Monthly Research 2017.01

IoT向けOS「Android Things」のセキュリティ

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

ＦＦＲＩ, Inc.
http://www.ffri.jp

目次

IoT デバイスのセキュリティ事情

- IoT デバイスのセキュリティ事情
  - IoT デバイスは近年、多くの攻撃にさらされている
    - マルウェアに感染した IoT デバイスがボットネットの一部となり、DDoS 攻撃が行われる被害も発生している
- Mirai
  - IoT デバイスに感染し、端末をボットネットに参加させるマルウェア
  - 端末で動作する telnet に対して、初期ユーザー名・パスワードに多用される約 60 組の単語を組み合わせた辞書攻撃によって侵入する

- Mirai ボットネットによると見られている DDoS 攻撃
  - 2016年10月12日に米国の DNS 提供業者 Dyn に対し最大10万台ほどの機器からの大規模な DDoS 攻撃が発生
  - この攻撃の影響で Twitter や Amazon なども一時利用不能に

Android Things とは

- Google が開発中の IoT 向け OS
  - 2016 年の12月に Developer Preview リリース
  - 前身の Brillo を改良、IoT 向けにセンサーなどを扱うライブラリが利用可能
  - スマートホーム等のデバイスへの利用が想定されている
  - Android Studio など既存の Android 開発環境やスキルを活用して IoT デバイスの開発が可能
  - 対応が発表されているボード

ボード	CPU(MCU)
Raspberry Pi 3	64-bit quad-core ARMv8 Cortex-A53 (1.2GHz CPU)
NXP Pico i.MX6UL	ARM® Cortex®-A7 Core
Intel® Edison	Intel® Atom™ SoC (500MHz dual-core x86 CPU) Intel® Quark™ (100MHz MCU)

主な特徴

- Things Support Library
  - 従来の Android フレームワークに様々なハードウェアを統合する API
    - Peripheral I/O API
      - センサーなどが接続される周辺 IF への入出力を扱う
        - » PWM, GPIO, I2C, SPI, UART
    - User Driver API
      - 様々なハードウェアイベントを Android アプリで利用可能にする
- 通常の Android との違い
  - Android 標準のシステムアプリなどが含まれていないため、Telephony や Settings など一部の API の使用は非推奨
  - また、Notification についても通知領域が存在しない為、非推奨
  - マニフェストに宣言した権限は全て付与される

インストールと初期設定

- インストール
  - 利用するボードごとにイメージが配布されている
  - 使用するボードに合わせたイメージファイルを SD カードに書き込む
    - 今回は Raspberry Pi 3 を使用
- 初期設定
  - 有線 LAN に接続する
- 起動後
  - ロゴが表示され、Ethernet アダプタの IP アドレスが表示される
- 接続
  - 上記の IP アドレスへ接続
    - adbで接続

ポート利用状況

- netstat の実行結果

```
$ adb shell
rpi3:/ $ netstat -antu
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 :::5555                 :::*                    LISTEN
（省略）
```

- nmap によるポートスキャンの結果
  - 5555/tcp で動作しているのは adb サービスだが Civilization というゲームのオープンソースクローン Freeciv と出力される
  - OSの種類とバージョンを識別することはできなかった

```
nmap 192.168.11.5 –O
（省略）
PORT     STATE SERVICE
5555/tcp open  freeciv
（省略）
No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).
```

セキュリティ設定の状況

- ファイアウォール
  - 設定されたポリシーに基づきパケットの監視・制御を行う
  - デフォルトの状態でファイアウォールが入っている様子はなかった

```
127|rpi3:/ # service check iptables
service check iptables
Service iptables: not found
```

- SELinux
  - Linux カーネルに対し強制アクセス制御機能を付加するモジュール
  - デフォルトでは Permissive になっており制限を行っていない

```
1|rpi3:/ $ getenforce
getenforce
Permissive
rpi3:/ $
```

セキュリティ設定の状況

- root へ権限昇格
  - 悪意ある第三者が root に昇格してしまった場合、端末を完全に乗っ取られてシステムにあらゆる改変が行われる恐れがある
  - デフォルトの状態で su コマンドを実行したところパスワードが要求されずに root に昇格できた

```
127|rpi3:/data $ whoami
whoami
shell
rpi3:/data $ su
su
rpi3:/data # whoami
whoami
root
```

まとめ

- セキュリティ上の注意点
  - 5555/tcp で Listen している adb に認証無しで接続してコマンドが実行可能
  - root へ権限昇格が su パスワードなしで可能
  - アプリの権限
    - Android Things ではアプリから要求された権限は全て許可してしまう
      - アプリが乗っ取られた場合、デバイスの異常動作や情報漏洩の恐れがある
- 想定される脅威
  - デフォルト設定の Android Things デバイスが公共ネットワークに接続されている場合、第三者に adb で接続され、root へ権限で任意のコマンドを実行される恐れがある

- 「普段は Android アプリ開発に携わっているが、ハードウェアもいじってみたい」というエンジニアには手頃だが、IoT デバイスで実用するにはセキュリティの強化が必要

- 今はまだ Developer Preview の段階のため、今後のデフォルト設定の変更やセキュリティ設定ガイドのリリースが期待される

参考情報

- Android Things
  - https://developer.android.com/things/index.html
- Raspberry Pi 3へのインストール方法
  - https://developer.android.com/things/hardware/raspberrypi.html
- System Image Downloads
  - https://developer.android.com/things/preview/download.html
- nmap
  - https://nmap.org/
- Raspberry Pi 3 のピン配置図
  - https://developer.android.com/things/hardware/raspberrypi-io.html
- Mirai-Source-Code
  - https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c
- JVNTA#95530271 Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威
  - http://jvn.jp/ta/JVNTA95530271/
- DNSサービス「Dyn」への大規模DDoS攻撃、発信源は10万台のIoT機器
  - http://itpro.nikkeibp.co.jp/atcl/idg/14/481542/102800290/
- Security-Enhanced Linux
  - https://ja.wikipedia.org/wiki/Security-Enhanced_Linux
- Freeciv - The Wireshark Wiki
  - https://wiki.wireshark.org/Freeciv