draft-moran-iot-nets-01

ietf 114 Philadelphia
Changes from v00

• Forget everything from v00
• This is a (nearly) complete rewrite
What is the root of a security architecture?

- Knowing which threats it mitigates
  - All security architectures should have threat models

- Restructured iot-nets as:
  - A threat model
  - Some guiding usability requirements
  - Some risks
  - Mitigations for the threats
  - Technologies that implement the mitigations

- More-closely approaches Eliot’s ask
  - A menu of technologies & what benefits they bring
Threats Covered

• 10 top-level threats:
  • IoT Network Credential Exposure
  • Trust Anchor Private Key Disclosure
  • Incorrect Firmware/Version
  • Vulnerable Firmware
  • Supply Chain Attacks
  • Verification Information Supply Chain
  • Spurious Network Capabilites
  • DoS of ACL server
  • Delays in ACL Remediation
  • Vulnerable Devices
Technologies Covered

• Credential deployment
  • LwM2M Bootstrap
  • BRSKI
  • FDO

• TA Rotation
  • LwM2M Bootstrap
  • FDO
  • EST

• Software Measurement
  • RATS

• Update Security
  • SUIT
  • TEEP

• SBOM
  • CoSWID
  • CoRIM

• Verifier Data
  • CoSWID
  • CoRIM

• Network ACLs
  • MUD
  • SUIT-MUD

• Device Isolation
  • RATS
  • MUD
  • EST
What next?

• Current threat model is minimal
  • Lots more out there

• Technologies covered are minimal
  • E.g. no mention of transports

• Missing guidance on non-security aspects of iotops
  • E.g. Human-readable formats are for humans => no YAML, JSON or XML on constrained nodes
  • Maybe non-security aspects in another document?
Authors needed!

• This guidance document will need a lot of work
• Needs many points of view & lots of input