Internet Draft
<draft-rja-ospf-hmac-shs-01.txt>
Category: Informational
Expires 28 Aug 2007
Updates: RFC-2328

R. Atkinson
Extreme Networks
M. Fanto
Ford Motor Company
T. Li
Cisco Systems

28 February 2007

OSPFv2 Authentication with HMAC-SHS
<draft-rja-ospf-hmac-shs-01.txt>

Status of this Memo

Abstract

This document describes how the NIST Secure Hash Standard family of algorithms can be used with OSPF version 2's built-in cryptographic authentication mechanism. This updates, but does not supercede, the cryptographic authentication mechanism specified in RFC-2328.

1. INTRODUCTION

This document provides an update to OSPFv2 Cryptographic Authentication, which is specified in Appendix D of RFC-2328. This document does not deprecate or supercede RFC-2328. OSPFv2 itself is defined in RFC-2328.

This document adds support for Secure Hash Algorithms defined in the US NIST Secure Hash Standard (SHS) as defined by NIST FIPS 180-2. [FIPS-180-2] includes SHA-1, SHA-256, SHA-384, and SHA-512. The HMAC authentication mode defined in NIST FIPS 198 is used.[FIPS-198]

The creation of this addition to OSPFv2 was driven by operator requests that they be able to use the NIST SHS family of algorithms in the NIST HMAC mode, instead of being forced to use the Keyed-MD5 algorithm and mode with OSPFv2 Cryptographic Authentication.

While there are no openly published attacks on the Keyed-MD5 mechanism specified in RFC-2328, some reports [Dobb96a, Dobb96b] create concern about the ultimate strength of the MD5 cryptographic hash function.

2. Background

All OSPF protocol exchanges are authenticated. The OSPF packet header (see Section A.3.1 of RFC-2328) includes an Authentication Type field, and 64-bits of data for use by the appropriate authentication scheme (determined by the type field).

The authentication type is configurable on a per-interface (or equivalently, on a per-network/subnet) basis. Additional authentication data is also configurable on a per-interface basis.

Authentication types 0, 1, and 2 are defined by RFC-2328. This document provides an update to RFC-2328 that is only applicable to Authentication Type 2, "Cryptographic Authentication".

3. Cryptographic authentication with NIST SHS in HMAC mode

Using this authentication type, a shared secret key is configured in all routers attached to a common network/subnet. For each OSPF protocol packet, the key is used to generate/verify a "message digest" that is appended to the end of the OSPF packet. The message digest is a one-way function of the OSPF protocol packet and the secret key. Since the secret key is never sent over the network in the clear, protection is provided against passive attacks.

The algorithms used to generate and verify the message digest are specified implicitly by the secret key. This specification discusses the computation of OSPF Cryptographic Authentication data when any of the NIST SHS family of algorithms is used in the Hashed Message Authentication Code (HMAC) mode.
Please also see RFC-2328, Appendix D.

With the additions in this document, the currently valid algorithms (including mode) for OSPFv2 Cryptographic Authentication include:

Keyed-MD5	(defined in RFC-2328, Appendix D)
HMAC-SHA-1	(defined here)
HMAC-SHA-256	(defined here)
HMAC-SHA-384	(defined here)
HMAC-SHA-512	(defined here)

An implementation of this specification must enhance allow network operators to specify any one of the above algorithms for use with each given Key-ID value that is configured into an OSPFv2 implementation.

3.1. Generating Cryptographic Authentication

First, following the procedure defined in RFC-2328, Appendix D, select the appropriate key for use with this packet and set the Key-ID field to the chosen key's Key-ID value.

Second, set the Authentication Data Length field to the length (measured in bytes, not bits) of the cryptographic hash that will be used. When any NIST SHS algorithm is used in HMAC mode with OSPFv2 Cryptographic Authentication, the Authentication Data Length is equal to the normal hash output length (measured in bytes) for the specific NIST SHS algorithm in use. For example, with NIST SHA-256, the Authentication Data Length is 32 bytes.

