UNLEASH YOUR SMARTHOME DEVICES: VACUUM CLEANING ROBOT HACKING

Why is my vacuum as powerful as my smartphone?

Dennis Giese and Daniel Wegemer
Post presentation remarks 28.12. 18:00

- Rooting is now possible without opening the device
- You can only root one device (your own)
  - If you read the Heise article you might think that we might root multiple devices in the internet
- We consider the Xiaomi Cloud as a good and safe design
- Due time restrictions (our time was cut from 45 minutes to 30 minutes, including FAQ), we had to exclude a lot of information
  - Look into the repo for more technical information
- Contact: dustcloud@1338-1.org
Why Xiaomi

“Xiaomi’s ‘Mi Ecosystem’ has 50 million connected devices” [1]

“[…] revenue from its smart hardware ecosystem exceeded 15 billion yuan” (1.9 billion €) [2]

Most important: The stuff is cheap

Why Vacuum Robots?

Three Processors

To provide more location stability there are three dedicated processors to track its movements in real-time, calculate the location and determine the best route.

Source: Xiaomi advertisement
Xiaomi Ecosystem

- WiFi
- BLE
- ZigBee
- Gateway
- HTTPS
- Xiaomi Cloud

Dennis Giese and Daniel Wegemer – 34C3
Xiaomi Ecosystem

Cloud Protocol (WiFi)

BLE

HTTPS

Cloud Protocol (WiFi)

Xiaomi Cloud

Gateway

ZigBee

Dennis Giese and Daniel Wegemer – 34C3
Device Overview

Source: Xiaomi advertisement

Dennis Giese and Daniel Wegemer – 34C3
Rooting: Challenges

• Hardware Access
  – Micro USB Port ?
  – Serial Connection on PCB ?

• Network Based
  – Portscan ?
  – Sniff Network traffic ?
Teardown
Frontside layout mainboard

- 512 MB RAM
- R16 SOC
- 4GB eMMC Flash
- WiFi Module
- STM32 MCU
Backside layout mainboard

- LIDAR UART
- STM UART (921600 baud)
- R16 UART (115200 baud)
Rooting

Our weapon of choice:
Rooting

Initial Idea:

- Shortcut the MMC data lines
- SoC falls back to FEL mode
- Load + Execute tool in RAM
  - via USB connector
  - Dump MMC flash
  - Modify image
  - Rewrite image to flash

Source: wikicommons
Software

- Ubuntu 14.04.3 LTS (Kernel 3.4.xxx)
  - Mostly untouched, patched on a regular base
- Player 3.10-svn
  - Open-Source Cross-platform robot device interface & server
- Xiaomi proprietary software (/opt/rockrobo)
  - AppProxy
  - RoboController
  - Miio_Client
  - Custom adbd-version
- iptables firewall enabled
  - Blocks Port 22 (SShd) + Port 6665 (player)
Available data on device

• Data
  – Logfiles (syslogs, duration, area, ssid, passwd)
  – “/usr/sbin/tcpdump -i any -s 0 -c 2000 –w”
  – Multiple MBytes/day
  – Maps

• Data is uploaded to cloud

• Factory reset
  – Restores recovery to system
  – does not delete data
    • Maps, Logs still exist
Available data on device

• Maps
  – Created by player
  – 1024px * 1024px
  – 1px = 5cm
Configurations

- **DeviceID**
  - Unique per device

- **Keys**
  - **Cloudkey** (16 byte alpha-numeric)
    - Is used for cloud communication
    - Static, is not changed by update or provisioning
  - **Token** (16 byte alpha-numeric)
    - Is used for app communication
    - Dynamic, is generated at provisioning (connecting to new WiFi)
Update process

milO.ota {"mode":"normal", "install":"1", "app_url":"https://[URL]/v11_[version].pkg", "file_md5":"[md5]","proc":"dnld install"}
Update process

2. Download [app_url]
Update process

2. Download [app_url]
Update process

- system_a
- system_b
- Download
- Data

Active copy

Dennis Giese and Daniel Wegemer – 34C3
Update process

- system_a
- system_b
- Download
- Data

MD5 ok?
Update process

system_a
system_b
Download
Data

Active copy

Dennis Giese and Daniel Wegemer – 34C3
Update process

- system_a
- system_b
- Download
- Decrypt + image OK?

