Internet Engineering Task Force (IETF)
Request for Comments: 6863
Category: Informational
ISSN: 2070-1721

S. Hartman
Painless Security
D. Zhang
Huawei Technologies Co., Ltd.

March 2013

Analysis of OSPF Security According to the Keying and Authentication for Routing Protocols (KARP) Design Guide

Abstract

This document analyzes OSPFv2 and OSPFv3 according to the guidelines set forth in Section 4.2 of the "Keying and Authentication for Routing Protocols (KARP) Design Guidelines" (RFC 6518). Key components of solutions to gaps identified in this document are already underway.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6863.

Table of Contents

1. Introduction

This document analyzes the current state of OSPFv2 and OSPFv3 according to the requirements of [RFC6518]. It builds on several previous analysis efforts regarding routing security. The OPSEC working group put together an analysis of cryptographic issues with routing protocols [RFC6039]. Earlier, the RPSEC working group put together a detailed analysis of OSPF vulnerabilities [OSPF-SEC]. Work on solutions to address gaps identified in this analysis is underway [OSPF-MANKEY] [RFC6506].

OSPF meets many of the requirements expected from a manually keyed routing protocol. Integrity protection is provided with modern cryptographic algorithms. Algorithm agility is provided: the algorithm can be changed as part of rekeying an interface or peer. Intra-connection rekeying is provided by the specifications, although apparently some implementations have trouble with this in practice. OSPFv2 security does not interfere with prioritization of packets.

However, some gaps remain between the current state and the requirements for manually keyed routing security expressed in [RFC6862]. This document explores these gaps and proposes directions for addressing the gaps.

1.1. Requirements to Meet

There are a number of requirements described in Section 3 of [RFC6862] that OSPF does not currently meet. The gaps are as follows:

- Secure Simple Pre-Shared Keys (PSKs): Today, OSPF directly uses the key as specified. Related key attacks, such as those described in Section 4.1 of [OPS-MODEL], are possible.

- Replay Protection: The requirements document addresses requirements for both inter-connection replay protection and intra-connection replay protection. OSPFv3 has no replay protection at all. OSPFv2 has most of the mechanisms necessary for intra-connection replay protection. Unfortunately, OSPFv2 does not securely identify the neighbor with whom replay protection state is associated in all cases. This weakness can be used to create significant denial-of-service issues using intra-connection replays. OSPFv2 has no inter-connection replay protection; this creates significant denial-of-service opportunities.

- Packet Prioritization: OSPFv3 uses IPsec [RFC4301] to process packets. This complicates implementations that wish to process some packets, such as Hellos and Acknowledgements, above others. In addition, if IPsec replay mechanisms were used, packets would need to be processed at least by IPsec even if they were low priority.

- Neighbor Identification: In some cases, OSPF identifies a neighbor based on the IP address. This operation is never protected with OSPFv2 and is not typically protected with OSPFv3.

The remainder of this document explains how OSPF fails to meet these requirements, and it proposes mechanisms for addressing them.

1.2. Requirements Notation

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 [RFC2119].

2. Current State

This section describes the security mechanisms built into OSPFv2 and OSPFv3. There are two goals to this section. First, this section gives a brief explanation of the OSPF security mechanisms to those familiar with connectionless integrity mechanisms but not with OSPF.

Second, this section provides the background necessary to understand how OSPF fails to meet some of the requirements proposed for routing security.

2.1. OSPFv2

Appendix D of [RFC2328] describes the basic procedure for cryptographic authentication in OSPFv2. An authentication data field in the OSPF packet header contains a key ID, the length of the authentication data, and a sequence number. A Message Authentication Code (MAC) is appended to the OSPF packet. This code protects all fields of the packet including the sequence number but not the IP header.

RFC 2328 defines the use of a keyed-MD5 MAC. While MD5 has not been broken as a MAC, it is not the algorithm of choice for new MACs.

However, RFC 5709 [RFC5709] adds support for the SHA family of hashes [FIPS180] to OSPFv2. The cryptographic authentication described in RFC 5709 meets modern standards for per-packet integrity protection. Thus, OSPFv2 meets the requirement for strong algorithms. Since multiple algorithms are defined and a new algorithm can be selected with each key, OSPFv2 meets the requirement for algorithm agility. In order to provide cryptographic algorithms believed to have a relatively long useful life, RFC 5709 mandates support for SHA-2 rather than SHA-1.

