Monthly Research 2016.08

Black Hat USA 2016
サーベイレポート

F F R I , Inc.
http://www.ffri.jp

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

目次

- Black Hat USA 概要
- 紹介する研究発表一覧
  - CANSPY: A Platform For Auditing CAN Devices
  - Advanced CAN Injection Techniques For Vehicle Networks
  - Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle
  - Into The Core – In-Depth Exploration of Windows 10 IoT Core
  - GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool
  - GreatFET: Making GoodFET Great Again
- まとめ
- 参考情報

Black Hat USA 概要

- 毎年8月にラスベガスで行われる世界最大のセキュリティカンファレンス
  - 世界中から投稿されたセキュリティに関する最新の研究が発表される
    - 内容は新しい脅威の実証から防御技術など高度で多岐にわたる
    - 一部を除き、プレゼン資料や論文がWeb で公開
  - FFRI 代表の鵜飼が研究発表の審査員(レビューボード)の一員を務める
  - 開催中は研究発表のほか、様々なツールや企画も発表される
    - Apple が最高20万ドルの賞金を支払う脆弱性懸賞プログラム「Apple Security Bounty」を発表
  - 同時期に DEFCON, BSideLV, USENIX などのセキュリティイベントも開催
    - 各イベントで研究発表・ワークショップが開催され、情報交換や入場バッジのリバースエンジニアリングなど盛り上がりを見せる

- 今回はFFRI Monthly Research 6月号でピックアップした発表結果を中心にご紹介

紹介する研究発表一覧 (1)

- 自動車セキュリティ関連
  - CANSPY: A Platform For Auditing CAN Devices
    - Jonathan-Christofer Demay & Arnaud Lebrun
  - Advanced CAN Injection Techniques For Vehicle Networks
    - Charlie Miller & Chris Valasek
  - Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (DEF CON 24)
    - Jianhao Liu, Chen Yan, Wenyuan Xu

紹介する研究発表一覧 (2)

- IoT関連
  - Into The Core – In-Depth Exploration of Windows 10 IoT Core
    - Paul Sabanal
  - GATTacking Bluetooth Smart Devices Introducing a New BLE Proxy Tool
    - Slawomir Jasek
  - GreatFET: Making GoodFET Great Again
    - Michael Ossmann

CANSPY: A Platform For Auditing CAN Devices (1)

- CAN バスに対し、MITM 攻撃を仕掛け監視を行うためのツール
  - オープンソースで基板データやソフトウェアを公開している
    - https://bitbucket.org/jcdemay/canspy
- OBD-II から CAN バスに接続、バスを通過する通信を傍受
  - サーバークライアント方式での MITM 攻撃を応用
    - ECU-ECU 間のバスへ割り込み、通信を傍受
- WiresharkによってCANパケットを解析できる
  - CANのプロトコルスタックとして SocketCAN を利用
  - SocketCAN は Wireshark でサポートされており、Dissector を記述する事でキャプチャしたフレームを Wireshark 上で確認可能

CANSPY: A Platform For Auditing CAN Devices (2)

- PC – ECU 間の通信を CAN over Ethernet で実装
  - ファームウェアに Ethernet サービスを実装することで、PC 側にタッピングや CAN バスをブリッジさせることを可能にしている
    - ブリッジ接続により、PC から CAN バスへのインジェクションが実現できる
    - Scapy を利用しフレームやパケットを書き換えが可能

