2015年4月28日
デジタルフォレンジック研究会「技術」分科会

IoT時代のセキュリティ

株式会社FFRI
代表取締役社長 鵜飼裕司
http://www.ffri.jp

自己紹介

鵜飼 裕司　博士（工学）

・株式会社FFRI　代表取締役社長
・独立行政法人情報処理推進機構 非常勤研究員
・BlackHat Content Review Board Member

総務省「クラウドセキュリティ検討会」、内閣官房「リスク要件リファレンスモデル作業部会」、「連携マップ作成作業部会」、独立行政法人情報処理推進機構「自動車セキュリティ検討会」、「制御システムセキュリティ検討会」、経済産業省「サイバーセキュリティと経済研究会」、「産業活性化検討WG」など多数の政府関連プロジェクトの委員、オブザーバーを歴任。

■ 略歴

1973年　徳島県阿波市(旧板野郡)生まれ
1993年　香川県詫間電波高専 情報工学科 卒業
2000年　徳島大学大学院工学研究科博士後期課程 修了
　　株式会社コダック研究開発センター 入社
2003年　米国 eEye Digital Security 入社
2007年　株式会社FFRI設立

(株) FFRI 事業概要

サイバー セキュリティ領域でのシーズ型R&D

- 標的型攻撃などに利用されるセキュリティ脆弱性研究、対策技術開発
  100を超える日本最多のクリティカルなセキュリティ脆弱性発見の実績
- 標的型攻撃マルウェアに関する研究、対策技術開発
  標的型攻撃など近年のマルウェア対策に関する研究成果を多数発表
- 組み込みセキュリティ
  組込みシステムのセキュリティ脆弱性脅威分析に関する研究成果を多数発表

製品開発

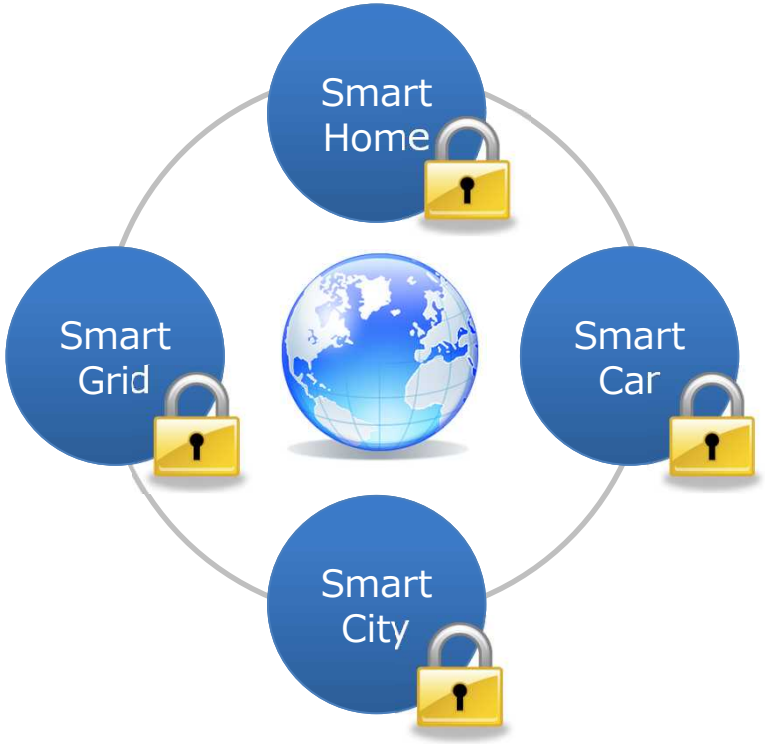
- 標的型攻撃対策ソフトウェア
- マルウェア自動解析システム
- MITB攻撃対策ソフトウェア
- 組み込み機器セキュリティ検査ツール
- P2Pシステムセキュリティ

