MITSUBISHI ELECTRIC
Changes for the Better

製品セキュリティと研究開発

木藤 圭亮(三菱電機/ICSS)

CWS2018 in CSS2018@長野

三菱電機株式会社

MITSUBISHI ELECTRIC
Changes for the Better

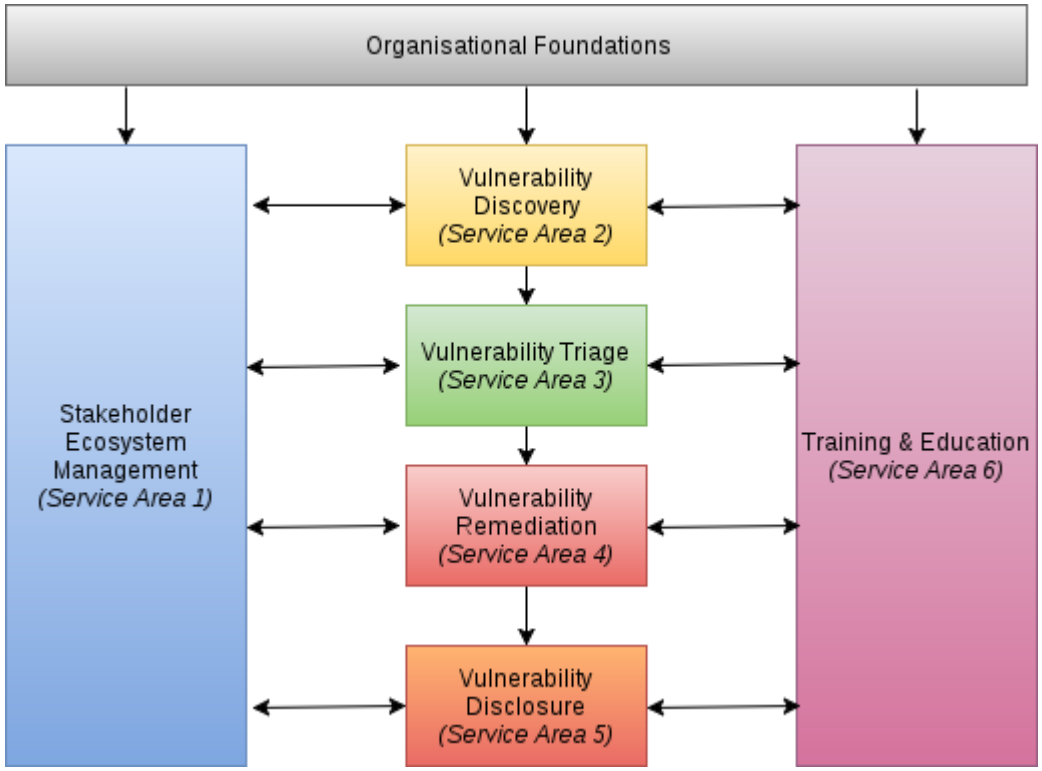
自己紹介

- 木藤 圭亮(きとう けいすけ)
  - 研究所にてサイバーセキュリティ関連を主に担当
  - 守るための技術、それを評価する技術(模擬攻撃技術)
  - いろんなモノのセキュリティ技術を幅広く担当

- そのほか
  - 電子情報通信学会 ICSS研究会 幹事補佐(2018-)
  - セキュリティ・キャンプ全国大会講師(2016-18)
  - IoTSecJP(http://ruffnex.net/iotsecjp/) 運営スタッフ

製品セキュリティの動向

- メーカー各社でPSIRT設置の動きが強まる
  - Black Hat/DEF CON等で製品の脆弱性が多数報告
  - FIRST PSIRT Services Framework v1.0



PSIRT Organizational Structure(FISRTより抜粋)

車載機器の分解・解析(2015)

- Jeep Cherokee Hack
  - “Remote Exploitation of an Unaltered Passenger Vehicle”(2015)
  - リバースエンジニアリングで車載機器の脆弱性発見

- 車載機器の分解とファームウェア抽出
  - Parking Assist Module(PAM)
  - PAMのMCUからファームウェア抽出
  - ファームウェアを専用ツールで解析

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)

Chris Valasek (cvalasek@gmail.com)

August 10, 2015

引用元：http://illmatics.com/Remote%20Car%20Hacking.pdf

工場ロボットコントローラ(2017)

- ロボットコントローラも分解解析
  - “Breaking the Laws of Robotics: Attacking Industrial Robots”(2017)
  - ファームウェア解析
  - 古いコンパイラ・ライブラリを使用
    - 保護機構が無く、メモリ破壊が容易
- 自動設定機能を悪用
  - 認証無しでFTPログイン可能(!?)
- リバースエンジニアリングで
  - 複数の脆弱性を発見

Industrial Robots Security

A joint research project between Politecnico di Milano and Trend Micro's FTR

引用元：http://robosec.org/

MITSUBISHI ELECTRIC
Changes for the Better

IoTSecJP

- IoT Securityを日本で盛り上げるコミュニティ
  - IoT機器の脆弱性動向
  - 機器のリバースエンジニアリング技術
  - サイドチャネル攻撃技術
  - IoT機器ペネトレーションテストの技術など

- 多くの情報は英語
  - IoTSecJPで最新のIoTセキュリティ情報を発信
  - 日本語で発信 → 日本製品をセキュアに！

IoTSecJP

ドキュメント

Vuln IoT
脆弱なIoTシステムについて
(著) 黒林檎

黒林檎のお部屋
IoTハック
黒林檎のお部屋~IoTハック編~
(著) 黒林檎

JTAG HACK
JTAGハッキングドキュメント
(著) 黒林檎

SP
SPIハッ
キュメン
(著) 黒林

FW
ファームウェア解析
(著) Yuki

UART
UARTハッキング
(著) Yuki

SPI HACK
SPIハッキング
(著) Yuki

IoTS
♬「IoT
ウェアと
(著) Yul

SDR
Car_SDR_replay.pdf
(著) Yuki

JTAG
JTAGハッキング
(著) Yuki

RFID
RFIDハッキング
(著) Yuki

http://ruffnex.net/iotsecjp/

https://iotsecjp.booth.pm/items/820202

PSIRTも情報交換が大切？

- PSIRTならでは？
  - いろいろな対象がある
    - CSIRTはコンピュータのみ。PSIRTは全ての製品。
    - それぞれのメーカー(業種)にあった組織形態
  - 脆弱性を作らない or 見つけるための技術
    - セキュアコーディング
    - (非情報)機器へのペネトレーションテスト
  - 攻撃者にハックされにくくする技術
    - ファームウェア難読化
    - デバッグポート無効化 or 回路図工夫など

まとめ

- メーカーでPSIRT設立の流れ
  - 組織的にどうすれば良いか、探り探りの状態
  - 技術的に対応できる人が不足
- 製品の脆弱性は公開される
  - Black Hat/DEF CONなどで公開
  - 脆弱性を世に放たないことが重要
- 「脆弱性を見つける人」と「報告される人」
  - 見つける人が研究領域のときもある
  - 報告される人の属する組織の構成が研究領域のときもある