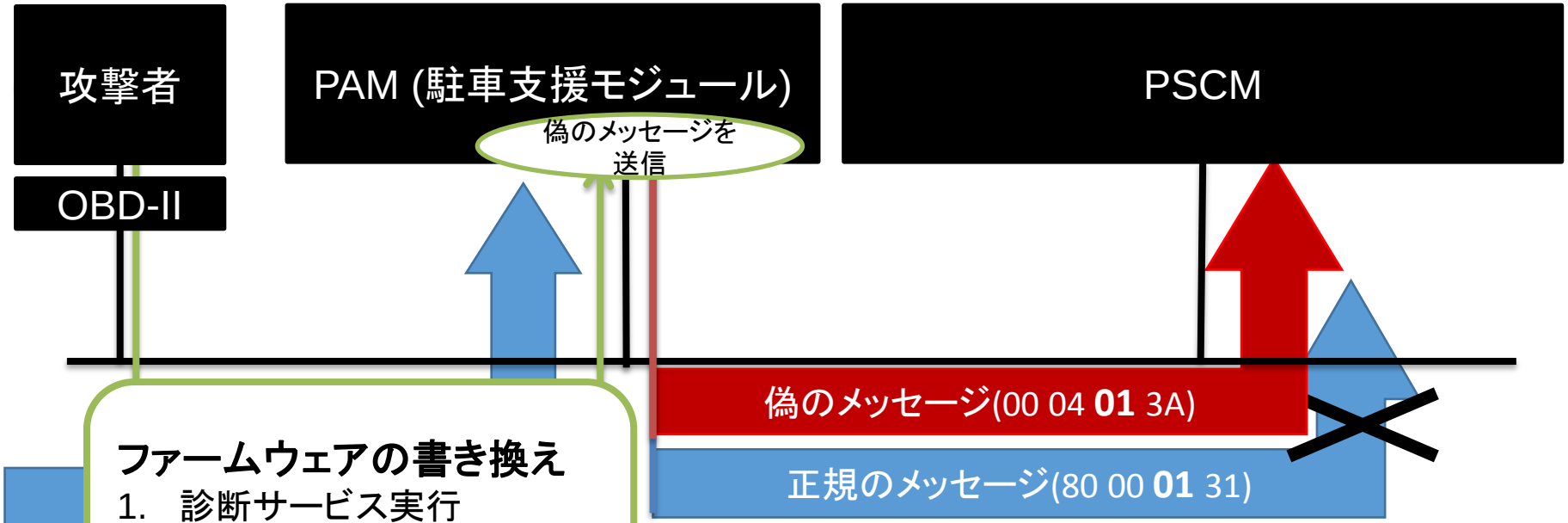
- **FFRI リサーチャーの考察**
  - 解析ツールとしての完成度は高い
  - 今後の改善点
    - 内部のフィルタリング機能
      - タイミング制約のある ECU 宛ての CAN フレーム操作
  - 上記の課題もあるが….
    - 現状、リアルタイム性が求められない機能に対する解析ツールとしては十分に期待できる
      - 例：故障診断機能(ECU側)、故障診断機(ECUに繋ぐ側) 等

Advanced CAN Injection Techniques For Vehicle Networks (1)

- 2014年から注目を集めているCharlie Miller 氏とChris Valasek 氏による所謂 Jeep Hack 研究の続報であり、今回も注目度が高く多くのメディアに取り上げられている
- 彼らは一連の研究により、The Pwnie Awards で“今年、専門家が最も知人からパニック状態で電話をかけられる原因になった研究者"に送られる「Pwnie for Best Junk or Stunt Hack」を受賞
- 今回の発表では、前年は不可能であった高速走行中のステアリングの制御に成功
  - これまでステアリングなどを制御するには低速走行中である必要があった
- パーキングアシストシステムや車間距離調節機能を利用し制限をバイパス、ブレーキ・アクセルやステアリングを操作
  - パーキングアシスト機能は、作動するために速度制限などの一定の条件が存在する
  - 今回はパケットの偽装やファームウェアの書き換えを行うことで制限をバイパス
- 特定のECUのファームウェアを書き換える
  - PSCM (パワーステアリング制御モジュール)ファームウェアの場合は、16bitのチェックサムが存在するがブルートフォース攻撃により9時間ほどで突破可能とのこと
- CANメッセージインジェクションにおける競合に対する防止措置
  - パーキングアシスト機能はメッセージが競合した場合、メッセージを無効化したりECUを再起動する
    - 競合例:ステアリングがほぼ同時に本来の「右30°」と偽の「左50°」というメッセージを受信

Advanced CAN Injection Techniques For Vehicle Networks (2)