サービス

- 標的型攻撃マルウェア調査分析
- Android端末セキュリティ分析サービス
- セキュリティ対策コンサルティング
- 受託研究開発
- Black URL提供サービス
- セキュリティ技術者向けトレーニング

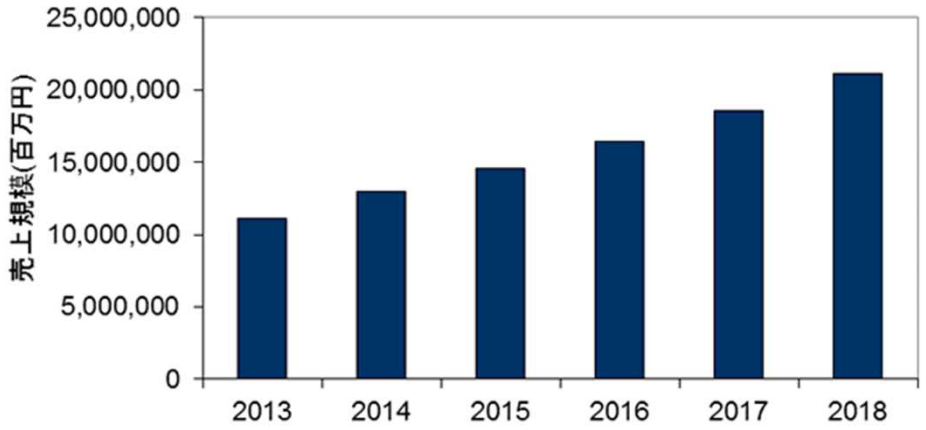
IoTを取り巻く環境

あらゆるモノがInternetに繋がるため
セキュリティは重要課題



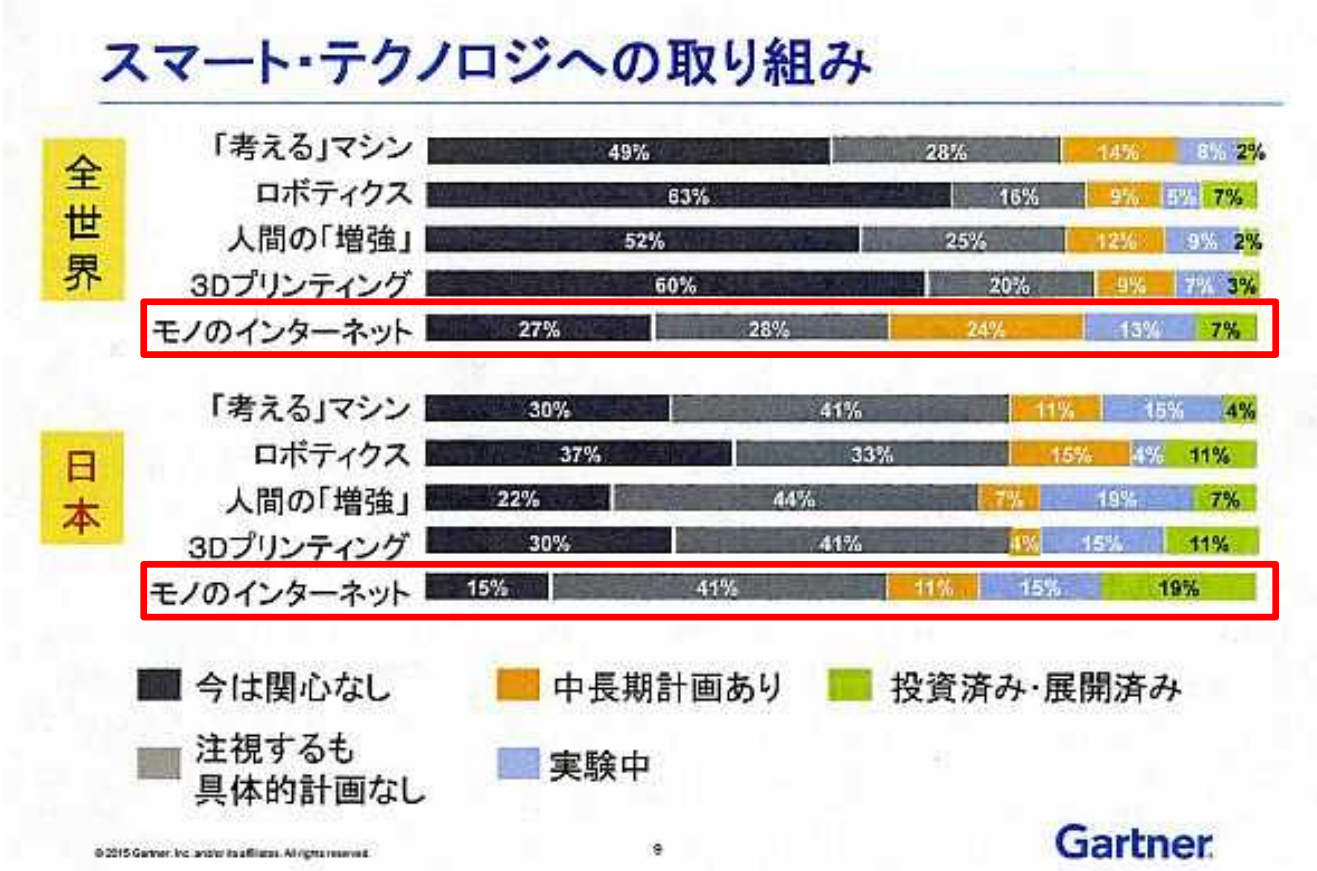
- 国内IoT市場
  - 国内IoT市場規模：11兆1,240億円
  - IoTデバイス数：4億9,500万台
  - 2013～2018年のCAGR：13.7%
  - 2018年には21兆1,240億円の市場規模に

＜参考資料＞
国内IoT市場 売上規模の実績と予測、2013年～2018年



Note: 2013年は実績、2014年以降は予測
Source: IDC Japan, 8/2014

日本が先行するIoTへの取り組み状況



出展元：@IT（2015/1/22掲載記事）
[ガートナージャパンがCIO調査結果を発表：「CIOは、3つの逆転思考でデジタル化のリーダーとなれ」]より抜粋
http://www.atmarkit.co.jp/ait/articles/1501/22/news137.html

社会インフラに対する脅威の増大

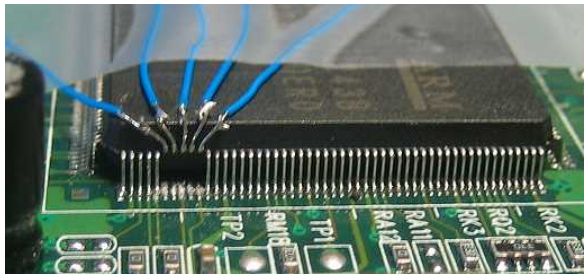
- 組み込みシステムの脅威分析技術が急速に向上、脅威が広まる

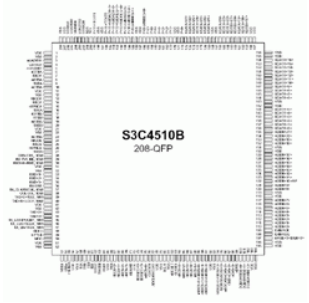
  スマートフォン、ネットワーク機器、複合機、セキュリティカメラ、医療機器、
  車、テレビ、情報家電、ATM、スマートグリッド、産業用制御システム、etc…