These security services provide integrity protection on each packet. In addition, limited replay detection is provided. The sequence number is non-decreasing. So, once a router has increased its sequence number, an attacker cannot replay an old packet. Unfortunately, sequence numbers are not required to increase for each packet. For instance, because existing OSPF security solutions do not specify how to set the sequence number, it is possible that some implementations use, for example, "seconds since reboot" as their sequence numbers. The sequence numbers are thus increased only every second, permitting an opportunity for intra-connection replay. Also, no mechanism is provided to deal with the loss of anti-replay state; if sequence numbers are reused when a router reboots, then inter-connection replays are straight forward. In [OSPF-MANKEY], the OSPFv2 sequence number is expanded to 64 bits, with the least significant 32-bit value containing a strictly increasing sequence number and the most significant 32-bit value containing the boot count. The boot count is retained in non-volatile storage for the deployment life of an OSPF router. Therefore, the sequence number will never decrease, even after a cold reboot.

Also, because the IP header is not protected, the sequence number may not be associated with the correct neighbor, a situation that opens up opportunities for outsiders to perform replay attacks. See Section 3 for analysis of these attacks. In [OSPF-MANKEY], this issue is addressed by changing the definition of Apad from a constant defined in [RFC5709] to the source address in the IP header of the OSPFv2 protocol packet. In this way, the source address from the IP header is incorporated in the cryptographic authentication computation, and any change of the IP source address will be detected.

The mechanism provides good support for key rollover. There is a key ID. In addition, mechanisms are described for managing key lifetimes and starting the use of a new key in an orderly manner. Performing orderly key rollover requires that implementations support accepting a new key for received packets before using that key to generate packets. Section D.3 of RFC 2328 requires this support in the form of four configurable lifetimes for each key: two lifetimes control the beginning and ending period for acceptance, while two other lifetimes control the beginning and ending period for generation. These lifetimes provide a superset of the functionality in the key table [CRYPTO-KEYS] regarding lifetime.

The OSPFv2 replay mechanism does not handle prioritized transmission of OSPF Hello and Link State Acknowledgement (LSA) packets as recommended in [RFC4222]. When OSPF packets are transmitted with varied prioritization, they can arrive out of order, which results in packets with lower prioritization being discarded.

2.2. OSPFv3

"Authentication/Confidentiality for OSPFv3" [RFC4552] describes how the IPsec authentication header and encapsulating security payload mechanism can be used to protect OSPFv3 packets. This mechanism provides per-packet integrity and optional confidentiality using a wide variety of cryptographic algorithms. Because OSPF uses multicast traffic, only manual key management is supported. This mechanism meets requirements related to algorithm selection and agility.

The Security Parameter Index (SPI) [RFC4301] provides an identifier for the security association. This identifier, along with other IPsec facilities, provides a mechanism for moving from one key to another, meeting the key rollover requirements.

Because manual keying is used, no replay protection is provided for OSPFv3. Thus, the intra-connection and inter-connection replay requirements are not met.

There is another serious problem with the OSPFv3 security: rather than being integrated into OSPF, it is based on IPsec. In practice, this has lead to deployment problems.

OSPF implementations generally prioritize packets in order to minimize disruption when router resources such as CPU or memory experience contention. When IPsec is used with OSPFv3, the offset of the packet type, which is used to prioritize packets, depends on which integrity transform is used. For this reason, prioritizing packets may be more complex for OSPFv3. One approach is to establish per-SPI filters to find the packet type and then act accordingly.

3. Impacts of OSPF Replays

As discussed, neither version of OSPF meets the requirements of inter-connection or intra-connection replay protection. In order to mount a replay, an attacker needs some mechanism to inject a packet. Physical security can limit a particular deployment's vulnerability to replay attacks. This section discusses the impacts of OSPF replays.

