2021年度
ISSスクエアシンポジウム
研究成果報告

2022/02/24

システム分科会

システム分科会のテーマ（概要）

● 概要

“The Information Security of things”をキーワードに、一般家庭の機器に組み込まれる小さいITシステムから、社会インフラの中に組み込まれる大規模ITシステムまでを俯瞰し、それを支えるセキュリティシステム技術の現状と課題について、研究を行っている。

● メンバーリスト（院生17名、指導教授1名）

RL　:情セ大　大久保　隆夫

幹事

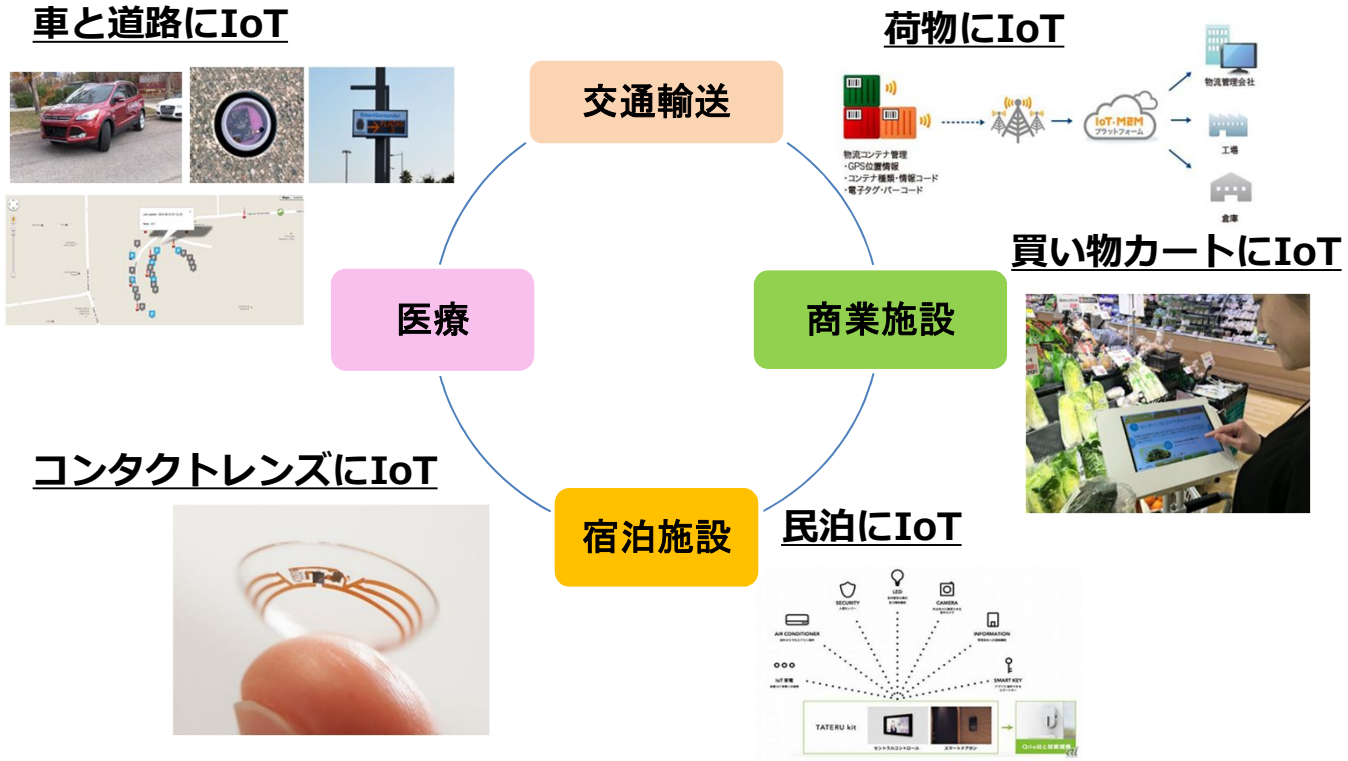
情セ大 M1：大木 圭介
中央大 M1：東 拓矢

メンバー

中央大：M1阿部 忠仁、M2小林 洋明、M2前川 美里
情セ大：M1末吉 璃子、M1上野 瑞己、M1林 泊舟、M1森田 叡
M1田代 雄也（1年制）M1米田智紀（NW分科会から出向）
M2荒木 粛志、M2仙田 眞之、M2橋本 真、M2何 其皓、
M2床波 大貴、M2鈴木 智之、M2梅田 真子

