Security Requirements of Time Synchronization Protocols in Packet Switched Networks

draft-ietf-tictoc-security-requirements-04

Tal Mizrahi
Marvell

IETF Meeting 86, March 2013

Main Topics Discussed in this Draft

- **Threat analysis.**
- **Security requirements.**
- **Additional security implications.**

Section	Requirement	Type
5.1	Authentication & authorization of sender.	MUST
	Authentication & authorization of master.	MUST
	Recursive authentication & authorization.	MUST
	Authentication of slaves.	MAY
	PTP: Authentication of TCs by master.	MAY
	PTP: Authentication & authorization of Announce messages.	MUST
	PTP: Authentication & authorization of Management messages.	MUST
	PTP: Authentication & authorization of Signaling messages.	MAY
5.2	Integrity protection.	MUST
	PTP: hop-by-hop integrity Protection.	MUST
	PTP: end-to-end integrity Protection.	SHOULD
5.3	Protection against DoS attacks.	SHOULD
5.4	Replay protection.	MUST
5.5	Key freshness.	MUST
	Security association.	SHOULD
	Unicast and multicast associations.	SHOULD
5.6	Performance: no degradation in quality of time transfer.	MUST
	Performance: computation load.	SHOULD
	Performance: storage, bandwidth.	SHOULD
5.7	Confidentiality protection.	MAY
5.8	Protection against delay and interception attacks.	SHOULD
5.9	Secure mode.	MUST
	Hybrid mode.	MAY

History of this Draft

- **Oct 2011 – 1st draft**
- **Nov 2011 – accepted as WG document**
- **Feb 2013 – current draft**
- **Feb 2013 – WG last call**

- **What happened since the previous draft?**
  - A lot of feedback from WG.
  - New section “Requirement Levels”
    - Explains the factors that affect the choice of the requirement levels (MUST/SHOULD/…).
  - For each requirement – added a “Requirement Level” subsection.

Next Steps

- **Currently in WG last call.**
- **Proceed to IETF last call.**