802.1AS Security

Rodney Cummings, Rob Mixer, Sundeep Chandhoke
National Instruments

Agenda

- Overview of security work in IEEE 1588
- What problems do we want to solve for 802.1AS?

Overview of 1588 Work

IEEE 1588 Security: History

- Security Subcommittee as part of 1588-Rev project
  - Security is an optional feature of 1588
- Started with analysis from IETF TICTOC, RFC 7384
  - https://tools.ietf.org/html/rfc7384
- 1588 Security created requirements from that
  - Uploaded to http://www.ieee802.org/1/files/public/docs2015/as-cummings-ieee-1588-security-requirements-0115-v41.pdf
- 1588 'standing document' contains assumptions
  - Overview in these slides; For details, join 1588
    - https://ieee-sa.centraldesktop.com/1588public

RFC 7384: Summary of Threats

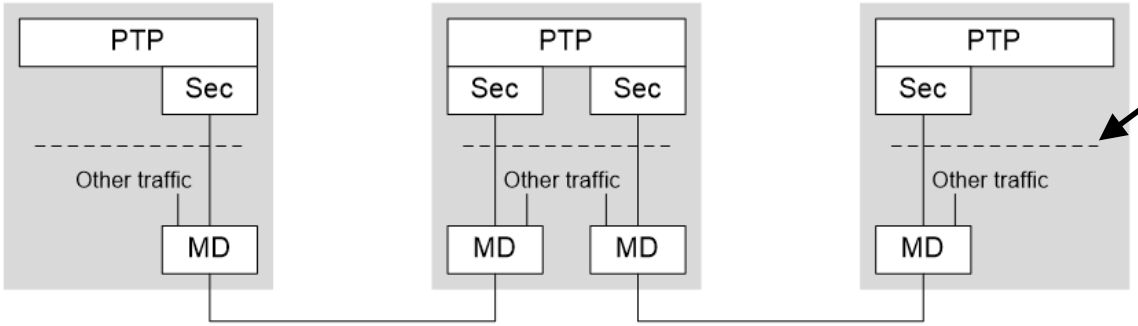
Threat	In RFC 7384	Examples of mitigation
Manipulation	3.2.1, 5.2, 5.9	Integrity protection, Redundant paths
Spoofing	3.2.2, 5.1, 5.3, 5.4	Authentication & authorization
Replay attack	3.2.3, 5.5, 7.5.2	Sequence numbering
Rogue master attack	3.2.4, 5.1, 5.4	Authentication & authorization
Packet removal	3.2.5, 5.9	Redundant paths
Packet delay manipulation	3.2.6, 5.8, 5.9	Redundant paths
L2/L3 DOS attack (non-time)	3.2.7	(outside 1588 scope)
Crypt performance attack	3.2.8	(outside 1588 scope)
Time protocol DOS attack	3.2.9, 5.1, 5.4	Authentication & authorization
Source attack (e.g. GPS)	3.2.10	Redundant GMs

RFC 7384: Summary of Other Issues

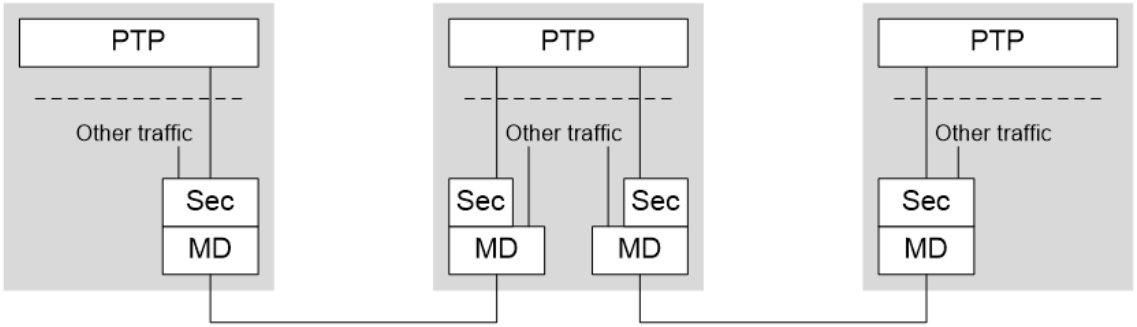
- Key freshness, unicast or multicast (5.6)
- Performance (5.7)
  - No degradation in quality of time
  - Practical impact on computation load, storage, bandwidth, etc
- Confidentiality (5.8): Not a major concern with time sync
- Mix of secured and unsecured clocks (5.10)
- Some security mechanisms need synced time (7.5)
  - This can be a catch-22
- Key management: Declared to be out-of-scope (8)

IEEE 1588 Standing Doc: Overview

- Solutions categorized into four 'prongs'
  - Prong A: PTP Integrated



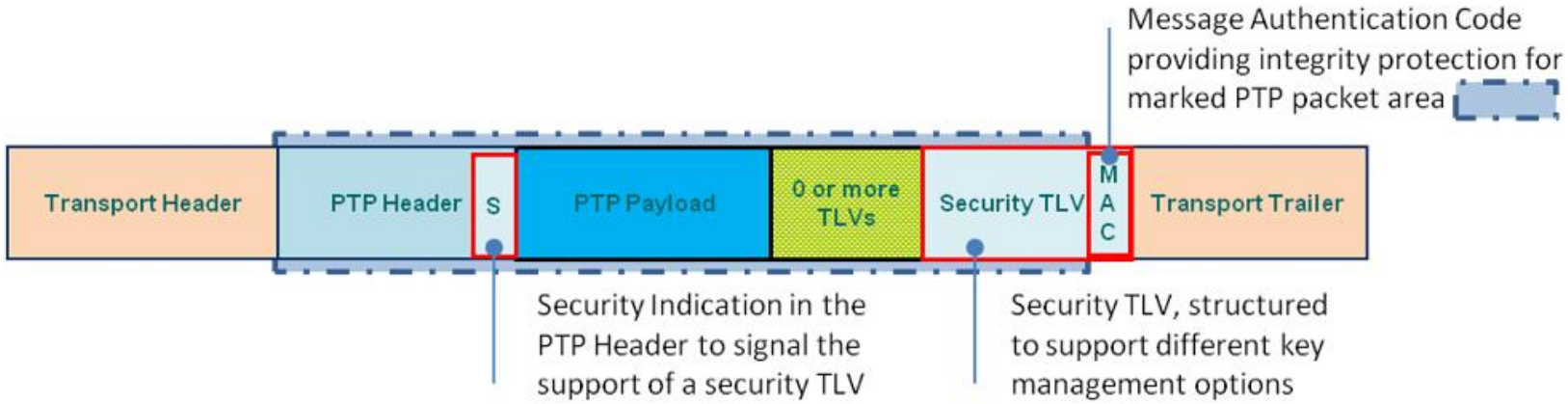
  - Prong B: PTP External Transport (e.g. IPSec, MACSec)



  - Prong C: Architectural Guidance (e.g. redundant paths/GMs)
  - Prong D: Monitoring and Management Guidance

IEEE 1588 Standing Doc: Prong A

- Assumption: Key management protocol selected by industry/application, for non-PTP packets
  - Power using GDOI (RFC 6407)
  - Telecom/Enterprise using TESLA (RFC 4082)
- 1588 specifies a Security TLV for its messages



  - 1588 uses the keys, but distribution is outside its scope