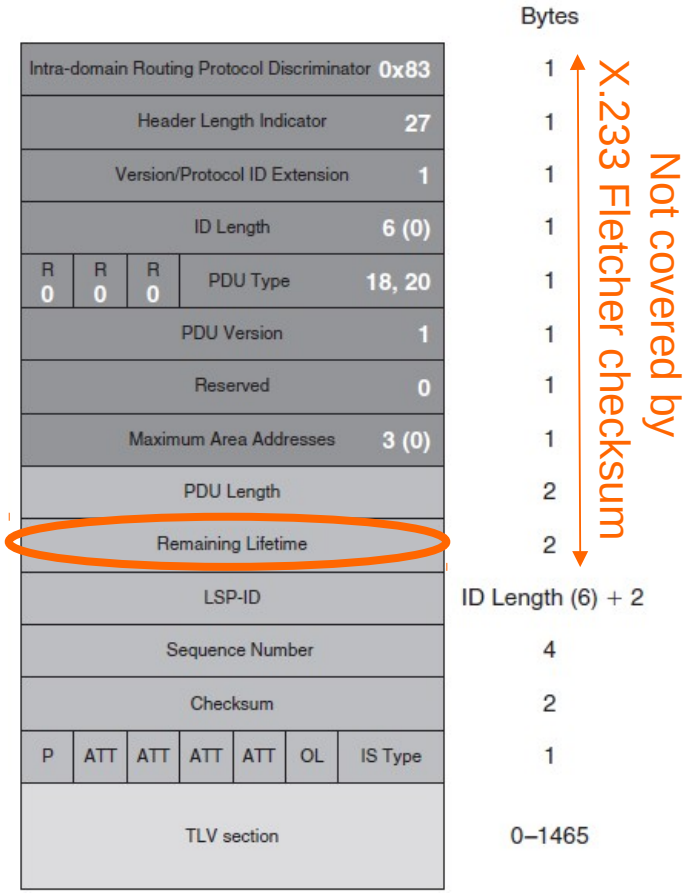
IS-IS LSP lifetime corruption Problem Statement

draft-decraene-isis-lsp-lifetime-problem-statement-00

Bruno Decraene	Orange
Christof Schmitz	Orange

LSP lifetime is not protected from corruption

- LSP lifetime is not protected
  - not by the Fletcher checksum
    - ISO spec
  - not by cryptographic checksum
    - TLV 10 defined in RFC 5304
- Hence LSP lifetime may be corrupted
  - error during transmission
    - line, line cards, switch matrix, RP
  - deliberate modification
    - by an attacker



Consequences (1): lifetime set to zero

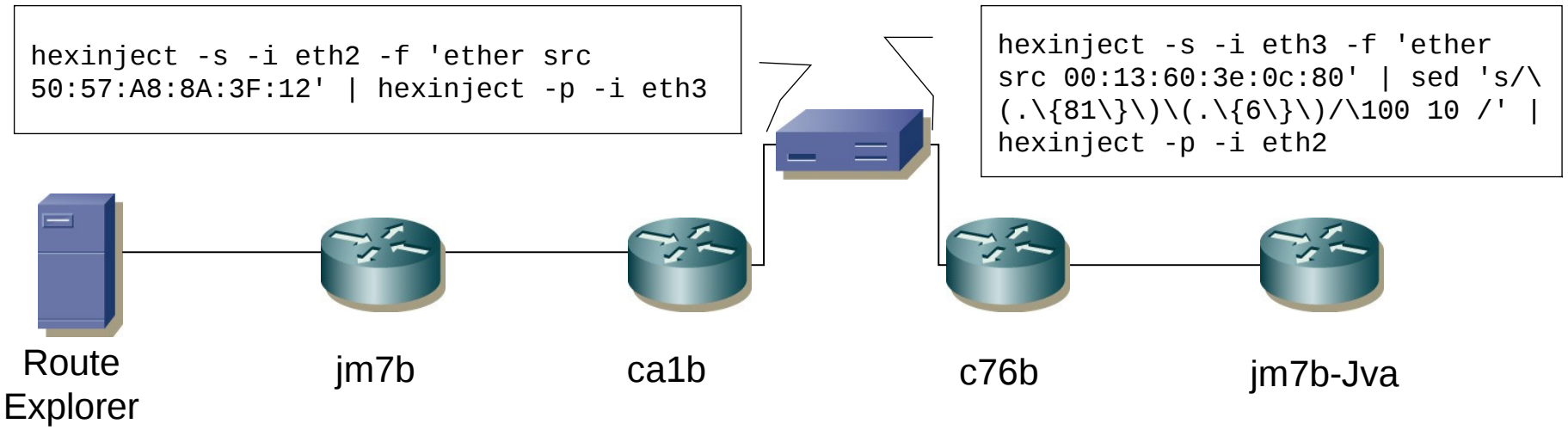
- Case 1: no cryptographic authentication
  - LSP accepted and processed as if lifetime has expired
  - Replace any non-expired version of the same LSP in the LSPDB
  - Purge flooded network wide → impact on topology/network
  - Re-origination (sequence number++) → impact on topology/network
  - If the corruption is systematic, the process cycles forever.
- Case 2: cryptographic authentication used
  - RFC 5304 & 6233 covered this issue by restricting the TLV code allowed in a purge.
  - LSP with zero lifetime and “regular” TLV are ignored
- Summary: cryptographic authentication is required
  - including for error detection i.e. no attackers inside the infrastructure
  - we are good

Consequences (2): lifetime set to non-zero

- LSP with corrupted lifetime is accepted as valid
  - Cryptographic authentication does not provide any additional protection.
- If the lifetime is corrupted to a (very) small value, the effect is virtually equivalent to a purge.
  - Cf previous slide
- RFC 5304 (crypto) is not effective
  - in "prevent[ing] a hostile system from receiving an LSP, setting the Remaining Lifetime field to [a small value], and flooding it, thereby initiating a purge without knowing the authentication password“
- Summary: Houston, we've had a problem here.

Lab testing

- IS-IS MD5 authentication enabled on LSPs.
- Corrupting all ethernet packets from c76b to ca1b
  - setting lifetime to 0x10 (bytes 28 & 29)
  - we used the hexinject tool
- 1 interface flap → 1 LSP corrupted
- → generates 103 LSPs in less than 30mn.
  - In a very small and simple network topology.



Consequences (3): network wide

- If the corruption is systematic on a given link, all LSPs flooded through that link are affected, creating flooding storm for multiple LSPs with severe impact in the network.

Next steps

- IGP MUST work.
  - All services and many protocols relies on it.
- Can be seen as a security issue
  - not previously documented (RFC 5304, draft-ietf-karp-isis-analysis)
- Calling for a protocol extension
  - Preferably, incrementally deployable with incremental benefit.

Comments welcomed

Thank you