Network Time Security

draft-ietf-ntp-network-time-security-01

Authors:

Dr. D. Sibold – PTB, Kristof Teichel – PTB,
Stephen Röttger

IETF 88, Vancouver, BC, Canada, November 3 - 8, 2013

Introduction

Scope:

Network Time Security shall provide

- Authenticity of time servers
- Integrity of synchronization data packets
- Conformity with the TICTOC Security Requirements
- It must support NTP
- It can/should support PTP if possible

Introduction

History

IETF 83	Presentation of security issues of RFC 5906 (autokey)
IETF 84	Plan for a new autokey standard was presented
IETF 85	I-D “draft-sibold-autokey-00”
IETF 86	I-D “draft-sibold-autokey-02”
IETF 87	I-D was renamed; it is presented as I-D “draft-ietf-ntp-network-time-security-00”

Changes since IETF 87

- **According to the comments of the last IETF meeting**
  - Brian Dickson about DANE Certificate exchange: This will be considered for the 02 version.

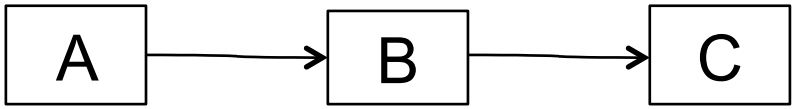
- **Mailing list comments**
  - Dave Mills comments about usage of asymmetric signature for the broadcast mode: This will be considered for the 02 version.
  - Kurt's comments about NTP Pools:
    A short section has been added to the draft. It states that the current version of NTS cannot be used together with NTP pools.
  - Kurt's hint about signature of the cookie exchanges has been added to the draft.

Changes since IETF 87

- **Other changes**
  - A nonce has been added to the time request message (6.5) in order to prevent replay attacks.
  - Editorial changes have been made especially in the description of the broadcast mode.
  - Comparison with the TICTOC requirements has been revised.

Open issues

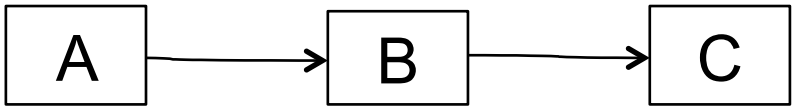
- **Authorization**
  - Is not yet addressed
- **Recursive authentication**
  - In the current approach each client (clock) authenticates only the intermediate server (master). B authenticates C and A authenticates B.



  - A certification trail (chain of trust) is not provided, i. e. client A does not learn about C if it authenticates B.

Open issues (continued)

- **Recursive authentication (continued)**



  - The challenge:
    - Chain of trust and chain of time do not coincide necessarily.
    - Chain of time can change dynamically.
    - Is a intermediate clock trustworthy because it is authenticated? Can or has to be considered in connection with authorization.

- **Delay attack**
  - To be discussed in section “Security Considerations” (multi-source approach, available for NTP)

Next steps

- **Review and comments are requested from**
  - TICTOC WG
  - NTP WG
  - NTP development team
- **Formal verification of the protocol**
  - Model checking