ファームウェアの書き換えとメッセージ競合防止策



ファームウェアの書き換え

1. 診断サービス実行
2. セキュリティアクセス取得
3. ファームウェアを書き換える

メッセージの競合防止

- 3バイト目はカウンタの役割
  メッセージの重複チェックに用いる
- 3バイト目を偽装し直前に挿入
- 正規のメッセージは無視される

Advanced CAN Injection Techniques For Vehicle Networks (3)

- 提案されているCANインジェクションへの対応策
  - 本研究で危険だと判明した、PSCMなどのアルゴリズムを修正する
  - 受信側でメッセージ到達頻度を保持し急激な増加をチェック
- クライスラー・Jeepとトヨタ・プリウスのブレーキシステムでメッセージを受け取った際の実装
  - Jeep -> 疑われるメッセージを無効化し、ECUを再起動する
  - プリウス -> メッセージを受信次第実行し、チェックは行わない
    - プリウスの対応は安全性を第一にした設計故だと研究者は考えている
- **FFRI リサーチャーの考察**
  - 運転補助など様々な機能を介し自動車を制御する手法を提案・実現しており、今後は車両システムに対するリスクアセスメントの際に、攻撃されることへの考慮がより必要になると考えさせられる
    - 攻撃者の視点で考えた場合、Jeepは危険な状況で急ブレーキを無効化でき、プリウスは簡単に急ブレーキをかけさせることができる
    - 脅威対策によって軽減するリスクと発生するリスクについて、今後も研究が必要
  - 対策として提唱されているメッセージ到達頻度の保持については、先行研究としてSCIS2015でCANの送信タイミングから不正なメッセージを検出する研究が提唱されている
    - 倉地 亮, 高田 広章, 上田 浩史, 堀端 啓史,“車載制御ネットワークにおける送信周期監視システムの提案”,SCIS2015

Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (1)

- DEFCON 24 で発表された車載センサーへの攻撃に関する発表
  - 中国の大学の研究者と Qihoo 360の研究者による発表
  - 車載センサーに対して行った攻撃について Tesla, Audi などの実車を利用して検証
  - 同様の研究が Black Hat EU 2015 などで発表されているが、今回の研究では攻撃対象を更に拡大させた内容となっている
- LiDAR、ミリ波レーダー、超音波センサーなどのセンサー類は ADAS (先進運転支援システム)を実現するための重要な構成要素である
- センサーに対する攻撃方法は性質によって幾つかに分類できる
  - ジャミング
    - 利用している周波数と同じ周波数、出力の大きい電波を発生させることによって受信の妨害を行う
  - スプーフィング
    - 受信信号と類似した信号を発生させ、機器の誤作動を狙う
  - リレー
    - 受信した信号をリレーする

Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (2)

- 超音波センサーに対する攻撃
  - 超音波センサーは超音波を利用して障害物との距離を計測するセンサー
  - 検証では超音波センサーに対して以下の 2 種類の攻撃を実施して結果を観測
    - ジャミング
      - ノイズとなる超音波をセンサーに向けて照射し、反射波を受信できないようにする攻撃
      - 攻撃前は前方にある障害物を検知していたが、攻撃中は障害物を検知せず
    - なりすまし
      - 反射波と同程度の出力の波形の超音波を照射してセンサーの誤作動を誘発させる攻撃
      - 攻撃前と攻撃中で障害物との距離の表示が変化
  - 実験装置はマイコンボードの Arduino と超音波発生器で自作
  - 悪用されると接触事故を意図的に引き起こせる恐れが判明した

Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle (3)

- ミリ波レーダーに対する攻撃
  - ミリ波レーダーは前方の車との距離を測ることができ、クルーズコントロールや衝突回避システムなどで利用されている
  - 検証では以下の 2 種類の攻撃を実施
    - ジャミング(77 GHz の妨害電波)
      - 攻撃前は前方の障害物について検知していたが、攻撃中は対象が消える結果となった
    - なりすまし
      - 攻撃前後で車と障害物との距離が変化した
- **FFRIリサーチャーの考察**
  - 理論のみではなく、実車を利用して検証を行っているので発見された脅威は実際に引き起こせることを意味するのでインパクトが大きい
  - ミリ波レーダーに対する攻撃は大掛かりな設備が必要になるが、超音波センサーに対する攻撃は比較的安価な装置を組み合わせて実現できることが確認されたので、今後実際に被害が発生する可能性を感じた

