Internet Engineering Task Force (IETF)
Request for Comments: 7645
Category: Informational
ISSN: 2070-1721

U. Chunduri
A. Tian
W. Lu
Ericsson Inc.

September 2015

The Keying and Authentication for Routing Protocol (KARP) IS-IS Security Analysis

Abstract

This document analyzes the current state of the Intermediate System to Intermediate System (IS-IS) protocol according to the requirements set forth in "Keying and Authentication for Routing Protocols (KARP) Design Guidelines" (RFC 6518) for both manual and automated key management protocols.

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/rfc7645.

Table of Contents

1. Introduction

This document analyzes the current state of the Intermediate System to Intermediate System (IS-IS) protocol according to the requirements set forth in "Keying and Authentication for Routing Protocols (KARP) Design Guidelines" [RFC6518] for both manual and automated key management protocols.

With currently published work, IS-IS meets some of the requirements expected from a manually keyed routing protocol. Integrity protection is expanded by allowing more cryptographic algorithms to be used [RFC5310]. However, even with this expanded protection, only limited algorithm agility (HMAC-SHA family) is possible. [RFC5310] makes possible a basic form of intra-connection rekeying, but with some gaps as analyzed in Section 3 of this document.

This document summarizes the current state of cryptographic key usage in the IS-IS protocol and several previous efforts that analyze IS-IS security. This includes the base IS-IS specifications: [RFC1195], [RFC5304], [RFC5310], and [RFC6039].

This document also analyzes various threats to IS-IS (as described in [RFC6862]), lists security gaps, and provides specific recommendations to thwart the threats for both manual keying and automated key management mechanisms.

1.1. Requirements Language

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].

1.2. Acronyms

DoS - Denial of Service

GDOI - Group Domain of Interpretation

IGP - Interior Gateway Protocol

IIH - IS-IS HELLO

IPv4 - Internet Protocol version 4

KMP - Key Management Protocol (automated key management)

LSP - Link State PDU

MKM - Manual Key Management

NONCE - Number Once

PDU - Protocol Data Unit

SA - Security Association

SNP - Sequence Number PDU

2. Current State

IS-IS is specified in International Standards Organization (ISO) 10589 [ISO10589], with extensions to support Internet Protocol version 4 (IPv4) described in [RFC1195]. The specification includes an authentication mechanism that allows for any authentication algorithm and also specifies the algorithm for clear text passwords. Further, [RFC5304] extends the authentication mechanism to work with HMAC-MD5 and also modifies the base protocol for more effectiveness. [RFC5310] provides algorithm agility, with a new generic cryptographic authentication mechanism (CRYPTO_AUTH) for IS-IS.

CRYPTO_AUTH also introduces a Key ID mechanism that maps to unique IS-IS SAs.

The following sections describe the current authentication key usage for various IS-IS messages, current key change methodologies, and the various potential security threats.

2.1. Key Usage

IS-IS can be provisioned with a per-interface, peer-to-peer key for IIH PDUs and a group key for LSPs and SNPs. If provisioned, IIH packets can potentially use the same group key used for LSPs and SNPs.

2.1.1. Subnetwork Independent

Link State PDUs, Complete and partial Sequence Number PDUs come under Sub network Independent messages. For protecting Level-1 SNPs and Level-1 LSPs, provisioned Area Authentication key is used. Level-2 SNPs as well as Level-2 LSPs use the provisioned domain authentication key.

Because authentication is performed on the LSPs transmitted by an IS, rather than on the LSP packets transmitted to a specific neighbor, it is implied that all the ISes within a single flooding domain must be configured with the same key in order for authentication to work correctly. This is also true for SNP packets, though they are limited to link-local scope in broadcast networks.

If multiple instances share the circuits as specified in [RFC6822], instance-specific authentication credentials can be used to protect the LSPs and SNPs within an area or domain. It is important to note that [RFC6822] also allows usage of topology-specific authentication credentials within an instance for the LSPs and SNPs.

2.1.2. Subnetwork Dependent

IIH PDUs use the Link Level Authentication key, which may be different from that of LSPs and SNPs. This could be particularly true for point-to-point links. In broadcast networks, it is possible to provision the same common key used for LSPs and SNPs to protect IIH messages. This allows neighbor discovery and adjacency formation with more than one neighbor on the same physical interface. If multiple instances share the circuits as specified in [RFC6822], instance-specific authentication credentials can be used to protect Hello messages.

2.2. Key Agility

Key roll over without effecting the routing protocols operation in general and IS-IS in particular is necessary for effective key management protocol integration.

