TICTOC Security Requirements

draft-ietf-tictoc-security-requirements-03

Tal Mizrahi
Marvell

IETF Meeting 85, November 2012

Main Topics Discussed in this Draft

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

Section	Requirement	Type
4.1	Authentication of sender.	MUST
	Authentication of master.	MUST
	Recursive authentication.	MUST
	Authentication of slaves.	SHOULD
	PTP: Authentication of TCs.	SHOULD
	PTP: Authentication of Announce Messages.	SHOULD
4.2	Integrity protection.	MUST
	PTP: hop-by-hop integrity Protection.	MUST
	PTP: end-to-end integrity Protection.	SHOULD
4.3	Protection against DoS attacks.	MUST
4.4	Replay protection.	MUST
4.5	Security association.	SHOULD
	Unicast and multicast associations.	SHOULD
	Key freshness.	MUST
4.6	Performance: no degradation in quality of time transfer.	MUST
	Performance: lightweight.	SHOULD
	Performance: storage, bandwidth.	MUST
4.7	Confidentiality protection.	MAY
4.8	Protection against delay attacks.	MAY
4.9	Secure mode.	MUST
	Hybrid mode.	MAY

History of this Draft

- **Oct 2011 – 1st draft**
- **Nov 2011 – accepted as WG document**
- **Sep 2012 – current draft**

- **What happened since the previous draft?**
  - Various fixes following feedback from WG.

Next Steps

- **Awaiting comments from additional reviewers.**
- **Proceed to WG last call.**