Third, The 32-bit Cryptographic sequence number is set in accordance with the procedures in RFC-2328, Appendix D applicable to the Cryptographic Authentication type.

Fourth, The message digest is then calculated and appended to the OSPF packet. The authentication algorithm and algorithm mode to be used in calculating the digest is indicated implicitly by the Key-ID. Input to the authentication algorithm consists of the OSPF packet and the secret key.

3.2 Cryptographic Aspects

This describes the computation of the Authentication Data value when any NIST SHS algorithm is used in the HMAC mode with OSPFv2 Cryptographic Authentication.

In the algorithm description below, the following nomenclature, which is consistent with [FIPS-198], is used:

```
     H    is the specific hashing algorithm (e.g. SHA-256).
     K    is the selected OSPFv2 key
     Ko   is the cryptographic key used with the hash algorithm.
     B    is the block size of H, measured in octets, rather than bits.
          Note that B is the internal block size, not the hash size.
             For SHA-1 and SHA-256:   B == 64
             For SHA-384 and SHA-512: B == 128
     L    is the length of the hash, measured in octets, rather than bits.
     XOR  is the exclusive-or operation.
     Opad is the hexadecimal value 0x5c repeated B times.
     Ipad is the hexadecimal value 0x36 repeated B times.
     Apad is the hexadecimal value 0x878FE1F3 repeated (L/4) times.
```

(1) PREPARATION OF KEY

In this application, Ko is always L octets long.

If the Authentication Key (K) is L octets long, then Ko is equal to K. If the Authentication Key (K) is more than L octets long, then Ko is set to H(K). If the Authentication Key (K) is less than L octets long, then Ko is set to the Authentication Key (K) with zeros appended to the end of the Authentication Key (K) such that Ko is L octets long.

(2) FIRST HASH

First, the OSPFv2 packet's Authentication Data field is filled with the value Apad and the Authentication Type field is set to 2.

Then, a first hash, also known as the inner hash, is computed as follows:

```
      First-Hash = H(Ko XOR Ipad || (OSPFv2 Packet))
```

(3) SECOND HASH

Then a second hash, also known as the outer hash, is computed as follows:

```
      Second-Hash = H(Ko XOR Opad || First-Hash)
```

(4) RESULT

The result Second-Hash becomes the Authentication Data that is sent in the Authentication Data field of the OSPFv2 packet. The length of the Authentication Data field is always identical to the message digest size of the specific hash function H that is being used.

This also means that the use of hash functions with larger output sizes will also increase the size of the OSPFv2 packet as transmitted on the wire.

Implementation Note: RFC-2328, Appendix D specifies that the Authentication Data is not counted in the OSPF packet's own length field, but is included in the packet's IP length field.

3.3. Message verification

Message verification follows the procedure defined in RFC-2328, except that the cryptographic calculation of the message digest follows the procedure above when any NIST SHS algorithm in the HMAC mode is in use. Kindly recall that the cryptographic algorithm/mode in use is indicated implicitly by the Key-ID of the received OSPFv2 packet.

4. Security Considerations

This document enhances the security of the OSPFv2 routing protocol by adding support for additional cryptographic hash functions. This document adds support for the algorithms defined in the NIST Secure Hash Standard (SHS) using the NIST Hashed Message Authentication Code (HMAC) mode to the existing OSPFv2 Cryptographic Authentication method.

This provides several alternatives to the existing Keyed-MD5 mechanism. Although there are no published attacks on the MD5 algorithm as used in RFC-2328, there are published concerns about the overall strength of the MD5 algorithm. [Dobb96a, Dobb96b]

The quality of the security provided by the Cryptographic Authentication option depends completely on the strength of the cryptographic algorithm and cryptographic mode in use, the strength of the key being used, and the correct implementation of the security mechanism in all communicating OSPF implementations. Accordingly, the use of high assurance development methods is recommended. It also requires that all parties maintain the secrecy of the shared secret key.