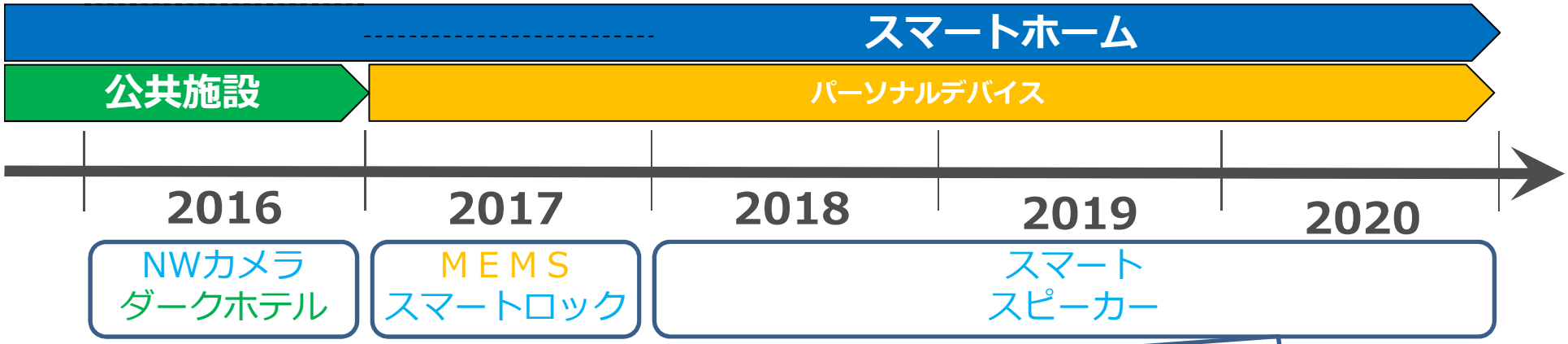
システム分科会のテーマ

- The Internet of Thing(IoT)s
  あらゆるものがインターネットにつながる（国内IoT市場は2025年に10.2兆円規模に）
  ※IDC Japan「国内IoTインフラ調査市場予測」
  https://www.idc.com/jp/research/report-list?search=JPJ46558621&document=JPJ46558621



キーワード：IoTの脅威検証

過去の取り組み



脅威シナリオの実現可能性検証
＋新たなAttack Surfaceの模索

キーデバイス：Webカメラ、スマートロック 、スマートリモコン、Firewalla


Web
カメラ


スマート
ロック


スマート
リモコン

Firewalla


Cujo smart firewall


Bitdefender box2

選定理由

- 比較的安価に入手が可能
- 現在普及しつつあるデバイスに新たな脅威が存在

今年度の取り組み～脅威シナリオ～

スマートホームの脅威シナリオ検証（前年度より継続）

分科会全体（これまでの脅威シナリオを踏まえ）

→アプローチを変えた脆弱性検証

例：アプリケーションの改ざん（無限ループ処理）、
第三者攻撃（MITM攻撃）　など

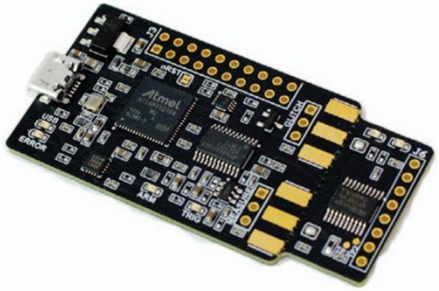
サイドチャネル攻撃班（新たな脅威シナリオの検討・実証）

→暗号化回路の消費電力の解析

ドローン班（製品の安全性の調査）

→擬似アクセスポイントからの攻撃

→root権限の奪取やリバースエンジニアリング　など



Holy Stone S-120D

サイドチャネル攻撃班

メンバー

M1：大木 圭介, 東 拓矢
M2：梅田真子、床波大貴

サイドチャネル攻撃班の研究概要

背景

IoTデバイスが急増する中、
セキュリティ対策をしなければいけない

システム分科会として
ハードウェアレベルでの攻撃手法を検証する

目的

① 電力解析攻撃について理解を深める
② 市販の攻撃ツールを用いて、攻撃手法を理解する
③ 実際のIoTデバイスへ攻撃を行い、対策を検討する(未達成)