In OSPFv2, two facilities limit the scope of replay attacks. First, when cryptographic authentication is used, each packet includes a sequence number that is non-decreasing. In the current specifications, the sequence number is remembered as part of an adjacency: if an attacker can cause an adjacency to go down, then replay state is lost. Database Description packets also include a per-LSA sequence number that is part of the information that is flooded. Even if a packet is replayed, the per-LSA sequence number will prevent an old LSA from being installed. Unlike the per-packet sequence number, the per-LSA sequence number must increase when an LSA is changed. As a result, replays cannot be used to install old routing information.

While the LSA sequence number provides some defense, the Routing Protocol Security Requirements (RPSEC) analysis [OSPF-SEC] describes a number of attacks that are possible because of per-packet replays. The most serious appear to be attacks against Hello packets, which may cause an adjacency to fail. Other attacks may cause excessive flooding or excessive use of CPU.

Another serious attack concerns Database Description packets. In addition to the per-packet sequence number that is part of cryptographic authentication for OSPFv2 and the per-LSA sequence numbers, Database Description packets also include a Database Description sequence number. If a Database Description packet with the incorrect sequence number is received, then the database exchange process will be restarted.

The per-packet OSPFv2 sequence number can be used to reduce the window in which a replay is valid. A receiver will harmlessly reject a packet whose per-packet sequence number is older than the one most recently received from a neighbor. Replaying the most recent packet from a neighbor does not appear to create problems. So, if the per-packet sequence number is incremented on every packet sent, then replay attacks should not disrupt OSPFv2. Unfortunately, OSPFv2 does not have a procedure for dealing with sequence numbers reaching the maximum value. It may be possible to figure out a set of rules sufficient to disrupt the damage of packet replays while minimizing the use of the sequence number space.

As mentioned previously, when an adjacency is dropped, replay state is lost. So, after rebooting or when all adjacencies are lost, a router may allow its sequence number to decrease. An attacker can cause significant damage by replaying a packet captured before the sequence number decrease at a time after the sequence number decrease. If this happens, then the replayed packet will be accepted and the sequence number will be updated. However, the legitimate sender will be using a lower sequence number, so legitimate packets will be rejected. A similar attack is possible in cases where OSPF identifies a neighbor based on source address. An attacker can change the source address of a captured packet and replay it. If the attacker causes a replay from a neighbor with a high sequence number to appear to be from a neighbor with a low sequence number, then connectivity with that neighbor will be disrupted until the adjacency fails.

OSPFv3 lacks the per-packet sequence number but has the per-LSA sequence number. As such, OSPFv3 has no defense against denial-of-service attacks that exploit replay.

4. Gap Analysis and Specific Requirements

The design guide requires each design team to enumerate a set of requirements for the routing protocol. The only concerns identified with OSPF are areas in which it fails to meet the general requirements outlined in the threats and requirements document. This section explains how some of these general requirements map specifically onto the OSPF protocol and enumerates the specific gaps that need to be addressed.

There is a general requirement for inter-connection replay protection. In the context of OSPF, this means that if an adjacency goes down between two neighbors and later is re-established, replaying packets from before the adjacency went down cannot disrupt the adjacency. In the context of OSPF, intra-connection replay protection means that replaying a packet cannot prevent an adjacency

from forming or cannot disrupt an existing adjacency. In terms of meeting the requirements for intra-connection and inter-connection replay protection, a significant gap exists between the optimal state and where OSPF is today.

Since OSPF uses fields in the IP header, the general requirement to protect the IP header and handle neighbor identification applies. This is another gap that needs to be addressed. Because the replay protection will depend on neighbor identification, the replay protection cannot be adequately addressed without handling this issue as well.

In order to encourage deployment of OSPFv3 security, an authentication option is required that does not have the deployment challenges of IPsec.

In order to support the requirement for simple pre-shared keys, OSPF needs to make sure that when the same key is used for two different purposes, no problems result.

In order to support packet prioritization, it is desirable for the information needed to prioritize OSPF packets (the packet type) to be at a constant location in the packet.

5. Solution Work

It is recommended that the OSPF Working Group develop a solution for OSPFv2 and OSPFv3 based on the OSPFv2 cryptographic authentication option. This solution would have the following improvements over the existing OSPFv2 option:

- Address most inter-connection replay attacks by splitting the sequence number and requiring preservation of state so that the sequence number increases on every packet.

