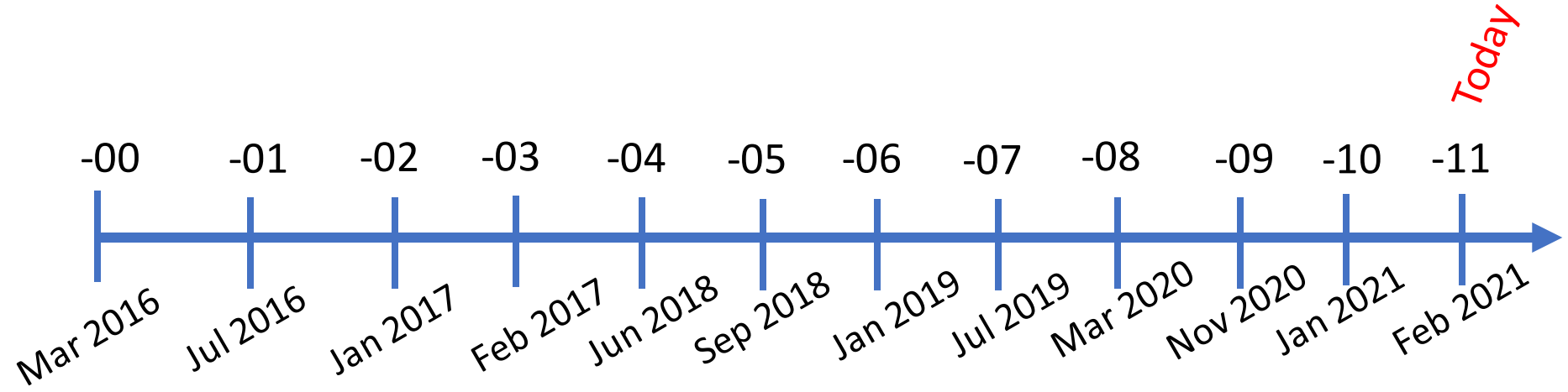
Secure IoT Bootstrapping: A Survey

Mohit Sethi, Behcet Sarikaya, Dan Garcia,
various other contributors

Secure IoT Bootstrapping: A Survey

draft-sarikaya-t2trg-sbootstrapping



Definition of bootstrapping

Classification DPP & Thread commissioning

LPWAN networks

Bootstrapping Terminology: Onboarding, Enrollment, Commissioning and relationship. FIDO onboarding

Terminology

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

DPP

- Wi-Fi Alliance Device Provisioning Protocol
- DPP has the following three phases/sub-protocols:
  - Bootstrapping: Configurator obtains public-key and metadata information from the enrollee using an out-of-band channel such as scanning a QR code or tapping NFC.
  - Authentication: Authentication of the responder to an initiator. Optional mutual authentication (only if bootstrapping information was exchanged out-of-band in both directions).
  - Configuration: Use key established from authentication protocol to configure network information such as the SSID and passphrase of the access point.

OMA LwM2M

- New device contacts a bootstrap-server which is responsible for provisioning essential information such as credentials.
- The client device registers itself with one or more LwM2M Servers which will manage the device during its lifecycle.
  - Factory bootstrap
  - Bootstrap from smartcard
  - Client Initiated bootstrap
  - Server Initiated bootstrap

FIDO alliance

- Automatic onboarding protocol.
- Provide IoT device with information for interacting securely with an online (cloud) IoT platform.
- Note: network connectivity is assumed.
- Late binding: owners choose IoT platform for their devices at a late stage in the device lifecyle.
- Composed of:
  - Device Initialization (DI) protocol: executed in the factory - embeds initial ownership and manufacturing credentials.
  - Transfer of Ownership (TO) protocols TO0, TO1, TO2: new device discovers rendezvous server (local/Internet). Protocols between the device, the rendezvous server, and the new owner (as the owner onboarding service) ensure that the device and the new owner authenticate each other. Owner establishes cryptographic control of the device and provides it with credentials of the IoT platform.

IETF - EST

- Enrollment over secure transport (RFC 7030)
- A profile of Certificate Management over CMS (CMC)
- Allows client devices to obtain client certificates and associated Certification Authority (CA) certificates.
  - companion specification for EST over CoAP (draft-ietf-ace-coap-est)
- Bootstrap Distribution of CA Certificates: allows minimally configured clients to obtain initial trust anchors.
  - Relies on human users to verify information such as the CA certificate fingerprint received over the unauthenticated TLS connection setup.
  - After successful bootstrapping, clients proceed to enrollment step during which they obtain certificates.

IETF - BRSKI

- Bootstrapping Remote Secure Key Infrastructures
- 802.1AR vendor certificates on device:
  - Discover
  - Identify
  - Request to join
  - Imprint
  - Enroll
- Works with link-local connectivity. Does not require a routable address.
- Vendor provides an Internet based service.

IETF - SZTP

- Secure Zero Touch Provisioning (SZTP) (RFC 8572)
- A bootstrapping strategy enabling devices to securely obtain bootstrapping data with no installer action
- Sources of bootstrap data:
  - DNS
  - DHCP
  - Removable storage
  - Bootstrap server
- Onboarding Server: a bootstrap server that only returns onboarding information (boot image, scripts, etc.).
- If source of info untrusted, then conveyed information is either signed or it is information that can be processed provisionally (unsigned redirect)

Summary

Bootstrapping terminology

- Several stages before a device becomes fully operational.
- Typically involves establishing some initial trust after which credentials and other parameters are configured.
  - DPP: bootstrapping is the first step before authentication and provisioning of credentials can occur.
  - EST: bootstrapping happens as the first step when the client devices have no certificates available for starting enrollment.
- Some protocols may only deal with parts of the process. For example, TLS maybe used for authentication after bootstrapping. A separate device management protocol then may run over this TLS tunnel for provisioning operational information and credentials.

Survey

Bootstrapping survey

- Device Bootstrapping Methods
  - Managed: EAP-TLS, OMA LwM2M, Kerberos (some credentials on device)
  - P2P and ad-hoc methods: Pairing (unauthenticated DH with OOB communication)
  - Leap-of-faith/opportunistic: SSH, WPS
  - Hybrid: DPP, Raw public keys
- Categorization of different methods is not always easy or clear: all the opportunistic and leap-of-faith methods become managed methods after the initial vulnerability window.

Secure IoT Bootstrapping: A Survey

- WG adoption? - Authors think document is super ready for adoption
- Is the document title reflective of the content?