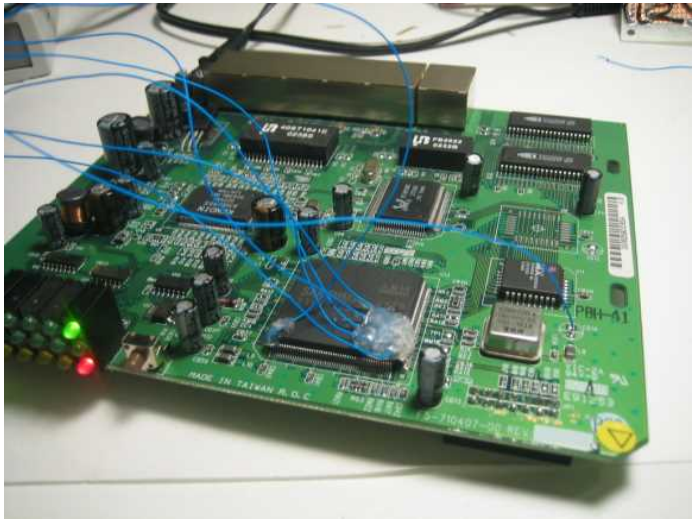
- 2000年以降、組み込みシステムのセキュリティ脆弱性脅威分析技術が確立

  - 影響が広範囲になりつつある。
  - 古典的な脆弱性を持つ組み込み機器が数多く存在。
  - 効率的なセキュリティ・テスト手法は研究途上。
  - セキュリティ・テスト可能な人材は希少。

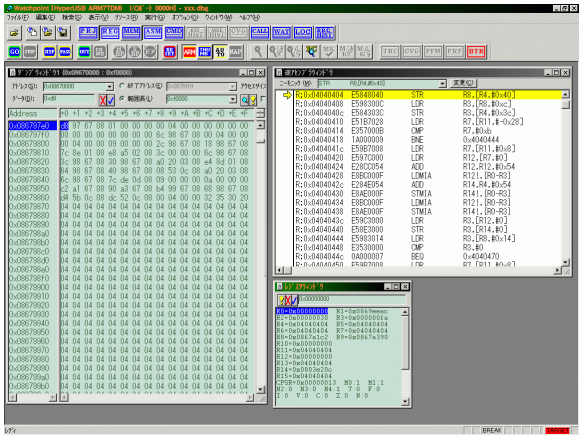
社会インフラのIP化と攻撃技術の高度化に伴い、
OA環境に対する脅威が社会インフラに対する脅威に







デバッガで解析



汎用JTAG

近年の情報セキュリティカンファレンスでの研究発表の傾向

- プラットフォームの解析や脅威分析が多いが、その種類が多岐にわたる
  Windows/Linux、Android、ICS、Chipset、Smart TV、Home Security、Camera etc・・・
- 比較的新しいテーマは、自動車、POSシステム、衛星通信、暗号通貨、クラウド、ビッグデータ
- 全体的にWindows/Linuxなど高セキュアプラットフォームに関する脅威分析は減少し、
  ハードウェアのリバースエンジニアリングを含む脅威実証が増加
- マルウェア解析などは個々の分析よりもスケーラブルな分析方法に移行
- 増え続けるマルウェアやIoTデバイスの脆弱性発見など、解析や調査を自動化しスケールアウトさせる技術がホットトピックになりつつある

「セキュリティ研究者の研究対象とアンダーグラウンドの攻撃対象」がIoTに移行

本セッションで紹介する研究内容が発表されたカンファレンスについて

- 世界最大規模のベンダーニュートラルな情報セキュリティカンファレンス
- USA、Europe、Asiaなど世界各国で開催
  - USA 2014：参加者数9,000人以上、100件以上の研究発表
  - 2008年には日本でも開催

- 日本発の国際情報セキュリティ会議
- USA、Europe、Asiaなど世界各国で開催
  - CODE BLUE 2014：参加者数450人以上
  - 2013年の第1回では、Black HatやDEFCON創設者のジェフ・モスが基調講演

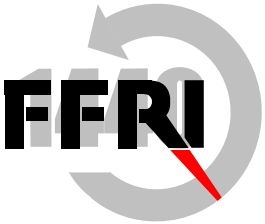
Black Hat USA 2013年の一部の発表について概要を紹介

Black Hat USA 2013

- Exploiting Surveillance Cameras - Like a Hollywood Hacker
  複数のネットワーク対応セキュリティカメラに存在する脆弱性の指摘と脅威に関する発表