Current HMAC-MD5 cryptographic authentication as defined in [RFC5304], suggests a transition mode so that ISes use a set of keys when verifying the authentication value to allow key changes. This approach will allow changing the authentication key manually without bringing down the adjacency and without dropping any control packet. But, this can increase the load on the control plane for the key transition duration, as each control packet may have to be verified by more than one key, and it also allows a potential DoS attack in the transition duration.

The above situation is improved with the introduction of the Key ID mechanism as defined in [RFC5310]. With this, the receiver determines the active SA by looking at the Key ID field in the incoming PDU and need not try with other keys when the integrity check or digest verification fails. But, neither key coordination across the group nor an exact key change mechanism is clearly defined. [RFC5310] says:

> Normally, an implementation would allow the network operator to configure a set of keys in a key chain, with each key in the chain having a fixed lifetime. The actual operation of these mechanisms is outside the scope of this document.

2.3. Security Issues

The following section analyzes various possible security threats in the current state of the IS-IS protocol.

2.3.1. Replay Attacks

Replaying a captured protocol packet to cause damage is a common threat for any protocol. Securing the packet with cryptographic authentication information alone cannot mitigate this threat completely. Though this problem is more prevalent in broadcast networks, it is important to note that most of the IGP deployments use P2P-over-lan circuits [RFC5309], which makes it possible for an adversary to replay an IS-IS PDU more easily than the traditional P2P networks.

In intra-session replay attacks, a secured protocol packet of the current session that is replayed can cause damage, if there is no other mechanism to confirm this is a replay packet. In inter-session

replay attacks, a captured packet from one of the previous sessions can be replayed to cause damage. IS-IS packets are vulnerable to both of these attacks, as there is no sequence number verification for IIH and SNP packets. Also with current manual key management, periodic key changes across the group are rarely done. Thus, the intra-connection and inter-connection replay requirements are not met.

IS-IS specifies the use of the HMAC-MD5 [RFC5304] and HMAC-SHA-1 family in [RFC5310] to protect IS-IS packets. An adversary could replay old IIHs or replay old SNPs that would cause churn in the network or bring down the adjacencies.

1. At the time of adjacency bring up an IS sends IIH packet with empty neighbor list (TLV 6) and with the authentication information as per the provisioned authentication mechanism. If this packet is replayed later on the broadcast network, all ISes in the broadcast network can bounce the adjacency to create a huge churn in the network.

2. Today, LSPs have intra-session replay protection as the LSP header contains a 32-bit sequence number, which is verified for every received packet against the local LSP database. But, if a node in the network is out of service (is undergoing some sort of high availability condition or an upgrade) for more than LSP refresh time and the rest of the network ages out the LSPs of the node under consideration, an adversary can potentially plunge in inter-session replay attacks in the network. If the key is not changed in the above circumstances, attack can be launched by replaying an old LSP with a higher sequence number and fewer prefixes or fewer adjacencies. This may force the receiver to accept and remove the routes from the routing table, which eventually causes traffic disruption to those prefixes. However, as per the IS-IS specification, there is a built-in recovery mechanism for LSPs from inter-session replay attacks and it is further discussed in Section 2.3.1.1.

3. In any IS-IS network (broadcast or otherwise), if an old and an empty Complete Sequence Number Packet (CSNP) is replayed, this can cause LSP flood in the network. Similarly, a replayed Partial Sequence Number Packet (PSNP) can cause LSP flood in the broadcast network.

2.3.1.1. Current Recovery Mechanism for LSPs

In the event of inter-session replay attack by an adversary, as an LSP with a higher sequence number gets accepted, it also gets propagated until it reaches the originating node of the LSP. The

originator recognizes the LSP is "newer" than in the local database, which prompts the originator to flood a newer version of the LSP with a higher sequence number than that received. This newer version can potentially replace any versions of the replayed LSP that may exist in the network.

However, in the above process, depending on where in the network the replay is initiated, how quickly the nodes in the network react to the replayed LSP, and how different the content in the accepted LSP is determines the damage caused by the replayed LSP.

2.3.2. Spoofing Attacks

IS-IS shares the same key between all neighbors in an area or in a domain to protect the LSP, SNP packets, and in broadcast networks even IIH packets. False advertisement by a router is not within the scope of the KARP work. However, given the wide sharing of keys as described above, there is a significant risk that an attacker can compromise a key from one device and use it to falsely participate in the routing, possibly even in a very separate part of the network.

