Network Time Security WGLC Design Team Discussions

Link to the agenda document (everyone may comment, only Dieter and Kristof may edit at the moment): https://docs.google.com/document/d/1CR5mFOP_WZ_FZDTf0IWsXLFOvhO4AXokZNvOb3PWI7E

Identified Agenda Items for the Design Team

- Top Priority:
    1. IP fragmentation of certificate-carrying messages during key exchange
    2. Key exchange protocol: do fewer exchanges?
- High Priority:
    3. Key exchange protocol: have fewer cryptographic operations?
    4. Key exchange protocol: what about two-way authentication?
    5. Discussion about Chicken-and-Egg Problem
    6. Improve Handling of Cipher Suites
- Medium Priority
    7. Improve Treatment of Peer Mode
    8. Symmetry of Message Sizes “time_request” and “time_response”
    9. Use of Initial (Unsecured) Timestamps
    10. Seed Refresh: Should this Be Mentioned
    11. Discussion about Different Security Approaches
    12. MAC-Algorithm instead of Hash (for HMAC) Algorithm

Meetings

First (teleconference) meeting likely on Monday, 25 April, 15:30 UTC; some form of minutes will be made available.

April 25th (Monday)

- Platform: Adobe Connect. Severe connection issues for Kristof.
- Attending: Danny, Dieter, Harlan, Karen, Kristof, Miroslav, Sharon.
- Meeting Agenda:
    - Introductions & organizational issues (minute taking)
    - Discussion on correctness & completeness of the team agenda list in the document linked above
    - Discussion on priorities of items (especially "must have" vs. "nice to have")
    - *Optional*: Start of discussion on high-priority items
    - Set date for next meeting
- Additional minutes:
    - Group: Declaring certificate exchange out of scope is bad idea
    - Group: (D)TLS seems promising option
    - Sharon: what is design goal behind custom key exchange (KE)?
    - Miroslav: solve fragmentation by limiting to one cert per exchange?
    - Karen: DTLS / IPsec people should be involved at some point

May 2nd (Monday)

- Platform: Adobe Connect. Issue with connectivity between dial-in and PC connections.
- Attending: Dieter, Harlan, Karen, Kristof, Miroslav, Sharon.
- Meeting Agenda:
    - Organizational issues
        - Minute taking
        - Date for next meeting

    - Discussion for item "IP fragmentation" (~10-15 min. each):
        - List of requirements by Miroslav
        - Option "Self-management" (NTS splits extension field data)
        - Option "External channel" (TCP/(D)TLS/HTTPS/...)
    - Flesh out item "Two-way authentication" (~5 min.)
    - Discussion of item "Peer mode" (~5 min.)
    - General discussion
- Additional minutes:
    - Next meeting same time following week. Karen agrees to provide better meeting room.
    - Group: more discussion on DTLS
    - Sharon: should ask DTLS folks specifically. Agrees to contact someone.
    - Miroslav: what about peer mode (expected to be dealt with alreday)
    - Kristof: peer mode via old symmetric approach?
    - Group: discussion about merits/disadvantages of two-way authentication

May 9th (Monday)

- Platform: WebEx? (room supplied by Karen).
- Attending: Dieter, Harlan, Kristof, Miroslav, Sharon
- Minutes:
    - Group: More discussion on mutual authentication
    - Harlan: needed for peer mode and also mode 6 NTP packets
    - Group: perhaps specify two KE procedures, one which sticks to UDP 123 etc., another which is fast

May 17th (Tuesday)

- Platform: WebEx? (room supplied by Karen).
- Attending: Harlan, Kristof, Miroslav

Week of May 22nd

-Meeting skipped-

May 31st (Tuesday)

- Platform: WebEx? (room supplied by Karen).
- Attending: Danny, Dieter, Harlan, Karen, Kristof, Miroslav, Sharon
- Meeting Agenda:
    - Changes by Dieter and Kristof (DTLS options)
- Additional minutes:
    - Group: Discussion on unauthenticated timing data
    - Sharon: is in favor of "MUST NOT" language
    - Kristof: would like to treat this in section "NTS assumptions about initial timing quality"
    - Group: eliminated some options for the fragmentation issue
    - Upcoming meeting cancelled in favor of only NTPWG call (Thursday, June 9th). After that, Design team calls can be moved back to Mondays, 15:30 UTC