Monthly Research 2017.02

Android Things Developer Preview 2 のセキュリティ調査

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

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

目次

- 背景と概要
- Android Things のユースケースと Weave
- Android Things のセキュリティ(前回の調査結果)
- Android Things 基本的な環境
- ファイルシステムの調査
- adb のポート変更方法
- ファイアウォールの設定方法
- SELinux の有効化方法と root 権限について
- まとめ
- 参考情報

背景と概要

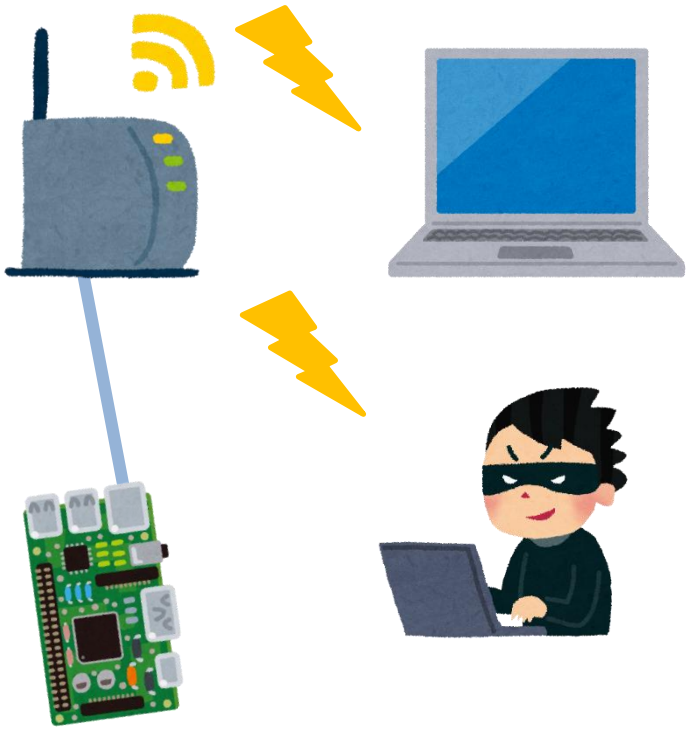
- 背景
  - Android Things の Developer Preview 2 が 2月9日にリリース
    - アップデートは下記の通り
      - Intel Joule のイメージを配布
      - C/C++ から周辺 I/O へ操作を行うための API を追加
      - 一部のデバイスでもUSBオーディオが利用可能に
      - 機械学習ライブラリ TensorFlow を利用するサンプルを同梱
      - 開発者がデバイスの物理ポートの状態を確認できるコマンドを実装
    - リリースノートにセキュリティ関連のアップデートは記載されていない
- 今回のリサーチの概要
  - Android Things の想定されるユースケースについて
  - システムのファイル構成の分析とセキュリティ設定の変更方法

Android Things のユースケースと Weave

- Android Things はユースケースとして電球やスマートプラグなどの制御を想定
  - Brillo ベースのスマート家電向けの OS である
  - スマート家電向け通信プロトコル Weave が利用可能になる予定

- Google Weave
  - 2015年に Google が Brillo と同時に発表
  - さまざまなスマート家電製品で利用可能
    - 空調や壁のスイッチなどをスマートフォンアプリから制御できる
    - 今後 Belkin WeMo, LiFX, Honeywell 等の製品が対応を予定している
  - Weave Device SDK と Weave Server を含む通信プロトコル
  - Weave デバイスはデバイススキーマ情報(コンポーネントと特性)で実装している機能を示す
  - Weave ではデバイススキーマ情報を利用し、デバイスに対し利用可能なコマンドなどを判断する
  - デバイス開発者のためのWebコンソールや管理アプリもリリースされている
  - iOS向けアプリでも利用可能
  - セキュリティガイドラインも存在する
    - TLS実装時の諸注意や強力なアルゴリズム等によるリソースの暗号化
    - 製品開発時は、商用利用手引のProgram Onboardingと同時に確認することが望ましい

Android Things のセキュリティ(前回の調査結果)



- 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
  - デフォルト設定のデバイスが公共ネットワークに接続された場合、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

Android Things 基本的な情報

- バージョン情報
  - getprop コマンドの実行結果は下記の通り
    - SDK バージョンは24で、リリースバージョンは 7.0 となっている

```
rpi3:/ # getprop | grep ro.build.version
（省略）
[ro.build.version.release]: [7.0]
[ro.build.version.sdk]: [24]
（省略）
```

  - APIから確認した結果は下記の通り
    - ソース

```
Log.d("Android SDK Version", ""+Build.VERSION.SDK_INT);
```

    - logcat の結果

```
03-07 08:43:37.075 9756-9756/com.example.test.myapplication D/Android SDK Version: 24
```

  - uname コマンドで取得したシステムの情報は下記の通り

```
rpi3:/ # uname -a
Linux localhost 4.4.19-v7+ #1 SMP PREEMPT Thu Feb 9 10:45:31 UTC 2017 armv7l
```

ファイルシステムの調査

- mount コマンドによるマウント状態のチェック
  - selinuxfs
    - SELinux を管理するためのファイルシステム

```
rpi3:/ # mount
/dev/root on / type ext4 (rw,seclabel,relatime,data=ordered)
（省略）
selinuxfs on /sys/fs/selinux type selinuxfs (rw,relatime)
（省略）
```

