NTS for PTP

Is this worth doing?
Should the NTP WG do it?

Doug Arnold

2021-06-09

Is this worth doing?

First, PTP is important

- Currently used in critical infrastructure
  - Power grids
  - Mobile communications
  - Broadcast/streaming
  - Finance
  - Manufacturing
  - Vehicular technology (under development at least)
- Millions of PTP appliances currently in the field
- Billions of dollars (or euros, or pick your currency) invested in development of PTP capable equipment by manufacturers

Why NTS for PTP?

- PTP could be secured by IPsec or MACsec, but
  - Easier for network operators to set up IPsec or MACsec associations using a PTP aware key management protocol
- PTP could be secured using GDOI (RFC 6407)
  - Group key approach
    - Works well with multicast protocols
    - Works with Boundary Clocks and Transparent Clocks
  - Good option if GDOI is being used with other protocols in the application
    - For example, in the power grid
- PTP could be secured using an expansion of NTS
  - PTP Grandmasters are usually also NTP servers
  - PTP networks usually also contain NTP

Efficient for equipment designers and network operators

What would NTS for PTP mitigate?

- Replay attacks
- Grandmaster impersonation
- Some man in the middle attacks
  - PTP message manipulation by non-PTP aware switches

- Mitigation for these attacks are out of scope
  - DOS attacks
  - Delay attacks
  - GNSS spoofing
  - PTP device taken over

Why the NTP Working Group?

- IETF has the most network security expertise
  - Sorely lacking in IEEE 1588
  - Easier to get review by cryptography gurus
- NTS is an NTP WG standard
  - Keep NTS for NTP and NTS for PTP coherent and consistent

Please review NTS for PTP proposals

https://datatracker.ietf.org/doc/draft-langer-ntp-nts-for-ptp/

- Provides support for all PTP communication modes
  - Multicast
  - Mixed multicast/unicast
  - Unicast

https://datatracker.ietf.org/doc/draft-gerstung-nts4uptp/

- Supports unicast only, but
  - Designed to be as similar to NTS for NTP as possible
  - Other modes could be added later or supported by GDOI

Conclusions

- NTS for PTP is worth doing
- The NTP working group is the right place for it
- NTS for PTP could be:
  1. Based on one of the two current proposals
  2. A combination of those two proposals
  3. A new proposal