draft-moran-iot-nets-00

ietf 113

Brendan Moran

2022-03-24

Security documents

- Architecture
- Threat model
- Requirements/mitigations

draft-moran-iot-nets-00

- Not an architecture
- Not a threat model (though it has one in mind)
- Mostly requirements/mitigations

- Without an architecture & threat model, mitigations are hard to justify

Where to go next

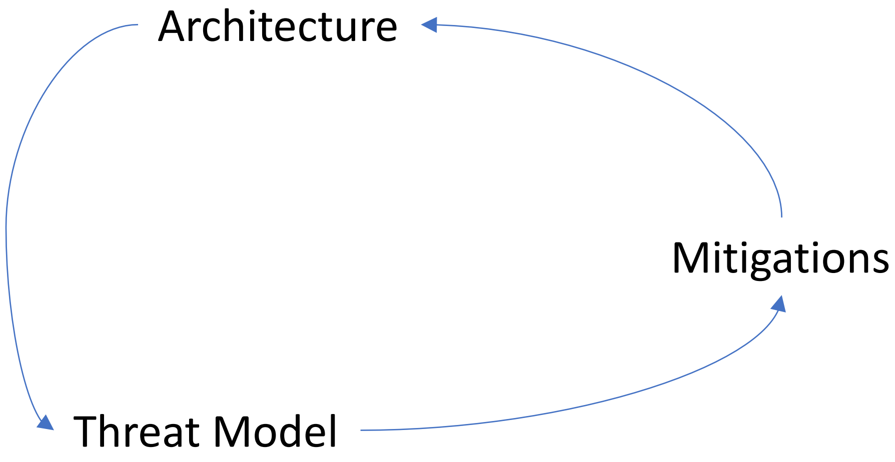
- Need architecture / threat model
    - But one constrained to only the problems that draft-moran-iot-nets addressed is quite limited. Why leave it there?
- Should we consider an IoT Architecture?
- Should we consider an IoT Threat Model?
- Where would these end?

Similar work

- ENISA has an “IoT best practices” document
- Arm’s PSA documents cover much of the device-side architecture

Circular nature of the documents

- New architecture elements add new threats
- New threats require new mitigations
- New mitigations need new elements in the architecture
- We cannot just start with an architecture; all three pieces need to be developed together



Hierarchical Architecture

- Many security-area WGs already have architecture & threat model
- No need to reproduce this work; reference it instead.
    - Draw out any important cross-standard considerations
    - Draw out any useful combinations of standards:
        - E.g. CoRIM + SUIT + RATS enables delivery of attestation verification information to the verifier, signed by the author of the firmware, so that the verifier always knows what to expect.

Opportunities

- Describe relationships between entities from different standards
- Many standards leave certain parts “open ended”
  - relationships undescribed
  - Portions of the system “up to the implementer”

- Example: Firmware author provides firmware details to attestation verifier.

IoT architectural variations

Centralised

- One (group) of authorities
- Communication is sent to the authorities
- Some shortcuts allowed if authorized by the centralized authority

Decentralised

- No authorities
- Peer to peer communication

Hybrid IoT architectures

- Many IoT systems must end up with hybrid architectures
    - E.g. decentralized communication with centralized attestation
- The IoT architecture should clearly articulate the benefits & drawbacks of each approach for each function of the IoT device

Questions/Comments?