Security consideration for the IoT

IETF97

Sandeep, Oscar (Philips)
Mohit (Ericsson)
Thing Lifecycle

- Manufactured
  - Installed
    - Commissioned
      - Application running
        - Bootstrapping
          - Operational
      - Maintenance & re-bootstrapping
    - Application reconfigured
      - Maintenance & re-bootstrapping
      - Operational
  - SW update
    - Application running
      - Removed & replaced
      - Reownership & recommissioned
  - Decommissioned
Threat Analysis

- Cloning of things
- Substitution
- Eavesdropping/Man-in-the-middle
- Privacy
- Denial-of-Service
- Firmware replacement
- Routing attacks
Challenges

• Device heterogeneity
• Protocol translation vs. end-to-end security
• Software update
• Verifying device behavior
• End-of-life
• Penetration testing
• Quantum resistance
Profiles/Architecture/State-of-the-art

- Home/managed home/industrial
- Trade-offs between centralized/distributed management of security
- Profiles for network/application security
- State-of-the-art: IPSec, Minimal IKEv2, DTLS
Contents in old draft-garcia-core-security-06

– Thing lifecycle
– Architectural considerations
– State of the art
– Challenges
  • Constraints
  • Bootstrapping
  • Operation
– Security profiles

- Thing lifecycle
- Architectural considerations <- updated
- State of the art <- some cleaning
- Challenges
  - Constraints
  - Bootstrapping <- removed, linked to bootstrapping draft.
  - Operation
  - Added challenges
- Security profiles
Next steps (1)

• Draft is rather long
• We would like to make the structure more consistent
• We suggest a uniform structure for each of those sections according to “Security pillars”:
  1. Security architecture (centralized/distributed)
  2. Security model of a “thing” (tamper-resistant h/w)
  3. Security bootstrapping
  4. Network security
  5. Application security
Next steps (2)

• Threats:
  – Threats that are included are relatively generic. A more exhaustive overview can be included
  – Possibly classify them according to different phases of the lifecycle
Next steps (3)

• Security profiles
  – Different application areas tend to have different security requirements
  – Further detail them, in particular, with the expected security properties that are to be provided
  – Keep classification based on “security pillars”
Next steps (4)

• State of the art
  – State of the art is outdated (old internet draft)
  – Classify according to security pillars
  – Include newer references
Next steps (5)

• Challenges
  – Classify them according to the “security pillars”
  
  – Include for each of them:
    • What the specific challenge is
    • What the potential solution direction might be
  
  – Note that some challenges are still to be added: