Internet Week 2017

知られざるデバイスセキュリティの世界

株式会社ＦＦＲＩ
http://www.ffri.jp

最高技術責任者 金居良治

2017-11-16

IoTシステムに対するセキュリティ研究の進歩

- 近年、IoT、組み込みシステムに対するセキュリティ脅威分析、脆弱性分析技術の研究がこれまで以上に進んでいる
- 研究の対象は非常に多岐にわたる
  - スマートフォン、ネットワーク機器、複合機、セキュリティカメラ、医療機器、 車、テレビ、情報家電、ATM、スマートグリッド、産業用制御システム、etc…

- セキュリティが全く考慮されていないままインターネット接続されるシステム
- 容易に攻撃可能な脆弱性を持つシステムも数多く存在
- デバイス製造企業、サービス提供企業にセキュリティを考慮した設計、実装、セキュリティテストができる人材が不足

急速なIoT化と攻撃技術の高度化に伴い、
OA環境に対する脅威が社会インフラに対する脅威に拡大

Exploiting Surveillance Cameras - Like a Hollywood Hacker

Black Hat USA 2013

- BlackHat USA 2013において発表
  - https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf

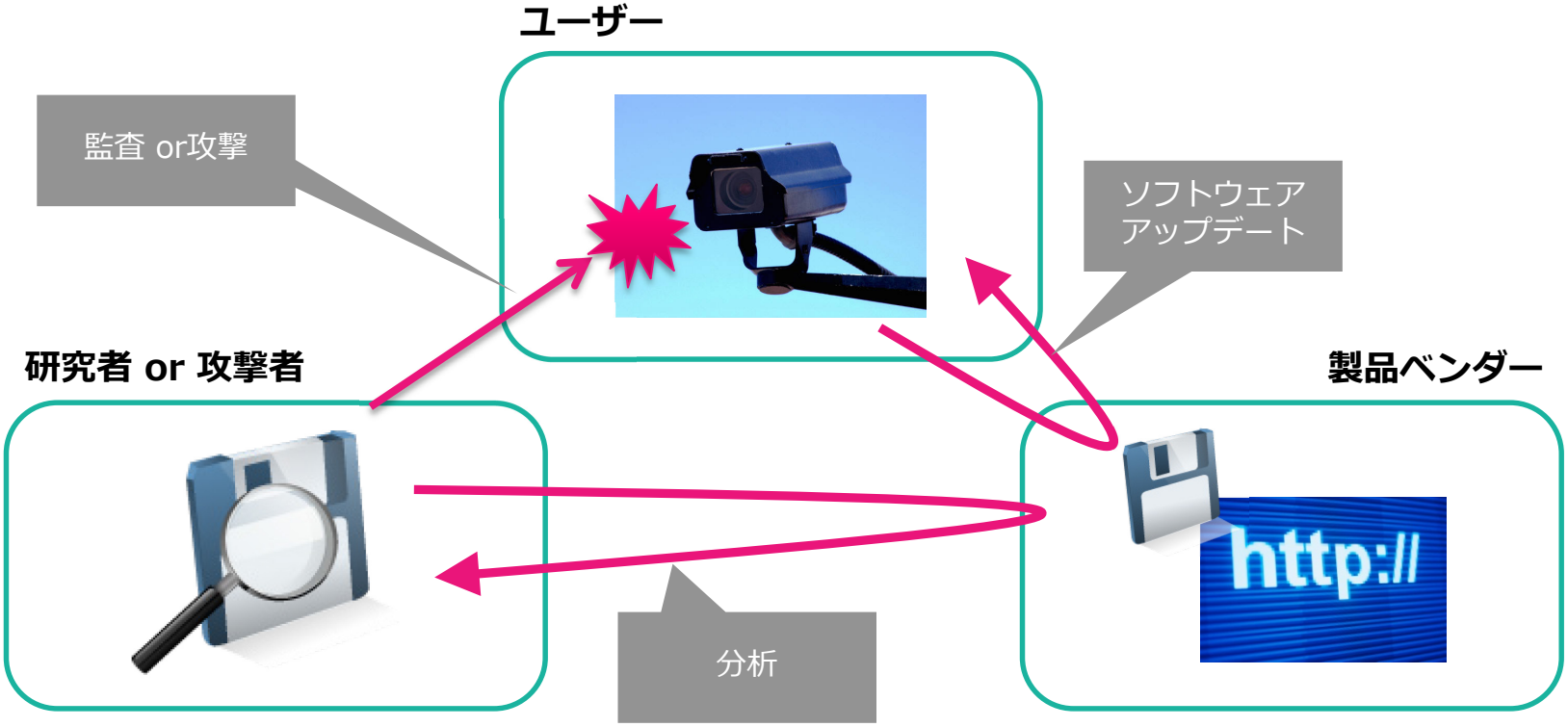
- 複数のネットワーク対応セキュリティカメラを調査、攻略
  - 脆弱性を悪用することで外部からカメラを自由に制御可能に
    撮影映像の不正閲覧、映像の差し替え、機器の停止等
  - 1モデルで発見した攻撃が他の複数メーカー、モデル製品にも適用可能
    1機種で発見した脆弱性を用いて最大40機種に同様の攻撃が可能
  - インターネット上に接続された脆弱なカメラをgoogle、shodan等で検索可能
    「thttpd/2.25 content-length:4121」等

- 発見された脆弱性はいずれも古典的なものばかり（攻撃に要する技術障壁は低い）
  - Windows、Linux等のPCプラットフォームでは既に撲滅されている

脆弱性調査手法

Black Hat USA 2013

- 製品ベンダーは、アップデートファイル（ファームウェア）を自Webサイトで公開
- ユーザーは、これをダウンロードしカメラのソフトウェアを最新状態に保つ
- 研究者は、これをダウンロード・解析し、脆弱性を発見・攻略（攻撃者も同様）



例1) Linksys WVC80N

Black Hat USA 2013

- Web管理画面を制御するCGIにバッファーオーバーフロー脆弱性が存在
  - 長い文字列を含むリクエストを送るとバッファオーバーフローが発生
    「GET /img/snapshot.cgi?aaaaaaaa……aaaaa HTTP/1.0」
  - 上記「aaa….」の部分に適切な機械語に格納することで任意コードが実行可能
  - 発表者は、管理者用パスワードの搾取を実証

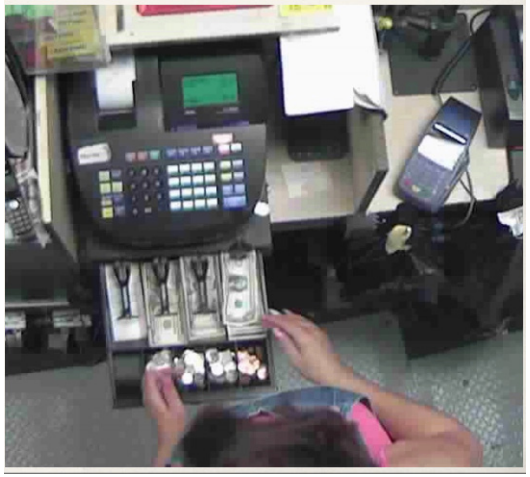
- 脆弱性の性質上、一度攻撃方法を確立させれば絨毯爆撃が可能
  - shodan等で脆弱なカメラを検索し、リスト化
  - 各カメラに攻撃コードを含むGETリクエストを自動送信

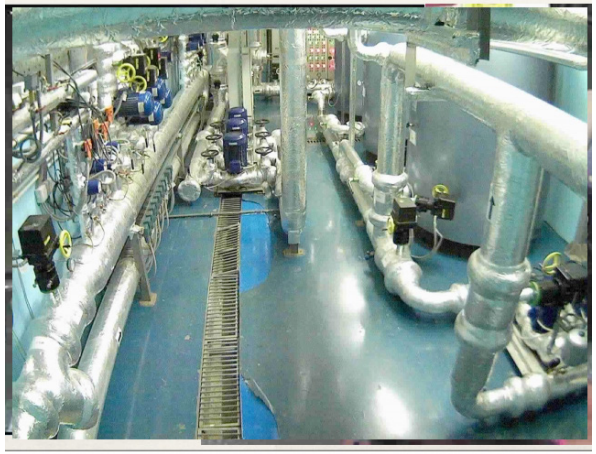
出典：https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf

例2) 3SVision N5071

Black Hat USA 2013

- Web管理画面の管理者ID、パスワードがファームウェア中にハードコードされている
  - 基本的なリバースエンジニアリングの知識があれば誰でも特定可能
  - 壁面据え付け型のため様々な施設で防犯用として利用されている模様
  - 計40機種以上の製品も同様の攻撃が可能なことを確認



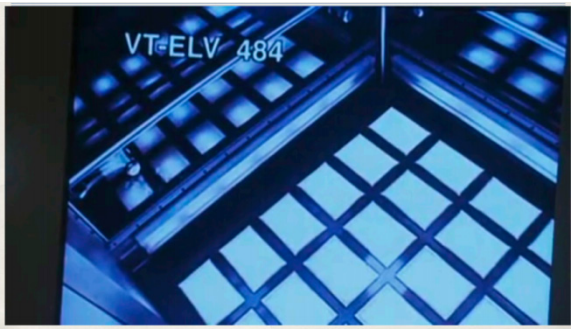


出典：https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf

例3) Trendnet TV-IP410WN

Black Hat USA 2013

- バックドアアカウントが存在、例2同様ファームウェア解析で容易に特定可能
- Web経由でカメラのストリーミング映像をブラウザ上で閲覧可能
  - ストリーミング配信は内部のmjpg.cgiが担当
  - 当該プログラム（デーモン）を停止すると「最後に映った画像」が表示され続ける



最後に映った画像

実際の画像

- mjpg.cgiを静止画像を表示し続けるプログラムに差し替えることも可能

```
#!/bin/sh
echo -ne “HTTP/1.1 200 OK¥r¥n Content-Type: image/jpeg¥r¥n¥r¥n”
cat /tmp/static_img.jpg
```

出典：https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf

ウェブカメラに関する問題

- ファームウェアを分析され、様々なウェブカメラのバックドアアカウントが明らかになっている
- ウェブカメラ研究発表後に現実的な脅威となっているため、研究動向なども注視する必要がある
- ファームウェアの更新やパッチ管理がされていない場合がほとんどであり、一度、乗っ取られると対応が難しい

自動車リモートサービスに対する攻撃

2015

Aug

出展:*Samy Kamkar,*
https://www.youtube.com/watch?v=3olXUbS-prU
Drive It Like You Hacked It: New Attacks And Tools to Wirelessly Steal Cars, DEFCON 23

Oct

出展:*Jianhao Liu, Jason Yan,*
https://www.syscan360.org/en/archives/,
Car Hacking: Witness Theory to Scary and Recover From Scare, SyScan360 2015

2016

Feb

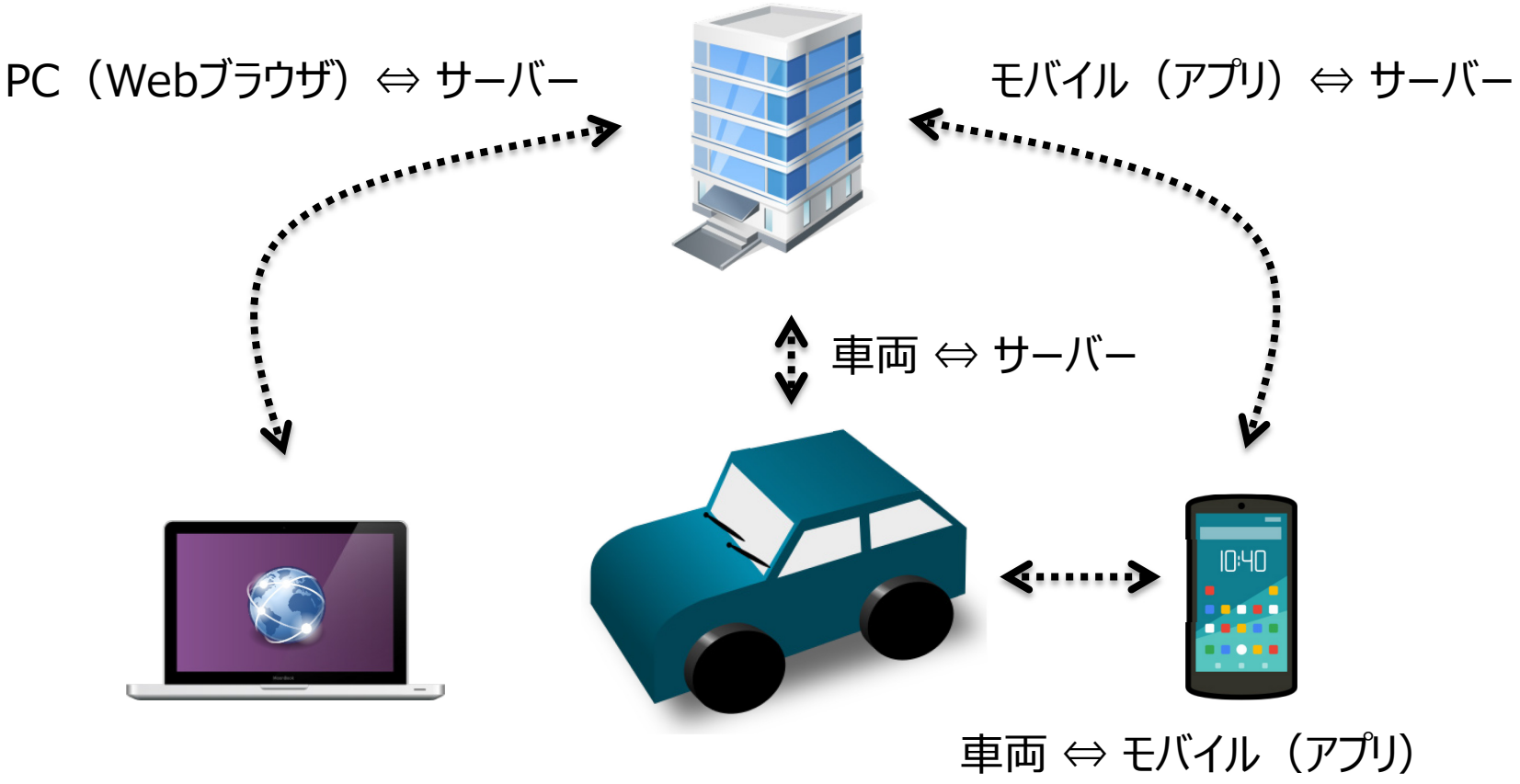
出展:*Troy Hunt,*
https://www.youtube.com/watch?v=Nt33m7G_42Q

Jun

出展:*Pen Test Partners LLP,*
https://www.youtube.com/watch?v=NSioTiaX_-Q

自動車リモートサービスに対する攻撃

- リモートサービスに対する攻撃は主に下記の領域に分類する事が出来る。



GM の OnStar サービスで指摘された脆弱性

- 2015年7月に、GM の OnStar サービスの脆弱性が指摘され、翌月のDEFCONで発表された。

- この脆弱性の基本原理はアプリの脆弱性に伴う中間者攻撃(MITM攻撃)によるユーザーの認証情報の窃取であるが、実証時における特徴として発表者はMITM攻撃用のデバイスを作成している点である。

- このデバイスによって、Wi-Fiの範囲内でアプリを使用した際に通信を傍受してユーザークレデンシャルを窃取、攻撃者にその内容を送信する事が可能となっている。

（出展）http://samy.pl/defcon2015/2015-defcon.pdf

CODE BLUE 2016 で指摘した脆弱性

- 2016年10月の CODE BLUE で、リモートコントロールサービスに潜むリスクの調査結果として各メーカーが提供しているアプリの検査結果を公開した。
- 検査は比較的容易に行う事が可能な Android アプリをターゲットとし、11種類のアプリに対して調査を行った。
- 調査の結果証明書の検証を正しく実装しておらず、その結果MITM攻撃される可能性のあるアプリが１つ見つかった。
  - GM の OwnStar のようなデバイスが作成される可能性もあり得る。
- その他、Android M から採用されているパーミッションモデルにまだ対応出来ていないアプリがあった（順次対応されていくものと思われる）。

CODE BLUE 2016 で指摘した脆弱性

アプリ提供元	リモートコントロール機能の有無	Criticalな脆弱性リスクの件数	不適切なプラットフォーム利用 (M1)	安全でないデータ保存 (M2)	安全でない通信 (M3)
A社	Yes	11	5	1	5
B社	No	5	3	1	1
C社	No	5	2	1	2
D社	No	5	2	1	2
E社	Yes	4	0	0	4
F社	Yes	4	1	1	2
G社	Yes	3	0	0	3
H社	Yes	2	1	0	1
I社	Partial	1	0	0	1
J社	Yes	1	0	0	1
K社	Partial	0	0	0	0