電力解析攻撃について

● サイドチャネル攻撃とは

非侵入型攻撃の一種。
コンピューターや周辺機器の動作により生じる消費電力や処理時間などの物理量を解析し、秘密鍵やパスワードなどの情報を盗み取る
例）・タイミング攻撃：入力に対する処理時間を解析する
・電力解析攻撃　：消費電力を解析する
・電磁波解析攻撃：機器から生じる電磁波を解析する

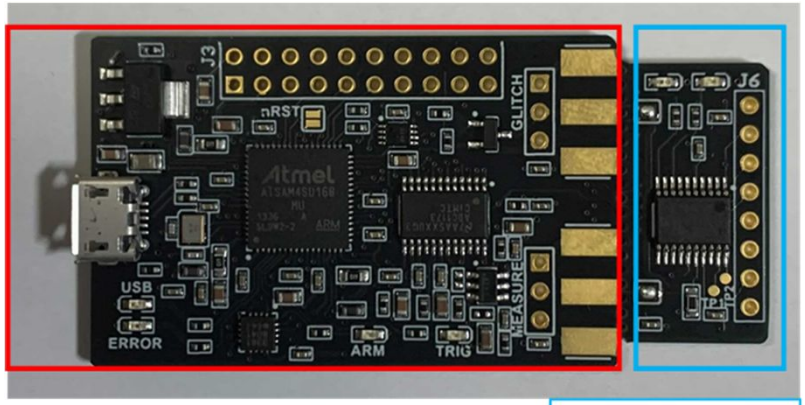
● 電力解析攻撃とは

サイドチャネル攻撃の一種。
暗号回路が動作する時の消費電力波形を測定する攻撃
機器に複数の入力を与えて、その時に消費する電力の違いから暗号鍵を推測する

実際に行ったこと

1．ChipWhisperer Nanoの環境セットアップ

・VirtualBoxの準備
・Firmwareのアップデート
・操作コマンドの習得

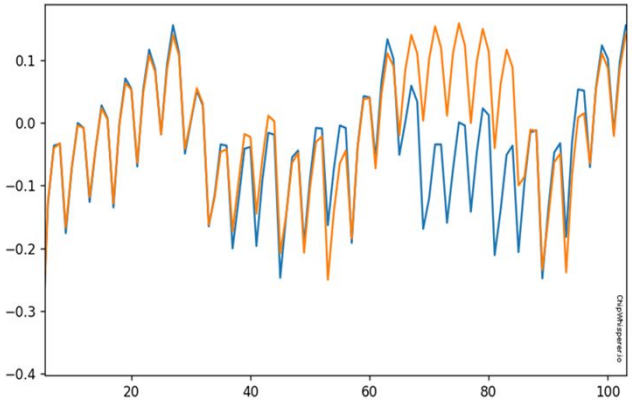


波形解析ボード

ターゲット
ボード

2．消費電力波形の取得・解析

・電力波形の出力
・正しいパスワードと
誤ったパスワードでの比較



成果

1．アップデートに関する問題の解決

2．消費電力波形の比較

成果１　アップデートに関する問題の解決

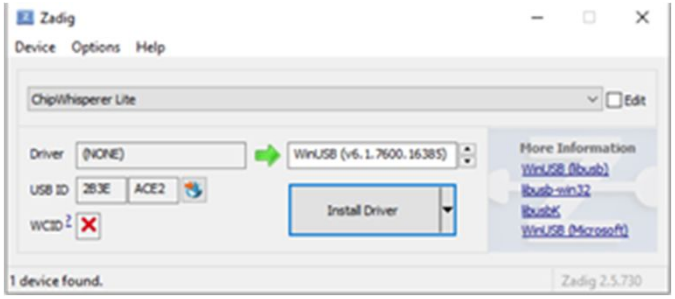
ファームウェアアップデートに関して

ファームウェアの更新（Jupyter ノートに記載のスクリプト）を実行すると、Chipwhisperer の接続が一旦解除される箇所があった。
原因はＣＯＭポートの識別がうまくできていないことが考えられる。