Active copy
Update process

- system_a
- system_b
- Download
- Data

Unpack + dd

Active copy
Update process

Update root pw in /etc/shadow

Data

Download

system_a

system_b
Update process

- system_a
- system_b
- Download
- Data

Active copy

Dennis Giese and Daniel Wegemer – 34C3
Update process

system_a
system_b
Download
Data

Active copy
Update process

- system_a
- system_b
- Download
- Data

Active copy

rebooting
Update process

system_a
system_b
Download
Data

Active copy

rebooting...
Update process

- system_a
- system_b
- Download
- Data

Active copy

Dennis Giese and Daniel Wegemer – 34C3
Update process

- system_a
- system_b
- Download
- Data

Active copy
Firmware updates

• Full and partial images
  – Encrypted tar.gz archives
  – Full image contains disk.img
    • 512 Mbyte ext4filesystem

• Encryption
  – Static password: “rockrobo”
  – Ccrypt [256-bit Rijndael encryption (AES)]

• Integrity
  – MD5 provided by cloud
Lets root remotely

• Preparation
  – Rebuild Firmware
    • Include authorized_keys
    • Remove iptables rule for sshd
  – Send „miLO.ota“ command to vacuum
    • Encrypted with token
      • From app or unprovisioned state
    • Pointing to own http server
login as: root
Authenticating with public key "rsa-key-gami" from agent
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.4.39 armv71)

* Documentation:  https://help.ubuntu.com/
Last login: Thu Dec 14 01:43:59 2017 from 192.168.8.67
root@rockrobo:~#
root@rockrobo:~ # apt-get update
Ign http://us.ports.ubuntu.com trusty InRelease
Get:1 http://us.ports.ubuntu.com trusty-updates InRelease [65.9 kB]
Get:2 http://us.ports.ubuntu.com trusty-security InRelease [65.9 kB]
Hit http://us.ports.ubuntu.com trusty Release
Hit http://us.ports.ubuntu.com trusty Release
Hit http://ppa.launchpad.net trusty InRelease
Get:3 http://us.ports.ubuntu.com trusty-updates/main Sources [409 kB]
Get:4 http://us.ports.ubuntu.com trusty-updates/restricted Sources [6322 B]
Get:5 http://us.ports.ubuntu.com trusty-updates/main armhf Packages [875 kB]
Hit http://ppa.launchpad.net trusty/main armhf Packages
Get:6 http://us.ports.ubuntu.com trusty-updates/restricted armhf Packages [8931 B]
Hit http://ppa.launchpad.net trusty/main Translation-en
Get:9 http://us.ports.ubuntu.com trusty-security/main Sources [147 kB]
Get:10 http://us.ports.ubuntu.com trusty-security/restricted Sources [4931 B]
Get:11 http://us.ports.ubuntu.com trusty-security/main armhf Packages [575 kB]
Get:12 http://us.ports.ubuntu.com trusty-security/restricted armhf Packages [8931 B]
<table>
<thead>
<tr>
<th>PID</th>
<th>USER</th>
<th>PRI</th>
<th>NI</th>
<th>VIRT</th>
<th>RES</th>
<th>SHR</th>
<th>S</th>
<th>CPU%</th>
<th>MEM%</th>
<th>TIME+</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>922</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>5.9</td>
<td>19.2</td>
<td>1h05:03</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>27788</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>2724</td>
<td>1324</td>
<td>932</td>
<td>R</td>
<td>3.9</td>
<td>0.3</td>
<td>0:00:45</td>
<td>htop</td>
</tr>
<tr>
<td>940</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>2.0</td>
<td>19.2</td>
<td>22:22:18</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>947</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>1.3</td>
<td>19.2</td>
<td>15:59:31</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>535</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>2452</td>
<td>1276</td>
<td>992</td>
<td>S</td>
<td>1.3</td>
<td>0.2</td>
<td>6:00:78</td>
<td>/bin/bash /usr/bin</td>
</tr>
<tr>
<td>719</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>40184</td>
<td>37692</td>
<td>3996</td>
<td>S</td>
<td>0.7</td>
<td>7.4</td>
<td>9:15:19</td>
<td>WatchDoge /opt/rocr</td>
</tr>
<tr>
<td>939</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>0.7</td>
<td>19.2</td>
<td>11:03:31</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>948</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>0.7</td>
<td>19.2</td>
<td>7:09:43</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>951</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>0.7</td>
<td>19.2</td>
<td>2:28:84</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>881</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>2552</td>
<td>1096</td>
<td>776</td>
<td>S</td>
<td>0.0</td>
<td>0.2</td>
<td>4:27:87</td>
<td>top -H -d 15 -b</td>
</tr>
<tr>
<td>938</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>329M</td>
<td>97900</td>
<td>6168</td>
<td>S</td>
<td>0.0</td>
<td>19.2</td>
<td>4:09:65</td>
<td>player /opt/rocr</td>
</tr>
<tr>
<td>520</td>
<td>syslog</td>
<td>20</td>
<td>0</td>
<td>30472</td>
<td>1352</td>
<td>828</td>
<td>S</td>
<td>0.0</td>
<td>0.3</td>
<td>0:11:07</td>
<td>rsyslogd</td>
</tr>
<tr>
<td>882</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>2540</td>
<td>1068</td>
<td>776</td>
<td>S</td>
<td>0.0</td>
<td>0.2</td>
<td>8:15:61</td>
<td>top -d 5 -b</td>
</tr>
<tr>
<td>27798</td>
<td>root</td>
<td>0</td>
<td>-20</td>
<td>2564</td>
<td>1400</td>
<td>1004</td>
<td>S</td>
<td>0.0</td>
<td>0.3</td>
<td>0:00:06</td>
<td>/bin/bash /opt/rocr</td>
</tr>
</tbody>
</table>
Gain independence

