Motivation

• Suppose...
  • You’re working for a company that makes
    • Medical devices
    • SCADA systems
    • Industrial Robots
    • Etc...
  • And it needs to be network-connected.
  • Your latest client tells you that they require their devices to adhere to...
    • ENISA Baseline Security Recommendations for IoT
    • NIST 8259A - IoT Device Cybersecurity Capability Core Baseline
    • Etc...
  • Now what?
Motivation, Cont’d

• Requirements documents don’t tell you how to implement them
• The IETF doesn’t have a landing pad document for implementing secure IoT devices
• The discovery process for finding the requisite standards is complicated at best.
• So what do you do?
  • A common choice is to adopt an IoT OS
  • How can you be sure it covers all the requirements?
Summary

• Maps from security requirements in existing standards to IETF and related technologies

• Provides implementors with a starting place for IoT security

• Serves three purposes:
  1. Directs implementors towards standards-based solutions to security requirements
  2. Helps make implementors aware of potential security problems that they may not have considered
  3. Maps security requirements between different requirements documents
    • Oops. I didn’t mean to do that.
Current Status

• Two sets of security requirements already covered:
  • ENISA Baseline Security Recommendations for IoT
  • NIST IoT Device Cybersecurity Capability Core Baseline

• WG asked NOT to have one mapping draft per security requirements document
  • Therefore, this will keep growing.

• Co-Authors needed

• Reviewers needed

• Next step is to add ETSI’s “Cyber Security for Consumer Internet of Things: Baseline Requirements”
Questions?

• Why isn’t my favorite set of requirements covered?
  • Because you’re not a co-author.
    • Yet.
      • Join me!

• What does this draft need for WGLC?