Monthly Research 2017.1

An Overview of the Android Things Security

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

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

Table of Contents

Security incidents related to IoT devices

- Many IoT devices have vulnerabilities
  - IoT devices are infected with malware
- IoT Malware - Mirai
  - This malware makes IoT devices bots
  - It expands infection by dictionary attack against telnet
  - The dictionary has about 60 patterns of id and password combination
- Large-scale DDoS attack by the Mirai botnet
  - Last Oct 12, The Dyn was attacked from about 100 thousand devices
  - That attack may have executed by the Mirai botnet
  - Twitter and Amazon were temporarily unavailable by that attack

About the Android Things

- An IoT platform by the Google
  - Developer preview version was released in Dec 2016
  - Improvement of Brillo
  - Libraries for using sensors are available
  - It will be used for smart home devices
  - Developers can create an IoT app using existing knowledge of Android app
  - Single board computers supported by the Android Things

Board	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)

Major features

- Things Support Library
  - Libraries for Integration hardware to core Android framework
  - Peripheral I/O API
    - Communicate with sensors and actuators
      - PWM, GPIO, I2C, SPI, UART
  - User Driver API
    - Hardware events become available the standard Android APIs

- Differences from Android
  - Android Things avoid using the system and content providers APIs
  - Android Things is no status bar therefore, NotificationManager API is not recommended
  - Android Things permit all permissions declared in a manifest to an app

Installation and Settings

- Install
  - Writing the image that matches the board to the SD card
    - We are using Raspberry Pi 3

- Boot
  - Connect to the LAN and turn on the power. Then the logo and IP address are displayed.

- Connect
  - Connect to the IP using adb

Accessible network service

- netstat

```
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
tcp        0     52 ::ffff:192.168.11.5:555 ::ffff:192.168.11.2:127 ESTABLISHED
tcp        0      0 ::ffff:192.168.11.5:590 ::ffff:64.233.189.188:5 ESTABLISHED
udp        0      0 192.168.11.5:68         192.168.11.1:67         ESTABLISHED
```

- Nmap
  - Could not identify the OS type and version
  - It is the adb service that operates at 5555/tcp, but it is output as Freeciv

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

Security configurations

- Firewall
  - iptables is not running

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

- SELinux
  - Linux kernel security module
  - SELinux is Permissive by default

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

Security configurations

- Privilege escalation
  - There is a danger that the system may be completely hijacked if an attacker gets promoted to root
  - root privilege could be obtained without a password by su command

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

Conclusions

- Security Considerations
  - Everyone can execute arbitrary command by connecting to adb listening on 5555/tcp without authentication
  - Privilege escalation to root with no password su command
  - App authority
    - All permissions requested by the application are allowed
    - When an application is compromised, there is a possibility of abnormal operation of the device and information leakage
- Assumed threat
  - If the Android Things device with the default setting is connected to the public network, the attacker may be executed arbitrary command with root privilege
- Opinion
  - It is still in Developer Preview.
    We would like to expect changes in its default settings or security configuration guide to be released.

References

- Android Things
  - https://developer.android.com/things/index.html
- Raspberry Pi 3
  - https://developer.android.com/things/hardware/raspberrypi.html
- System Image Downloads
  - https://developer.android.com/things/preview/download.html
- Security-Enhanced Linux
  - https://en.wikipedia.org/wiki/Security-Enhanced_Linux
- nmap
  - https://nmap.org/
- Mirai-Source-Code
  - https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c
- Freeciv - The Wireshark Wiki
  - https://wiki.wireshark.org/Freeciv