Monthly Research

Overview and usage examples of TPM 2.0

FFRI, Inc.
http://www.ffri.jp

Ver 1.00.01

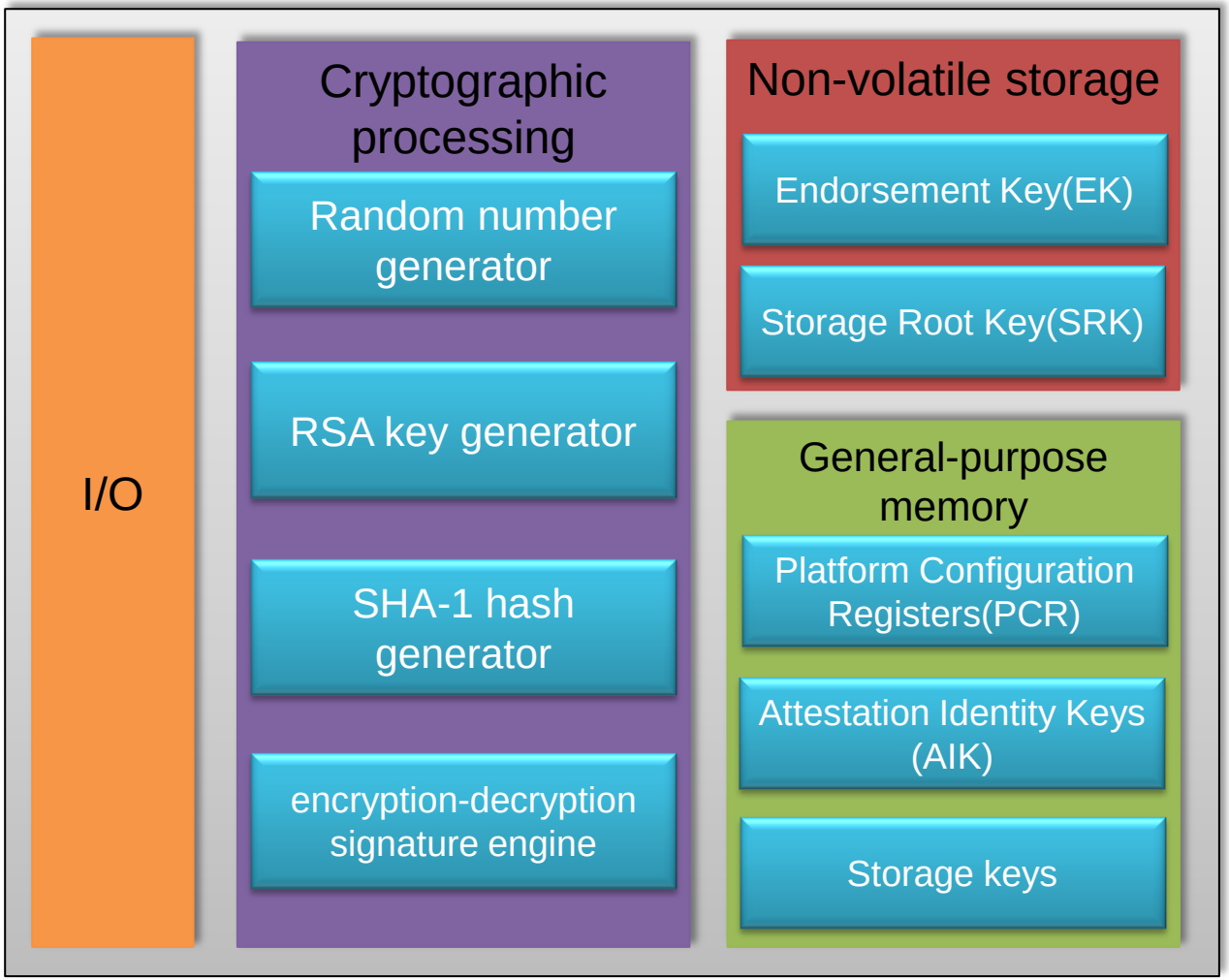
Introduction

- The “Trusted Platform Module (TPM)” is security chip which have hardware tamper-resistance for cryptography.
- Specification of the TPM has designed by “Trusted Computing Group (TCG)”.And they were released latest version TPM 2.0 in October 2014.
- It has become a high-performance configuration than before by such as to support more encryption algorithms.
- In this report, we show the overview of TPM 2.0 and usage example for IoT devices.