- ルート直下を確認
  - /init.rc
    - Android の初期設定などが記述されているファイル

```
rpi3:/ # ls -al
total 2400
（省略）
-rwxr-x---   1 root   shell  806624 2017-02-09 10:39 init
-rwxr-x---   1 root   shell     887 2017-02-09 10:39 init.environ.rc
-rwxr-x---   1 root   shell   24183 2017-02-09 10:39 init.rc
（省略）
```

adb のポート変更方法

- 懸念点
  - adb をデフォルトポート 5555 で利用するのはポートスキャンで見つかりやすく危険
- /init.rc の修正
  - Android Things では etc 下に service や sysconfig などLinuxで一般的なネットワーク設定ファイルは存在しない
  - Android Things の初期設定ファイル ”/init.rc” に直接書き込む
  - init.rc を PC などに取得し、on init の末尾に下記を記述

```
setprop service.adb.tcp.port [変更するポート番号]
```

  - (1) 変更した init.rc ファイルを Android Things の方に上書き
  - (2) adb から書き込んだ際に権限が変更されるので修正
  - 再起動時にファイルが読み込まれデフォルトのポートが変更される
  - これによりポートスキャンによってサービスが特定される危険性を軽減できる

```
C:¥Users¥test>adb root
C:¥Users¥test>adb connect [IP Address]
C:¥Users¥test>adb remount
remount succeeded
C:¥Users¥test>adb push init.rc /init.rc ← (1)
[100%] /init.rc
C:¥Users¥test¥Documents¥17_02>adb shell chmod 750 /init.rc ← (2)
C:¥Users¥test¥Documents¥17_02>adb shell ls -al /init.rc
-rwxr-x---    1 root    root     24249 2017-02-20 12:16 init.rc
```

ファイアウォールの設定方法

- 前回 service コマンドでは iptables が確認できなかったが、
  iptables コマンドは存在し、使用することが可能
  - rootへ昇格後、iptables -L コマンドで現在のフィルタリングが確認可能

```
rpi3:/ # iptables -L
iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
bw_INPUT   all  --  anywhere             anywhere
```

  - フィルタリングの実施
    - Wi-Fiアダプタ経由での5555ポートへのアクセス禁止を設定
    - Wi-Fi等を有効にする際は適宜フィルタリングルールを設定することが望ましい

```
C:¥Users¥test>adb devices
List of devices attached
192.168.0.10:5555       device    ← Wi-Fi 経由でadb接続

C:¥Users¥test>adb shell iptables -A INPUT -i wlan0 -p tcp --destination-port 5555 -j DROP
C:¥Users¥test>adb devices
List of devices attached
                                  ← 拒否されていた
```

SELinux の有効化方法と root 権限について

- SELinux の有効化
  - Android Things の SELinux はデフォルトで permissive
    - setenforce コマンドで有効化しても再起動時に初期化される
  - イメージを書き込んだ SD カードを PC などから読み込む
  - CMDLINE.TXT ファイルの末尾に下記が記載されていることを確認
    - androidboot.selinux=permissive
  - permissive を enforcing に変更して保存
  - ボードに挿入し起動すると SELinux が有効になっている事が確認できる

```
rpi3:/ # getenforce
Enforcing
```

  - 関連コマンドとしてchconやrestoreconは存在するが、semanage は存在しない
- su での root への権限昇格
  - Android Things では passwd コマンドは存在せず、/etc 直下に passwd, shadow ファイルを設置しても効果はない
  - root にパスワードを設定するもしくは su を実行させない方法について調査を継続中

まとめ

- ユースケースについて
  - ベースとなった Brillo がスマートホーム向けであることから Android Things でも同じ分野を目指すと考えられる
  - Android Things に搭載される予定の Weave はスマートフォンとデバイスなどの通信をサポートする
- ファイル構成
  - 一般的な Android の構成と似ている点も多いが、通信関係などの設定ファイルは位置などで違いがある
- ポートの変更
  - ポート番号はデフォルトから変更しておくことが望ましい
    - nmap による一般的なポートスキャンでは port 番号 1000 以上でもよく利用されるポートをチェックされる
      - port 5555 はチェックされるが適切に変更すればチェックされなくなる
- ファイアウォール
  - ポート変更はあくまで気休め程度でありフルポートスキャンなどには耐え得ないので、Wi-Fi等のネットワーク設定を有効にする際はサービスに合わせたファイアウォールの設定が必要
- root パスワード設定方法など、今後も検証すべき点が多い

参考情報

- Android Things
  - https://developer.android.com/things/index.html
- Android Things Developer Preview 2
  - https://android-developers.googleblog.com/2017/02/android-things-developer-preview-2.html
- Weave
  - https://developers.google.com/weave/
- SELinuxで組み込み機器のセキュリティを高める（後編） —— 組み込み機器にSELinuxを適用する
  - http://www.kumikomi.net/archives/2008/09/19selin2.php?page=6
- Android Debug Bridge
  - https://developer.android.com/studio/command-line/adb.html?hl=ja
- Android起動周りのノウハウ
  - http://www.slideshare.net/chancelab/android-27395892
- Validating SELinux
  - https://source.android.com/security/selinux/validate.html
- Weave Developer Tools
  - https://developers.google.com/weave/guides/apps-tools/overview