Two methods:

• **Replacing** the cloud interface
• **Proxy** cloud communication

Source: 20th Century Fox
Replacing the cloud interface

cloud client
https, mqtt, etc...

Replacing the cloud interface

Miio_client
0.0.0.0:54322 (tcp)
0.0.0.0:54321 (udp)

RoboController
uart_mcu
uart_lds
compass
player
0.0.0.0:6665

wifimgr

AppProxy

Android/iPhone App

IPC

plain json (tcp)
enc(key) json (tcp/udp)
enc(token) json (udp)

Dennis Giese and Daniel Wegemer – 34C3
Replacing the cloud interface

- commands, reports ->

Player 0.0.0.0:6665

Wifimgr

RoboController

AppProxy

Compass uart_lds uart_mcu

*fds.api.xiaomi.com (https)

IPC
plain json (tcp)
enc(key) json (tcp/udp)
enc(token) json (udp)
Replacing the cloud interface

My cloud client
(local):54322 (tcp)
https, mqtt, etc...

FHEM
Home Assistant

 IPC
plain json (tcp)
enc(key) json (tcp/udp)
enc(token) json (udp)
Replacing the cloud interface

My cloud client
(local):54322 (tcp)
https, mqtt, etc...

/FET/hosts
127.0.0.1 awsbj0...
127.0.0.1 aswbj0-files...
127.0.0.1 cdn.cnbj0....

FHEM
Home Assistant

IPC
plain json (tcp)
enc(key) json (tcp/udp)
enc(token) json (udp)
Proxy cloud communication

Robot intern

compass  uart_lds  uart_mcu
player
0.0.0.0:6665
wifimgr
RoboController
AppProxy

Miio_client
(local):54322 (tcp)
0.0.0.0:54321 (udp)

*.fds.api.xiaomi.com (https)

ot.io.mi.com:80(tcp)
ott.io.mi.com:8053(udp)

Android/
iPhone App

IPC
plain json (tcp)
enc(key) json (tcp/udp)
enc(token) json (udp)
Proxy cloud communication

RoboController

compass  uart_lds  uart_mcu

player
0.0.0.0:6665

wifimgr

AppProxy

Miio_client
(local):54322 (tcp)
0.0.0.0:54321 (udp)

Dustcloud

*.fds.api.xiaomi.com (https)

ot.io.mi.com:80 (tcp)
ott.io.mi.com:8053 (udp)

Android/
iPhone App

/etc/hosts
130.83.x.x ot.io.mi.com
130.83.x.x ot.io.mi.com

IPC
plain json (tcp)
enc(key) json (tcp/udp)
enc(token) json (udp)

Dennis Giese and Daniel Wegemer – 34C3
Usecases

• Home automation server
• Webradio
• Fileserver
  – with integrated UPS
• Bitcoin mining
### Device Overview

<table>
<thead>
<tr>
<th>this.vacuum</th>
<th>Docked</th>
<th>start</th>
<th>pause</th>
<th>charge</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fan_power</strong></td>
<td>60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>clean_summary</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Internals

- **DEF**: 127.0.0.1 656c423233624835384f46374a445177
- **FD**: 5
- **NAME**: this.vacuum
- **NR**: 20
- **STATE**: connected
- **TYPE**: XiaomiDevice
- **device_type**: unknown
- **mac**: 34:CE:00:
- **model**: rockrobo.vacuum.v1
- **token**: 656c423233624835384f46374a445177

### Readings

- **battery**: ok 2017-12-2
- **batteryLevel**: 100 2017-12-2
DLC

• Modified firmware (SSH + FHEM)
• Dustcloud (Cloud emulation)
  – totally broken, insecure code!
• Pictures, Pinouts, and much more

⇒ www.dontvacuum.me
One word of warning...

