NSF2019
【A2】パネルディスカッション
IoT時代の「トラスト」は何か？
- IoTにおける標準化 -

2019/1/22

株式会社レピダム
菅野 哲

lepidum
https://lepidum.co.jp/

この人、誰？

- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - 株式会社 レピダム 代表取締役
  - ココン株式会社 技術研究室 室長
- どんなことやっていた／やっているの？
  - 学生時代～
    - 暗号プロトコルの研究、ベンチャーで暗号製品を売り歩く（？）
  - 社会人時代～
    - 暗号ライブラリや情報セキュリティ関連システム開発
    - IETFなどでCamellia関連の標準化活動
  - ここ最近
    - もっぱら会社経営と営業的な活動が色濃い
    - TCG Invited Expertとして活動（2018年10月～）

本パネルディスカッションの俯瞰図

ここではIoT時代の「トラスト」について考える上での**標準化に関する情報**を提供します

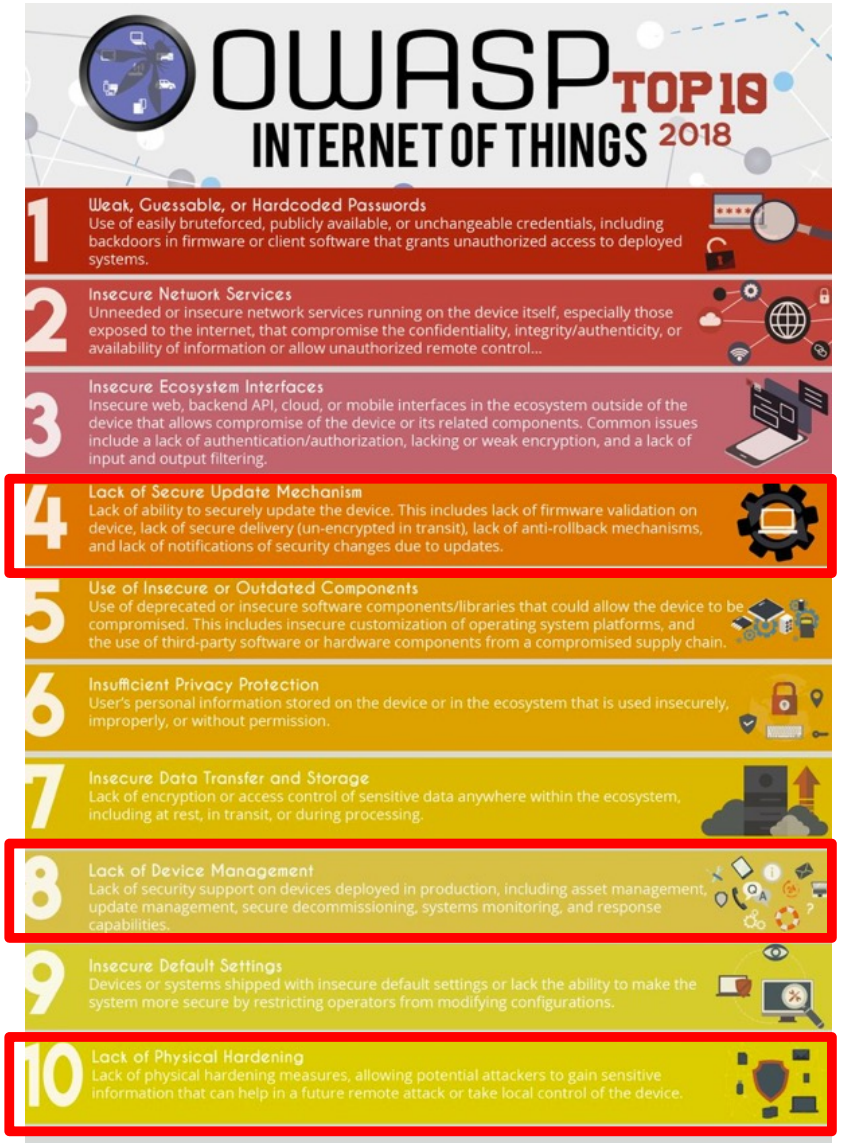
(`･ω･´)ゞ

IoTにおけるトラストを脅かす Attack Surface

※ Attack Surface： ざっくり説明すると「攻撃可能な箇所」という感じです。

lepidum
https://lepidum.co.jp/

OWASP Internet of Things TOP10



https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

IoTデバイスで留意すべき10の脆弱性が共有されています。

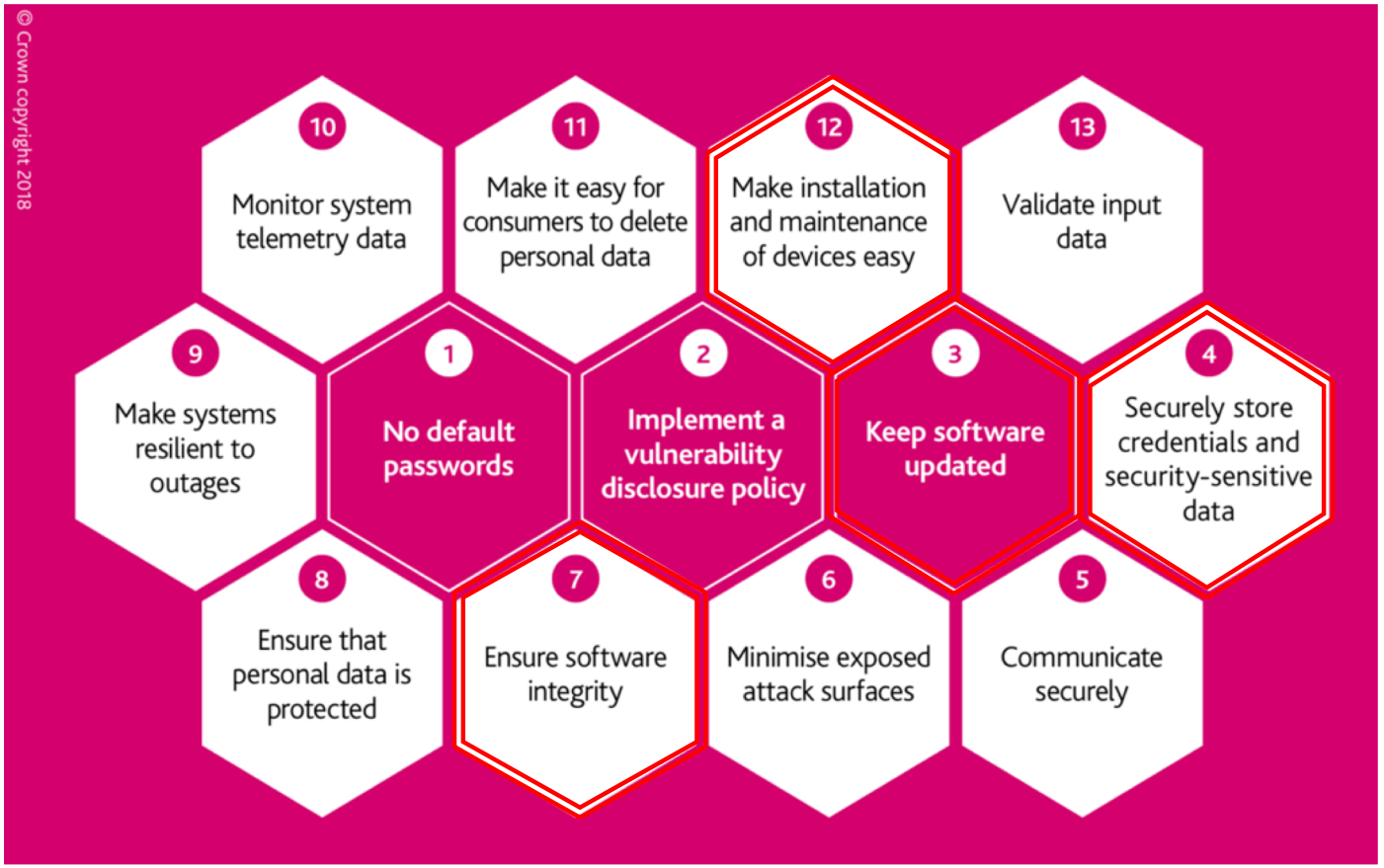
例えば・・・

- 安全な更新メカニズムの欠如
- デバイス管理の欠如
- 物理的な堅牢化の欠如

「トラスト」を実現に向けた課題

Code of Practice for Consumer IoT Security

英国デジタル・文化・メディア・スポーツ省によるデバイスメーカー、IoTサービス提供事業者、モバイルアプリ開発事業者、小売業者に対するIoTセキュリティに関するドキュメントです



