Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Network Time Security

draft-ietf-ntp-network-time-security-02

Dr. Dieter Sibold Kristof Teichel Stephen Röttger

IETF 89 (London), March 2-7, 2014

Agenda

1. Introduction

2. Changes from version 02

3. 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:** Presentation of results from input and further development as “draft-ietf-ntp-network-time-security-01”

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

Changes

- **Considered:** authorization as well as recursive authentication and authorization
- **Revised:** comparison with TICTOC requirements
- **Split section:** "Protocol Sequence"
  - "Protocol Messages": list of message types
    - generic description
    - realization for NTP
      (important: Internet-Draft "Using NTP Extension Fields without Authentication")
  - "Protocol Sequence": behavior description
    - client's behavior given as chronological sequence
    - server's behavior described as reactions to incoming messages
- **Added:** two appendices
  - list of extensions field types needed for realization of NTS message types in NTP
  - flow diagrams for the client's behavior
- **Altered:** negotiation of cryptographic algorithms during association

Current discussion

- **Comments during last meeting:**
  - About usage of DANE for certificate exchange:
    under consideration
- **Comments from the mailing list:**
  - About usage of asymmetric signatures for broadcast mode:
    will be considered for future version
- **External comments:**
  - Requests regarding a more generic formulation of authentication/certification methods:
    under consideration
  - About details of negotiations:
    - format for negotiation of algorithms
    - wrapping schemes

    not yet considered, scheduled for future version

Next steps

- **Delay attack:**
  - Scheduled to be addressed in a subsection in Security Considerations
- **Formal verification of the protocol:**
  - Inductive Approach
  - Model Checking
- **Review and comments are requested from:**
  - TICTOC Working Group
  - NTP Working Group
  - NTP development team