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

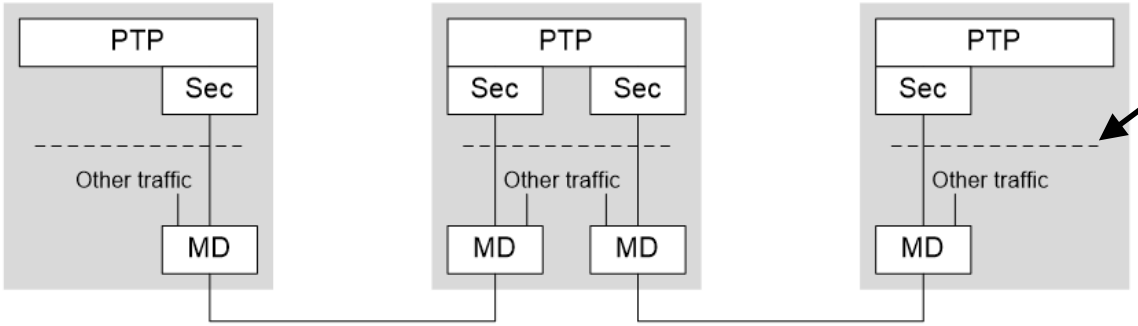
Threat	In RFC 7384	Examples of mitigation
Manipulation	3.2.1, 5.2, 5.9	Integrity protection, Redundant paths
Spoofing	3.2.2, 5.1, 5.3, 5.4	Authentication & authorization
Replay attack	3.2.3, 5.5, 7.5.2	Sequence numbering
Rogue master attack	3.2.4, 5.1, 5.4	Authentication & authorization
Packet removal	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

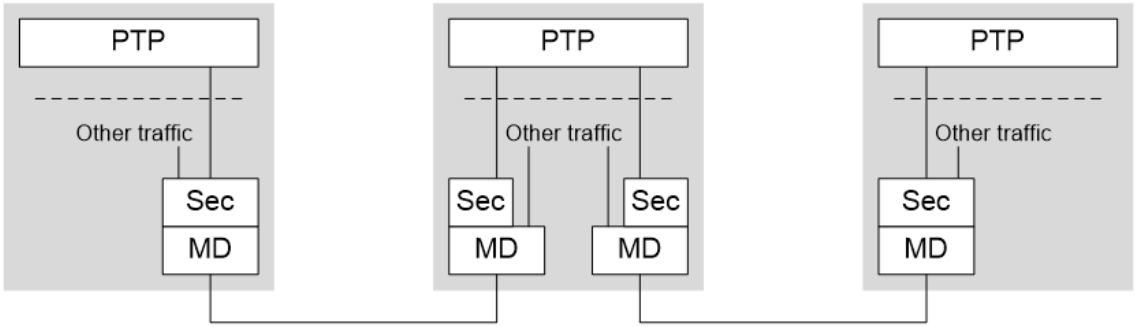
- Key freshness, unicast or multicast (5.6)
- Performance (5.7)
  - No degradation in quality of time
  - Practical impact on computation load, storage, bandwidth, etc
- Confidentiality (5.8): Not a major concern with time sync
- Mix of secured and unsecured clocks (5.10)
- Some security mechanisms need 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



