Secure IoT Bootstrapping: A Survey

draft-sarikaya-t2trg-sbootstrapping-01

Behcet Sarikaya and Mohit Sethi

Secure Bootstrapping

- What is bootstrapping and what is secure bootstrapping? <- Updated
  - What is onboarding
  - What is identity and identifier
  - What is user and device identity and identifier
- Possible goals of secure bootstrapping:
  - Identity: authentication of a pre-established identity vs. creation of a new identity
  - Authorization for network access, incl. configuration of communication parameters
  - Registration or joining a domain or group
  - Pairing with a specific node, or connecting to a cloud service
- Some example of bootstrapping:
  - pairing of phones over bluetooth to exchange files, and
  - securely connecting IEEE 802.15.4 sensors factory to the backend both require some form of secure bootstrapping

Managed methods

- Pre-established trust relations and authentication credentials
- Centralized or federated
- Examples:
  - AAA / Extensible Authentication Protocol (EAP)
  - Generic Bootstrapping Architecture (GBA) with SIM
  - Open Mobile Alliance (OMA) Light-weight M2M:
    - Factory Bootstrap, Bootstrap from Smartcard, Client Initiated Bootstrap, Server Initiated Bootstrap
  - Kerberos
  - ANIMA <- Updated
  - Vendor certificates

P2P / ad-hoc methods

- No pre-established credentials
- Out-of-band channel used for distributing or confirming keys
  - Typically Diffie-Hellman exchange + MitM prevented with OOB communication
- Examples: <- Updated
  - Bluetooth simple pairing
  - Wi-Fi protected setup
  - EAP-NOOB (out-of-band authentication for EAP)
  - Magic wand, e.g. commissioning tool in I-D.kumar-6lo-selective-bootstrap

Opportunistic / leap-of-faith methods

- Continuity of identity or connection, rather than initial authentication
- Some methods assume that the attacker is not present at the inititial setup
- Examples: <- Updated
  - SEND and CGA
  - WPS push button
  - SSH, gmail, Facebook

Hybrid methods

- Most deployed methods are hybrid:
    - Components from both managed and ad-hoc methods
    - E.g. central management after ad-hoc registration
- Categorization is not always easy or clear

- Choice of bootstrapping method depends heavily on the business case:
    - What third parties available?
    - Who wants to retain control or avoid work?
    - Manufacturer/vendor, system admin, user, fully ad-hoc

Secure Bootstrapping

- Next steps:
  - Hidden gems and best practices?
  - Text on ownership transfer and how does it affect bootstrapping:

    https://www.iab.org/wp-content/IAB-uploads/2016/03/draft-farrell-iotsi-00.txt