Routing Working Group
Internet-Draft
Intended status: Informational
Expires: January 7, 2016

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

July 6, 2015

KARP IS-IS security analysis
draft-ietf-karp-isis-analysis-07

Abstract

This document analyzes the threats applicable for Intermediate system to Intermediate system (IS-IS) routing protocol and security gaps according to the KARP Design Guide. This document also provides specific requirements to address the gaps with both manual and auto key management protocols.

Table of Contents

1. Introduction

This document analyzes the current state of Intermediate system to Intermediate system (IS-IS) protocol according to the requirements set forth in [RFC6518] for both manual and auto 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 with more cryptographic algorithms and also limited algorithm agility (HMAC-SHA family) is provided with [RFC5310]. Basic form of Intra-connection re-keying capability is provided by the specification [RFC5310] with some gaps as explained in Section 3.

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

This document also analyzes applicability of various threats to IS-IS (as described in [RFC6862]), lists gaps and provide specific recommendations to thwart the applicable threats for both manual keying and for auto 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 PDU.

IPv4 - Internet Protocol version 4.

KMP - Key Management Protocol (auto key management).

LSP - IS-IS Link State PDU.

MKM - Manual Key management Protocols.

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, 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 new generic crypto authentication mechanism (CRYPTO_AUTH) for IS-IS. The CRYPTO_AUTH also introduces

Key ID mechanism that map to unique IS-IS Security Associations (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 IS-IS HELLO (IIH) PDUs and a group key for Link State PDUs (LSPs) and Sequence number PDUs (SNPs). If provisioned, IIH packets potentially can use the same group key used for LSPs and SNPs.

2.1.1. Sub network 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.

Since 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, [RFC6822] also allows usage of topology specific authentication credentials within an instance for the LSPs and SNPs.

2.1.2. Sub network dependent

IS-IS HELLO 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 crypto 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 control plane for the key transition duration as each control packet may have to be verified by more than one key and also allows to mount a potential Denial of Service (DoS) attack in the transition duration.

The above situation is improved with the introduction of Key ID mechanism as defined in [RFC5310]. With this, the receiver determines the active security association (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 co-ordination across the group nor 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 security threats possible, in the current state for 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, most of the IGP deployments use P2P-over-lan [RFC5309], which makes an adversary replay 'easier' than the traditional P2P networks

In intra-session replay attacks a secured protocol packet of the current session is replayed, can cause damage, if there is no other mechanism to confirm this is a replay packet. In inter-session replay attacks, captured packet from one of the previous session can be replayed to cause the damage. IS-IS packets are vulnerable to both these attacks, as there is no sequence number verification for

IIH packets and SNP packets. Also with current manual key management periodic key changes across the group are done rarely. 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 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 LSP header contains 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 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 LSP with 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 and this prompts the originator to flood a newer version of the LSP with higher sequence number than the received. This newer version can

potentially replace any versions of the replayed LSP which may exist in the network.

But in the above process, depending on where in the network the replay is initiated, how quick the nodes in the network react to the replayed LSP and also how different the content in the accepted LSP 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 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 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 as a means for launching 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 having access to the common key used to protect the LSP, can send an LSP, setting the Remaining Lifetime field to zero, and flooding it thereby initiating a purge. Subsequently, this also 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

Denial-of-service (DoS) attacks using the authentication mechanism is possible and an attacker can send packets which 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 KARP Design Guidelines [RFC6518]. The section focuses on where IS-IS protocol fails to meet general requirements as specified in the threats and requirements document.

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

3.1. Manual Key Management

1. With CRYPTO_AUTH specification [RFC5310], IS-IS packets can be protected with HMAC-SHA family of cryptographic algorithms. The specification provides the 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 sequence number should be there 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. 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 and one can only assume due to

operational considerations at that time. The alternative approach to thwart this threat would be by using 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 then periodically rekeyed, per packet identity or authentication check may not be needed.

4. In general DoS attacks may not be preventable with mechanism from routing protocols itself. But some form of Admin controlled lists (ACLs) at the forwarding plane can reduce the damage. There are some other forms the DoS attacks common to any protocol are not in scope as per the section 3.3 in [RFC6862].

As discussed in Section 2.2, though Key ID mechanism in [RFC5310] helps, better key co-ordination mechanism for key roll over is desirable even with manual key management. But, it fell short of specifying exact mechanism other than using key chains. The specific requirements:

a. Keys SHOULD be able to change without affecting the established adjacency and even better 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 further 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 was described in [I-D.weis-gdoi-mac-tek].

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

In some deployments, where IS-IS point-to-point (P2P) mode is used for adjacency bring-up, sub network dependent messages (IIHs) can use a different key shared between the two point-to-point peers, while all other messages use a group key. When 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 to be deployed together. If 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 the [RFC6822].

Effective key change capability within the routing protocol which 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 deployment of group key management protocol, IS-IS can be protected from various threats not limited to intra and inter session replay attacks and spoofing attacks.

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

4. IANA Considerations

This document defines no new namespaces.

5. Security Considerations

This document is mostly about security considerations of IS-IS protocol, lists potential threats and security requirements for solving those threats. This document does not introduce any new security threats for 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 HMAC-SHA family [RFC5310] instead of HMAC-MD5 [RFC5304] for protecting IS-IS PDUs. For more detailed security considerations please refer the Security Considerations section of the IS-IS Generic Cryptographic Authentication [RFC5310], KARP Design Guide [RFC6518] document as well as KARP threat document [RFC6862].

6. Acknowledgements

Authors would like to thank Joel Halpern for initial discussions on this document and giving valuable review comments. 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 IESG review process.

7. References

7.1. Normative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.

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

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, October 2008.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.

7.2. Informative References

[I-D.weis-gdoi-mac-tek] Weis, B. and S. Rowles, "GDOI Generic Message Authentication Code Policy", draft-weis-gdoi-mac-tek-03 (work in progress), September 2011.

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

[RFC5309] Shen, N. and A. Zinin, "Point-to-Point Operation over LAN in Link State Routing Protocols", RFC 5309, October 2008.

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

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, October 2011.

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

[RFC6822] Previdi, S., Ginsberg, L., Shand, M., Roy, A., and D. Ward, "IS-IS Multi-Instance", RFC 6822, December 2012.

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

[RFC7210] Housley, R., Polk, T., Hartman, S., and D. Zhang, "Database of Long-Lived Symmetric Cryptographic Keys", RFC 7210, April 2014.

Authors' Addresses

Uma Chunduri
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
USA

Phone: 408 750-5678
Email: uma.chunduri@ericsson.com

Albert Tian
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
USA

Phone: 408 750-5210
Email: albert.tian@ericsson.com

Wenhu Lu
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
USA

Email: wenhu.lu@ericsson.com