- THE OUTER LIMITS: HACKING THE SAMSUNG SMART TV
  サムソンの Smart TV の脆弱性と攻撃の脅威についての発表

- HACKING, SURVEILLING, AND DECEIVING VICTIMS ON SMART TV
  ファームウェアの解析によって発見したSmart TV の脆弱性に関する発表



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

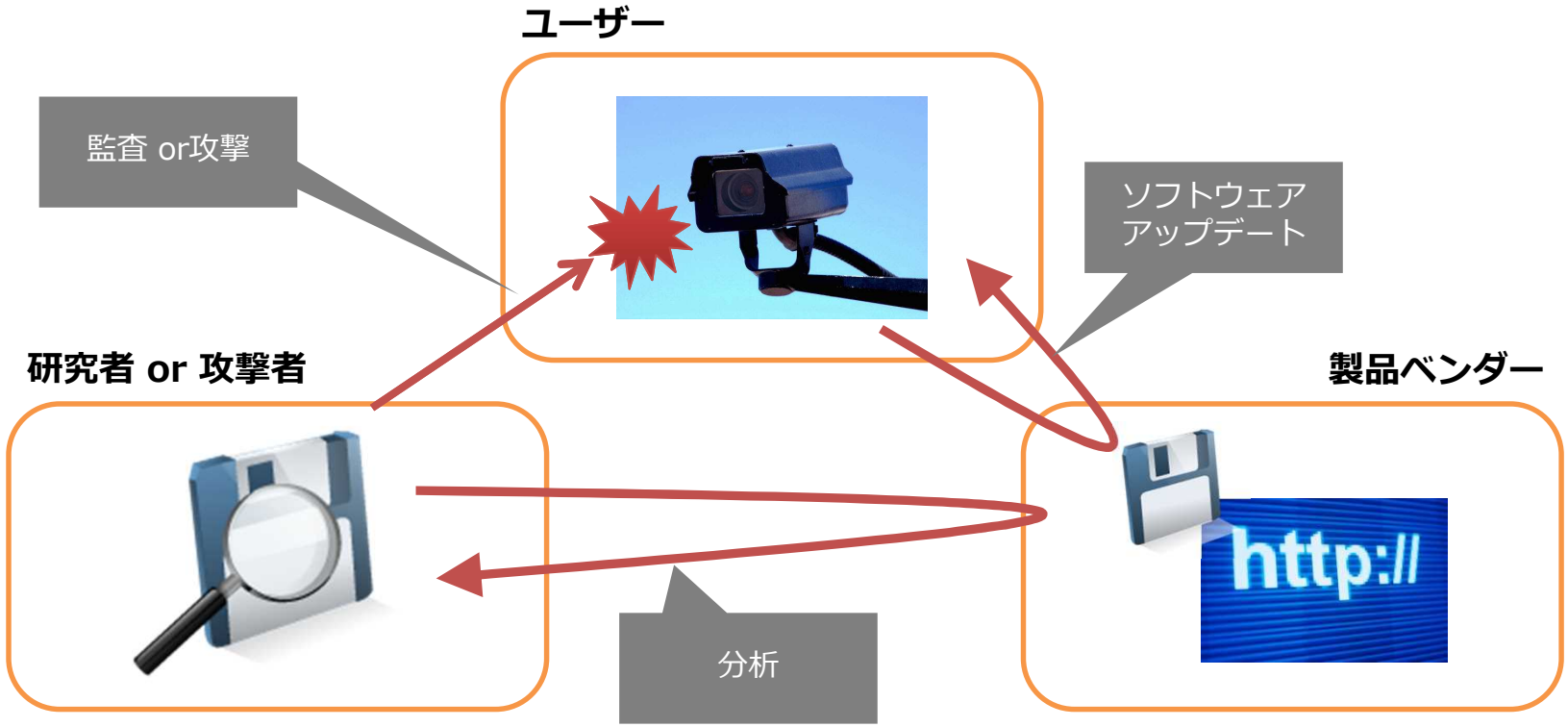
- 複数のネットワーク対応セキュリティカメラを調査、攻略
  - 脆弱性を悪用することで外部からカメラを自由に制御可能に
    撮影映像の不正閲覧、映像の差し替え、機器の停止等
  - 1モデルで発見した攻撃が他の複数メーカー、モデル製品にも適用可能
    1機種で発見した脆弱性を用いて最大40機種に同様の攻撃が可能
  - インターネット上に接続された脆弱なカメラをgoogle、shodan等で検索可能
    「thttpd/2.25 content-length:4121」等

