human-readable data. But we also have to take into account that a variant of SHA-1 was already affected by recent collision attacks and we have to prepare for future improved attacks.

3.4. Attacks against Key Hash in RSA Signature option

Key Hash field in the RSA Signature option is a SHA-1 hash of the public key from the CGA parameters structure in the CGA option of SeND message. Key Hash field is a typical example of data fingerprinting, which is potentially dangerous because input field is a non human-readable data. But the problem for the attacker is that a public key, which is input data is authorized through CGAs, and sometimes additionally through a certification path if peer has configured trust anchor. For the succesfull attack, attacker has to break both SHA-1 hashed public key, as well as corresponding CGA and possiblly a certification path. Otherwise, changed key pair will be detected in the process of CGA verification. The same as in previous cases, this attack is theoretically possible, but very hard to

perform in practice.

4. Support for the hash agility in SeND

While all of analyzed hash functions in SeND are theoretically affected by recent collision attacks, these attacks indicate the possibility of future real-world attacks. In order to increase the future security of SeND, we suggest the support for the hash and algorithm agility in SeND.

The most effective and secure would be to bind the hash function option with something that can not be changed at all, like [rfc4982] does for CGA - encoding the hash function information into addresses. But, there is no possibilty to do that in SeND. We could decide to use by default the same hash function in SeND as in CGA, but this solution is architecturally strange and it does not really increase the security since the difficulty for attackers remain to break one single hash function. Furthermore, it may even reduce the security level by providing more relevant information of the hash function. On the other side, the use of two different hash algorithms makes attacker's life harder.

Another solution is to incorporate the hash function option into SeND message. By putting a new hash function option in SeND message before RSA Signature option, attacker will have to break both the signature and the hash input at the same time since the new option will be input field for the Digital Signature in RSA Signature option. However, we can not avoid a downgrade attack totally because peer might be using just ND and not SeND. A completely safe solution here does not exist. A new hash function option in SeND message is a reasonable and the best solution for the hash algorithm agility support in SeND.

4.1. Hash algorithm option

In order to provide hash algorithm agility, each SeND implemenation MUST support the Hash algorithm option. The Hash algorithm option defines:

- a hash algorithm that MUST be used for producing the RSA Signature option (Key Hash field and Digital Signature field),

- a PKIX signature algorithm that the sender of the Hash algorithm option is ready to accept and validate. In order to enhance interoperability, implementations SHOULD also accept and validate PKIX certificates with a signature algorithm that has the higher encoding number than requested signature algorithm. Implementations MUST NOT accept PKIX certificates with signature algorithms marked with lower encoding.

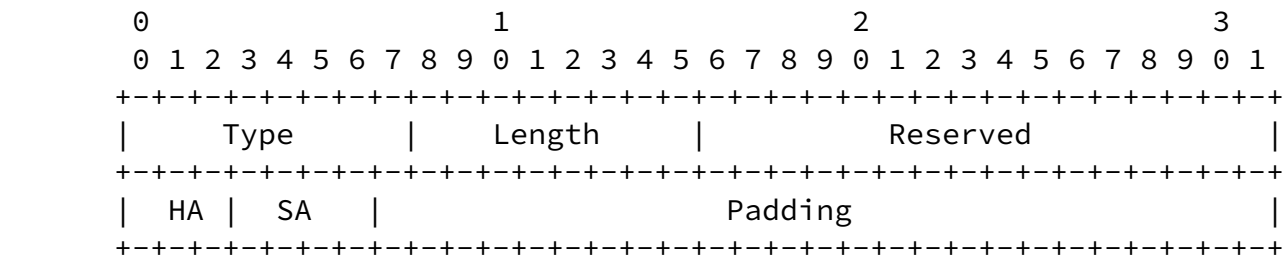

Figure 1

Type

13

Length

The length of the option (including the Type, Length, Reserved, HA, SA, and Padding) in units of 8 octets.

Reserved

A 16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the received.

Hash Algorithm (HA)

Hash algorithm used for producing the Key Hash field and the Digital Signature field in the RSA Signature option. E.g. 000 = md5, ...

Signature Algorithm (SA)

Signature algorithm of the PKIX certificate used in ADD process, in accordance with rfc3279. E.g. 0000 = md5 with RSA encryption, 0001 = sha with DSA encryption.

5. Security Considerations

This document analyzes the impact of hash attacks in SeND and offeres a higher security level for SeND by providing solution for the hash agility support.

6. References

6.1. Normative References

[new-hashes] Bellovin, S. and E. Rescorla, "Deploying a New Hash Algorithm", RFC 4270, November 2005.

[rfc3971] b, a. and K. S, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[rfc4270] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashed in Internet Protocols", RFC 4270, November 2005.

[rfc4982] Bagnulo, M. and J. Arrko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, July 2007.

6.2. Informative References

[rfc2119] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[rfc3280] Housley, R., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[sha-1] K, S. and K. S, "Secure Hash Standard (see rfc3971 [14])", RFC 4301, April 1995.

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
KuiKe Building, No.9 Xinxi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing
P.R. China

Email: shengjiang@huawei.com

Full Copyright Statement

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.