IoT Initial Security Setup

Players, Beliefs, and Processes

Carsten Bormann 2021-04-20 • IoTOPS Interim

Initial Security Setup

- Bootstrapping
- Provisioning
- **Onboarding**
- **Enrollment**
- Commissioning
- Initialization
- Configuration
- Registration
- **Discovery**

- IoT environments need to be **set up**
  - Things (devices) need to know **Purpose in Life** (PiL)
  - Environment needs to know something about devices
- Part of this is **security setup**, part is enabled by security setup
  - Players: What are the parties that are set up/play a role in setup?
  - Beliefs: What knowledge (belief) is instilled during setup?
  - Processes: What is the sequence of events and interactions that leads to setup?

From Phenomenology to Taxonomy

- For each IISS mechanism: how does it work, and what does it do?
- ➔ Terms for different approaches and results
- Current T2TRG RG document: draft-irtf-t2trg-secure-bootstrapping
- Taxonomy needs to be clear about:
  - (Types and Instances of) Players
  - beliefs: prerequisites and results
  - processes

Players

- Obvious: Thing (device) vs. Environment
- Can structure Thing (e.g., TEEs/REEs in a device [TEEP])
- Almost always need to structure Environment:
  - Network vs. Application vs. Platform; specific entities within each
  - Device vs. Owner vs. Manufacturer, Facilitators (e.g., smartphone)

Device ⟷ Network, Platform, Application

- Device has:
  - Identities (often supported by Roots of Trust)
    (see also draft-richardson-t2trg-idevid-considerations)
  - Trust Anchors (“root certificates”)
  - Authorizations (owner allows device A to do X),
    Authorizations (other player B allows holder of identity A to do Y), and
    Authorizations (device A allows holder of identity B to do Z)

Important Milestones in Device Life

- Network Onboarding
  - Some network access helps in all these onboarding processes
- (Platform Onboarding)
- Application Onboarding

Device ⟷ Owner vs. Manufacturer, Facilitators

- Device has
  - Owner (not in legal sense: ➔ “overseeing principal”)
  - Original owner (“manufacturer”)
  - Facilitators (entities mediating owner control over the device)

Important Milestones in Device Life

- Ownership Transfer
  - New owner gains (some) control
  - Original owner may retain some control
  - Some authorizations remain in place
- Software Update
  - Software provider has full control
  - Limited by hardware shields

Processes

- Install Authorization on Device
  - Possibly derived from chain of authorizations
  - Possibly obtained from “leap of faith”
- Install Authorization on some other Player (Network, Platform, Application)
- (Possibly removing some authorizations, too)
  - “Factory reset”? (Who is authorized to do that?)
- Create identities to be used (authenticated) in some of the authorizations

Flavors

- “Managed” vs. “unmanaged”
- Which Players are under same ownership or control, e.g.:
  - Manufacturer and Platform: Enables back-channel pre-authorization
  - Device and Network: Enables leap-of-faith authorization
- Which Players are swapped in and out in regular use, e.g.:
  - Device and Network (“roaming”)
  - Device and Application (no strict vertical integration)
- Does physical access imply full authorization (factory reset, commissioning)?

Taxonomy?

- Create terms for (recurring) process design patterns
- Create terms for identities and authorizations that seem to recur
- Describe specifications and proposals in these terms