ACE Clock Design Team Update

Hannes Tschofenig

Terminology

- Many (if not most) microcontrollers contain one or even multiple (real-time) clocks.
- These clocks offers a counter, often used as a source for triggering periodic interrupts, timeouts, alarms, etc.
  - Can offer relative time (unless the device is turned off and not battery powered).
- Some of these clocks also work in low power modes.
- For wall time, a reference value is needed. For example, can be obtained via NTP.

Goal

- What are the implications of not having wall time for protocols?
- The following persons volunteered to be part of this design team:
  - Ludwig Seitz
  - Renzo Navas
  - Thomas Watteyne
  - Carsten Bormann
  - + ACE chairs

Implications

- TLS Exchange
  - Certificates with expiry date / revocation checking
  - Caching of state, retransmission timers
  - Certain ciphersuites like Kerberos rely on timestamp support for replay protection / freshness guarantee
- Tokens with lifetime

What was discussed so far?

- What parts of DTLS/TLS require time?
  - Conclusion: Only raw public key-based / PSK-based cipher suites get away without wall time.
- Can we re-use NTP (+NTP security) for configuring wall time?
  - Conclusion: No, since there is a circular dependency. NTP security mechanisms are also very heavy.
- Can existing protocols be re-used for relative time?
  - Renzo surveyed literature and found various three party protocols (using nonces)

What is next? More hardware experience

- Asked Peter Aldworth (ARM) to share experience about hardware-based support for real-time clocks.
- Conference call:
  - Monday, 20th June 2016
  - 3pm – 4pm CEST
  - Join WebEx meeting
    Meeting number: 805 387 005
    Meeting password: sp2JE8uP