Secure Enterprise Data Center Profile for IEEE 1588 Precision Time Protocol (PTP)

Doug Arnold, Ph.D.

Meinberg

Steve Guendert, Ph.D.

IBM

Agenda

- Financial regulations driving PTP adoption/interest
- “Data Center”
- IEEE 1588 PTP and security to date
- Requirements
- Recommendations

Financial regulations driving PTP adoption

- U.S. FINRA (Financial Industry Regulatory Authority)
  - 2016: FINRA Rule 4590 and SEC Regulatory Notice 16-23
  - Effective 2018:
    - **Requires synchronization of equipment to within 50ms of NIST(UTC)**
    - Also requires audit log capability to prove compliance
    - Log of all times when clocks are synchronized and the results
    - Includes notice of clock drift outside required tolerance
- EU: ESMA (European Securities and Markets Authority)
  - MiFID II clock synchronization requirements are more stringent than the latest U.S. requirements
    - Max divergence from UTC of 100 microseconds
  - Went into effect in January 2018
- Many network operators implement measurement systems which requires a much tighter timing accuracy

“Data Center”

- Business continuity/resiliency and disaster recovery planning are a fact of life for the enterprise end users we are discussing here
- Multi site, geographically separated data center enterprise architectures are the norm.
  - The financial/banking enterprises have many government imposed regulations mandating this
    - Data replication, minimum distance between sites, etc
- For purposes of our work, we need to account for these facts as well

IEEE 1588 PTP and security to date

- Historically, PTP security has been an afterthought
  - Not included in any published PTP Profile
- Historically, PTP security has been “optional”
  - IEEE 1588 PTP V2 (2008) Annex K
  - Annex K not widely implemented
  - Security weaknesses identified in Annex K
- IEEE 1588 PTP v2.1 (2019) addresses some of the Annex K faults
  - “Four pronged approach” good, but security is still “optional”
  - Many things “outside the scope of this standard”

The problem with this approach

- Enterprise Data Center end users, especially in the finance/banking industry never view security as optional
  - Many papers written on PTP vulnerabilities dues to lack of security
  - Too risky to implement PTP
  - What's worse, a fine from the government or a security issue that makes the press?
- These same end users routinely ask for "best practices", or "reference architectures"
- Development of a new PTP profile for "security" is a good step to provide those best practices/reference architectures and to meet the requirement for PTP security that is fairly simple to implement

Additional Data Center Requirements

- End customers are already implementing key exchange mechanisms for other purposes, and would like to limit the number of mechanisms which they have to support
- Some PTP slaves will be software apps running on standard server hardware

PTP secure enterprise data center profile

- We are recommending going forward with a new draft IETF RFC for this profile
- The profile will indicate which “optional” PTP items will be implemented as part of the profile
- The profile will indicate which items are preferable for security purposes. Possible choices include:
  - i.e. Peer to Peer delay better than End to end for security purposes
  - Use of delayed authentication (TESLA)
  - Two step (not one step)
  - Boundary Clocks, not Transparent Clocks

PTP secure enterprise data center profile

- We are recommending going forward with a new draft IETF RFC for this profile
- The profile will indicate which “optional” PTP items will be implemented as part of the profile
- The profile will indicate which items are preferable for security purposes. Possible choices include:
  - i.e. Peer to Peer delay better than End to end for security purposes
  - Use of delayed authentication (TESLA)
  - Two step (not one step)
  - Boundary Clocks, not Transparent Clocks

Please contact the authors if you are interested in participating

Doug.arnold@meinberg.de

Steve.Guendert@ibm.com