LWIG Working Group
Internet Draft
Intended status: Experimental

P. Urien
Telecom ParisTech

November 22 2018

Expires: May 2019

# Security Classes for IoT devices
# draft-urien-lwig-security-classes-00.txt

## Abstract

This draft attempts to define security classes for constraint IoT devices. A device security is characterized by five Boolean security attributes: one time programmable memory (OTP), firmware loader (FLD), secure firmware loader (FLD-SEC), tamper resistant key (TRT-KEY) and diversified key (DIV-KEY).

This leads to the definition of 6 classes of devices, embedding or not OTP resource, whose security increases with the class number (0 to 5). The suffix + indicates OTP availability.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 2019.

.

Table of Contents

## 1 Overview

This draft attempts to define security classes for IoT devices, supporting SUIT [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.

According to this draft a device comprises a main processor (MP), an optional communication processor (CP), actuators and/or sensors. The communication task may be handled by the main processor. The main processor manages the update of other processor(s).

The main processor embeds several types of memories:
- One Time Programmable Memory (OTP)
- Non Volatile Memory (NVR)
The logical architecture of the optional communication processor is similar to those of the main processor.

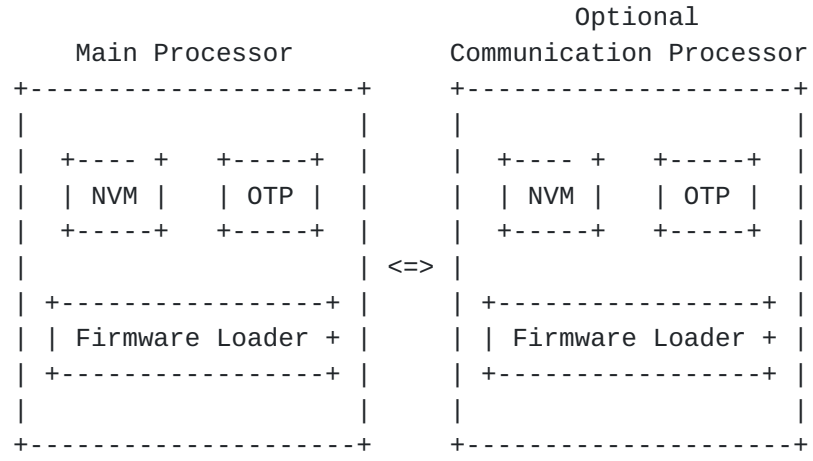


Figure1. Device architecture

Firmware update MAY be handled by a firmware loader (FLD) entity, and/or by other physical protocols (PHYP), for example Serial Programming (SP) or Parallel Programming (PP).

When OTP memory is available, it stores a permanent part of the update procedure (named firmware loader in this draft).

Non volatile memory such as FLASH may be fully erased. When no OTP is available the main processor may be totally reprogrammed through physical protocols; i.e. physical access to the device may lead to its full control.

A firmware loader enables the remote update of the NVR of the main processor. It MAY be secure (FLD-SEC) or not. If it is secure, a symmetric or asymmetric procedure (and associated keys) is used in order to check the firmware authenticity. The two main classes of

security procedures deal with symmetric algorithms (for example AES-

CCM) or asymmetric signatures (for example ECDSA). It MAY support post quantum [POSTQUANTUMCRYPTO] cryptographic algorithms.

Even if the firmware loader is secure, cryptographic keys may be recovered by side-channel attacks [SIDECHANNEL][DIVKEY]. Therefore Tamper Resistant key (TRT-KEY) is a very important attribute. The impact of a side channel attack may be limited to a single object if the keys are diversified (DIV-KEY).

We propose to characterize a device by a set (SecAtt) of five boolean attributes (0/1).

SecAtt = {OTP, FLD, FLD-SEC, TRT-KEY, DIV-KEY}

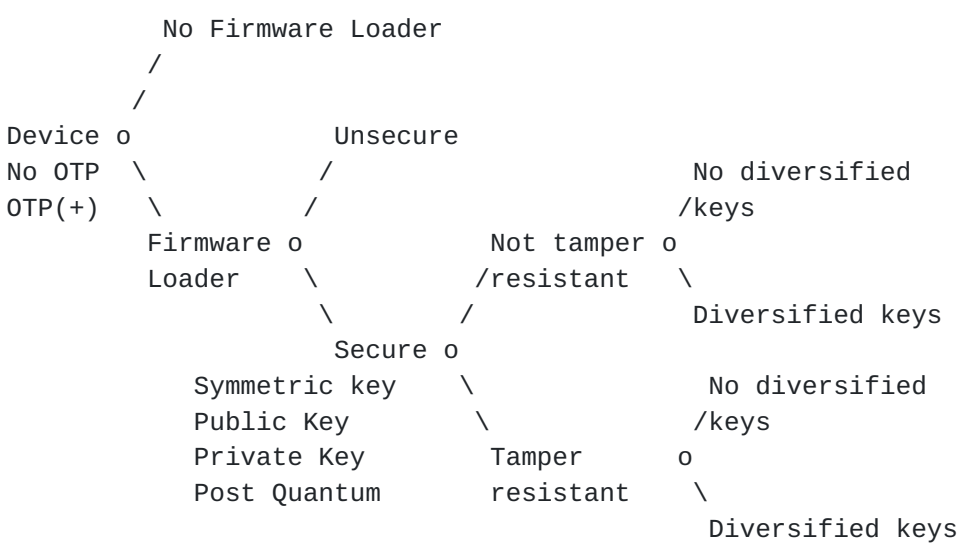


Figure2. Security classes

This leads to the definition of 6 classes of devices, embedding or not OTP resource, whose security increases with the class number. The suffix + indicates OTP availability.

