WASEDA University

Smart SE

スマートエスイー 修了制作

セキュリティフレームワーク・ナレッジベース「MITRE ATT&CK」のIoTプラットフォームへの拡張

長柄 啓悟

開発における問題点

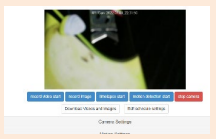
- 近年、IoT機器が普及し、その脆弱性も明らかになり、その脆弱性とその対策を検討する必要がある。
- 一方、攻撃者の攻撃手法・戦術を分析して作成されたセキュリティのフレームワーク・ナレッジベースである"MITRE ATT&CK"などでは、IoTシステムを対象としたものは、まだリリースされていない。

手法・ツールの適用による解決

- 「MITRE ATT&CK」をIoT（プラットフォーム）への拡張し、その整理・検証を実施する。各IoT（プラットフォーム）に対する「MITRE ATT&CK」のマッピングを完成させ、実際の脆弱性や攻撃の実施によりその妥当性を確認する。

「MITRE ATT&CK」をIoT（プラットフォーム）への拡張

- Raspi＋Webカメラで、ネットワークカメラの開発

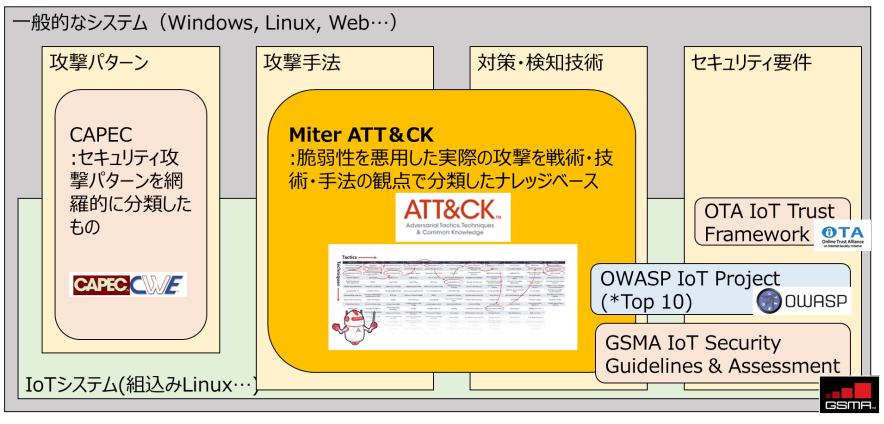


- STRIDE観点で脅威を洗い出し

IoTシステムにおける攻撃手法（Miter ATT&CK）ベースでのより網羅的なセキュリティ評価の実現

Miter ATT&CKによる嬉しさ

- ATT&CKのような攻撃手法観点のものは、他にないため、今回の取り組みにおけるATT&CKにおける対応付けは、網羅的で有効
- IoTシステム観点で、今回の取り組みのように整理し、手順化して実施したことによるうれしさは他のシステムにも活用可能



結果

Miter ATT&CKと対象シナリオの対応付け結果（一部抜粋）

- ネットワークカメラにおける具体的な攻撃手法を洗い出し
- セキュリティ要件（OWASP IoT ProjectのTop 10）とも、対応付け関連を確認。