Unleash your smart home devices: vacuum cleaning robot hacking

Why is my vacuum as powerful as my smartphone

Dennis Giese and Daniel Wegemer
Post presentation remarks 27.12. 21:00

• Rooting is now possible without opening the device
• 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 path for cleaning.

Source: Xiaomi advertisement
Xiaomi Ecosystem

- WiFi
- BLE
- ZigBee
- Gateway
- HTTPS

Dennis Giese and Daniel Wegemer – 34C3
Xiaomi Ecosystem

Cloud Protocol (WiFi)

BLE

ZigBee

Gateway

Xiaomi Cloud

HTTPS

HTTPS

Cloud Protocol (WiFi)
Device Overview

Source: Xiaomi advertisement
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

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

Data

Decrypt + image OK?

Active copy
Update process

- system_a
- system_b
- Download
- Data

Unpack + dd

Active copy

Dennis Giese and Daniel Wegemer – 34C3
Update process

System a
System b
Download
Data

Active copy

Update root pw in /etc/shadow
Update process

system_a

system_b

Download

Data

dd

Active copy
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

Dennis Giese and Daniel Wegemer – 34C3
Firmware updates

• Full and partial images
  – Encrypted tar.gz archives
  – Full image contains disk.img
    • 512 Mbyte ext4-filesystem

• 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
root@rockrobo: ~

login as: root
Authenticating with public key "rsa-key-gami" from agent
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.4.39 armv7l)

* 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]
Gain independence

Two methods:

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

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

```
compass  uart_lds  uart_mcu

player
0.0.0.0:6665

wifimgr

RoboController

AppProxy

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

<commands, reports->
```

---

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

```
compass  uart_lds  uart_mcu

player
0.0.0.0:6665

wifimgr

RoboController

AppProxy

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

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

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

FHEM
Home Assistant

<-commands, reports->

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

Dennis Giese and Daniel Wegemer – 34C3
Proxy cloud communication

```
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)

Android/ iPhone App

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

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

<commands, reports->

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

- Dustcloud
  - *fds.api.xiaomi.com (https)
  - ot.io.mi.com:80(tcp)
  - ott.io.mi.com:8053(udp)

- Miio client
  - (local):54322 (tcp)
  - 0.0.0.0:54321 (udp)

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

- RoboController
  - wifimgr

- Robot intern
  - compass
  - uart_lds
  - uart_mcu

- Android/iPhone App
  - IPC
  - plain json (tcp)
  - enc(key) json (tcp/udp)
  - enc(token) json (udp)
Usecases

• Home automation server
• Webradio
• Fileserver
  – with integrated UPS
• Bitcoin mining
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 firmare
    • Snoop on your appartment

• 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>Partition</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>

Dennis Giese and Daniel Wegemer – 34C3
Communication relations

Dennis Giese and Daniel Wegemer – 34C3
Communication relations

---

**Miio client**
- (local):54322 (tcp)
- 0.0.0.0:54321 (udp)

**Miio_client_helper_nomqtt.sh**
- Miio_send_line
- Miio_recv_line

**player**
- 0.0.0.0:6665 (udp)
- 0.0.0.0:6665 (tcp)

**RoboController**

**rrlogd**

**AppProxy**

**SysUpdate**

**wifimgr**

**uart_lds**

**uart_mcu**

**compass**

---

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

---

**Android/iPhone App**

**awsbj0.fds.api.xiaomi.com (https)**

**awsbj0-files.fds.api.xiaomi.com (https)**

**cdn.cnbj0.files.fds.api.xiaomi.com (https)**

**ot.io.mi.com:80(tcp)**

**ott.io.mi.com:8053(udp)**
Communication relations

Dennis Giese and Daniel Wegemer – 34C3

**Miio_client**

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

**Miio_client_helper_nomqtt.sh**

**Miio_send_line**

**Miio_recv_line**

**Miio_send_line**

**Miio_recv_line**

**player**

- 0.0.0.0:6665 (udp)
- 0.0.0.0:6665 (tcp)

**RoboController**

**rrlogd**

**AppProxy**

**SysUpdate**

**wifimgr**

**uart_mcu**

**uart_lds**

**compass**

**File:**
- gridmap
- player_server_*.log
- SLAM_*.log
- NAV_*.log

**IPC**

plain json (tcp)

enc(key) json (tcp/udp)

enc(token) json (udp)

**awsbj0.fds.api.xiaomi.com (https)**

**awsbj0-files.fds.api.xiaomi.com (https)**

**cdn.cnbj0.files.fds.api.xiaomi.com (https)**

**ottio.mi.com:80(tcp)**

**ott.io.mi.com:8053(udp)**