CODE BLUE 2016 で指摘した脆弱性

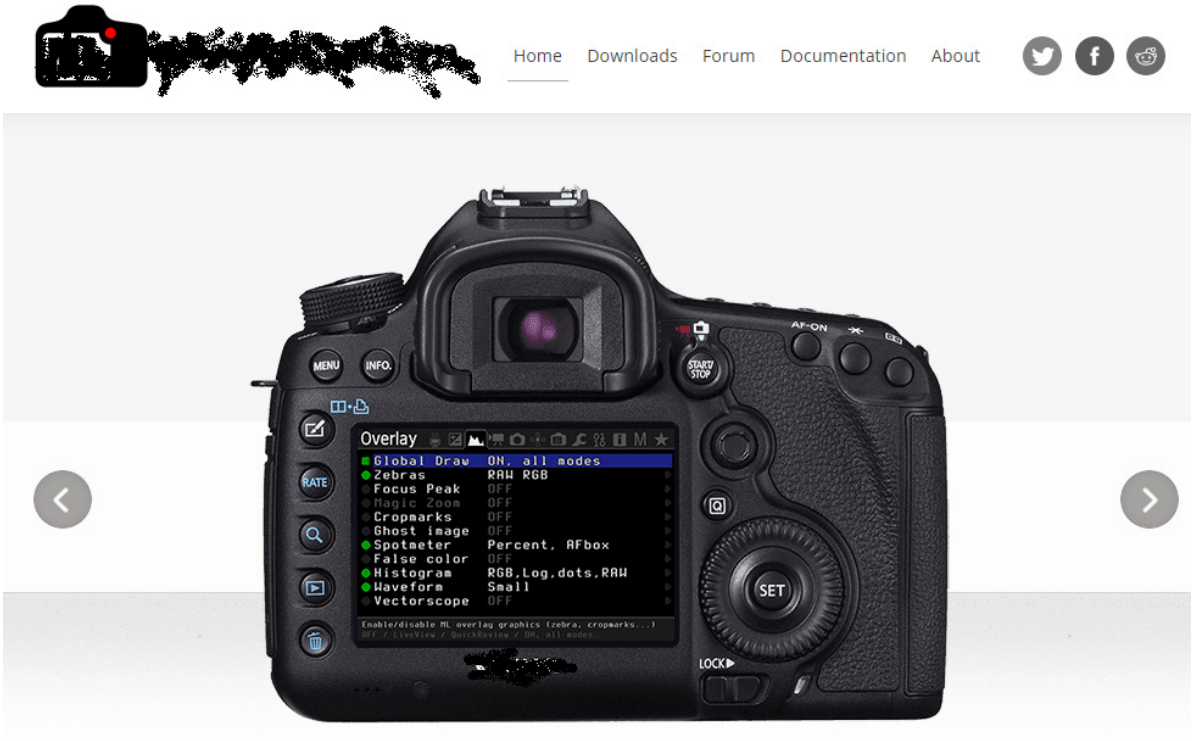
アプリ提供元	評価
A社	脆弱性の存在を確認。MITM攻撃を受けるリスクが存在する。 PreferenceActivity を継承したクラスで isValidFragment() を実装していないため、関連アクティビティを公開した場合に Fragment Injection によってアプリがクラッシュさせられる可能性。
B社	現状において、攻撃が可能となる問題は見つからなかった。
C社	現状において、攻撃が可能となる問題は見つからなかった。
D社	現状において、攻撃が可能となる問題は見つからなかった。 難読化されているため、詳細な解析には時間がかかる。
E社	現状において、攻撃が可能となる問題は見つからなかった。 セキュリティ脆弱性では無いが、Android M 以降の新たなパーミッションモデルに対応していないため一部機能にてアプリがクラッシュする。
F社	現状において、攻撃が可能となる問題は見つからなかった。 難読化されているため、詳細な解析には時間がかかる。
G社	現状において、攻撃が可能となる問題は見つからなかった。
H社	現状において、攻撃が可能となる問題は見つからなかった。
I社	現状において、攻撃が可能となる問題は見つからなかった。
J社	現状において、攻撃が可能となる問題は見つからなかった。
K社	現状において、攻撃が可能となる問題は見つからなかった。

証明書に関する問題

- よくある脆弱性の1つとして、証明書に関する問題があげられる
- 実際の自動車アプリの検証の結果、問題が見付かっている
- MITM Proxyなどを使うことにより簡単に中間者攻撃が可能である

