SUIT Working Group
Internet Draft
Intended status: Experimental

P. Urien
Telecom ParisTech

April 21, 2019
Expires: October 2019

Security Classes For Software Updates for IoT
draft-urien-suit-security-classes-01.txt

Abstract

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). This classification creates 18 device classes.

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

.

Copyright Notice

Table of Contents

1 Overview

The [SUIT] working focuses on firmware update for Class 1 (as defined in RFC 7228) devices, i.e., devices with ~10 KB RAM and ~100 KB flash.

This draft attempts to define security classes for devices targeted by SUIT protocols. The goal is to provide a qualitative estimation of risk 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 SHOULD manage the update of other processor.

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.

```
                                             Optional
             Main Processor          Communication Processor
         +---------------------+     +---------------------+
         |                     |     |                     |
         |  +---- +   +-----+  |     |  +---- +   +-----+  |
         |  | NVM |   | OTP |  |     |  | NVM |   | OTP |  |
         |  +-----+   +-----+  |     |  +-----+   +-----+  |
         |                     | <=> |                     |
         | +-----------------+ |     | +-----------------+ |
         | | Firmware Loader + |     | | Firmware Loader + |
         | +-----------------+ |     | +-----------------+ |
         |                     |     |                     |
         +---------------------+     +---------------------+
```

Figure1. Device architecture

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

When OTP memory is available, it MAY 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 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 = {FML, OTP, FLD-SEC, TRT-KEY, DIV-KEY}

This leads to the definition of 2 + 16 = 18 classes of objects.
- {0,0,0,0,0}, no firmware loader, no OTP.
- {0,1,0,0,0}, no firmware loader, OTP available.
- {1,1/0,1/0,1/0,1/0}, firmware loader available.

For example some objects firmware (class = {0,0,0,0,0}) are just updated via HTTPS requests.

Some highly secure devices similar to banking cards, SHOULD have all the security attributes (class = {1,1,1,1,1});

2 Security Considerations for Firmware Update

2.1 Firmware Loader, FLD

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

2.2 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.

2.3 Secure Firmware Loader, FLD-SEC

A secure bootloader checks the authenticity and integrity of the firmware update 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 cryptographic algorithms.

2.4 Tamper Resistant Key, TRT-KEY

Cryptographic keys may be recovered by side-channel attack. A Tamper Resistant computing environment SHOULD avoid these attacks.

2.5 Diversified Key, DIV-KEY

The use of diversified secrets 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, Adi Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights", 2016 IEEE European Symposium on Security and Privacy (EuroS&P)

6 Authors' Addresses

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