Agenda

- Basic structure of TPM
- Overview and difference between TPM 1.2 and TPM 2.0
- Threat example of IoT devices
- Usage example on IoT devices
- Applications and future of TPM
- Summary

Basic structure of TPM



https://en.wikipedia.org/wiki/Trusted_Platform_Module#/media/File:TPM.svg

Overview of TPM 2.0

- It has been enhanced from TPM 1.2 to support more platforms.
  - Adding encryption algorithms
  - Enhancing availability for application
  - Enhancing authentication feature
  - Simplifying of TPM management
  - Adding features that enhancing security of platform service

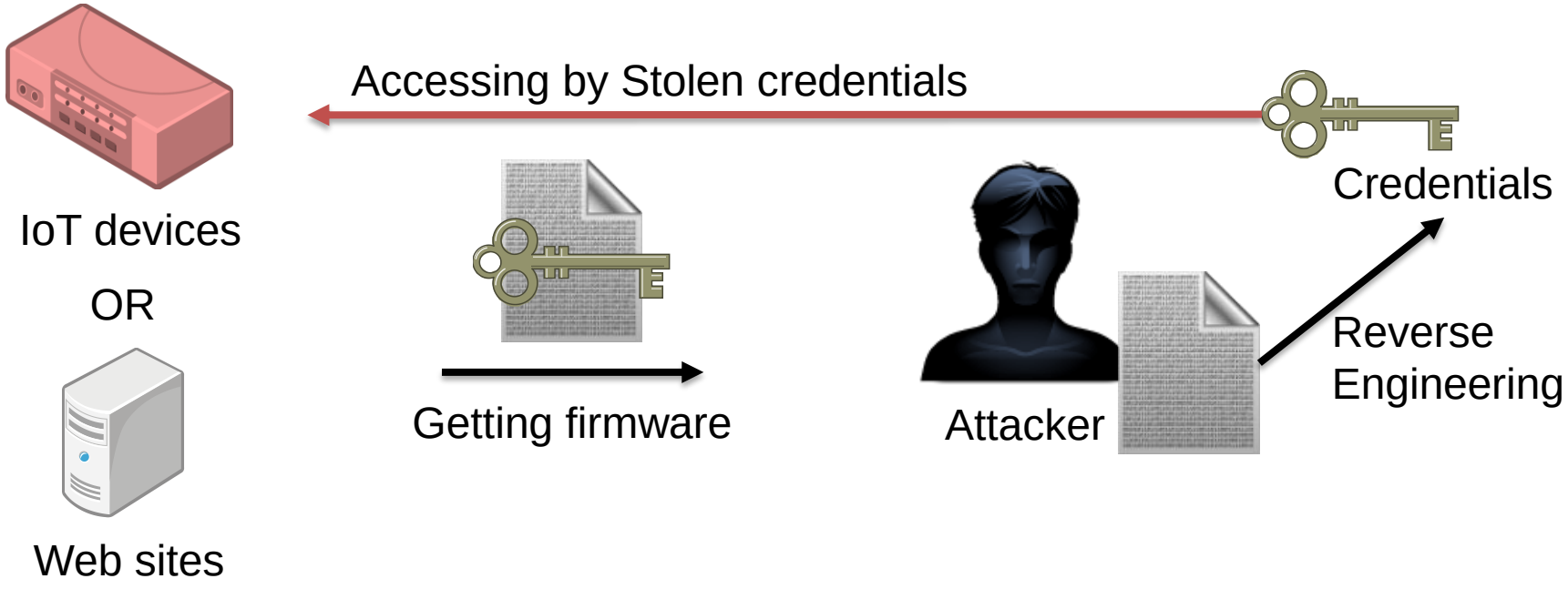
- TPM software stack specifications (TSS) have designed for various platforms such as PC, mobile, embedded and virtualization.
  - http://www.trustedcomputinggroup.org/developers/trusted_platform_module