・重要なデータを安全な保存

・ソフトウェアの完全性確保

・容易なデバイスの設置＆メンテナンス

運用的な観点での考慮すべき事項も

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

標準化とIoT

標準種別標準化団体

- デジュール標準

- フォーラム標準

- デファクト

IETFにおけるIoTでのトラスト

- IETFはインターネットプロトコルに関する標準化団体のため、IoTに関する通信プロトコルを検討しているが、今回は「**トラスト**」に関連するWGを紹介します。

- INT Area
  - lwig (Light-Weight Implementation Guidance) WG

制約のある機器（例：IoT）に関する利用を主眼に検討

- SEC Area
  - SUIT (Software Updates for Internet of Things) WG
  - TEEP (Trusted Execution Environment Provisioning) WG
  - RATS (Remote ATtestation ProcedureS) **BoF**

IoTでのトラストを実現するための仕組みを検討

https://datatracker.ietf.org/wg/

lwig WG

- 制約のあるデバイスで実際に利用され他のデバイスとの相互運用性に影響を及ぼさない技術を題材にしています。検討範囲としてメモリ使用量、電力使用量の削減などです。

- 代表的なドキュメント
  - RFC7228, Terminology for Constrained-Node Networks
    - CPU、メモリ、電力使用量など制約された機器に対して、処理能力毎にクラスが定義
    - 具体例：
      - Class 0 Device：
        - ROM « 100KiB / RAM « 10KiB とサイズ 小
        - デバイス単体ではインターネット接続不可
        - SSL/TLSなどのセキュア通信は困難
      - Class 1 Device：
        - ROM ~100KiB / RAM ~ 10KiB とサイズ 小
        - インターネットに直接接続可能でSSL/TLSなどの通信はギリギリ可能
      - Class 2 Device：
        - ROM ~ 250KiB / RAM ~ 50KiB とサイズ 小
        - PCで利用可能なプロトコルスタックが全て利用可能