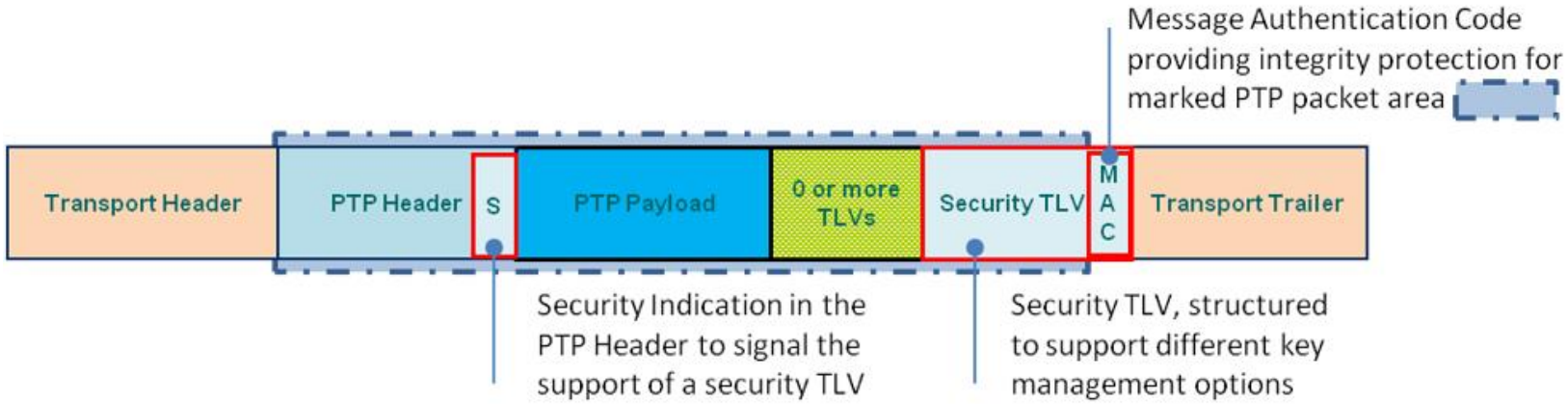
  - Prong B: PTP External Transport (e.g. IPSec, MACSec)



  - 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

802.1AS Discussion

What Problems to Solve for 802.1AS?

- Goal: Fill in subsequent slides as we discuss
  - Answer questions, add/delete/change text, ...

- Defer discussion of specific solutions / mechanisms
- Ideally apply to other aspects of TSN (e.g. streams)
  - Defer this discussion as well

- Possible guiding question: How is 802.1AS different?
  - Helps to decide what we are not doing

How Is 802.1AS Different?

- Layer-2 typically excludes attacks from the Internet
  - Nevertheless, local network is not always physically secure
    - E.g. Disgruntled employee installs MITM/DOS device
- 802.1AS uses subset of 1588 options:
  BC, P2P, pDelay, multiple slaves per GM
  - Narrows solution space
  - More to secure: Each master-slave exchange
    - RFC 7384 did not focus on this 'hop-by-hop'

How Is 802.1AS Different?

- Some 802.1AS applications use fixed configuration
  - Topology fixed, GMs fixed, paths fixed, port states fixed...
    - Describe use of static FDB filters, ACLs, ... ?
  - 2014 Automotive Ethernet presentation
    - http://standards.ieee.org/events/automotive/2014/19_Ethernet_Car_Security.pdf
- Use rate-limiting for 802.1AS messages?

How Is 802.1AS Different?