Difference between TPM 1.2 and TPM 2.0

- **Cryptographic algorithms and primitives were added**
  - It becomes possible to make strong and multi-hierarchy encryption by combining multiple algorithms.
- **Multi-hierarchy**
  - Distribute the load of encryption
- **Multiple root key**
  - Make strong encryption by diversification of risk
- **Removing other than HMAC from authentication methods. Adding policy authorization**
  - No backward compatibility
  - Advanced authentication methods by password or policy are available
- **Extended Non-volatile storage(NVRAM)**
  - Supported counter, Bitmap, Extend

Threat example on IoT devices

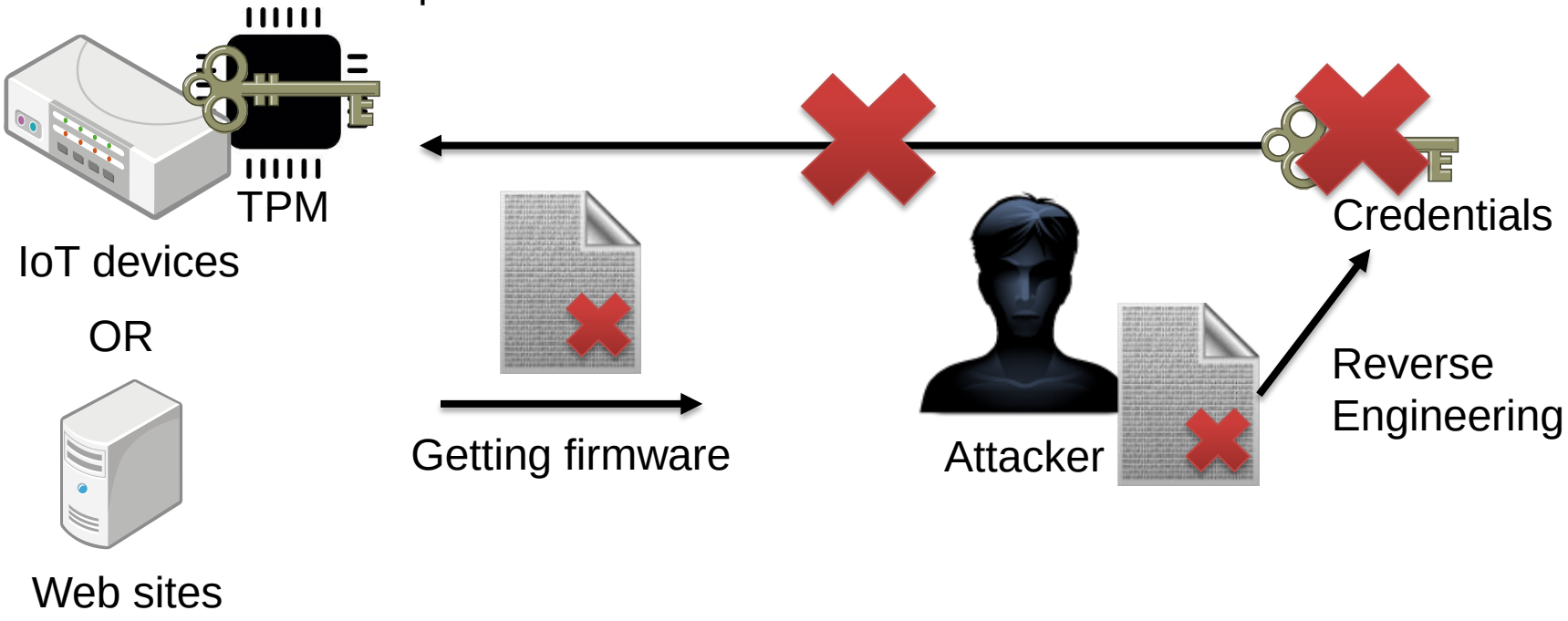
- Stealing credentials from firmware by reverse engineering.
- A lot of IoT devices had been hacked by using common credentials in same products stolen from firmware.