- 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

THE OUTER LIMITS: HACKING THE SAMSUNG SMART TV (1)

Black Hat USA 2013

- サムソンの Smart TV の脆弱性と攻撃の脅威についての発表
- リサーチは 2012/12 に実施、2013/6 にサムスンが修正完了
- 2012年モデル2機種について15種類の脆弱性を報告
- Smart TV の内部は スマートフォンによく似ており、類似の攻撃に対して脆弱
- 脆弱性探しはいつもデベロッパーサイトにある仕様書の調査から始める

THE OUTER LIMITS: HACKING THE SAMSUNG SMART TV (2)

Black Hat USA 2013

- 攻略の起点
  - 全てのアプリがSSL接続を行う
  - http://samygo.tv の情報を解析
  - patcher.py に鍵が含まれていた
  - OSのファイルシステムのレイアウトが混沌としている
  - 19パーティション
    - いくつかのパーティションは書き込み可能、リマウント防止機構あり
  - ライブラリが数百もある
  - Lighttpd サーバーが動作している
  - 8 つのポートが開いている
  - ファイアウォールなし
  - すべてのサービスがroot権限で実行されている

THE OUTER LIMITS: HACKING THE SAMSUNG SMART TV (3)

Black Hat USA 2013

- アプリの調査を実施
- ほとんどのアプリケーションは、HTML/ JavaScript で書かれている
- アプリインストール時のセキュリティチェックをどのようにおこなっているか調査
  - アプリはZipでパッケージングされている
  - 難読化された JavaScript が使われていた

- 攻撃者がスマートテレビをハッキングして何ができるか
  - TV の映像が off の状態でもカメラやマイクを乗っ取り所有者を常時監視することができる
    - 監視映像を攻撃者のサーバーに送信するデモンストレーション
    - TVに偽のニュース映像を流すことができる（TV版フィッシング）

HACKING, SURVEILLING, AND DECEIVING VICTIMS ON SMART TV（1）

Black Hat USA 2013

- SmartTVはPCと似ている　Smart TV = TV + PC
- 調査の障壁
  - ドキュメント不足
  - ブラックボックス（ソースコードが非公開）
  - ソフトウェアが巨大（数100MBの容量、大半のコードをベンダーが開発）
  - 調査中、ファクトリーリセットができなくなり、サービスセンターに送った

HACKING, SURVEILLING, AND DECEIVING VICTIMS ON SMART TV（2）

Black Hat USA 2013

- 考えられるアタックベクタ
  - アプリケーションマーケットからのマルウェアの侵入
    - ブラウザのバグ
    - SDKのバグ
      - パス処理などの不具合
      - インストーラーのファイル展開、検証処理のバグ
  - ネットワーク経由
    - ネットワークデーモン
    - MITM
  - 物理的な攻撃
    - USBなど
    - リモコン、TV電波

HACKING, SURVEILLING, AND DECEIVING VICTIMS ON SMART TV（3）

Black Hat USA 2013

- 実際に行った攻撃
  - ファームウェアの解析
    - ファームウェアは暗号化されているが Samygo にパスワードがある
    - 復号したファームウェアをリバースエンジニアリング
      - IDAによるARMバイナリの静的解析
    - デバッグ情報が出力されるService Mode(デフォルトは無効)を有効にするためにUARTを詳細に解析
      - 静的解析で Service Mode の有効化方法を特定
      - Arduino というマイコンボードを使用し、UARTにコマンドを送信して実際に Service Mode を有効化した
    - 上記を用いて、複数の脆弱性を発見