ファームウェア改造

- デジタルカメラのファームウェアを解析、勝手に機能を追加した改造ファームウェアを配布しているユーザーもいる



FFRIにおけるハードウェア分析の研究

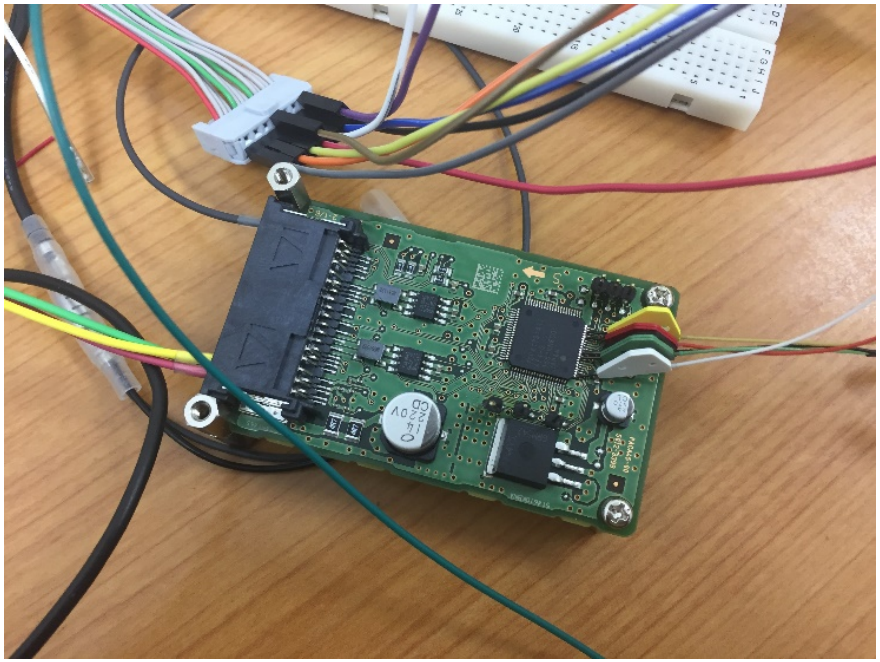
- **表層解析**
  - 使われているチップなどをボードから調査
  - 表層解析が簡単な機器と難しい機器がある

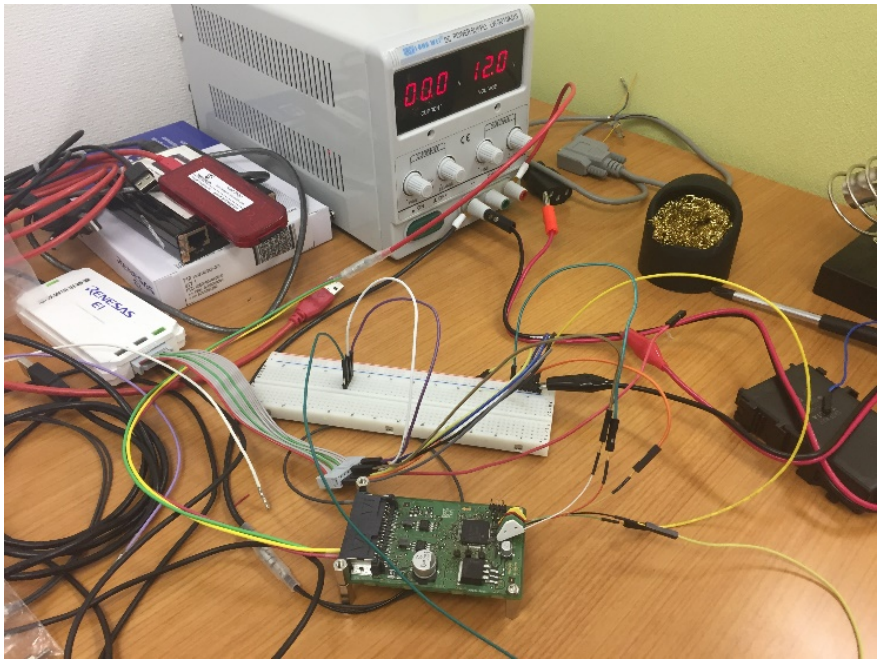
リードが出ていないので、周辺のスルーホールやパッドを介してデバッグする必要がある。

FFRIにおけるハードウェア分析の研究

◆静的解析

- □表層解析の調査をもとに、ハードウェアデバッガ等を配線





FFRIにおけるハードウェア分析の研究

- **静的解析**
  - ファームウェアをディスアセンブラで解析する
  - マルウェア解析等により、ディスアセンブラーの性能は向上している
  - 動的解析と組み合わせると効果的

```
seg000:000029B2 -- ============== S U B R O U T I N E ============================
seg000:000029B2
seg000:000029B2
seg000:000029B2 FCN_Register_Config?:                   -- CODE XREF: sub_60+320↑p
seg000:000029B2                                         -- port_group_config+1E0↑p
seg000:000029B2                 mov     0xFF480000, r19
seg000:000029B8                 movea   0x200, r0, r11
seg000:000029BC                 mov     1, r12
seg000:000029BE                 movea   0x87, r0, r13
seg000:000029C2                 ld.bu   0x580D[r19], r0
seg000:000029C6                 or      r0, r0
seg000:000029C8                 ld.bu   0x600D[r19], r0
seg000:000029CC                 or      r0, r0
seg000:000029CE                 ld.bu   unk_6F8D, r0
seg000:000029D2                 andi    0x7A0, r0, lp
seg000:000029D6                 jarl    0xFFEE2896, r13
seg000:000029DA                 ld.bu   unk_6FCD, r0
seg000:000029DE                 andi    0x633, r0, lp
seg000:000029E2                 nop
seg000:000029E4                 st.b    lp, 0x5E20[r10]
seg000:000029E8                 callt   0
seg000:000029EA                 mov     1, r12
seg000:000029EC                 movea   0x87, r0, r13
seg000:000029F0                 ld.bu   0x580D[r19], r0
seg000:000029F4                 or      r0, r0
seg000:000029F6                 ld.bu   0x600D[r19], r0
seg000:000029FA                 or      r0, r0
seg000:000029FC                 ld.bu   unk_696D, r0
```

