Secure IoT Bootstrapping: A Survey

draft-irtf-t2trg-secure-bootstrapping-00

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 many IETF and non-IETF protocols).
  - ~~Classify techniques based on requirements and assumptions.~~

Terminology

- Current list:
  - Bootstrapping - Registration
  - Provisioning - Commissioning
  - Onboarding - Configuration
  - Initialization - Discovery

- Bootstrapping one example among many

Terminology

- New title: Terminology and processes for initial security setup of IoT devices
- 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.

Device Provisioning Protocol (DPP)

- Wi-Fi alliance protocol for user friendly Wi-Fi setup
- Relies on a configurator, e.g. a smartphone application, for setting up all all other devices, called enrollees, in the network.
- 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

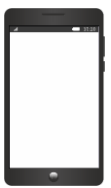
Device Provisioning Protocol (DPP)

- Players:
  - Manufacturer installs a key pair and prints the public-key and other metadata on device/packaging
  - User also the device owner
  - Companion device aka smartphone
- Beliefs:
  - Pre-setup: Manufacturer installed asymmetric key pair
  - Post-setup: Device is instilled with knowledge such as target network, SSID, passphrase, etc.
- Processes:
  - User scans QR code or taps NFC for authentication
  - Twice if mutual authentication is desired
  - Send information such as SSID, passphrase of home AP

Bluetooth Mesh - Provisioning

- Provisioning: adding a new device to the mesh network
- Provisioner: smartphone for provisioning new devices

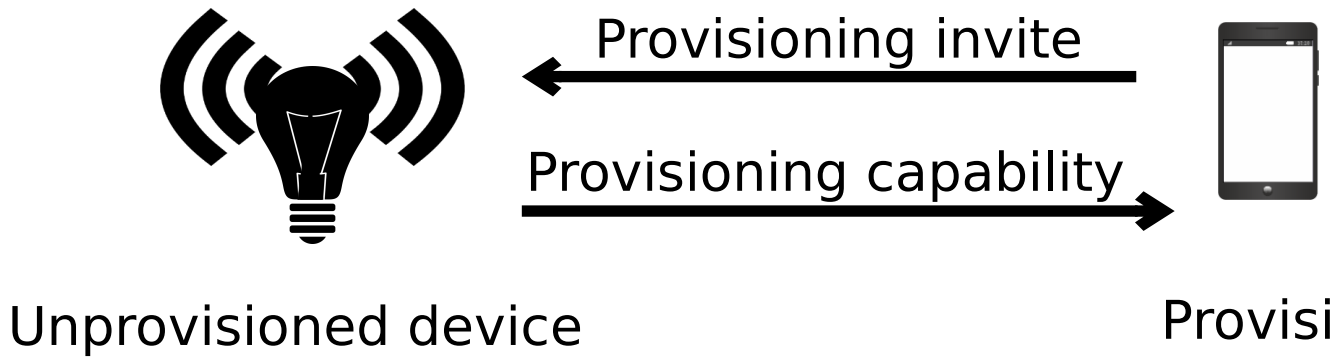
Unprovisioned device



Provisioner

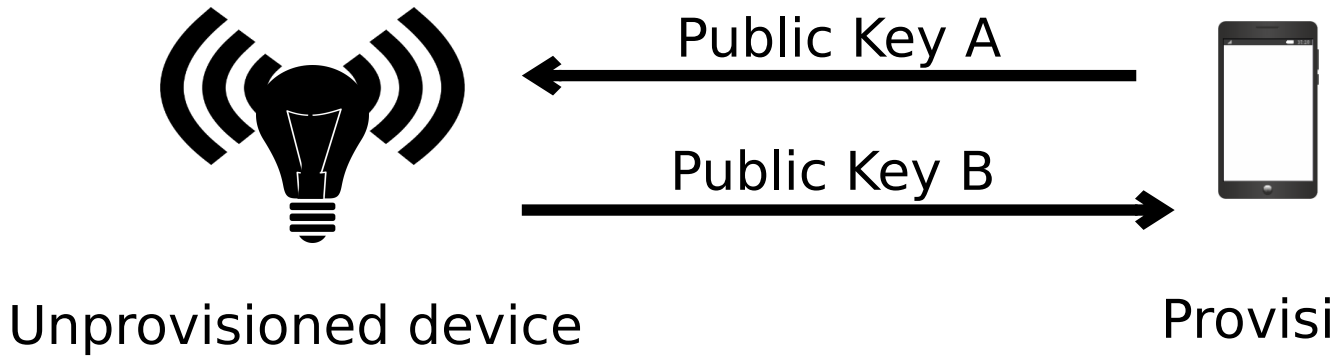
Bluetooth Mesh - Provisioning

- Invitation: provisioner discovers new device via beacon and sends an invitation.
- New device responds with provisioning capabilities (including elements, security algorithms, I/O capability etc.)