解決策

①ドライバーを変更するためにZadig.exeをhttps://zaddig.akeo.ie/からダウンロード
②図のようにDriverにWinUSBを選択し、ドライバーをインストール
③jupyter上で下記コマンドを実行

- import chipwhisperer as cw
- scope = cw.scope()
- scope.upgrade_firmware()



上記操作により、ファームウェアアップデートを完了した。

成果２　消費電力波形の比較

・パスワードの１文字目に対する消費電力の比較を行った。
・正しいパスワードと誤ったパスワードで消費電力が異なる
　ことが確認できた。

chipwhisperer.py

```
#トレースの実行
import chipwhisperer as cw
scope = cw.scope()
target = cw.target(scope, cw.targets.SimpleSerial)
scope._cwusb.usbtx.rep = 0x81
scope._cwusb.usbtx.wep = 0x02
def capture_trace(_ignored=None):
    ktp = cw.ktp.Basic()
    key, text = ktp.next()
    return cw.capture_trace(scope, target, text).wave
wave = capture_trace()

#波形の出力
%matplotlib notebook
import matplotlib.pylab as plt

plt.figure()
plt.plot(wave, 'r')
plt.show()
```

図　操作プログラム

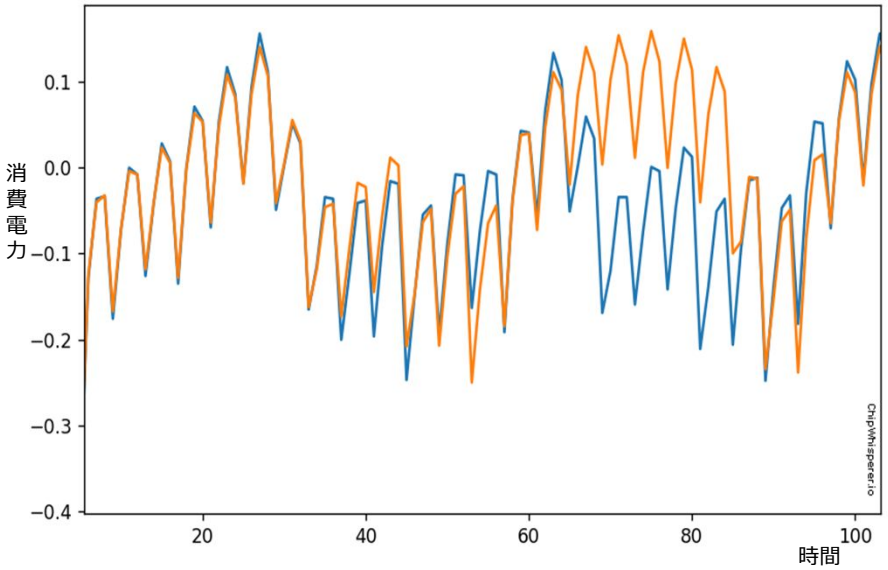


図　消費電力波形の違い

オレンジ：正しいパスワード
ブルー：誤ったパスワード

まとめ と 今後の展望

まとめ

- ChipWhisperのセットアップ方法と操作方法について学んだ。
- 暗号回路から漏れ出る電流から暗号化の処理の差を解析することができた。

今後の展望

- 様々な暗号方式に対して、調査を行い、攻撃の有効性の評価をする
- IoTデバイスなどの製品に対して攻撃を実施して、脆弱性を調査する

ドローン班

メンバー

M1：上野、田代、末吉、阿部、林、米田、森田

M2：荒木、 仙田、小林、前川、何、鈴木

選定機種［Holy Stone HS 120 D］

- **HS 120 D**
  - ✔ **Wi-Fi対応**によりスマホと連動
  - ✔ アプリ**HS GPS V1**により、カメラ映像・ドローン位置の確認が可能
  - ✔ 接続が途絶えた場合やパイロットのリクエストに応じて、ドローンが自動的に離陸地点に戻る
    リターンホーム機能搭載
  - ✔ **1080P HDカメラ付き&リアルタイム**