If the same underlying topology is shared across multiple instances to transport routing/application information as defined in [RFC6822], it is necessary to use different authentication credentials for different instances. In this connection, based on the deployment considerations, if certain topologies in a particular IS-IS instance require more protection from spoofing attacks and less exposure, topology-specific authentication credentials can be used for LSPs and SNPs as facilitated in [RFC6822].

Currently, possession of the key itself is used as an authentication check and there is no identity check done separately. Spoofing occurs when an illegitimate device assumes the identity of a legitimate one. An attacker can use spoofing to launch various types of attacks, for example:

1. The attacker can send out unrealistic routing information that might cause the disruption of network services, such as block holes.

2. A rogue system that has access to the common key used to protect the LSP can flood an LSP by setting the Remaining Lifetime field to zero, thereby initiating a purge. Subsequently, this can cause the sequence number of all the LSPs to increase quickly to max out the sequence number space, which can cause an IS to shut down for MaxAge + ZeroAgeLifetime period to allow the old LSPs to age out in other ISes of the same flooding domain.

2.3.3. DoS Attacks

DoS attacks using the authentication mechanism is possible and an attacker can send packets that can overwhelm the security mechanism itself. An example is initiating an overwhelming load of spoofed but integrity-protected protocol packets, so that the receiver needs to process the integrity check, only to discard the packet. This can cause significant CPU usage. DoS attacks are not generally preventable within the routing protocol. As the attackers are often remote, the DoS attacks are more damaging to area-scoped or domain-scoped packet receivers than link-local-scoped packet receivers.

3. Gap Analysis and Security Requirements

This section outlines the differences between the current state of the IS-IS routing protocol and the desired state as specified in the KARP Design Guidelines [RFC6518]. This section focuses on where the IS-IS protocol fails to meet general requirements as specified in the threats and requirements document [RFC6862].

This section also describes security requirements that should be met by IS-IS implementations that are secured by manual as well as automated key management protocols.

3.1. Manual Key Management

1. With CRYPTO_AUTH specification [RFC5310], IS-IS packets can be protected with the HMAC-SHA family of cryptographic algorithms. The specification provides limited algorithm agility (SHA family). By using Key IDs, it also conceals the algorithm information from the protected control messages.

2. Even though both intra- and inter-session replay attacks are best prevented by deploying key management protocols with frequent key change capability, basic constructs for the sequence number should be in the protocol messages. So, some basic or extended sequence number mechanism should be in place to protect IIH packets and SNP packets. The sequence number should be increased for each protocol packet. This allows mitigation of some of the replay threats as mentioned in Section 2.3.1.

3. Any common key mechanism with keys shared across a group of routers is susceptible to spoofing attacks caused by a malicious router. A separate authentication check (apart from the integrity check to verify the digest) with digital signatures as described in [RFC2154] can effectively nullify this attack. But this approach was never deployed, which we assume is due to operational considerations at that time. The alternative approach to thwart

this threat would be to use the keys from the group key management protocol. As the group key(s) are generated by authenticating the member ISes in the group first and are then periodically rekeyed, per-packet identity or authentication checks may not be needed.

4. In general, DoS attacks may not be preventable with the mechanism from the routing protocol itself. But some form of admin-controlled lists at the forwarding plane can reduce the damage. There are some other forms of DoS attacks common to any protocol that are not in scope per Section 3.3 of [RFC6862].

As discussed in Section 2.2, though the Key ID mechanism described in [RFC5310] helps, a better key coordination mechanism for key roll over is desirable even with manual key management. But, [RFC5310] does not specify the exact mechanism other than requiring use of key chains. The specific requirements are as follows:

a. Keys SHOULD be able to change without effecting the established adjacency, ideally without any control packet loss.

b. Keys SHOULD be able to change without effecting the protocol operations; for example, LSP flooding should not be held for a specific Key ID availability.

c. Any proposed mechanism SHOULD also be incrementally deployable with key management protocols.

3.2. Key Management Protocols

In broadcast deployments, the keys used for protecting IS-IS protocols messages can, in particular, be group keys. A mechanism is needed to distribute group keys to a group of ISes in a Level-1 area or Level-2 domain, using the Group Domain of Interpretation (GDOI) protocol as specified in [RFC6407]. An example policy and payload format is described in [GDOI].

If a group key is used, the authentication granularity becomes group membership of devices, not peer authentication between devices. The deployed group key management protocol SHOULD support rekeying.