Black Hat USA 2014年の一部の発表について概要を紹介

Black Hat USA 2014

- SATCOM TERMINALS: HACKING BY AIR, SEA, AND LAND
  衛星通信端末における複数のバックドア、プロトコル、暗号の脆弱性の存在を指摘とデモ。
  ファームウェアのリバースエンジニアリング方法の解説

- CELLULAR EXPLOITATION ON A GLOBAL SCALE: THE RISE AND FALL OF THE CONTROL PROTOCOL
  携帯電波(GSM/CDMA/LTE)による制御プロトコルを解析して、OTAでコード実行(ロック解除、jailbreak)の可能性と脅威について解説

- BADUSB - ON ACCESSORIES THAT TURN EVIL
  汎用的なUSBコントローラのファームウェアを改ざんすることによって、密かに悪意のあるコードを実行できるという指摘とデモ

Black Hat Europe 2014年の一部の発表について概要を紹介

Black Hat EU 2014

- Lights off! The darkness of the smart meters
  実際のスマートメータをリバースエンジニアリングし、プロトコルや機能を推定
- Don’t trust your USB! How to find bugs in usb device drivers
  ファジングでUSBデバイスドライバのバグを見つけるツールの発表
- Hack Your ATM with friend’s Rasberry.Py
  ATMのハッキングを、Rasberry Piを使って行う発表
- Firmware.RE: Firmware unpacking, analysis and vulnerability-discovery as a service
  組み込みデバイスのファームウェアの脆弱性調査に関する発表

Lights off! The darkness of the smart meters

Black Hat EU 2014

- 実際のスマートメータをリバースエンジニアリングし、プロトコルや機能を推定した
  - Flash MCE、EEPROMをJTAG経由でダンプし、解析して機能を推測
  - 調べた結果、カスタムASICといいつつ、汎用品だったり
- リバースエンジニアリング実演あり（本当にリアルデバイスをREしていた）
- メータ間の通信は暗号化されるが、その暗号化鍵は容易にリセット可能であったり、読み取り可能
- 家庭のネットワークに侵入したり、電源供給をカットオフしたり、いろいろ悪いことができる

Don’t trust your USB! How to find bugs in usb device drivers

Black Hat EU 2014

- ファジングでUSBデバイスドライバのバグを見つけるツールの発表
  - CVE-2013-1285, CVE-2013-1680など、USBデバイスドライバの脆弱性はカーネル権限の奪取に繋がる
- QEMUのUSB Redirection を使い、vUSBfというシステムを開発した
- 並列でVirtualBoxのインスタンスを立ち上げ、効率的にファジングする

Hack Your ATM with friend's Rasberry.Py

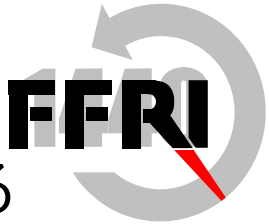
Black Hat EU 2014

- ATMのハッキングを、Rasberry Piを使って行う発表
- Traditional な方法は、スキミング、ショルダーハッキング、偽のPINパッド、偽のATMで口座番号と暗証番号を盗むという方法だった
- ちなみに、ATMは50秒で開けて内部にアクセス出来る（50秒でATMを開けるデモ動画が流れる）
- 中にアクセスできるということは、小型で、数々のインターフェースを接続でき、汎用OSのツールが動くコンピュータをおいておけば、情報を盗み取ることができる
- →Rasberry Piを使えばいい（10秒でATMにRasberry Piを設置する動画）
- USB接続でプログラムを送り込み、CEN/XFSという銀行取引プロトコルをスニッフィングし、ATMを操作するデモあり
- PINデバイスとATMの通信を盗聴するデモあり