- 価格が安価
  - ✔ 価格が公式HP ¥21,989(税込) HS120D - Holy Stone

→ **機能（Wi-Fi対応/アプリ連携/GPS搭載/カメラ搭載）、レビュー評価、価格、GPS搭載により決定**

- その他の機器等

機器	型番等
スマートフォン	AQUOS sense3 lite (Android:ver 9)，アプリ：EufyHome
無線ルーター	tp-linK　AC1200(Archer C1200)
パソコン（OS）	kali-Linux,　Windows10

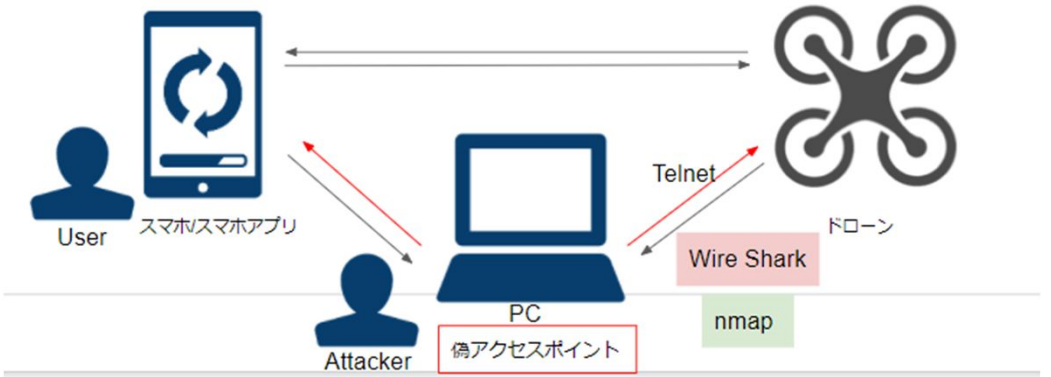
攻撃シナリオ検討とツールの調査

●攻撃シナリオ構成図

①ドローンの空いているサービスを調べて、
不正な制御が可能な入口を確認。

②入れそうな入口からの権限昇格

③偽のアクセスポイントを設けて、
MITM攻撃ができるかどうか

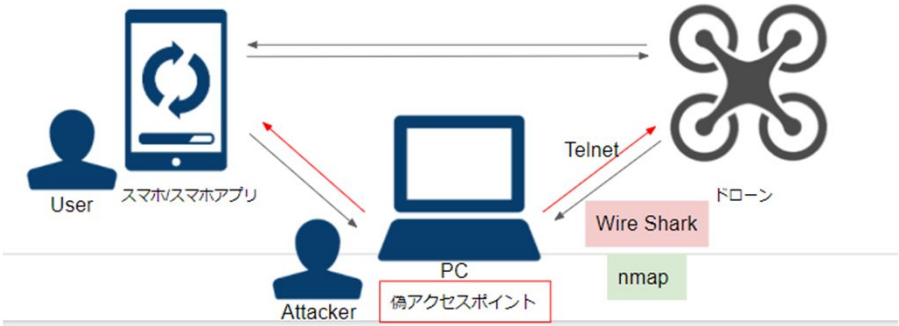


●ソフトウェアツールの調査

ツール名	概要（調査担当者）
Nmap	開放ポートの調査（ポートスキャン）のためのコマンドツール
noxprayer	PCでandroid環境を操作する為のエミュレータ
Wireshark	ネットワーク上のトラフィック、プロトコルの確認
burp suite	HTTPSでの通信の挙動を観測できる
GVM	ドローンに対する脆弱性スキャン