In some deployments, where IS-IS point-to-point (P2P) mode is used for adjacency bring-up, subnetwork-dependent messages (e.g., IIHs) can use a different key shared between the two P2P peers, while all other messages use a group key. When a group keying mechanism is deployed, even the P2P IIHs can be protected with the common group keys. This approach facilitates one key management mechanism instead of both pair-wise keying and group keying protocols being deployed together. If the same circuits are shared across multiple instances,

the granularity of the group can become per instance for IIHs and per instance/topology for LSPs and SNPs as specified in [RFC6822].

Effective key change capability within the routing protocol that allows key roll over without impacting the routing protocol operation is one of the requirements for deploying any group key mechanism. Once such mechanism is in place with the deployment of group key management protocol; IS-IS can be protected from various threats and is not limited to intra- and inter-session replay attacks and spoofing attacks.

Specific use of cryptographic tables [RFC7210] should be defined for the IS-IS protocol.

4. Security Considerations

This document is mostly about security considerations of the IS-IS protocol, and it lists potential threats and security requirements for mitigating these threats. This document does not introduce any new security threats for the IS-IS protocol. In view of openly published attack vectors, as noted in Section 1 of [RFC5310] on HMAC-MD5 cryptographic authentication mechanism, IS-IS deployments SHOULD use the HMAC-SHA family [RFC5310] instead of HMAC-MD5 [RFC5304] to protect IS-IS PDUs. For more detailed security considerations, please refer the Security Considerations section of the IS-IS Generic Cryptographic Authentication [RFC5310], the KARP Design Guide [RFC6518] document, as well as the KARP threat document [RFC6862].

5. References

5.1. Normative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <http://www.rfc-editor.org/info/rfc1195>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <http://www.rfc-editor.org/info/rfc5304>.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009, <http://www.rfc-editor.org/info/rfc5310>.

5.2. Informative References

[GDOI] Weis, B. and S. Rowles, "GDOI Generic Message Authentication Code Policy", Work in Progress, draft-weis-gdoi-mac-tek-03, September 2011.

[ISO10589] International Organization for Standardization, "Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)", ISO/IEC 10589:2002, Second Edition, November 2002.

[RFC2154] Murphy, S., Badger, M., and B. Wellington, "OSPF with Digital Signatures", RFC 2154, DOI 10.17487/RFC2154, June 1997, <http://www.rfc-editor.org/info/rfc2154>.

[RFC5309] Shen, N., Ed., and A. Zinin, Ed., "Point-to-Point Operation over LAN in Link State Routing Protocols", RFC 5309, DOI 10.17487/RFC5309, October 2008, <http://www.rfc-editor.org/info/rfc5309>.

[RFC6039] Manral, V., Bhatia, M., Jaeggli, J., and R. White, "Issues with Existing Cryptographic Protection Methods for Routing Protocols", RFC 6039, DOI 10.17487/RFC6039, October 2010, <http://www.rfc-editor.org/info/rfc6039>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <http://www.rfc-editor.org/info/rfc6407>.

[RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", RFC 6518, DOI 10.17487/RFC6518, February 2012, <http://www.rfc-editor.org/info/rfc6518>.

[RFC6822] Previdi, S., Ed., Ginsberg, L., Shand, M., Roy, A., and D. Ward, "IS-IS Multi-Instance", RFC 6822, DOI 10.17487/RFC6822, December 2012, <http://www.rfc-editor.org/info/rfc6822>.

[RFC6862] Lebovitz, G., Bhatia, M., and B. Weis, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", RFC 6862, DOI 10.17487/RFC6862, March 2013, <http://www.rfc-editor.org/info/rfc6862>.

[RFC7210] Housley, R., Polk, T., Hartman, S., and D. Zhang, "Database of Long-Lived Symmetric Cryptographic Keys", RFC 7210, DOI 10.17487/RFC7210, April 2014, <http://www.rfc-editor.org/info/rfc7210>.

Acknowledgements

Authors would like to thank Joel Halpern for initial discussions on this document and for giving valuable review comments. The authors would like to acknowledge Naiming Shen for reviewing and providing feedback on this document. Thanks to Russ White, Brian Carpenter, and Amanda Barber for reviewing the document during the IESG review process.

Authors' Addresses

Uma Chunduri
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
United States
Phone: 408 750-5678
Email: uma.chunduri@ericsson.com

Albert Tian
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
United States
Phone: 408 750-5210
Email: albert.tian@ericsson.com

Wenhu Lu
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
United States
Email: wenhu.lu@ericsson.com