A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors

Michael Richardson
<mcrr@sandelman.ca>

https://www.sandelman.ca/SSW/talk/2023-t2trg-taxonomy-installed-keys/
An even briefer history of this draft

- ANIMA documents
  - masa-considerations
  - registrar-considerations
  - common contents,
- Went to SECDISPATCH in virtual interim meeting in July 2022, at IETF108
  - https://datatracker.ietf.org/meeting/108/session/secdispatch

- Profit!

Non-Goals of the document

1) Not aiming to write an ISO27001-ish evaluation process.

2) Not going to make any recommendation as to an appropriate solution for a given risk situation.
Goals of this document

• Enumerate the reasonable, and maybe some less reasonable ways to provision and secure keys, and give them names.

• Not just the most secure way, because it is not always worth it.
Recent events at CA/B FORUM and LAMPS

- CA/Browser Forum decided that code-signing keys need to be in an HSM
- CA that signs code-signing key must have some kind of attestation from HSM about key provenance
- CSR needs to hold this attestation
- LAMPS still debating about what the format of attestation will be
Taxonomy: Key Generation Process

- **where/how is the device key generated**
  - **internal?**
  - **external/factory?**
  - **CPU-provisioned seed?**
  - **threshold methods?**

  • **Key Attributes**
    - > Source/Creation (enum)
      - >> Loaded
      - >> Device Derived (e.g. Derived from a device permanent master secret such as a TPM hierarchy seed)
      - >> Generated on Device
      - >> Key Agreement (???) (Derived from a key agreement)
      - >> Co-Generated (???) (Securely cogenerated on more than one machine)
      - >> KDF (???) (Derived from a master secret which was in turn derived from a two - or greater - party protocol).

  • **Protection (enum - ordered from least to most protected)**
    - >> Unknown
    - >> None/Software
    - >> Extractable/Migratable (by the user)
    - >> Extractable for Backup (encrypted under a key migratable to another HSM)
    - >> Extractable for Storage (encrypted under a PUF, not migratable)
    - >> Non Extractable

LAMPS notes:
https://mailarchive.ietf.org/arch/msg/spasm/d0xsQZIBgizetVRaZVULmTkEdlk/
Next Steps

• Additional bikeshedding over some of the terminology/definitions
• Promote the terms more widely
  – Within the IETF and IRTF and also outside
  – Listen to feedback, look for awkward usages
• Publish in late 2023
Questions!

T2TRG / Sandelman
https://datatracker.ietf.org/doc/draft-richardson-t2trg-idevid-considerations/