draft-moran-iot-nets-02

ietf 115 London

Changes from v01

- ~~Forget everything from v00~~
- Forget everything from v01
- This is a (nearly) complete rewrite

Target Audience

- IoT experts, software developers and manufacturers
- Information security experts
- IT/Security solutions architects
- Chief Information Security Officers (CISOs)
- Critical Information Infrastructure Protection (CIIP) experts

There are lots of baseline security recommendations documents

- We don't need to repeat that work
  - ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures
  - ETSI Cyber Security for Consumer Internet of Things: Baseline Requirements
  - NIST IoT Device Cybersecurity Capability Core Baseline
  - More?

- What we need is a map from these requirements to IETF (and related) technologies

Status of iot-nets

- ENISA baseline requirements mapped

- TODO:
    - NIST requirements
    - ETSI requirements
    - Others

Types of requirement

- Procedural
  - These are flagged, but no technology mapping is provided
- Architectural
  - Some architectural requirements have corresponding IETF architectures.
- Technological
  - These are the most interesting parts

Summary of technical ENISA requirements

- Broad Categories
  - Data Protection
  - Secure Software / Firmware updates
  - Software Isolation
  - Access Control
  - Cryptography
  - Secure and Trusted Communications
  - Data Security / Authenticity
  - Secure Transport
  - Least Privilege Communication

What next?

- Currently, only has ENISA requirements.
  - NIST requirements are next.
- Need a thorough review to identify any gaps in these requirements

Authors needed!

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