Holy Stone HD 120 D 分析結果

● 構成図



● 脆弱性スキャン実行結果　　（GVM)

✔ 対象：IP 172.16.10.1(デフォルトゲートウェイ)
✓ 診断結果：特に脆弱性は見当たらず

● MITM攻撃

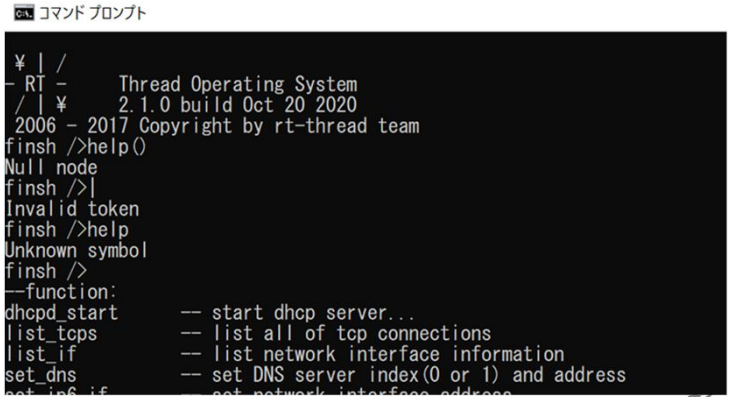
✓ PCをアクセスポイントにて、スマホ、ドローンをそれぞれPCに接続する。
→接続はできたが、アプリでドローンを制御出来ない
→PCから通信の挙動を観察出来なかった

● ポートスキャン（Nmap：Ver.7.91）

✔ TCPスキャン・UDPスキャン
✔ Openポート
TCP：23　サービス：telnet
TCP：8830　サービス：unknown
TCP：8888 サービス：sun-answerbook

✓ UDP：67
UDP：49153
UDP：8080　http alt

✔ telnetに関しては、接続可能であり、finsh />のようなシェルが現れ、以下のようなOS情報を見ることができた。



telnetから権限昇格できるのか？

・Finsh shell　とは

→　RT-thread　（https://github.com/RT-Thread/rt-thread）

・中国のリアルタイムOS

・10進数の入力でコマンドラインを操作する

・helpで出てきたコマンドをチェック

```
finsh />finsh()
Null node
finsh />ping
        -1609808104, 0xa00c4718
finsh />hello
        -1610001908, 0xa009520c
finsh />venc
        -1609882596, 0xa00b241c
```

・10進数（左）１６進数（右）で書かれている
・アスキーでデコードしても分からなかった

→IDやパスワードといった中身が見れる可能性はなし

・調べると、mshモードはbashと同じような機能がある

→オーソリティや権限の情報が入手できるのでは・・・？

バージョンが低い為、攻撃の可能性のある、mshモードがサポートされていない

→今後も調査が必要

まとめ と 今後の展望

- まとめ

✓Holy stone 120 Dから攻撃シナリオで想定していたMITMの脆弱性は確認することができなかった。
✓さらに、GVMでの脆弱性は確認できなかった
✓telnetは接続可能であり、mshモードが使えれば権限昇格できる可能性は高い

- 今後の展望

✓wi-fiのアダプターを買い、フェイクアクセスポイントを作る
✓ OSの情報のバージョンが高いドローンを攻撃する
✓アプリの調査
✓リバースエンジニアリング(ファームウェアの抽出)
✓5G/AIドローンのハッキング

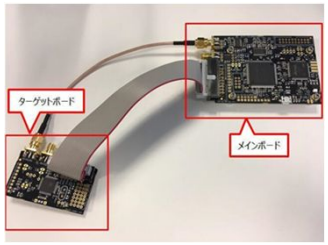
今後のロードマップ

スマートホーム

5G

2020　2021　2022　2023　2024

スマートデバイス
（暗号化回路、ドローン）



電力解析攻撃の実践

ドローン等
の脆弱性調査

IOT機器の脅威シナリオ検証

（来年度も継続予定）

✔ 2021年度成果を踏まえアプローチを変えた
脆弱性検証、実証

→実際のデバイスに対する電力解析攻撃
→5G・AIドローンのハッキング