ファームウェア解析に関する問題

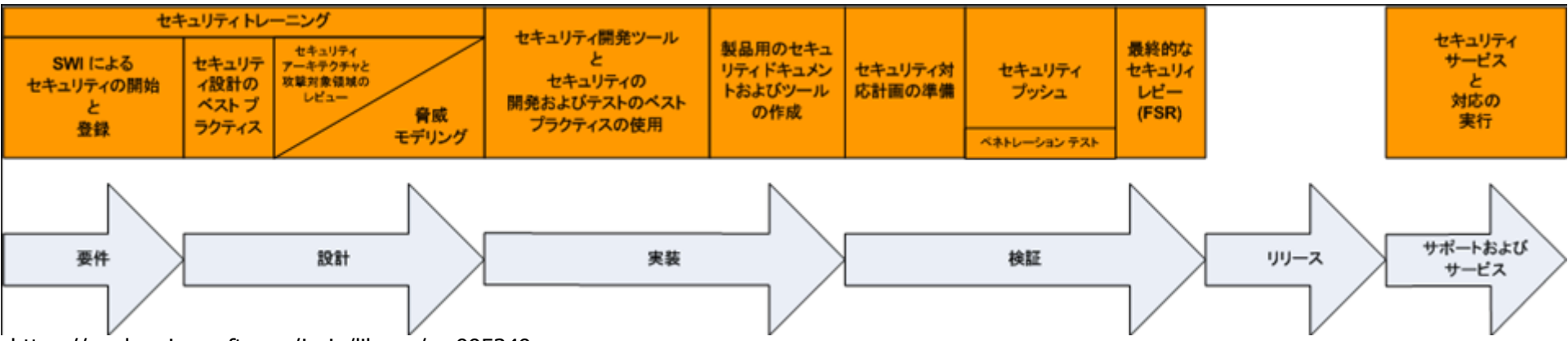
- ファームウェア解析を支援するツールが年々、整備されており、難易度は下ってきている

- 解説ページなども存在するため、もはやファームウェア解析は容易である前提での製品開発が必要

SDLC

- IT業界ではMicrosoftが提唱しているSecure Development Lifecycleが有名
  https://msdn.microsoft.com/ja-jp/library/ms995349.aspx

- 俯瞰的に対策を検討する際の参考になる



https://msdn.microsoft.com/ja-jp/library/ms995349.aspx

Fuzzing

- セキュリティテスト手法のうちの1つであり、未知の脆弱性を発見することができる

- 一般的な通信プロトコルやファイルフォーマットであれば対応した製品が存在し、容易に実施できる

https://www.ipa.go.jp/security/vuln/fuzzing.htm IPA 独立行政法人 情報処理推進機構 セキュリティセンター 2017年3月

