IS-IS ESN TLV

draft-chunduri-isis-extended-sequence-no-tlv-03

Uma Chunduri, Wenhu Lu, Albert Tian
Ericsson Inc.
Naiming Shen
Cisco Systems, Inc.

IETF 85, Atlanta, GA
Nov 4-9, 2012

IS-IS ESN TLV

- Problem Briefly described in
  - Sec. considerations section of [RFC5304]

Sec 3.1 - "This mechanism does not prevent replay attacks; however, in most cases, such attacks would trigger existing mechanisms in the IS-IS protocol that would effectively reject old information."

  - [RFC5310]

Sec 4 - "The mechanism detailed in this document does not protect IS-IS against replay attacks. An adversary could in theory replay old IIHs and bring down the adjacency [CRYPTO]…."

  - OPSec WG [RFC6039]

Sec 4.2 -"IS-IS does not provide a sequence number. IS-IS packets are vulnerable to replay attacks; any packet can be replayed at any point of time. So long as the keys used are the same, protocol elements that would not be rejected will affect existing sessions."

Brief Recap

Presented in 83rd IETF Paris

Problem??

- Replay attacks with IS-IS protocol messages to create churn in the networks
  - ✓ discussed briefly in the draft and also in
  - ✓ Section 2.3.1 of http://tools.ietf.org/html/draft-chunduri-karp-is-is-gap-analysis-03

Background & Recap

- IS-IS is not only restricted to few Tier-1 ISP backbones but..
- Has been adopted widely in various L2 and L3 routing deployment of the data centers for critical business operations.
- Continue to being adopted in various “forms” of SDN, where messages are directly being sent to the nodes

How?

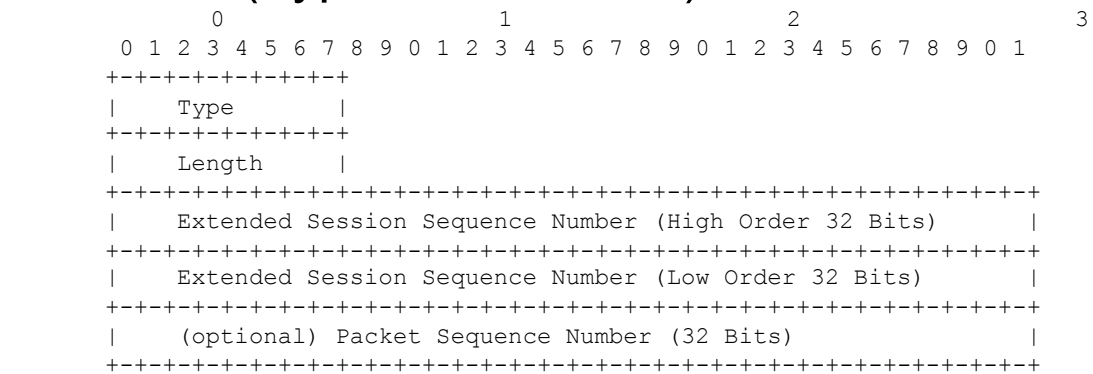
- IIH
  - ADJ flaps in broadcast by replying empty neighbor list (TLV 6)
- SNP
  - Can mount DoS attacks by sending old CSNP/PSNP packets

  ✓The above two are most important and easy to protect
- LSP
  - Already protected from intra session replay attacks with header seq. no
  - But still vulnerable for inter session attacks
    - Existing recovery applicable in some cases

Solution

- ESN TLV
  - IIH
  - SNPs
  - LSPs (for inter-session replay prevention)

ESN TLV (Type – IANA TBD)



ESSN ➔ Starts with non-zero and incremented in PSN wrap scenario, session refresh, cold restarts etc..

PSN ➔ Incremented per packet (only applicable for IIH and SNPs)

Further details in:

http://tools.ietf.org/html/draft-chunduri-isis-extended-sequence-no-tlv-03

Partial Deployment

- Gradual deployment in the network without requiring a flag day
- Can be deployed for the links in a certain area of the network where the maximum security mechanism is needed, or it can be deployed for the entire network

IIH & SNPs:

- When the router software is upgraded to include this feature, one can configure the IS-IS to 'send' the ESN TLV
- When all the routers attached to the link or links have been upgraded with this feature, network operators can start to configure 'verify' on the IS-IS interfaces for all the routers sharing the same link (s)

Partial Deployment (Contd.)

LSPs

- **This feature has to be done for the entire IS-IS area or levels with in the same flooding domain.**
- The deployment and upgrade to support ESN TLV
  - can be gradual and
  - from node to node.
- Provision ‘Send’ in the network. No 'verify' is enabled until all the routers in the entire IS-IS area/level or entire network is upgraded
- In the face of active attack - it is recommended that provisioning of 'verify' SHOULD be done in a timely fashion by the network operators from first node to the last node (with out much delay).

Next Steps:

Request for WG adoption..

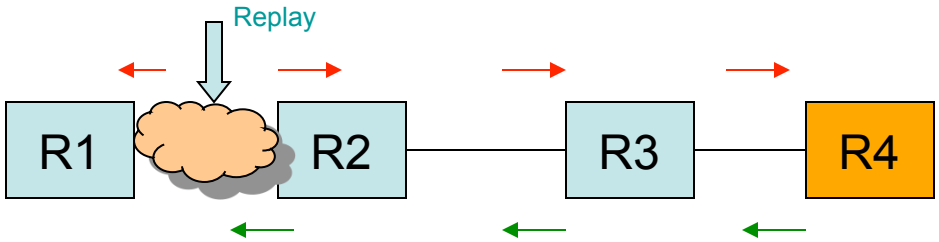
Questions & Comments?

Thank You!

Backup Material

(LSP inter session replay attack)

Inter Session Replays – issues with LSP



- After Restart/upgrade/failure LSP Sequence number get's back to previous value
  - **"if rest of the network has it's old copies" i.e., the nodes come back online before the refresh time**

Existing Recovery

- Once replay reaches to the actual node
  - **it quickly** (?) updates the sequence number and floods
    - Traverse all the way to the actual node, processing in the node, flooding the entire network…

Key Q?

- **Can a node after upgrade/out-of-service brought-in before network age out it's LSPs ?**
- **Can an accepted reply is not being processed before it get's the updated LSP ?**
  - Think of FC timers on all the nodes where replay is being processed
- Damage depends on
  - Change in the LSP content in the replays
  - This can potentially happen to any node and any LSP fragment
  - And every time all nodes are impacted

Discussed in Section 2.3.1 of http://tools.ietf.org/html/draft-chunduri-karp-is-is-gap-analysis-03