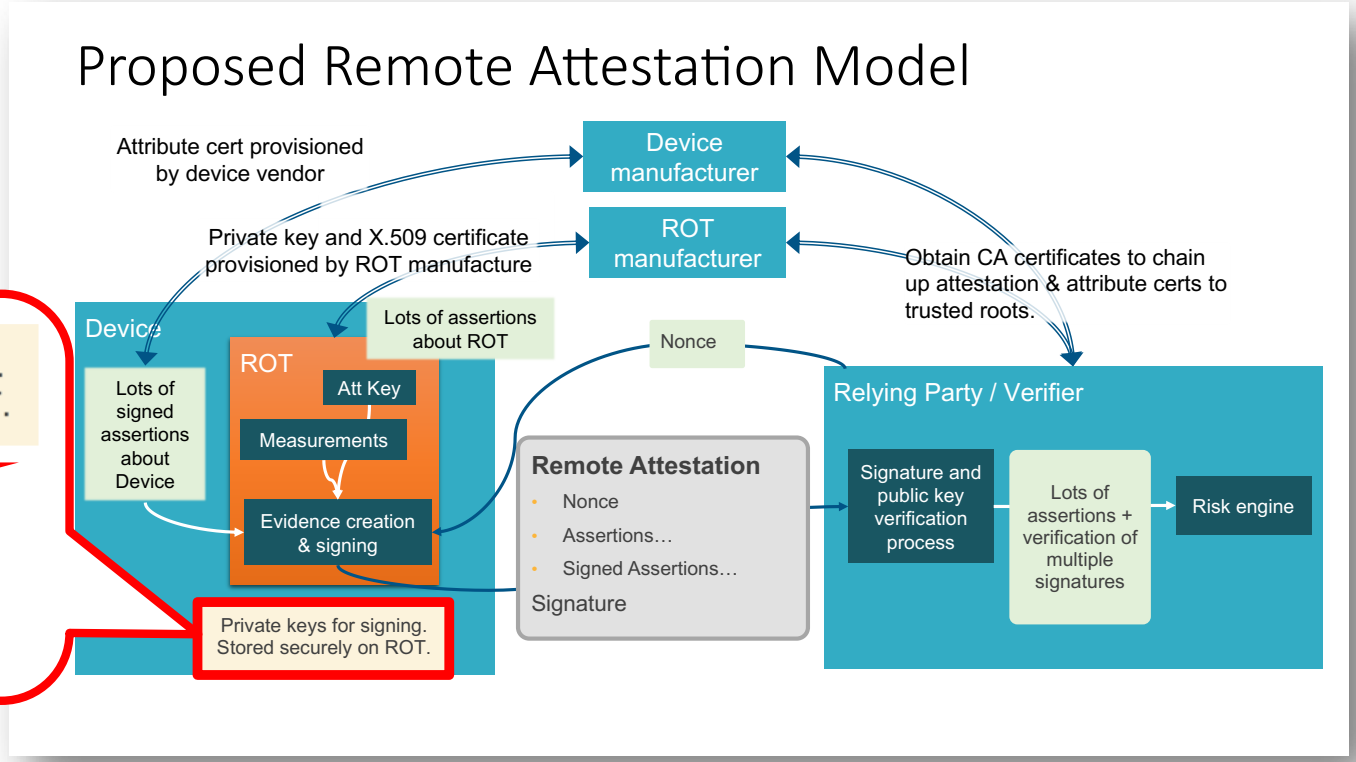
SUIT WG & TEEP WG

- ほぼ同時期に設置され、ターゲット的に似てるけど異なる「安全なアップデート」を行うための仕組み

- SUIT WG
  - IoT機器の安全な**ファームウェア更新**の仕組みを検討
  - 取り扱うデバイス性能
    - Class1 (~10KiB RAM、~100KiB ROM) が対象
    - ファームウェア以外(例:PCのソフトウェア)の更新は対象外
- TEEP WG
  - TEE(Trusted Execution Environment)上で動く信頼できる**アプリケーション**(TA: Trusted App)**のライフサイクル管理**(インストール、アップデートなど)プロトコルを検討

RATS BoF

- IoTデバイス等が自身の正当性(システムとして認定されたものであること)を証明する仕組みを検討
- Remote Attestation
  - ベンダーを信頼する第三者があるデバイスをそのベンダーによって製造されたものであることの検証



Private keys for signing. Stored securely on ROT.

安全に秘密鍵が格納される前提

https://datatracker.ietf.org/meeting/103/materials/slides-103-rats-rats-problem-statement-02

参考：Attestationに関する類似および関連技術

- IETF 102 secdispatch ”Entity Attestation Token (EAT)”においてAttestationに関する類似および関連技術が示されています。

Technology	Use Case
FIDO Attestation	Attestation of FIDO Authenticator implementations
Android Key Store	Attestation key pairs in the key store
NEA	Collect and send endpoint security posture (e.g. anti-virus SW state and config) to enterprise collection / monitoring point
RATS / NSF	Attestation / Measurement of SW on Network Security Functions (e.g., firewalls)
TPM	Attestation / Measurement of SW running on a device
BRSKI / Zero Touch	Authenticates IoT devices for enrollment in IoT management system

https://datatracker.ietf.org/meeting/102/materials/slides-102-secdispatch-entity-attestation-token-draft-mandyam-eat-00-00

パネルディスカッションに向けたトピックス

IETFにおいてIoT時代の「トラスト」を実現するためのビルディングブロックは整いつつあります。その一方で・・・

- 標準化によりトラストを実現する仕組みが提供され安全に？！
  - 統一化される事で攻撃対象が絞られるリスクが顕在化
- トラストを実現する仕組みが正しく機能しても、悪意あるデバイスだった場合は...
  - 製造メーカー自体のトラスト？！
- 機能制約があるIoT自体を頼るには、限界があることを意識しておく必要があるのでは？
  - デバイス数が増加した時に点での管理が困難になる？！
  - トラストを考慮した管理基盤が急務？