TICTOC Security Requirements

draft-mizrahi-tictoc-security-requirements-00

Authors: Tal Mizrahi and Karen O'Donoghue

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

Section 3: 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

Section 5: Requirements Summary

Section	Requirement	Type
4.1	Authentication of Sender	MUST
	Proventication	MUST
	Authentication of Slave	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

Section 5: Requirements Summary (cont.)

Section	Requirement	Type
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

Section 5: Requirements Summary (cont.)

Section	Requirement	Type
4.7	Confidentiality protection	MAY
4.4	Protection against delay attacks	MAY

Section 6: 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?

Section 7: Issues for Further Discussion

- Integrity - end-to-end vs. hop-by-hop.
- Supporting a hybrid network, where some nodes are security enabled and others are not.
- Key Distribution
  - The key distribution is outside the scope of this document.