Usage example on IoT devices

- It is possible to protect credentials from reverse engineering by using TPM.

- It is impossible to steal credentials from firmware because TPM chip has hardware tamper-resistance.



Applications of TPM

- TPM has been adopted mainly for business laptop.
  - Windows Vista has supported TPM
  - Windows 8 has supported TPM 2.0
  - TPM is available for BitLocker which is disk encryption feature on Windows.
  - Other applications of Windows security features
    - Secure Boot, Trusted Boot
    - Windows Hello
    - Device Guard
- Recently, the following devices also have adopted TPM.
  - OnHub （Google Wi-Fi Router）
  - Surface Pro 3（Microsoft Tablet）

TPM for automotive

- TCG has formulated "TPM 2.0 Automotive Thin Profile" for automotive.

- It requires hard specs such as the following.
  - Temperature, vibration, limited memory usage, reduction in power consumption, long-term service life

- Features of “TCG TPM 2.0 Automotive Thin Profile”
  - Testing ECU firmware and software integrity
  - Management of encryption keys used by ECU
  - Authentication and assurance of the integrity of ECU
  - Secure Update of ECU firmware
  - Protecting memory from write-back of information in ECU

Summary

- TPM 2.0 possible to introduce to platforms or systems easily by such as supporting multi encryption algorithms.
- TPM is available to protect IoT devices from attacks.
- TPM is expected to apply in various fields like “TCG TPM 2.0 Automotive Thin Profile”.

References

- Trusted Platform Module - Wikipedia
  https://ja.wikipedia.org/wiki/Trusted_Platform_Module
- Trusted Platform Module Library Part 1: Architecture
  http://www.trustedcomputinggroup.org/files/static_page_files/8C56AE3E-1A4B-B294-D0F43097156A55D8/TPM%20Rev%202.0%20Part%201%20-%20Architecture%2001.16.pdf
- Trusted Platform Module Library Part 2: Structures
  http://www.trustedcomputinggroup.org/files/static_page_files/8C56AE3E-1A4B-B294-D0F43097156A55D8/TPM%20Rev%202.0%20Part%201%20-%20Architecture%2001.16.pdf
- TCG PC Client Platform TPM Profile (PTP) Specification
- http://www.trustedcomputinggroup.org/files/static_page_files/28CBF489-1A4B-B294-D038AC358AD39A6A/PC%20Client%20Specific%20Platform%20TPM%20Profile%20for%20TPM%202%200%20v43%20150126.pdf
- インフィニオン、関心が高まっているIoTやコンピューティングに向けた認証セキュリティ技術「OPTIGA™ TPM2.0」が初めてコモンクライテリア認証を取得 - Infineon Technologies
- http://www.infineon.com/cms/jp/about-infineon/press/press-releases/2015/INFCCS201509-083.html
- 自動車にもPCと同じセキュリティチップ「TPM」を搭載へ、規格策定が完了
- http://monoist.atmarkit.co.jp/mn/articles/1504/14/news026.html
- TCG TPM 2.0 Automotive Thin Profile
- http://www.trustedcomputinggroup.org/files/static_page_files/72EC6BF8-1A4B-B294-D07BBA4AE8F4A04F/TCG%20TPM%202.0%20Automotive-Thin%20Profile_v1.0.pdf

Contact Information

E-Mail ：research—feedback@ffri.jp
Twitter：@FFRI_Research