Survey of Existing Routing Authentication Methods

Brian Weis

Survey of Existing Routing Authentication Methods

- Considered only the protocols listed in the draft charter:
  - BGP, LDP, PCE
  - OSPF, OSPFv3
  - ISIS
  - RIPv2, RIPng
  - MSDP,
  - PIM (SM and DM),
  - RSVP-TE
  - BFD

Security Properties

- Looked at the properties described in the charter: *message authentication*, *packet integrity*, and *denial of service*
  - All have the same *message authentication* property: only a legitimate peer (sharing a key) can create a valid Integrity Check Value (ICV)
  - The *packet integrity* results varies depending on the type of Message Authentication Code (MAC) used (e.g., SHA1-HMAC)
  - The *denial of service* property takes into consideration replay protection
    - Not addressing DoS issues resulting from the additional overhead of computing or verifying a MAC.
    - Not taking into consideration non-cryptographic anti-DoS issues that may be useful (e.g., GTSM “TTL Hack”)

BGP/LDP/PCE

Security RFC or I-D	Packet Integrity	Denial of Service	See Also
RFC 2385	ICV field & keyed MD5	Partial protection from a non-peer: TCP sequence number checking protects against spoofing except if both wrap concurrently and result in being valid within the same window	RFC 4272
TCP-AO I-Ds	ICV field & HMAC-SHA1, AES-CMAC	Good protection: TCP sequence number checking & choose a new key every time the seq. num wraps	

OSPF

Security RFC or I-D	Packet Integrity	Denial of Service
RFC 2328 (OSPFv2)	ICV field & keyed MD5	Partial protection: Neighbor sequence number checking, except when the sequence number wraps or set to 0. Same seq. number accepted more than once?
draft-ietf-ospf-hmac-sha (OSPFv2)	ICV field & HMAC-SHA (SHA-1 through SHA-512)	(Same as RFC 2328)
RFC 5340, RFC 4552 (OSPFv3)	ESP or AH with HMAC-SHA1 or better	No replay protection when manual keys used.

ISIS

Security RFC or I-D	Packet Integrity	Denial of Service
RFC 5304	ICV field & HMAC-MD5	Poor protection: no sequence number or time value included in frame
RFC 5310	ICV field & HMAC-SHA (SHA-1 through SHA-512)	(Same as RFC 5304)

RIP

Security RFC or I-D	Packet Integrity	Denial of Service
RFC 4822 (RIPv2)	ICV field & Keyed MD5, HMAC-SHA (SHA-1 through SHA-512)	Partial protection: The sequence number “0” may be sent by originator at any time (e.g., at reboot), therefore it can be replayed.
draft-ietf-rip-ripng-03 (RIPng)	(Same as RIPv2?)	(Same as RIPv2?)

MSDP & PIM

Security RFC or I-D	Packet Integrity	Denial of Service	See Also
RFC 3618 (MSDP)	ICV field & Keyed MD5	No protection?	
RFC 4601 (PIM-SM)	AH (no integrity algorithm specified)	No protection with manual keying of AH	RFC 4609, draft-ietf-pim-sm-linklocal-09
RFC 3973 (PIM-DM)	AH (no integrity algorithm specified)	No protection with manual keying of AH	

RSVP-TE

Security RFC or I-D	Packet Integrity	Denial of Service	See Also
RFC 3209, (RFC 2747)	ICV field & HMAC-MD5, HMAC-SHA1	Counter and Clock-based sequence numbers available. Wrap of counter-based sequence numbers are an issue.	RFC 2205, draft-ietf-tsvwg-rsvp-security-groupkeying

BFD

Security RFC or I-D	Packet Integrity	Denial of Service
draft-ietf-bfd-base	ICV field & Keyed MD5, Meticulous Keyed MD5, Meticulous Keyed SHA1	Partial protection (Keyed MD5), Better protection (Meticulous MD5/ SHA1) However, atacker mau be able to take advantage of a wrapped sequence number

Summary

- Lots of good work is already ongoing, mostly with a focus in updating MAC algorithms
  - But the algorithms differ from protocol to protocol
  - And only some attention is given to algorithm agility
- There seem to be some many semantics around sequence number handling which are not so good
  - It would be a good idea to address these issues with a consistent method or set of semantics