Firmware.RE: Firmware unpacking, analysis and vulnerability-discovery as a service

Black Hat EU 2014

- IoTは組み込みデバイスがインターネットに繋がるが、インセキュアな組み込みデバイスがたくさんある
  - D-Linkのルータなど
- Router, printer, VoIP, Cars, Drones、これらのファームウェアを全部取り出して手動で調べるのは大変
- IoTでインターネットに繋がるデバイスが爆発的に増えるということは、解析・分析もなるべくスケールさせたい
- インターネットからファームウェアを集め、非常に簡単な静的解析と、Fuzzy Hashingを使い、脆弱性のあるデバイスを効率よく見つける手法を提案



TriCoreで動作する自動車用ECUソフトの攻撃手法に関する検討と試行（1）

CODE BLUE 2014

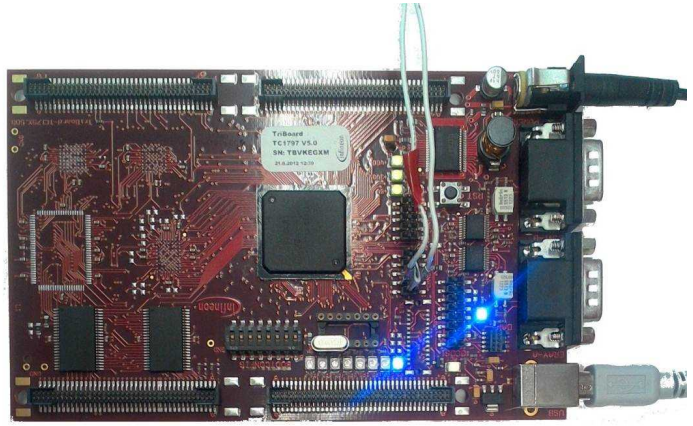
- FFRI とETASの共同研究
- ECUソフトに脆弱性があった場合、それを攻撃可能かどうかを理論的に検証
  - PCやスマフォとはアーキテクチャが異なる ECU マイコンでバッファオーバーフロー等のメモリ破壊脆弱性による任意コード実行の攻撃が成立するかどうか
- オープンな情報をもとにマイコンの仕様(レジスタ、命令、コンテキスト管理）を調査し、攻撃手法の仮説を立案
- 評価ボードを用いて、検証した結果、ECUソフトに脆弱性があった場合、リモートから任意コードを実行できる可能性があることを示唆

TriCoreで動作する自動車用ECUソフトの攻撃手法に関する検討と試行（2）

CODE BLUE 2014

- 検討した3つの攻撃手法
  - バッファオーバーフローによるスタック上の関数ポインタ上書き
    - 前提条件が厳しい
  - バッファオーバーフロー等によるTriCore独自のコンテキスト保存領域の上書き
    - 実際に攻撃される可能性あり
  - 割り込み・トラップハンドラの上書き
    - プロテクトされており不可

- 評価ボードを用いたデモ
  - CANバス経由でデータを送りつけ、バッファオーバーフローを発生させて点灯しないはずのLEDを点灯させた



TriCoreで動作する自動車用ECUソフトの攻撃手法に関する検討と試行（3）

- まとめ
  - ECUソフトにメモリ破壊脆弱性が存在する場合、任意コードを実行できる可能性はある
  - 今後、ECUソフトが複雑化し、処理する情報の種類・量が増加すると、実際のECUソフトにも脆弱性が多数発見される可能性がある
    - 対策として、ECUソフトに対する脆弱性検査やセキュアプログラミング・適切なメモリ保護の適用などが必要になると考えられる
- 課題
  - PCやスマートフォンなどと違って、脆弱性の実証と対策は環境、コスト的な理由で容易ではない点が懸念点
    - 検証のために車体が必要
    - ソフトのアップデートが容易にできない

さいごに

IT領域のイノベーション、IT技術の普及を妨げる要因を
排除するための技術研究が重要