TICTOC Security Requirements

draft-ietf-tictoc-security-requirements-01

Authors: Tal Mizrahi and Karen O'Donoghue

IETF Meeting 83, March 2012

History of this Draft

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

- **What happened since the previous draft?**
  - Typo fixes, editorial changes.
  - Added subsection about mixing secured and unsecured nodes.

Document Overview

- **Section 3 – Security Threats**
- **Section 4 – Security Requirements**
- **Section 5 – Summary of requirements**
- **Section 6 – Additional security implications**
- **Section 7 – Issues for Further Discussion**

Security Threats

- **Packet Interception and manipulation**
- **Spoofing**
- **Replay attack**
- **Rogue master attack**
- **Packet Interception and Removal**
- **Packet delay manipulation**
- **Cryptographic performance attacks**
- **DoS Attacks**
- **Time Source Spoofing**

Security Requirments – Summary

Section	Requirement	Type
4.1	Authentication of sender.	MUST
	Authentication of master.	MUST
	Proventication.	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

Security Requirments – Summary (2)

Section	Requirement	Type
4.5	Security association.	MUST
	Unicast and multicast associations.	MUST
	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

Additional Security Implications

- **What external security practices impact the security and performance of time keeping? (and what can be done to mitigate these impacts?)**
- **What are the security impacts of time synchronization protocol practices? (e.g. on-the-fly modification of timestamps)**
- **What are the dependencies between other security services and time synchronization?**

Next Steps

- **Needs further work.**
  - Security requirements need some beefing up.
  - Add some discussion about existing security solutions, and existing related documents.
  - “Additional Security Implications” section.
  - …
- **Need comments and feedback from the WG.**