Security Classes For Software Updates for IoT
draft-urien-suit-security-classes-00.txt

Pascal.Urien@Telecom-ParisTech.fr
Scope

• This draft attempts to define security classes for devices targeted by SUIT protocols.

• A device security is characterized by five boolean security attributes: firmware loader (FLD), one time programmable memory (OTP), secure firmware loader (FLD-SEC), tamper resistant key (TRT-KEY) and diversified key (DIV-KEY).
  – More Attributes needed?

• This classification creates 18 device classes.

• \{FLD, OTP, FLD-SEC, TRT-KEY, DIV-KEY\}
Goal

• This draft attempts to define security classes for devices targeted by SUIT protocols.
• The goal is to provide a qualitative estimation of risks induced by firmware remote updates according to device logical and hardware security resources.
Device Architecture

Main Processor

- NVM
- OTP
- Firmware Loader

Communication Processor

- NVM
- OTP
- Firmware Loader

Non Volatile Memory

One Time Programmable Memory

Physical Protocols
Device

- FML=1
  - Firmware Loader "BootLoader"
    - OTP=1
      - Part of Loader
        - Minimum device behavior
    - OTP=0
      - No minimum device behavior
  - Physical Protocols Serial - Parallel
  - Supply Chain Attack
    - OTP=0
      - Part of Firmware
        - Minimum device behavior
    - OTP=1
      - Minimum device behavior

- FML=0
  - No Firmware Loader
    - OTP=0
      - No minimum device behavior
    - OTP=1
      - Minimum device behavior

*{0,0} HTTPS Firmware update
Firmware Loader
"BootLoader"

One Time Programmable Memory, OTP=0/1

Secure Firmware Loader, FLD-SEC = 0/1

Tamper Resistant Key, TRT-KEY= 0/1

Diversified Key, DIV-KEY =0/1

Is it possible to erase the bootloader?

Symmetric
Asymmetric
Certificate
Post –Quantum Crypto

Side Channel Attacks enable key recovery

The use of diversified secrets keys limits the side channel attack effect to a single device

Exemple Bank Card = { 1,1,1,1,1}
Questions