Notes from Discussion of 802.1AS Security

Rodney Cummings
National Instruments

Introduction

The following slides capture the discussion on 802.1AS security that occurred in the November 802.1 meeting in Dallas with TSN and Security task groups.

This discussion occurred after the following presentation:

http://www.ieee802.org/1/files/public/docs2015/as-cummings-security-1115-v2.pdf

Notes on 802.1AS Security

- Should we work on security for other TSN protocols (e.g. SRP, stream data)?
  - Time sync has unique problems (e.g. delay attack)
  - Solutions for time sync seem likely to apply for other traffic
  - To avoid 'boiling the ocean', let's focus on 802.1AS first
- Regarding 1588 Security TLV proposal:
  Security experts in 802.1 view location of security at the end of the frame as adding unnecessary delay

Notes on 802.1AS Security

- Agreement that the subset of 1588 options in 802.1AS enables more focused solutions for security
- Security will be an optional feature for 802.1AS
- 802.1AS is required for all bridges/routers in its domain
  - 802.1AS threat model assumes that integrity is applied along the path from GM to slave(s)
  - Trust model of MACsec matches the trust model of 802.1AS

Notes on 802.1AS Security

- We want security that is integrated with the network
  - Not sitting above
  - In 1588 terms, assume a Prong B solution for 802.1AS
- Support for 802.1X is assumed
- If you encrypt, you get integrity and confidentiality
- Authentication of the GM will be evaluated
- You can use a group key, or use pairwise keys with transitive trust
  - This part is easy... just decide what you want to do

Notes on 802.1AS Security

- The hard part is mitigating a fake GM that is internal
  - E.g. Fake GM has the group key
  - TESLA resolves this sort of problem, but it has drawbacks
  - If residence time can be longer, we can solve this
    - That would hurt 802.1AS accuracy, so we cannot go that way
  - Pragmatic approach may be to monitor time down the line
  - Some 802.1AS applications are 'fixed' (e.g. automotive)
    - No dynamic protocol selects the GM or its path
    - Enables filtering from any port that is not the fixed GM

Notes on 802.1AS Security

- For fixed applications, 802.1AR enables transfer of credentials with an associated identity
  - Without the installation of passwords
  - E.g. Replacing a module in a car

Notes on 802.1AS Security

- For future 802.1 face-to-face meetings, we agreed to add 802.1AS as a topic for the Security meeting
  - Task group chairs will work out overlap with TSN topics
  - Goal is draft text for security in 802.1AS
  - We will share our work with 1588 as we go