Monthly Research

TPM 2.0 の概要と IoT デバイスでの利用例

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

はじめに

- Trusted Platform Module (TPM) は、安全な暗号処理を実現するための、ハードウェア耐タンパー性を持つセキュリティチップのことである。

- TPM の仕様は TCG (Trusted Computing Group) という団体を中心に検討され、ISO/IEC により標準化されている。最新版は 2014 年 10 月にリリースされた TPM 2.0 である。

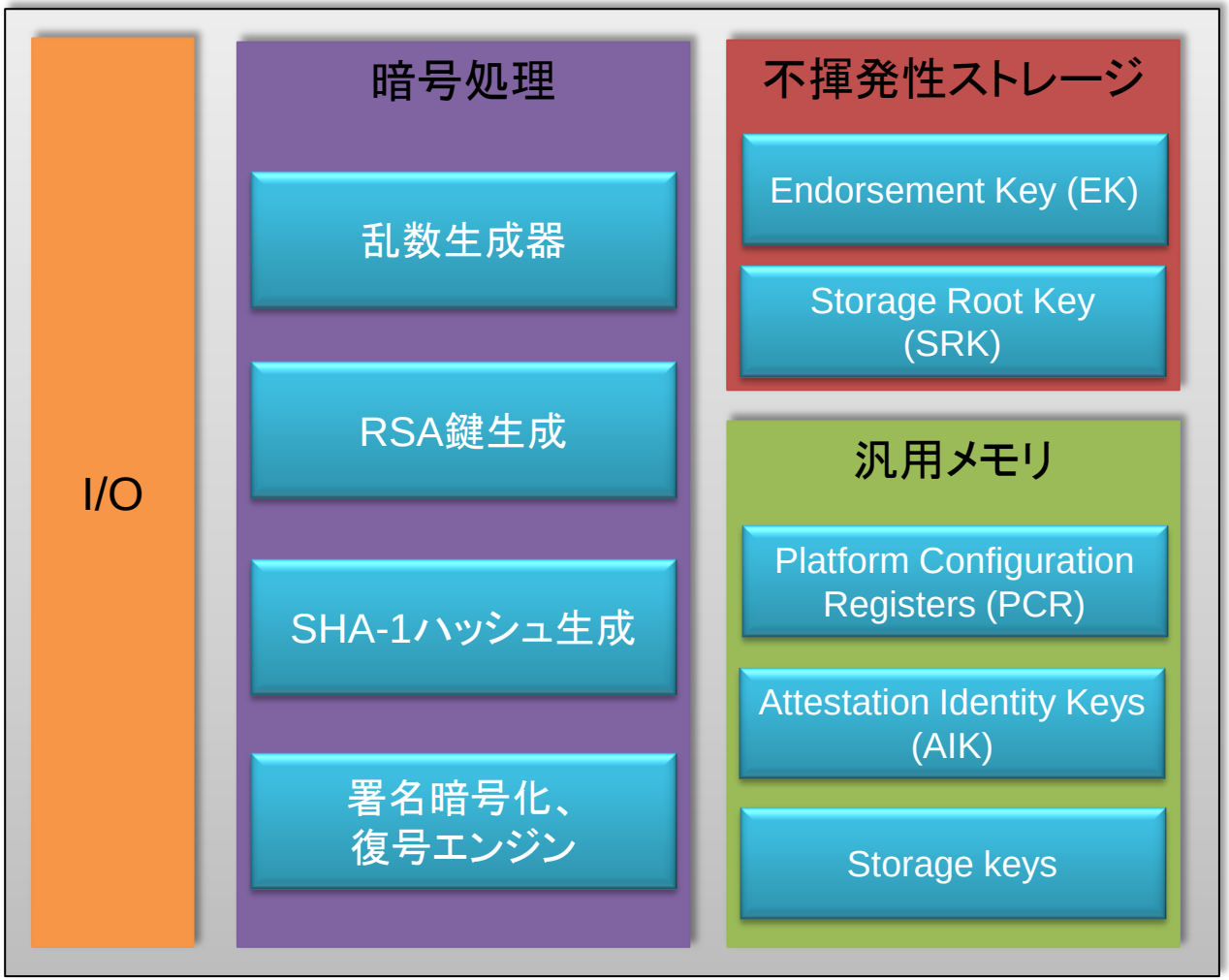
- TPM 2.0 は TPM 1.2 と比べて、利用可能な暗号アルゴリズムが増えるなどの強化が行われている。

- 本レポートでは TPM 2.0 の概要と最新の IoT デバイスでの利用例などを紹介する。

アジェンダ

- TPM の基本構造
- TPM 2.0 の概要と TPM 1.2 との比較
- IoT デバイスにおける脅威の例
- IoT デバイスでの TPM の利用例
- TPM 採用事例と今後の可能性
- まとめ

