Secure IoT Bootstrapping: A Survey

draft-sarikaya-t2trg-sbootstrapping-08

Mohit Sethi, Behcet Sarikaya, and Dan Garcia-Carillo

Secure Bootstrapping

- Goals of this document:
  - Overview of bootstrapping related terminology.
  - Identify common patterns and provide recommendations on the applicability of terms.
  - Illustrative examples of bootstrapping techniques (cover all IETF and many non-IETF protocols).
  - Classify techniques based on requirements and assumptions.

Bootstrapping Terminology

- Current list:
  - Bootstrapping - Registration
  - Provisioning - Commissioning
  - Onboarding - Configuration
  - Initialization
- What is missing?

OMA Lightweight M2M (LwM2M)

- A new IoT device (LWM2M client) contacts a Bootstrap-server which is responsible for "provisioning" essential information such as credentials.
- The LwM2M client device then "registers" itself with LwM2M Servers which manage the device during its lifecycle.
- 4 bootstrapping modes:
  - Factory Bootstrap
  - Smartcard
  - Client Initiated
  - Server Initiated

Open Connectivity Foundation

- The process before a device is operational as onboarding.
- The first step of this onboarding process is "configuring" the ownership using an Onboarding tool (OBT) and Owner Transfer Methods (OTMs):
  - Just works – unauthenticated DH
  - Random PIN – copy PIN generated on device to OBT
  - Manufacturer certificate
  - Vendor specific
- At the end of owner transfer, the OBT "provisions"/"configures" the device with Owner credential.
- After ownership is established, the device is also prepared for provisioning by providing it bootstrapping parameters (BP) that include bootstrapping credential (BC) and bootstrapping server (BS) metadata.

Device Provisioning Protocol (DPP)

- Describes itself as standardized protocol for providing user friendly Wi-Fi setup
- DPP relies on a configurator, e.g. a smartphone application, for setting up all all other devices, called enrollees, in the network.
- Has the following three phases/sub-protocols:
  - Bootstrapping: configurator obtains bootstrapping information from the enrollee using an out-of-band channel such as scanning a QR code or tapping NFC.
  - Authentication: provides authentication of the responder to an initiator. Can optionally authenticate the initiator to the responder.
  - Configuration: Using keys established from the authentication protocol, the enrollee asks the configurator for information such as the SSID and passphrase.

Z-wave S2 security protocol

- Requires devices to have factory provisioned asymmetric key pair.
- Device also has the first 16 bytes of the 32 byte public key printed as a QR code and a 40 digit string.
- A new device joining an existing network advertises its garbled public key (by setting the first 16 bits to zero).
- User then manually adds the missing 16 digits to the network controller by scanning the QR code of the new device (or copying the first 5 digits of the 40 digit printed string).
- Controller and device perform ECDH key exchange after which the network key is sent over the secure channel established.

Common Patterns

- Multi-step process
- Common to use a tool/device that assists in the bootstrapping process
- Asymmetric key pairs
- Opinion: bootstrapping the overarching term that involves steps such as onboarding, authentication, followed by configuration, provisioning and eventual ownership transfer?

IETF protocols in next version

- Enrollment over Secure Transport (EST)
- Bootstrapping Remote Secure Key Infrastructures (BRSKI)
- Secure Zero Touch Provisioning
- TEAP Update and Extensions for Bootstrapping (EAP-TEAP-BRSKI)
- Nimble out-of-band authentication for EAP (EAP-NOOB)

Classification

- Managed methods: Pre-established trust relations and authentication credentials
- P2P / ad-hoc methods: No pre-established credentials. Out-of-band channel used for distributing or confirming keys.
- Opportunistic / leap-of-faith methods: Continuity of identity or connection, rather than initial authentication. May assume that the attacker is not present at the inititial setup
- Hybrid methods: Most deployed methods are hybrid. Components from both managed and ad-hoc methods. For example, central management after ad-hoc registration.

Reset and Ownership transfer

- Is it enough to factory reset the device?
- Is co-operation of the prior owner required to factory reset? Google ‘Factory Reset Protection’ on Android prevents reset if you don’t know account information.
- Is physical access to device necessary for revoking any credentials? FIBARO Flood sensor requires you to press a button for removing it from your network.
- Important but often overlooked area which fundamentally affects the bootstrapping process.