TICTOC Security Requirements

draft-ietf-tictoc-security-requirements-02

Authors: Tal Mizrahi and Karen O'Donoghue

IETF Meeting 84, July 2012

History of this Draft

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

- **What happened since the previous draft?**
  - Various fixes following feedback from WG.
  - Added threat model (Section 3.1).
  - Added “Additional Security Implications” (Section 6).

Threat Model

- **Internal vs. external.**
- **Man In The Middle (MITM) vs. Injector.**

Attack	Impact			Attacker Type			
				Internal		External	
	False Time	Accuracy Degrad.	DoS	MITM	Injector	MITM	Injector
Interception and modification	•			•			
Spoofing	•			•	•		
Replay	•			•	•		
Rogue master	•			•	•		
Interception and removal		•		•		•	
Delay manipulation	•			•		•	
L2/L3 DoS			•	•	•	•	•
Cryptographic performance			•	•	•	•	•
Time source spoofing	•			•	•	•	•

Additional Security Implications

- **Informational section.**
- **Does not define requirements.**

- **Main topics discussed:**
  - Security and on-the-fly Timestamping
  - Security and Two-Step Timestamping
  - Intermediate Clocks
  - The Effect of External Security Protocols on Time Synchronization
  - External Security Services Requiring Time Synchronization

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
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

Next Steps

- **Need more comments and feedback from the WG.**
- **Proceed to WG last call.**