Network Time Security for PTP

Martin Langer, Ostfalia University of Applied Sciences
Rainer Bermbach, Ostfalia University of Applied Sciences
Douglas Arnold, Meinberg-USA

Need for Secure PTP

- Network operators and PTP Profile standards committees are asking for a secure version of PTP

- IEEE 1588-2019 features a message extension for that including an ICV
  - AUTHENTICATION TLV
  - **Detailed description of automated key management mechanisms not included**

- Key management mechanisms mentioned in IEEE 1588-2019
  - TESLA
  - GDOI

Why NTS should be an option for PTP

- Time server appliances include both NTP and PTP
  - Manufacturers are going to implement NTS for NTP
  - Implementation is efficient if NTS is also the key management for PTP

- Networks already include TLS key management
  - For https and other protocols
  - Many networks with PTP also have NTP running
  - “please don’t make me deploy and maintain another key management protocol” --- Network operator

PTP is not NTP

- Multicast is the most common mode for PTP
- Most networks include on path support (switches and routers participate in protocol)
  - **Major security challenge**
- PTP deployments are usually in small private networks
- Message rates are high
  - For example, 128 Sync messages/second
- Unicast PTP is client-server mode and most like NTP
  - But includes a negotiation phase before synchronization starts
  - PTP Grandmasters keep state on devices they synchronize

NTS for PTP

- NTS for Multicast PTP
  - All nodes in a “group” get a shared group key from NTS-KE server
  - Similar to GDOI, but based on TLS rather than IPsec
    - (Something like this might be needed for ntpv5 if on path support becomes important)
- NTS for Unicast PTP
  - Operates more like NTS for NTP than the multicast group key approach
  - Unicast requester sends security information, so-called ticket, to unicast grantor during negotiation
    - Following unicast communication uses key from ticket
    - Ticket optained from NTS-KE server
- Cyclic update for all security information at NTS-KE server
  - For multicast and unicast

NTS for PTP standards work

- Currently being discussed in IEEE 1588 Security subcommittee
  - Chaired by Karen O'Donoghue
- We would like to move it here and make it (eventually) an IETF RFC
  - More security expertise in IETF than in IEEE 1588
  - This working group familiar with NTS
  - Keep NTS for NTP and NTS for PTP coordinated