Class0/Class0+ = {0/1,0}, no firmware loader, other attributes (excepted OTP) are not taken into account.
Class1/Class1+ = {0/1,1,0,0,0}, unsecure firmware loader
Class2/Class2+ = {0/1,1,1,0,0}, secure firmware loader, not tamper resistant, no diversified keys
Class3/Class3+ = {0/1,1,1,0,1} secure firmware loader, not tamper resistant, diversified keys
Class4/Class4+ = {0/1,1,1,1,0} secure firmware loader, tamper resistant, no diversified keys.
Class5/Class5+ = {0/1,1,1,1,1} secure firmware loader, tamper resistant, diversified keys.

For example

- Class0 objects are uploaded (flashed) thanks to physical protocols, and as an illustration may be updated via HTTPS requests.

- Many micro-controller units (MCU) support an unsecure bootloader and belong to Class1.
- Some USB flash drives [BADUSB] belong to Class1+; they include an unsecure bootloader stored in ROM.
- Some smart bulbs [DIVKEYS] devices are Class2 devices; they use secure bootloader with a single symmetric key shared by multiple devices
- SUIT protocols SHOULD target secure bootloader with public key i.e. Class2+, or secure bootloader with diversified symmetric key i.e. Class3+.
- Class4 uses a secure bootloader, with a single key shared by multiple devices, and protected by tamper resistant means.
- Highly secure devices similar to bank cards belong to Class5+.

## 2 Security Attributes

### 2.1 One Time Programmable Memory, OTP

The OTP attribute means that the main processor stores permanent software typically a firmware loader or a subset of this entity.

If no OTP is available the full memory content of the main processor can be erased and fully updated. No minimum device behavior is guaranteed in this case.

### 2.2 Firmware Loader, FLD

A firmware loader is mainly a command interpreter that enables logical/remote firmware update. It avoids the use of physical procedures such as Serial Programming a Parallel Programming. It is stored either in non erasable or erasable non volatile memory.

### 2.3 Secure Firmware Loader, FLD-SEC

A secure bootloader checks the authenticity and integrity of firmware updates by cryptographic means. This implies the use of symmetric secret keys, asymmetric private keys, or asymmetric public keys associated to certificates. Most of cryptographic algorithms may be broken by side-channel attacks.

If a long term vision is required it MAY support post quantum [POSTQUANTUMCRYPTO] cryptographic algorithms. Quantum computer may break asymmetric algorithm dealing with RSA or elliptic curves. In case of symmetric cryptography the recommended key size is about 256 bits.

### 2.4 Tamper Resistant Key, TRT-KEY

Cryptographic keys may be recovered by side-channel attacks. A tamper resistant computing environment SHOULD avoid these attacks.

### 2.5 Diversified Key, DIV-KEY

The use of diversified secret keys limits the side channel attack scope to a single object. The lack of tamper resistant computing and the use of single secret shared by multiple nodes MAY create major security threats.

## 3 IANA Considerations

TODO

## 4 Security Considerations

TODO

## 5 References

### 5.1 Normative References

[SUIT], Moran, B., Meriac, M., Tschofenig, H., and D. Brown, "A Firmware Update Architecture for Internet of Things Devices", draft-ietf-suit-architecture-01 (work in progress), July 2018.

### 5.2 Informative References

[SIDECHANNEL] David Oswald, "IMPLEMENTATION ATTACKS: FROM THEORY TO PRACTICE DISSERTATION", zur Erlangung des Grades eines Doktor ingenieurs der Fakultat fur Elektrotechnik und Informationstechnik an der Ruhr-Universitat Bochum, Bochum, September 2013

[DIVKEY] Eyal Ronen and Colin O'Flynn and Adi Shamir and Achi-Or Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction", Cryptology ePrint Archive, Report 2016/1047.

[POSTQUANTUMCRYPO] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Josang, "The Impact of Quantum Computing on Present Cryptography", International Journal of Advanced Computer Science and Applications (IJACSA), 9(3), 405-414, March 2018

[BADUSB] Karsten Nohl, Sascha KriBler, Jakob Lell, "BadUSB - On Accessories that Turn Evil", Blackhat USA 2014.

## 6 Authors' Addresses

Pascal Urien
Telecom ParisTech
23 avenue d'Italie
75013 Paris Phone: NA
France Email: Pascal.Urien@telecom-paristech.fr