Network Time Security

draft-ietf-ntp-network-time-security-05

draft-ietf-ntp-cms-for-nts-message-00

Dr. Dieter Sibold[1] Kristof Teichel[1] Stephen Röttger[2]

[1]PTB

[2]Google Inc.

IETF 91 (Honolulu), Nov 9 – 14, 2014

Motivation

- Reliability of clocks essential for most security protocols.

  For current example see: this paper by Selvi (2014)

- Existing solutions for NTP/PTP inadequate for various

  reasons. Example: Autokey, see analysis by S. Röttger

Scope

Network Time Security shall provide:

- Authenticity of time servers
- Integrity of synchronization data packets
- Conformity with the TICTOC Security Requirements (described in RFC 7384)
- Support of NTP (unicast and broadcast mode)
- Support of PTP as far as possible

Scope (Continued)

Out of scope:

- Defense against NTP Amplification DDoS attacks

  (to be addressed by NTP BCP)

Not yet considered:

- Security when using NTP pools

Special Requirements

Due to time synchronization context:

- Minimal performance degradation (especially added latencies)
- Consideration of non-crypto attacks, most importantly delay attacks (which degrade synchronization performance)
- UDP-based connections, stateless on server side

Concept Overview

Unicast

- X.509-certificate-based authentication of servers
- Integrity protection of time synchronization packets
  - HMAC-based MAC, using cookie as key
  - Cookie: re-generatable shared secret (inspired by Autokey protocol, but with improved security), unique per association
  - Cookie exchange via asymmetric crypto, using CMS

Broadcast

- Employs a customized version of TESLA (RFC 4082)
- Initial rough synchronization rooted on unicast
- Additional check to counteract an attack based on interaction of synchronization and security
  (fits well for use with IEEE1588/PTP)

Meeting the Requirements (RFC 7384)

Meeting the Requirements: Unicast

- Re-generatable nature of cookie

  $\rightarrow$ server stateless

- Cookie and MAC generation via HMAC (RFC 2104)

  $\rightarrow$ fast (for time sync packets)

- Timing-based attacks can be mitigated by checks on round-trip time (not included in draft yet)

- Explicit replay protection by usage of nonces

Meeting the Requirements

Meeting the Requirements: Broadcast

- TESLA: server does not keep state per client
- MAC calculations via hash functions → fast
- Timing-based (delay) attacks mitigated by disclosure schedule (plus added key check)
- Explicit replay protection by choice of TESLA scheme

Implementation

- Companion document
  - Use of CMS (RFC 5083)

    $\rightarrow$ simplifies handling of cryptographic aspects
  - Details on how to realize encodings of NTS messages

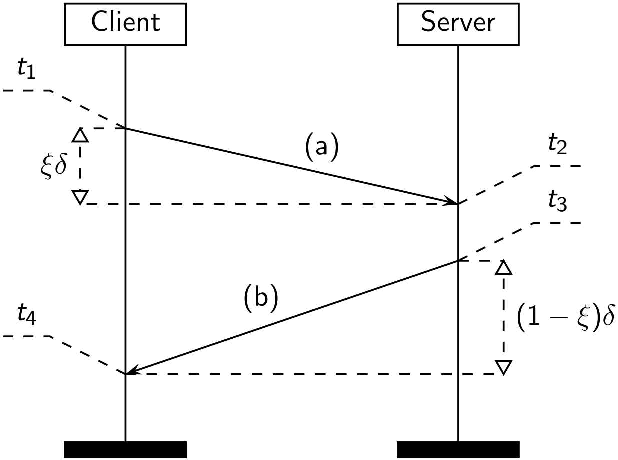
Summary

- Presented security measures for time synchronization protocols compliant with security requirements of time protocols (RFC 7384)
- Comments and guidance from the security area would be appreciated
- Relevant documents:
  - draft-ietf-ntp-network-time-security-05
  - draft-ietf-ntp-cms-for-nts-message-00
  - RFC 7384 (Security Requirements)
  - RFC 4082 (TESLA)

Backup Slides

Unicast

Typical Unicast Time Synchronization Exchange



TESLA (used in Broadcast)

- Server generates one-way chain of keys
- Time divided into intervals
- Each packet gets MAC with key of current interval
- Receiver checks timeliness of packet (key not yet disclosed), then buffers packet for later authentication
- Sender discloses key after pre-scheduled time
- After key is disclosed, receiver checks its validity, then uses it for authentication of past packets

TESLA (used in Broadcast)