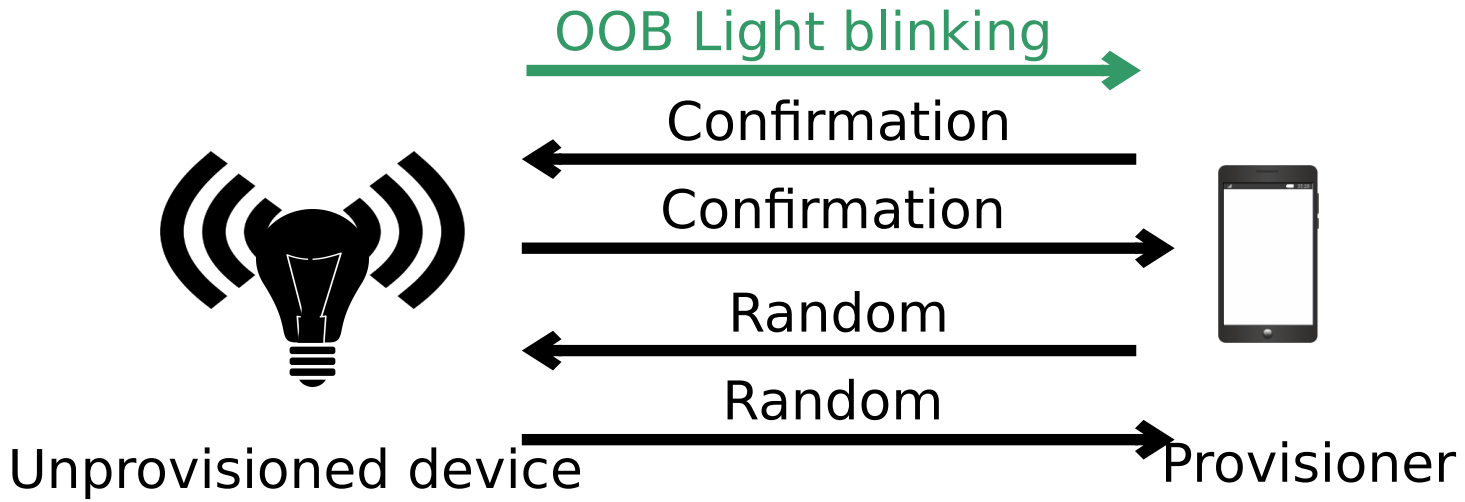
Bluetooth Mesh - Provisioning

- Public key exchange: ECDH key exchange with fresh keys (if OOB input or OOB output authentication used)



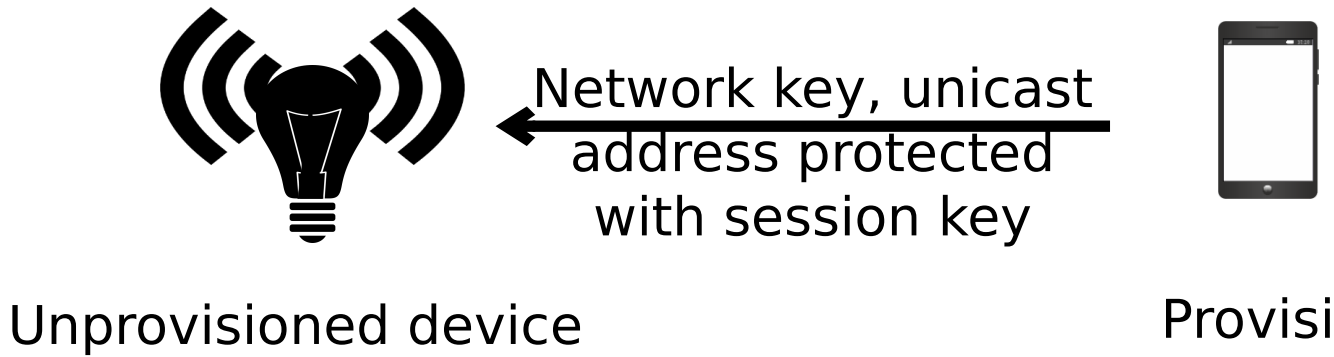
Bluetooth Mesh - Provisioning

- Authentication: Device or Provisioner generate and show a random number (as blinking LED, audio etc.) that is input on the other side. Both send commitments with random number and reveal random numbers after. Generate session key



Bluetooth Mesh - Provisioning

- Distribution of provisioning data: Provisioner sends data: network key, IV index, unicast address assigned etc



Bluetooth Mesh - Provisioning

- Players:
  - User also the device owner
  - Provisioner aka smartphone
- Beliefs:
  - Pre-setup: None no installed/hard-coded credentials
  - Post-setup: Device learns about the target network, credentials, application (lighting etc.)
- Processes:
  - User scans a blinking light
  - Sends information such as application/group etc.

Status

- Draft on github: https://github.com/t2trg/sbootstrapping
- Pull Requests and issues on github and mailing list are welcome.