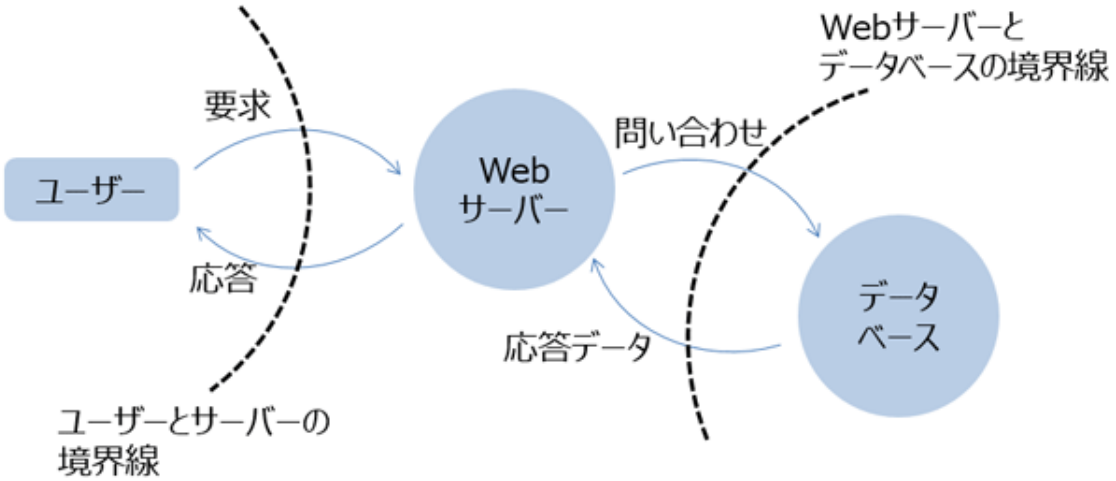
アップデート

- Windows等のPC用のソフトウェアであれば、更新プログラムを配布することは容易である
- IoT機器のファームウェア更新はどのように行うのか？
  費用負担は？
- 携帯電話や自動車では、OTA(Over The Air)といわれるソフトウェア更新が用いられる

脅威分析

- 設計書などをもとに、脅威を分析し必要な対策(セキュリティ機能)を検討するための技術

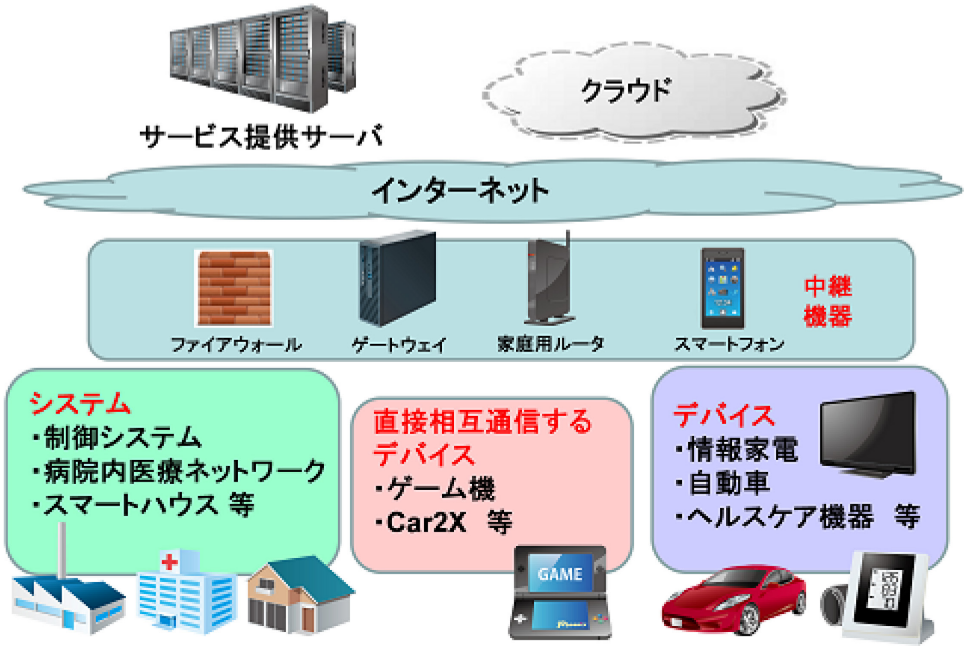
- 優先順位付けなどを検討する枠組みなどもあり、セキュリティ設計の際に役立つ



http://www.ffri.jp/blog/2016/10/2016-10-14.htm

IoT開発におけるセキュリティ設計の手引き

- IoT機器の開発において有用な、想定される脅威情報と対策が整理されている
  https://www.ipa.go.jp/security/iot/iotguide.html
- 「IoTセキュリティ」のページがよいリンク集となっている
  https://www.ipa.go.jp/security/iot/index.html



IoTセキュリティガイドライン

- 経済産業省がガイドラインを出している
  http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html
- IPAの資料とあわせて見ると理解が早い

脅威分析研究会

- 仕様や設計のセキュリティ分析を行うための手法として脅威分析や脅威モデリングがあるが、これらを対象にした勉強会
  https://sites.google.com/view/sigsta/
- 非常に有用な資料などが公開されていて参考になる

設立趣旨

コンピュータシステムのセキュリティを確保するための技術には疑似攻撃検査技術やソースコード静的解析技術などが普及していますが、この研究会では自然言語で記述されることが多い仕様や設計に関してセキュリティ分析する脅威分析や脅威モデリングといった脅威分析技術をターゲットにいたします。
・・・

ご清聴ありがとうございました。

株式会社ＦＦＲＩ
http://www.ffri.jp

最高技術責任者 金居良治
kanai at ffri dot jp