Monthly Research 2016.6

Black Hat USA 2016 事前調査

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

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

目次

- 概要
- 注目セッションの一覧
- 自動車セキュリティ関連
- IoT関連
- 考察
- 参考情報

概要

- Black Hat USA は毎年 8月にラスベガスで開催されている
  世界最大のセキュリティカンファレンス
  - 今年は7月30日から8月4日まで開催予定
  - 世界中から投稿された最新のセキュリティ研究が発表される
  - 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

- 採択された投稿のうち、Internet of Things, Hardware/Embedded に
  関連する研究発表は約 20 セッション

- 今回の Monthly Research では Black Hat USA 2016 セッションのアブ
  ストラクトを事前調査し、注目の研究発表をピックアップして紹介

注目セッションの一覧

- 自動車セキュリティ関連
  - CANSPY: A Platform For Auditing CAN Devices
  - Advanced CAN Injection Techniques For Vehicle Networks
- IoT関連
  - 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

自動車セキュリティ関連 (1)

- CANSPY: A Platform For Auditing CAN Devices
  - Arnaud Lebrun, Jonathan-Christofer Demay
  - CANSPYという、オンザフライで CAN メッセージをブロックしたり書き換えたりする事が可能なプラットフォームに関する発表
    - Webアプリケーションの脆弱性診断で利用される Burp の様なイメージ

- Advanced CAN Injection Techniques For Vehicle Networks
  - Charlie Miller, Chris Valasek
  - CAN メッセージの挿入による車両制御の乗っ取りには様々な制限がある
  - 運転中にスピードメーターの異常動作を起こすのは簡単だが、ブレーキやステアリング、アクセル操作を乗っ取るのは困難
    - そこでブレーキやステアリング、アクセル操作に掛けられている制限をバイパスし操作するテクニックを解説する

自動車セキュリティ関連 (2)

予定されているセッションは、いずれも CAN がキーワード

- CAN プロトコルは以前から脆弱である事が指摘されている
- 2016年現在でも多くの研究者に注目されている
  - 物理アクセスがしやすいインタフェース
  - リッチ化が進む情報系機器との接続(カーナビなど)

自動車を乗っ取るための条件とその攻略法に注目

- アブストラクトによれば、自動車の制御を乗っ取るためにはいくつかの条件が必要であり、例として速度が挙げられるという
- CAN メッセージの挿入によるステアリング操作・ブレーキ操作は、通常は特定の速度以下の場合などに限り有効
  - 我々の推測だが、パーキング・アシスト機能の為の仕様
- パーキング・アシスト機能が有効であると偽装するなどの手法で速度制限を回避すると考えられる
- 類似する研究発表として立命館大学の学生が CAN メッセージを挿入する事で意図的に ADAS (緊急ブレーキ) を無効化した例がある

IoT関連 (1)

- Into The Core – In-Depth Exploration of Windows 10 IoT Core
  - Paul Sabanal
  - Windows 10 IoT Core は新たな IoT プラットフォームとして将来重要な役割を果たすとし、セキュリティ機能を初めとした OS の特徴紹介
  - アタックベクタやマルウェアによって起こりえる攻撃の解説
  - 静・動的解析やファジングによるセキュリティアセスメント手法についての発表

- GATTAttacking Bluetooth Smart Devices – Introducing A New BLE Proxy Tool
  - Slawomir Jasek
  - モバイルアプリやデバイスの同意なしに、偽装した BLE (Bluetooth Low Energy) デバイスに接続させてプロキシとして動作することで BLE 通信を傍受できる可能性がある
  - 想定される攻撃の紹介やデバッグ・検証するための BLE MITM プロキシの発表

IoT関連 (2)

- GreatFET: Making GoodFET Great Again
  - Michael Ossmann
  - オープンソースの JTAG アダプターである GoodFET に関する発表

IoT 時代におけるハードウェアを理解するセキュリティエンジニアの重要性

- IoT関連でハードウェア構成に対してセキュリティ観点での評価を行う為にはチップのI/Oやバスを利用する方法に精通したセキュリティエンジニアが必要
  - 一般的な IoT 機器はインターネットに接続するための RJ45 イーサネットポートを持っているため、そこから様々な評価が可能
  - 一方で接続されているエッジのハードウェア（単なるデバイスだけではなく、ICやLSIを含む）は UART や SPI、I2C などのバス接続であると考えられる
- GoodFET や Hardsploit (CanSecWest Vancouver 2016) 等のオープンソースハードウェアはこうしたセキュリティエンジニアの手助けをするツールである

IoT関連 (3)

Windows 10 IoT Core は研究事例が少ない

- Windows 10 IoT Core に関するカンファレンス発表は今回の例を除くとCODE BLUE 2015 で FFRI のリサーチャーが脅威分析結果を発表したのみ
- 認証機能を持たない FTP やそれらを悪用する可能性のあるマルウェアの脅威について警鐘を鳴らした
- 今回はどのような結果が発表されるか注目

IoT デバイスに多用される BLE とその脅威

- アブストラクトでも言及されている通り、 BLE を利用した IoT デバイスやサービスは近年増加しており、研究テーマとして今後も注目され続けると予想される
- 研究例..Smart Wars: Attacking Smart Locks with a Smart Phone
  - 2016年1月開催のCanSecWest Vancouver 2016で発表されたスマートロックの脆弱性についての研究
  - BLEデバイスをキー・フォブとして利用しているスマートロック本体とのペアリングに介入するテクニックを利用して DoS 攻撃を試行

考察

- 自動車セキュリティのジャンルでは尚もCANに対する注目度が高く、前例からどのように進展していくのか期待

- IoTというキーワードが一般化されたことによって、組み込みセキュリティの需要が増加しており、この傾向は今後も続くと考えられる

- 上記に加えて、 GoodFET や Hardsploit などのオープンソースハードウェアの登場や、研究人口の増加に伴い、ハードウェアハッキングに関する敷居は下がっていく可能性が高い

- 今回は、Black Hat USA 2016 をトピックにしているが、7月から8月まで多くの著名なセキュリティカンファレンスが開催されるため、そちらにも注目
  - Shakacon VIII, Bsides Las Vegas, DEFCON 24, USENIX ‘16, etc…

参考情報

- Black Hat USA 2016 Official
  - https://www.blackhat.com/us-16/
- DEFCON 24
  - https://defcon.org/html/defcon-24/dc-24-index.html
- Bsides Las Vegas
  - https://www.bsideslv.org/
- REcon 2016
  - https://recon.cx/2016/
- Shakacon VIII
  - https://www.shakacon.org/
- USENIX
  - https://www.usenix.org/
- CanSecWest Vancouver 2016
  - https://cansecwest.com/
- ADAS ECUの動作条件を悪用した自動車の衝突回避システムに対する攻撃手法と軽量MAC認証の提案, 中野将志(立命館大学)他, SCIS2016
  - http://www.iwsec.org/scis/2016/program.html
- openclipart
  - https://openclipart.org/