Network Time Security

draft-ietf-ntp-network-time-security-14

draft-ietf-ntp-using-nts-for-ntp-05

draft-ietf-ntp-cms-for-nts-message-06

Dr. Dieter Sibold  Kristof Teichel  Stephen Röttger

IETF 95 (Buenos Aires, Argentina) April 3–8, 2016
Outline

History

Document’s Dependency Graph

Scope

Progress/Major Changes
- Implementation Status
- Major Changes Before WG Last Call
- Working Group Last Call
- Next Steps
History

- **IETF 83**: Presentation of security issues of RFC 5906 (autokey)
- **IETF 84**: Presentation of plan for a new autokey standard
- **IETF 85–86**: I-D “draft-sibold-autokey-\(nn\)”
- **IETF 87–90**: I-D “draft-ietf-ntp-network-time-security-\(nn\)”
- **Since IETF 92**:
  - draft-ietf-ntp-network-time-security-\(NN\)
  - draft-ietf-ntp-cms-for-nts-message-\(NN\)
  - draft-ietf-ntp-using-nts-for-ntp-\(NN\)
New Structure: Overview

- network-time-security
- using-nts-for-ntp
- cms-for-nts-messages
- (tictoc) shpiner-multi-path-synchronization
- network-time-security for PTP / IEEE1588

- Cryptographic Message Syntax (CMS) RFC5652
- Security Requirements of Time Protocols RFC 7384
- NTP RFC5905
Scope

Network Time Security provides:

- Authenticity of time servers
- Ability to authenticate time clients to the server
- Ability to perform authorization checks for clients and servers
- Integrity of synchronization data packets
- Conformity with TICTOC’s Security Requirements (RFC 7384)
- Support for NTP
- Ability for support of other time sync protocols, e.g. PTP
Implementation Status

Network Time Foundation

- Authentication framework (association, cookie exchange)
  - Coded, advanced testing still in progress
- Unicast time message exchange
  - Coding and testing in progress
- Allocation of OID values
  - testing using *unofficial* values
  - NTF has applied for a Private Enterprise Number (not going to be used)
Implementation Status

University of Applied Science Wolfenbüttel

- Currently: dealing with OpenSSL issues, getting underlying NTP implementation ready
- Next item: integrating NTS message exchanges
- Deadline: extended to July 2016
Major Changes in the drafts

Main Changes in Preparation for Last Call

- From last WG session:
  - Updates to IANA considerations (for early allocations)
  - Introduced MAC protection of time_request
  - Modification in use of CMS structures for carrying certificates
- Further description of using extended key usage identifiers (usage of certificates for authentication/authorization)
- Specification of ASN.1 structure of the MAC for NTP
- Cross-draft corrections (e.g. use of access messages)
- Editorial changes
Feedback from WGLC – General NTS Issues (1)

- Commitment to HMAC as only MAC algorithm too strong?  
  [x] Changed across current NTS submission
- NTS’ proposed key exchange protocol:
  - Can it be condensed into fewer exchanges?  
    [ ] Could be done. Problem: server seed refresh
  - Can it be executed with fewer cryptographic operations?  
    [ ] Combining of step 2 and 3 will reduce crypto operations  
    [ ] Further reduction need feedback from the list
Feedback from WGLC – General NTS Issues (2)

- Why not use external protocols (e.g. IPsec, (D)TLS)?
  - [x] Some text in RFC 7384 & Security Considerations of NTS
  - [ ] Could be treated in another document, e.g. NTP BCP(?)
    - matching layers; precision; tailorability, . . .

- Need further treatment of chicken-and-egg problem?
  (Need local time for security/need security for reliable time)
  - [x] Agreement: need assumptions in NTS docs
  - [ ] Text still to be written
  - [ ] In-depth discussion elsewhere?
    (Same document as external protocols?)
Feedback from Last Call – NTS-4-NTP Specific Issues

- How to deal with lost packets?
  - [x] Proposal(s) sent to mailing list
  - [ ] Will treat in NTS documents, most likely NTS-4-NTP

- How to treat NTP peer (symmetric) mode?
  - [ ] In discussion. RFC 5905 is not specific.

- Should cipher suites be specified in more detail?
  - [x] Yes. Current “or stronger/weaker” wording is problematic
  - [ ] How much detail?

- Size of initial key exchange messages:
  How to deal with IP fragmentation issues?
  - [ ] How much of an issue is this?
  - [ ] If difficult: piggybacking onto NTP packets still sensible?
Next Steps

- Further discuss feedback from WGLC
- Include appropriate changes
- Schedule another WGLC