Security Requirements for P1588

Purpose

This document describes the requirements for the security mechanisms. It will be used to scope and prioritize the efforts of the subcommittee.

Scope

The P1588 Security functionality will be an optional functionality for P1588 conformance.

This requirements document will specify what the solution(s) specified must or should include. Note: It is clear that we will not be able to develop all possible security services in the timeframe provided.

The solution may provide multiple mechanisms and will utilize existing mechanisms where possible.

Once the solution(s) is specified, it is expected that there will be required and optional portions of that solution.

Requirement Descriptions

The base requirements are defined in the below referenced document:

[TICTOC-Security] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", draft-ietf-tictoc-security-requirements (work in progress), October 2013.

Modifications to [TICTOC-Security]

- The requirements in sections 5.2, 5.2.1 and 5.2.2 (see Table 2) will be merged to a single integrity protection requirement. The rationale is that depending on the specific application, in some cases it may be necessary to use hop-by-hop integrity protection, while in other cases end-to-end integrity protection will be used.
- The requirement for protection against delay and removal attacks (section 5.8) will be modified to MUST. This requirement addresses attacks that can be performed by man-in-the-middle attackers, as does the requirement for integrity protection (section 5.2). Hence, to align the requirement levels of these two requirements, the requirement in section 5.8 is modified to a MUST.

Security Threats

Sec.	Threats	P1588

3.2.1	Manipulation	Yes
3.2.2	Spoofing	Yes
3.2.3	Replay attack	Yes
3.2.4	Rogue master attack	Yes
3.2.5	Packet removal	Yes*
3.2.6	Packet delay manipulation	Yes*
3.2.7	L2/L3 DoS attacks	No
3.2.8	Crypt performance attacks	No
3.2.9	Time protocol DoS attacks	Yes
3.2.10	Master time source attack (e.g. GPS spoofing)	Yes*

Table 1 P1588 Security Threats

* These threats can be mitigated by using multiple masters or multiple paths. Thus, the mechanisms that mitigate these threats will not necessarily be addressed in the security subcommittee, but potentially in the architecture subcommittee.

Security Requirements

This following table summarizes the set of requirements from the 1588 security solution. The list is based on Table 2 of [TICTOC-Security], with two additional columns:

- The column 'P1588' defines to what extent the corresponding requirement should be addressed in the current work of the P1588 security subcommittee.
  This column uses three requirement levels: must, should and may.
  Note that the 'P1588' column does not indicate whether the corresponding feature in the IEEE 1588 standard will be required or optional to implementers.
- The column 'Threat' specifies for each requirement which threat it is aimed to prevent. Note that some requirements are mapped to more than one threat, while others are not mapped to any specific threat.

Sec.	Requirement	Threats	IETF Draft	P1588
5.1	Authentication & authorization of sender.	3.2.2 3.2.4	MUST	must
5.1.1	Authentication & authorization of master.	3.2.2 3.2.4	MUST	must
5.1.2	Recursive authentication & authorization.	3.2.2 3.2.4	MUST	must
5.1.3	Authentication of slave only ports.	3.2.9	MAY	may
5.1.4	Authentication of TCs by master.	3.2.9	MAY	may
5.1.5	Authentication & authorization of Announce	3.2.2	MUST	must

	messages.	3.2.4		
5.1.5	Authentication & authorization of Management messages.	3.2.2 3.2.4	MUST	must
5.1.5	Authentication & authorization of Signaling messages.	3.2.2 3.2.4	MAY	may
5.2	Integrity protection.	3.2.1	MUST	must
5.2.1	Hop-by-hop integrity Protection.		MUST	See note[1]
5.2.2	End-to-end integrity Protection.		SHOULD	
5.3	Protection against DoS attacks.	3.2.9	SHOULD	should[2]
5.4	Replay protection.	3.2.3	MUST	must
5.5.1	Key freshness.		MUST	must
5.5.2	Security association.		SHOULD	should
5.5.3	Unicast and multicast associations.		SHOULD	should
5.6	Performance: no degradation in quality of time transfer.		MUST	may
5.6	Performance: computation load.		SHOULD	may
5.6	Performance: storage, bandwidth.		SHOULD	may
5.7	Confidentiality protection.	See note[3]	MAY	may
5.8	Protection against delay and removal attacks.	3.2.6 3.2.5 3.2.1	SHOULD	must[4]
5.9.1	Secure mode.		MUST	must
5.9.2	Hybrid mode.		MAY	should

Table 2 P1588 Security Requirements

[1] These two items will be removed from the next version of the TICTOC document, and merged into a single "Integrity protection" requirement.

[2] This requirement refers to DoS attacks against PTP; it refers neither to L2/L3 DoS attacks, nor to cryptographic performance attacks.

[3] Confidentiality protection may address: (1) Eavesdropping attacks, and (2) Collecting information about the network which may assist in some of the other attacks. Since none of these two attacks are considered a significant threat in the context of PTP, they are not listed in the threat list (Table 1).

[4] The requirement level will also be updated in the TICTOC document to MUST.

Additional Goals

This section provides additional goals that will be used as guidelines during the development of the IEEE 1588 security solution.

1. **Algorithm agility**.
   An important property of security protocols is crypto algorithm agility so that protocols can support multiple cryptographic algorithms (including hash functions) and provide clean, tested transition strategies between algorithms.

   The security mechanism should be defined in a way that enables future migration to new algorithm suites.

2. **Mappings.**
   The security solution(s) should address all the mappings defined in IEEE 1588.