Into The Core – In-Depth Exploration of Windows 10 IoT Core (1)

- Windows 10 IoT Core についてあらゆる視点で研究、挙動をまとめている
- ブートプロセスのフロー
  - SoCファームウェア > ブートローダー > UEFI > ブートマネージャー > Windows ブートローダ > メインOS
- セキュリティ機能の状況(研究当時)
  - Windows Defender は未対応
  - マイクロソフトパスポート未対応
    - Win10 からはじまった生体認証や PIN による二段階認証機能
  - セキュアブート
    - ブート対象が正規の証明書を持っていない場合、システム停止しブートしない
      - ブートキットやルートキットなどから保護
  - 軽量版 BitLocker
    - ユーザー及びシステムファイルの暗号化
  - Windows Update は強制自動更新だが、Pro 版は延期が可能

Into The Core – In-Depth Exploration of Windows 10 IoT Core (2)

- ネットワークサービスやドライバの状況
  - デフォルトでインストールされているWirelessアダプタ系のドライバ
    - Wi-Fi、Bluetooth、ZigBee、Z-Wave
    - 研究者はドライバへ攻撃された場合、カーネルモードが取得される可能性もあると懸念している
  - UDP マルチキャストによる存在の通知
    - Windows IoT デバイスは UDP マルチキャストにより他の端末に存在を通知する
    - パケットのデータ部分からはデバイス名や IP アドレス, OS バージョン, アーキテクチャなどが確認出来る
- 物理的に PC と接続しデバッキング
  - Raspberry Pi 3 と Shikra(USB-UARTアダプタ)を接続
  - SSH や PowerShell を介してデバイスに対しコマンドを実行,シリアルデバッグをON
  - PowerShell のコマンドから COM ポートを見つけ、WinDbg を利用しデバイスをカーネルデバッグ
- 他にユーザーモードでのプロセスのデバッグやクラッシュダンプの作成も行っている

Into The Core – In-Depth Exploration of Windows 10 IoT Core (3)

- Windows 10 IoTデバイスに対するセキュリティリスク軽減策の提案
  - ネットワークセグメンテーション
    - 所有している他のPCやサーバーと分離する
    - 内部ネットワークを介した感染への対策に有効
  - ファイアウォールにより不要な通信を遮断
  - TPMをサポートするデバイスを使用する
    - Minnowboard + Dragonboard や Raspberry Pi + Discrete TPM
  - セキュアブートやBitLockerなど利用可能なセキュリティ機能を活用
- 発表の結論
  - 他の OS に比べ攻撃されるリスクは少ないが、IoT 向けとして脅威は存在している
  - ベンダーやメーカーは設定ミスに注意する必要がある
  - 今後もセキュリティに対する研究は必要であり推奨される
- **FFRI リサーチャーの考察**
  - FFRI が Win 10 IoT Core のセキュリティ分析を行った際にもネットワークの問題を確認しており、注意は必要である
  - 本研究ではハードを中心に様々な研究手法が提案されている
  - 具体的なデバッキング方法を説明しており、今後のハード面の研究発展に貢献している

GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool (1)

- BLE に対してプロキシ的な振る舞いをするツール ”GATTacker“ の紹介
- このツールにより通信が暗号化されていな端末に対して以下の攻撃が可能としている
  - なりすまし, 通信の傍受, 改竄, MITM 攻撃
- 主な攻撃例
  - BLE を用いた Smart Lock 等への盗聴と信号のブロッキング
    - 任意のタイミングで家屋や車両のロックを解錠できる
    - 利用者の送信した施錠信号を無効化し、施錠したと誤認させる
  - ペイメントサービス情報への割り込み
  - GPS 情報の偽装とパケットのクローニングによる入店ポイントを不正に入手
- MITM 攻撃のフロー
  - BLE デバイスが送出するアドバタイジングパケット を GATTacker が独占、同じ情報を持ったアドバタイジングパケットを GATTacker から発信
  - 操作アプリがペアリングを要求すると、双方に気づかれないように GATTacker が BLE デバイスと要求を橋渡しする
  - ペアリング成立後は BLE デバイスと操作アプリの通信に GATTacker が割って入り、パケットのクローニングや改竄による別コマンドを実行を実現する

GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool (2)

- 公開されているサービス(ペイメントなど)への攻撃対策
  - サービス提供側で認証情報に期限を設ける
    - 期限を超過した場合は認証情報を破棄する
- ペアリングへの攻撃対策
  - 適切な BLE の暗号化
  - ランダム MAC アドレスの使用
  - MAC アドレスをもとにしたホワイトリスト方式のフィルタリング

- **FFRI リサーチャーの考察**
  - 攻撃の対処法としてホワイトリスト方式フィルタリングの導入があるが、BLE デバイスのMAC アドレス偽装により回避されてしまう可能性があるため、他の対策との併用が望ましい

GreatFET: Making GoodFET Great Again

- GoodFET の改良版ツール GreatFET の紹介
- GoodFET とはオープンソースの JTAG アダプタ、現在は 20以上の派生プロジェクトが存在する
    - http://goodfet.sourceforge.net/
- GoodFET の問題点
    - ソフトウェアは複雑化し維持が難しい
    - インターフェイスがSPIなどでビットバンギングされており、周辺機器を高速で利用不可
- GreatFET の特徴
    - USB インターフェイスを備える高性能 LPC4330 を使用、安価なままパフォーマンスを向上
    - ボタンを押すだけで　LPC4330 の USB ブートローダを利用可能
- GreatFET の問題点
    - パフォーマンスの向上や高速周辺機器に対応したことによりパーツが増えた
        - GoodFET 同様、手作業で作成は可能だが手順が多い
- **FFRI　リサーチャーの考察**
    - 周辺機器を高速のまま使用可能である点は評価が高い
    - 費用が掛かるので、資金に余裕があり GoodFET より高性能なものを求める際に、選択肢となる
    - 手作業でも可能としているがある程度技術が必要であると思われる

まとめ

- 自動車や IoT への攻撃研究はより現実的な内容に
  - 自動車の遠隔操作は高速走行中でも可能になった
  - IoT 機器は重要な通信プロトコルである BLE に対して、より簡単に MITM 攻撃を行うツールが考案された

- 防御側として多くの対策や研究が行われている
  - 既に個別の考察で示した通り、偽造 CAN メッセージや IoT 機器への研究は、過去の研究を元に国内外で多くの研究が進んでいる
    - 現実的な対策方法は今後増えると思われる
  - 各業界のベンダーが攻撃者に対し優位性を得る為、バグバウンティプログラムなどの取り組みを行っている

- Black Hat USA 2016 全体も例年通りレベルが高く、本スライドで紹介した以外にも興味深い研究が多数発表されていた

参考情報

- BlackHat USA 2016
  - https://www.blackhat.com/us-16/
- DEF CON
  - https://www.defcon.org/html/defcon-24/dc-24-index.html
- CANSPY: A Platform For Auditing CAN Devices
  - https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platorm-For-Auditing-CAN-Devices-wp.pdf
- Advanced CAN Injection Techniques For Vehicle Networks
  - https://www.blackhat.com/us-16/briefings.html#advanced-can-injection-techniques-for-vehicle-networks
- Into The Core – In-Depth Exploration of Windows 10 IoT Core
  - https://www.blackhat.com/docs/us-16/materials/us-16-Sabanal-Into-The-Core-In-Depth-Exploration-Of-Windows-10-IoT-Core-wp.pdf
- GATTacking Bluetooth Smart Devices Introducing a New BLE Proxy Tool
  - https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf
- GreatFET: Making GoodFET Great Again
  - https://www.blackhat.com/docs/us-16/materials/us-16-Ossmann-GreatFET-Making-GoodFET-Great-Again-wp.pdf
- Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle
  - https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles-WP.pdf