Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Network Time Security

draft-ietf-ntp-network-time-security-04

Dr. Dieter Sibold Kristof Teichel Stephen Röttger

IETF 90 (Toronto), July 21-25, 2014

Outline

History

Scope

Major Changes
- From version 02 to 03
- From version 03 to 04

Next steps

History

- **IETF 83:** Presentation of security issues of RFC 5906 (autokey)
- **IETF 84:** Presentation of plan for a new autokey standard
- **IETF 85:** I-D “draft-sibold-autokey-00”
- **IETF 86:** I-D “draft-sibold-autokey-02”
- **IETF 87:** Renaming of I-D and presentation as “draft-ietf-ntp-network-time-security-00”
- **IETF 88/89:** Continuation as “draft-ietf-ntp-network-time-security-*nn*”

Scope

Network Time Security shall provide:

- Authenticity of time servers
- Integrity of synchronization data packets
- Conformity with the TICTOC Security Requirements
- Support of NTP (all of its modes)
- Support of PTP as far as possible (is to be discussed)

Changes from version 02 to 03

- **Altered:**
  - Correction of an error in the formula for the cookie calculation, introduced in the draft's 02 version

Changes from version 03 to 04

- **Altered:**
  - Usage of the client's certificate instead of its public key in the cookie calculation. Enables authorization of the client (suggested by Steven Bellovin)
  - Introduction of a nonce in the server_cert message to mitigate a possible replay attack (suggested by Steven Bellovin)
  - Correlation of the transmit time stamp (t_1) with the nonce in the time_request message in order to avoid a spoofing attack (results from a discussion with T. Mizrahi)

Changes from version 03 to 04 (continued)

- **Altered:**
  - Mitigation of a spoofing attack on the cookie exchange (revealed by K. Teichel via investigation with a model checker)
  - Introduction of message IDs in all messages. (Among other benefits, this mitigates a second attack discovered via model checking.)
  - Introduction of different server seeds for different hash algorithms, for damage control in case of broken hash functions (suggested by S. Röttger)

Changes from Version 03 to 04 (continued)

- **Added:**
  - The delay attack is discussed in the section security considerations
  - Appendix D. to describe usage of TESLA for the broadcast/multicast mode
- **Revised:**
  - Increased minimum requirements on the applied hash algorithm (suggested by Steven Bellovin)
  - Comparison with current TICTOC requirements

Next steps

- **Version 05 (already in progress)**
  - CMS scheme for the message exchanges
  - Merge of association and certification messages
- **Future versions**
  - Consideration of DANE
  - Companion document for the utilized security algorithms (algorithm agility)
  - IANA Considerations
  - Applicability of NTS for PTP? Security for PTP is currently also considered in IEEE's P1588 WG.
- **Review and comments are requested from:**
  - TICTOC Working Group
  - NTP Working Group
  - NTP development team