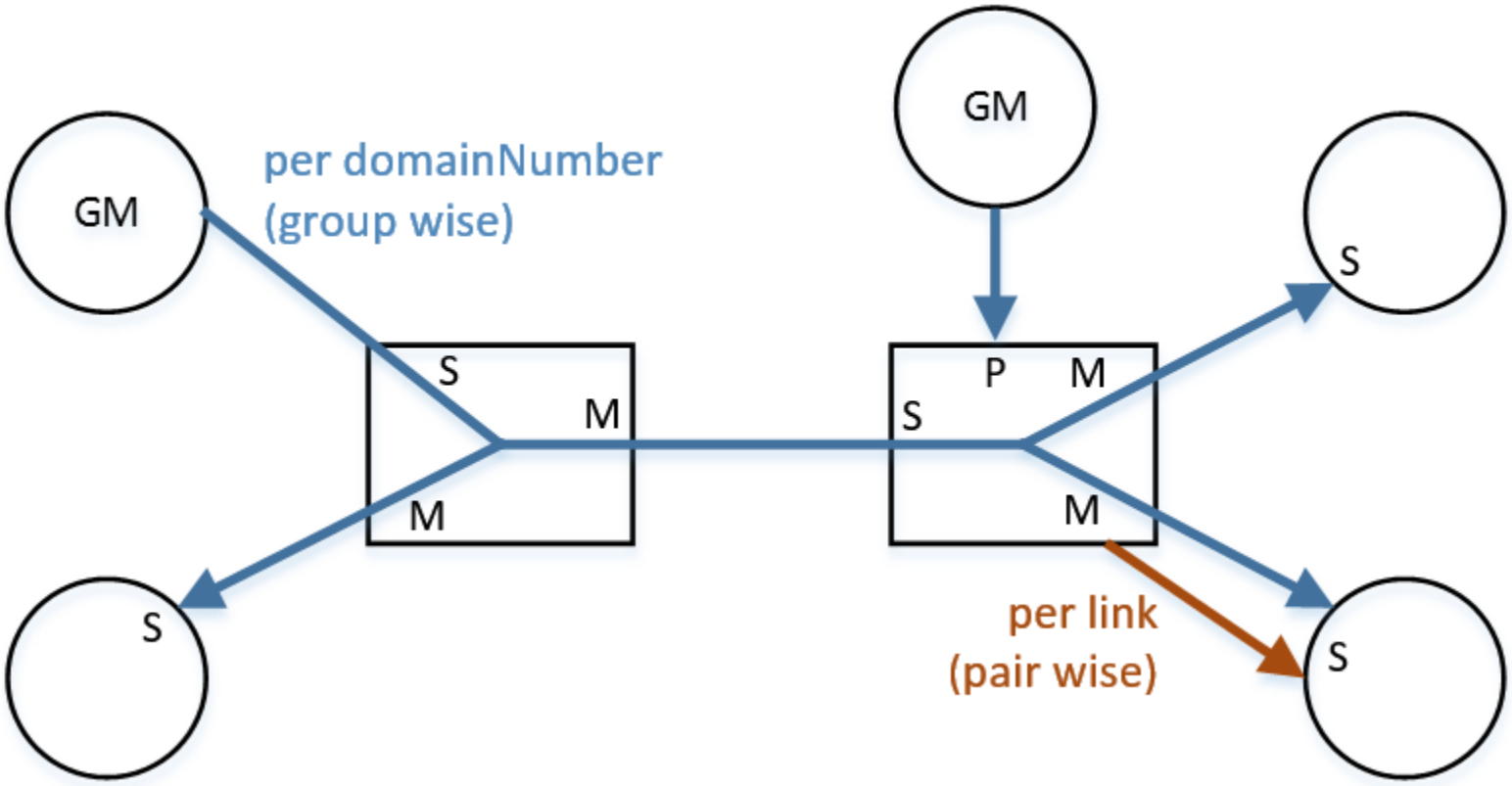
- 802.1AS applications can use redundancy
  - Describe how this mitigates many attacks?
- 802.1AS Working Clock mitigates time source attack?
  - Uses local oscillator of GM, so GPS attack is not relevant

How Is 802.1AS Different?

- Assume security is all-or-nothing option?
  - No mix of secured and unsecured in 802.1AS domain
- Prioritize subtle attacks over complete loss of time?
  - Many cyber-physical apps can handle complete loss
  - Prioritize spoofing/manipulation over DOS?

How Is 802.1AS Different?

- Is key association per domainNumber, or link (master/slave pair)?



How Is 802.1AS Different?

- Key management: Protocol to generate/distribute/update keys (e.g. 802.1X, GDOI)
- 802.1AS supports two models
  - Plug&play (BMCA, PCR4Sync)
  - Centrally managed
- 802.1AS key mgmt. approach works for both models?
- Select a single key management protocol?
  - Excludes use of 802.1AS in industries that use another
- Create mechanisms to negotiate key mgmt. protocol?
  - This would presumably apply to plug&play only

How Is 802.1AS Different?

- TBD

Other Items to Capture

- TBD

Other Items to Capture

- TBD