TPM の基本構造



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

TPM 2.0 の概要

- 様々なプラットフォームで TPM の活用を実現するため、TPM 1.2 から以下の様な点が強化された。
  - 追加の暗号化アルゴリズムのサポート
  - アプリケーションへの TPM の可用性の強化
  - 認証機構の強化
  - TPM 管理の簡素化
  - プラットフォームサービスのセキュリティを強化するための追加機能

- PC、モバイル、組み込みおよび仮想化プラットフォーム用に別に TPM ソフトウェアスタック仕様(TSS)の仕様が策定されている。
  - http://www.trustedcomputinggroup.org/developers/trusted_platform_module

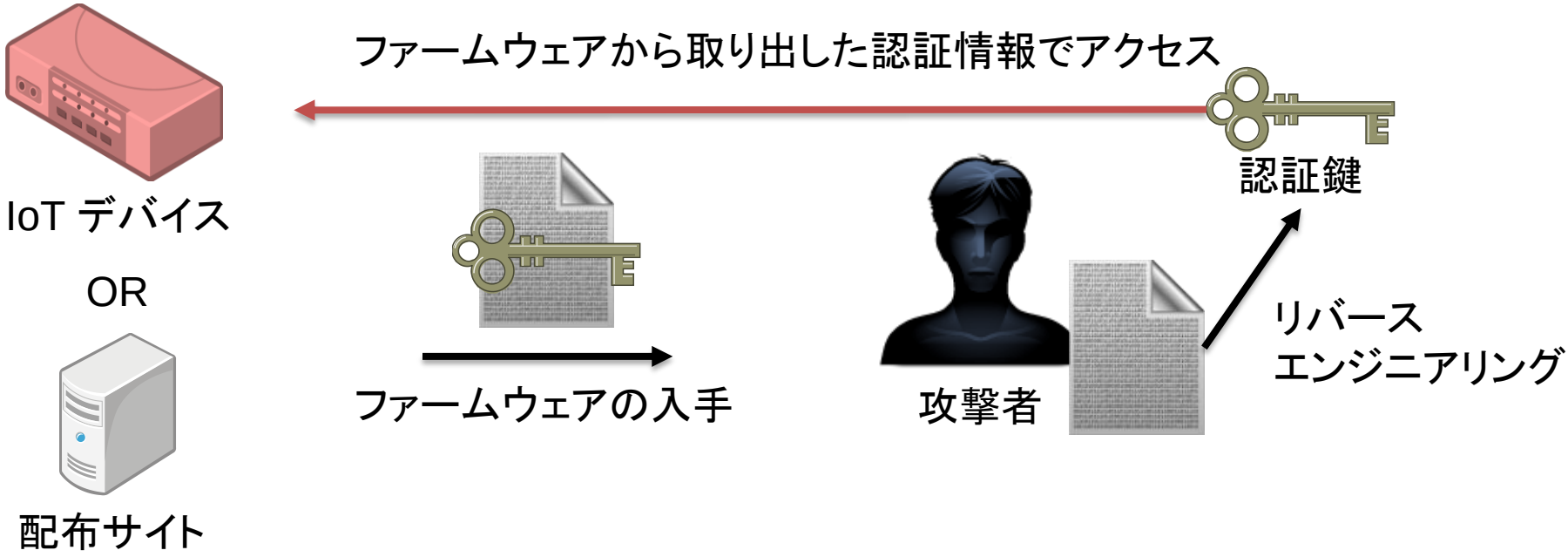
TPM 1.2 と TPM 2.0 の比較

- **対応アルゴリズム、暗号プリミティブが増加**
  - 複数のアルゴリズムを組み合わせることで、強固かつマルチ階層な暗号化が可能となった。
- **多階層ヒエラルキー構造に対応**
  - 暗号化の負荷分散を実現。
- **ルートキーが複数鍵に対応**
  - リスク分散による暗号強化を実現
- **HMAC以外の認証方式が除外され、パスワード、ポリシーによる認証に対応**
  - 対応認証方式に差異が生じ、下位互換性に影響。
  - パスワード、ポリシーを受け入れることで先進的な認証方法に対応。
- **不揮発性メモリ（NVRAM）が拡張**
  - カウンター, Bitmap, Extend が新たに対応