- Add a form of simple key derivation so that if the same pre-shared key is used for OSPF and other purposes, cross-protocol attacks do not result.

- Support OSPFv3 authentication without use of IPsec.

- Specify processing rules sufficient to permit replay detection and packet prioritization.

- Emphasize requirements already present in the OSPF specification sufficient to permit key migration without disrupting adjacencies.

- Specify the proper use of the key table for OSPF.

Protect the source IP address.

Require that sequence numbers be incremented on each packet.

The key components of this solution work are already underway. OSPFv3 now supports an authentication option [RFC6506] that meets the requirements of this section; however, this document does not describe how the key tables are used for OSPF. OSPFv2 is being enhanced [OSPF-MANKEY] to protect the source address, provide inter-connection replay and describe how to use the key table.

6. Security Considerations

This memo discusses and compiles vulnerabilities in the existing OSPF cryptographic handling.

In analyzing proposed improvements to OSPF per-packet security, it is desirable to consider how these improvements interact with potential improvements in overall routing security. For example, the impact of replay attacks currently depends on the LSA sequence number mechanism. If cryptographic protections against insider attackers are considered by future work, then that work will need to provide a solution that meets the needs of the per-packet replay defense as well as protects routing data from insider attack. An experimental solution is discussed in [RFC2154] that explores end-to-end protection of routing data in OSPF. It may be beneficial to consider how improvements to the per-packet protections would interact with such a mechanism to future-proof these mechanisms.

Implementations have a number of options in minimizing the potential denial-of-service impact of OSPF cryptographic authentication. The Generalized TTL Security Mechanism (GTSM) [RFC5082] might be appropriate for OSPF packets except for those traversing virtual links. Using this mechanism requires support of the sender; new OSPF cryptographic authentication could specify this behavior if desired. Alternatively, implementations can limit the source addresses from which they accept packets. Non-Hello packets need only be accepted from existing neighbors. If a system is under attack, Hello packets from existing neighbors could be prioritized over Hello packets from new neighbors. These mechanisms can be considered to limit the potential impact of denial-of-service attacks on the cryptographic authentication mechanism itself.

7. Acknowledgements

Funding for Sam Hartman's work on this memo was provided by Huawei.

The authors would like to thank Ran Atkinson, Michael Barnes, and Manav Bhatia for valuable comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC4552] Gupta, M. and N. Melam, "Authentication/ Confidentiality for OSPFv3", RFC 4552, June 2006.

[RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", RFC 6518, February 2012.

[RFC6862] Lebovitz, G., Bhatia, M., and B. Weis, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", RFC 6862, March 2013.

8.2. Informative References

[CRYPTO-KEYS] Housley, R., Polk, T., Hartman, S., and D. Zhang, "Database of Long-Lived Symmetric Cryptographic Keys", Work in Progress, October 2012.

[FIPS180] US National Institute of Standards and Technology, "Secure Hash Standard (SHS)", August 2002.

[OPS-MODEL] Hartman, S. and D. Zhang, "Operations Model for Router Keying", Work in Progress, October 2012.

[OSPF-MANKEY] Bhatia, M., Hartman, S., Zhang, D., and A. Lindem, "Security Extension for OSPFv2 when using Manual Key Management", Work in Progress, October 2012.

[OSPF-SEC] Jones, E. and O. Moigne, "OSPF Security Vulnerabilities Analysis", Work in Progress, June 2006.

[RFC2154] Murphy, S., Badger, M., and B. Wellington, "OSPF with Digital Signatures", RFC 2154, June 1997.

[RFC4222] Choudhury, G., "Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance", BCP 112, RFC 4222, October 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, October 2009.

[RFC6039] Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues with Existing Cryptographic Protection Methods for Routing Protocols", RFC 6039, October 2010.

[RFC6506] Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", RFC 6506, February 2012.

Authors' Addresses

Sam Hartman
Painless Security

EMail: hartmans-ietf@mit.edu
URI: http://www.painless-security.com/

Dacheng Zhang
Huawei Technologies Co., Ltd.
Huawei Building No. 3 Xinxi Rd.
Shang-Di Information Industrial Base Hai-Dian District, Beijing
China

EMail: zhangdacheng@huawei.com