• Never leave your devices unprovisioned
  – Someone else can provision it for you
    • Install malicious firmware
    • Snoop on your apartment

• Be careful with used devices
  – e.g. Amazon Marketplace
  – Some malicious software may be installed
Acknowledgements & FAQ

- Secure Mobile Networking (SEEMOO) Labs

- Prof. Guevara Noubir (CCIS, Northeastern University)
Backup
Pin Layout CPU

Dennis Giese and Daniel Wegemer – 34C3
Overview sensors

• 2D LIDAR SLAM (5*360°/s)
• Ultrasonic distance sensor
• multiple IR sensors
• 3-axis Magnetic Sensor
• 3-axis accelerometer
• 3-axis gyroscope
• Bump sensors
Sound packages

• Contents of /mnt/data/sounds
  – Encrypted tar.gz archives
  – Contains wav-files in specific language or style

• Encryption
  – Static password: “r0ckrobo#23456”
  – Ccrypt [256-bit Rijndael encryption (AES)]

• Integrity
  – MD5 provided by cloud
# eMMC Layout

<table>
<thead>
<tr>
<th>Label</th>
<th>Partion</th>
<th>Size in MByte</th>
<th>Start address</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot-res</td>
<td>a</td>
<td>8</td>
<td>0x00008000</td>
</tr>
<tr>
<td>env</td>
<td>b</td>
<td>16</td>
<td>0x0000c000</td>
</tr>
<tr>
<td>app</td>
<td>c</td>
<td>16</td>
<td>0x00014000</td>
</tr>
<tr>
<td>recovery</td>
<td>d</td>
<td>512</td>
<td>0x0001c000</td>
</tr>
<tr>
<td>system_a</td>
<td>e</td>
<td>512</td>
<td>0x0011c000</td>
</tr>
<tr>
<td>system_b</td>
<td>f</td>
<td>512</td>
<td>0x0021c000</td>
</tr>
<tr>
<td>Download</td>
<td>g</td>
<td>528</td>
<td>0x0031c000</td>
</tr>
<tr>
<td>reserve</td>
<td>h</td>
<td>16</td>
<td>0x00424000</td>
</tr>
<tr>
<td>UDISK</td>
<td>i</td>
<td>~1900</td>
<td>0x0042c000</td>
</tr>
</tbody>
</table>
## eMMC Layout

<table>
<thead>
<tr>
<th>Label</th>
<th>Content</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot-res</td>
<td>bitmaps &amp; some wav files</td>
<td></td>
</tr>
<tr>
<td>env</td>
<td>uboot cmd line</td>
<td></td>
</tr>
<tr>
<td>app</td>
<td>device.conf (DID, key, MAC), adb.conf, vinda</td>
<td>/mnt/default/</td>
</tr>
<tr>
<td>recovery</td>
<td>fallback copy of OS</td>
<td></td>
</tr>
<tr>
<td>system_a</td>
<td>copy of OS (active by default)</td>
<td>/</td>
</tr>
<tr>
<td>system_b</td>
<td>copy of OS (passive by default)</td>
<td></td>
</tr>
<tr>
<td>Download</td>
<td>temporary unpacked OS update</td>
<td>/mnt/Download</td>
</tr>
<tr>
<td>reserve</td>
<td>config + calibration files, blackbox.db</td>
<td>/mnt/reserve/</td>
</tr>
<tr>
<td>UDISK</td>
<td>logs, maps, pcap files</td>
<td>/mnt/data</td>
</tr>
</tbody>
</table>
Communication relations
Communication relations

Dennis Giese and Daniel Wegemer – 34C3
Communication relations

Dennis Giese and Daniel Wegemer – 34C3
Communication relations
Communication relations

Dennis Giese and Daniel Wegemer – 34C3
Communication relations

- **RoboController**
  - **uart_mcu**
  - **uart_lds**
  - **compass**

- **AppProxy**
  - **SysUpdate**
  - **rrlogd**

- **Miio_client**
  - (local):54322 (tcp)
  - 0.0.0.0:54321 (udp)

- **Miio_send_line**
- **Miio_recv_line**

- **Miio_client_helper_nomqtt.sh**

- **wifimgr**

- **Android/iPhone App**

- **Start**
  - **awsbj0-fds.api.xiaomi.com (https)**
  - **awsbj0-files.fds.api.xiaomi.com (https)**
  - **cdn.cnbj0.files.fds.api.xiaomi.com (https)**
  - **ott.io.mi.com:8053(udp)**
  - **ot.io.mi.com:80(tcp)**

- **IPC**
  - **plain json (tcp)**
  - **enc(key) json (tcp/udp)**
  - **enc(token) json (udp)**