Autokey Version 2 Specification

draft-sibold-autokey-02

Authors: Dr. D. Sibold – PTB, Stephen Röttger
IETF 86, Orlando, USA, March 10-15, 2013
Introduction

Scope:

Autokey V2 shall provide

- Authenticity of NTP servers
- Integrity of NTP data packets
- Conformity with the TICTOC Security Requirements
- Compatibility with the current NTP specification
Introduction

History

IETF 83  Presentation of security issues of RFC 5906 (autokey)
IETF 84  Plan for a new autokey standard was presented
IETF 85  00-version of draft (and preliminary 01-version )
Changes since IETF 85

- **Broadcast Mode**
  - Authentication and integrity check for NTP broadcast mode.
  - Based on TESLA (Time Efficient Stream Loss-Tolerant Authentication), RFC 4082

- **Unicast Modes (client-server, symmetric)**
  - HMAC approach for the generation of the MAC
  - No need for pseudo random keys (autokeys)

- **Revision of Appendix A**
  - Verification against TICTOC Security Requirements draft 04
Broadcast mode

Authentication of the server
- Same procedure as in the unicast modes
Broadcast mode (cont. …)

Integrity protection

- The approach for the unicast modes fails in the broadcast mode
  - The generation of the MAC is based on a shared secret between client and server → this conflicts with the broadcast mode
- Asymmetric cryptography could solve this problem but conflicts with precise time synchronization requirements
- Suggested solution is based on TESLA (RFC4082)
  - TESLA uses symmetric cryptography
  - The required “asymmetric” property is introduced by time-delayed key disclosure
  - TESLA requires “loosely” time synchronization between sender and receivers
Protocol sketch

- Assumption: Broadcast client is time synchronized to the broadcast server
- The server computes a one-way key chain and associates each key to a time interval
- Packets are appended by a MAC calculated with the current key from the one-way key chain
- The client ensures that the packet was sent before the key for the MAC was disclosed; it buffers the packet for later authentication
- The server discloses a key after a pre-defined time delay by appending the key to a packet
- If a key is disclosed the client checks that the key belong to the key-chain and verifies the correctness of the MAC.
Broadcast Protocol Sequence

1. Association message
   - Unicast mode

2. Certificate message
   - Unicast mode

3. Cookie message
   - Unicast mode

4. Time request message
   - Unicast mode

5. Broadcast parameter message
   - Unicast mode

6. Broadcast message
   - Broadcast

Authenticated? (Decision point)

If no: Proceed to next message.
If yes: Proceed to broadcast.

Flowchart diagram:
- Association message → Certificate message → Cookie message → Time request message → Broadcast parameter message → Broadcast message
- Authentication check: yes → Broadcast, no → Proceed to next message
Next steps

• A new name for the protocol (suggestions?)
• Awaiting for comments to the current state of the draft
• Acceptance as working group document