IoT デバイスにおける脅威の例

- IoT デバイスにて懸念される脅威として、ファームウェアのリバースエンジニアリング等による認証情報の窃取が考えられる。

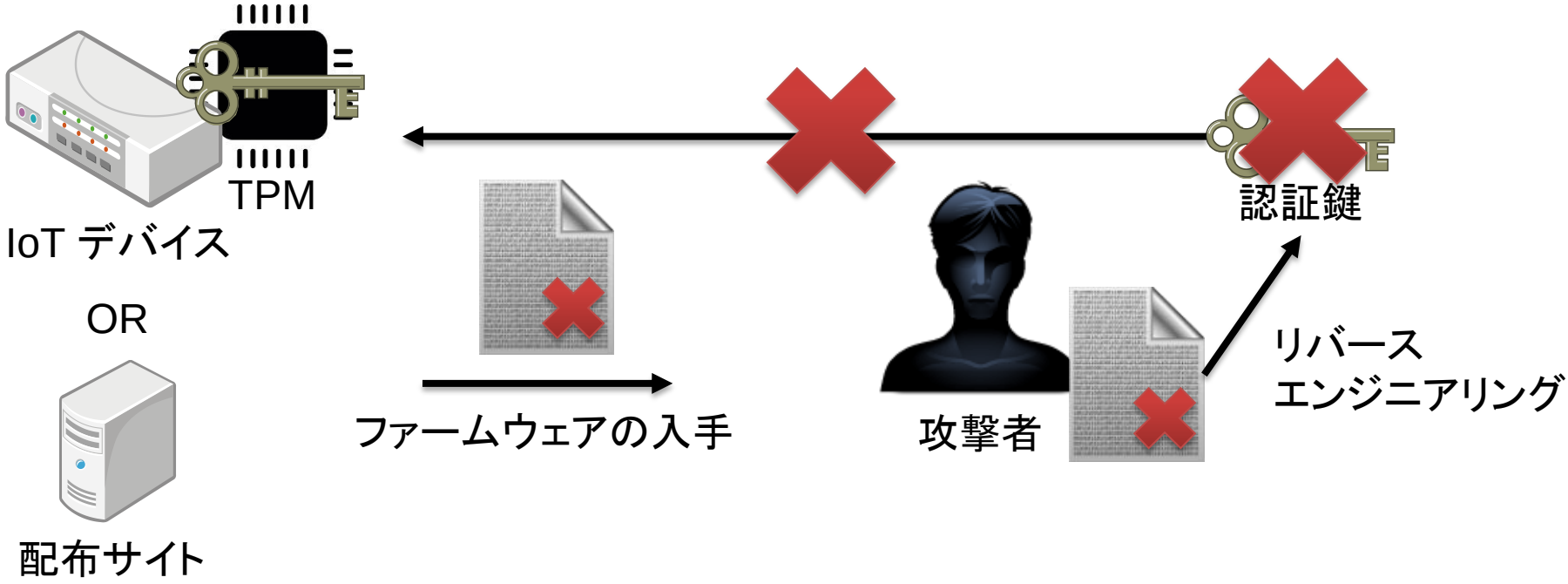
- これまでも多くのネット接続デバイスのファームウェアから非公開の認証情報やコマンド、バックドア等が明らかにされ、通信が傍受されるなどの攻撃に悪用されている。



IoT デバイスでの TPM の利用例

- 前述のような脅威への対策として、認証情報などの重要情報を TPM を用いて保護する方法がある。

- TPM は耐タンパー性を備えた別チップとして実装されるため、ファームウェアの解析では重要情報を窃取することは不可能である。



TPM の採用事例

- これまで TPM チップは主にビジネス向けのノート PC を中心に採用されてきた。
  - Windows は Windows Vista から TPM をサポートしており、Windows 8 からは TPM 2.0 をサポートしている。
  - Windows では、ドライブ暗号化機能である BitLocker で使用する鍵を TPM を利用してより安全に保管することができる。
  - 他にも TPM を利用して強化できる Windows のセキュリティ機能がある
    - Secure Boot, Trusted Boot
    - Windows Hello
    - Device Guard
- また、最近では次のようなデバイスにも TPM チップが搭載されている。
  - OnHub （Google 社製 Wi-Fi ルーター）
  - Surface Pro 3（Microsoft 社製タブレット端末）

自動車における TPM 活用の可能性

- Trusted Computer Group (TCG) は TPM の自動車向け仕様「TCG TPM 2.0 Automotive Thin Profile」も策定している。

- 従来の TPM チップと比べ、PC よりも過酷な環境である自動車向けに、温度や振動、メモリ使用量の制限、消費電力の低減、長期にわたる製品寿命などが要求される。

- TCG TPM 2.0 Automotive Thin Profile 機能例
  - ECU のファームウェア／ソフトウェアの完全性検査
  - ECU で用いられる暗号鍵の生成、収納、管理
  - ECU の完全性の認証と保証
  - ECU のファームウェア／ソフトウェアのセキュアな更新
  - ECU 内の情報の書き戻しを防ぎ、記憶装置を安全に管理

まとめ

- TPM 2.0 では対応暗号化アルゴリズムを拡充するなど、多くのプラットフォーム、システムで導入しやすくなっている。
- IoT デバイスで扱う認証情報などの重要情報を TPM に保存することで、リバースエンジニアリングなどの脅威に備える事ができる。
- TPM技術はTCG TPM 2.0 Automotive Thin Profile のように広い分野での応用が期待されており、それに応えるポテンシャルを持っていると言える。

参考情報

- 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