Terminology and processes for initial security setup of IoT devices

draft-irtf-t2trg-security-setup-iot-devices-00

Mohit Sethi, Behcet Sarikaya, and Dan Garcia-Carrillo

T2TRG Interim meeting – May 24th 2023

Initial security setup of IoT devices

Changes to the document

- Rename document name to match title

~~draft-irtf-t2trg-secure-bootstrapping~~ becomes draft-irtf-t2trg-security-setup-iot-devices

- Received some off list feedback on OMA

Initial security setup of IoT devices

Goals of the document

- Overview of the terminology related to the initial security setup
- Identify common patterns on the applicability of terms, processes, beliefs
- Illustrative examples of security setup techniques (cover IETF and non-IETF protocols)

Terminology

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

Terminology

Break down protocols into

- Players: What are the parties: e.g., manufacturer, user, network administrator

- Beliefs:
  - Pre-setup: What knowledge is available before setup. e.g.: manufacturer issued certificates containing IDevID
  - Post-setup: What knowledge is instilled during setup. e.g.: SSID, network key, etc.

- Processes: Sequence of events and interactions required setup? e.g.: power up device and scan a QR code.

Protocols reviewed

- Device Provisioning Protocol (DPP)
- Open Mobile Alliance (OMA) Lightweight M2M (LwM2M)
- Open Connectivity Foundation (OCF)
- Bluetooth
- Fast IDentity Online (FIDO) alliance
- Enrollment over Secure Transport (EST)
- Bootstrapping Remote Secure Key Infrastructures (BRSKI)
- Secure Zero Touch Provisioning (SZTP)
- Nimble out-of-band authentication for EAP (EAP-NOOB)
- LPWAN
- Thread

Comparison among the protocols

We compare the following among the protocols

- Terminology
- Players
- Initial beliefs
- Processes
- Knowledge imparted

Next steps

Better identification of terminology, players, processes, and beliefs for each standard

OMA - Beliefs

- Initial Beliefs: Location and credentials for communication with bootstrap server (factory, smartcard, client-initiated, server-initiated)

- Beliefs imparted: registration with one or more LwM2M management server

OMA - terminology

- Terms: Bootstrapping, provisioning, initialization, configuration, registration, discovery

- Terminology used once: "*This functionality could be used for <u>initialization</u> purposes before LwM2M Bootstrap-Server sends Write operation(s) to the LwM2M Client*"

- Focus on terminology focused on initial security setup – bootstrap, discover, provision?

OMA - processes

- Processes: ~~Factory Bootstrap, Bootstrap from Smartcard, Client Initiated Bootstrap and Server Initiated Bootstrap~~.

- Should we explain how the protocol works in Processes? Or focus only on actions that a owner/user needs to perform?

OMA - players

- Players: ~~Bootstrap Server, Client, Device~~, Manufacturer, Owner, ~~Server, User~~

- Who are the players:
  - Service provider running LwM2M server?
  - User/Owner
  - Manufacturer

Next steps

- You are an experts on:
  - Device Provisioning Protocol (DPP)
  - Open Mobile Alliance (OMA) Lightweight M2M (LwM2M)
  - Open Connectivity Foundation (OCF)
  - Bluetooth
  - Fast IDentity Online (FIDO) alliance
  - Enrollment over Secure Transport (EST)
  - Bootstrapping Remote Secure Key Infrastructures (BRSKI)
  - Secure Zero Touch Provisioning (SZTP)
  - Nimble out-of-band authentication for EAP (EAP-NOOB)
  - Thread
- We look forward to your comments

Status

- Draft on GitHub:

https://github.com/t2trg/security-setup-iot-devices

- Pull requests and issues on GitHub and mailing list are welcome