Because a routing protocol contains information that need not be kept secret, privacy is not a requirement. However, authentication of the messages within the protocol is of interest, to reduce the risk of an adversary compromising the routing system by deliberately injecting false information into the routing system.

The technology in this document enhances an authentication mechanism for OSPFv2. The mechanism described here is not perfect and need not be perfect. Instead, this mechanism represents a significant increase in the work function of an adversary attacking OSPFv2,

as compared with plain-text authentication or null authentication, while not causing undue implementation, deployment, or operational complexity. Denial of service attacks are not generally preventable in a useful networking protocol. [VK83]

Because of implementation considerations, including the need for backwards compatibility, this specification uses the same mechanism as specified in RFC-2328 and limits itself to adding support for additional cryptographic hash functions. Also, some large network operators have indicated they strongly prefer to retain the basic mechanism defined in RFC-2328 due to deployment and operational considerations. If all the OSPFv2 systems deployed by a given network operator also supported using the IP Authentication Header to protect OSPFv2, then such a network operator might consider using the IP Authentication Header in lieu of this mechanism.

If a stronger authentication were believed to be required, then the use of a full digital signature [RFC-2154] would be an approach that should be seriously considered. It was rejected for this purpose at this time because the computational burden of full digital signatures is believed to be much higher than is reasonable given the current threat environment in operational commercial networks. Also, moving to full digital signatures significantly increases the deployment complexity and operational burden for network operators.

5. IANA CONSIDERATIONS

There are no IANA considerations for this document.

6. ACKNOWLEDGEMENTS

The authors would like to thank Bill Burr, Tim Polk, John Kelsey, and Morris Dworkin of (US) NIST for review of portions of this document that are directly derived from the closely related work on RIPv2 Cryptographic Authentication [RFC-4822].

7. REFERENCES

7.1 Normative References

[FIPS-180-2] US National Institute of Standards & Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-2, August 2002.

[FIPS-198] US National Institute of Standards & Technology,

"The Keyed-Hash Message Authentication Code (HMAC)",
FIPS PUB 198, March 2002.

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

[RFC-2328] Moy, J., "OSPF Version 2", RFC-2328, April 1998.

7.2 Informative References

[Bell89] S. Bellovin, "Security Problems in the TCP/IP Protocol
Suite", ACM Computer Communications Review, Volume 19,
Number 2, pp. 32-48, April 1989.

[Dobb96a] Dobbertin, H, "Cryptanalysis of MD5 Compress",
Technical Report, 2 May 1996. (Presented at the
Rump Session of EuroCrypt 1996.)

[Dobb96b] Dobbertin, H, "The Status of MD5 After a Recent
Attack", CryptoBytes, Vol. 2, No. 2, Summer 1996.

[RFC-1704] N. Haller and R. Atkinson, "On Internet
Authentication", RFC 1704, October 1994.

[RFC-2154] Murphy, S., Badger, M. and B. Wellington,
"OSPF with Digital Signatures", RFC 2154, June 1997.

[RFC-4086] Eastlake, D., 3rd, Schiller, J., and S. Crocker,
"Randomness Requirements for Security", BCP-106,
RFC-4086, June 2005.

[RFC-4822] R. Atkinson, M. Fanto, "RIPv2 Cryptographic Authentication",
RFC-4822, February 2007.

[VK83] Voydock, V. and S. Kent, "Security Mechanisms in High-level
Networks", ACM Computing Surveys, Vol. 15, No. 2, June 1983.

AUTHORS

Randall J. Atkinson
Extreme Networks
3585 Monroe Street
Santa Clara, CA 95051 USA

Phone: +1 (408) 579-2800
EMail: rja@extremenetworks.com

Matt Fanto
Ford Motor Company
Michigan
USA

EMail: tbd

Tony Li
Cisco Systems
Tasman Drive
San Jose, CA
USA

EMail: tli@cisco.com

Full Copyright Statement

Intellectual Property