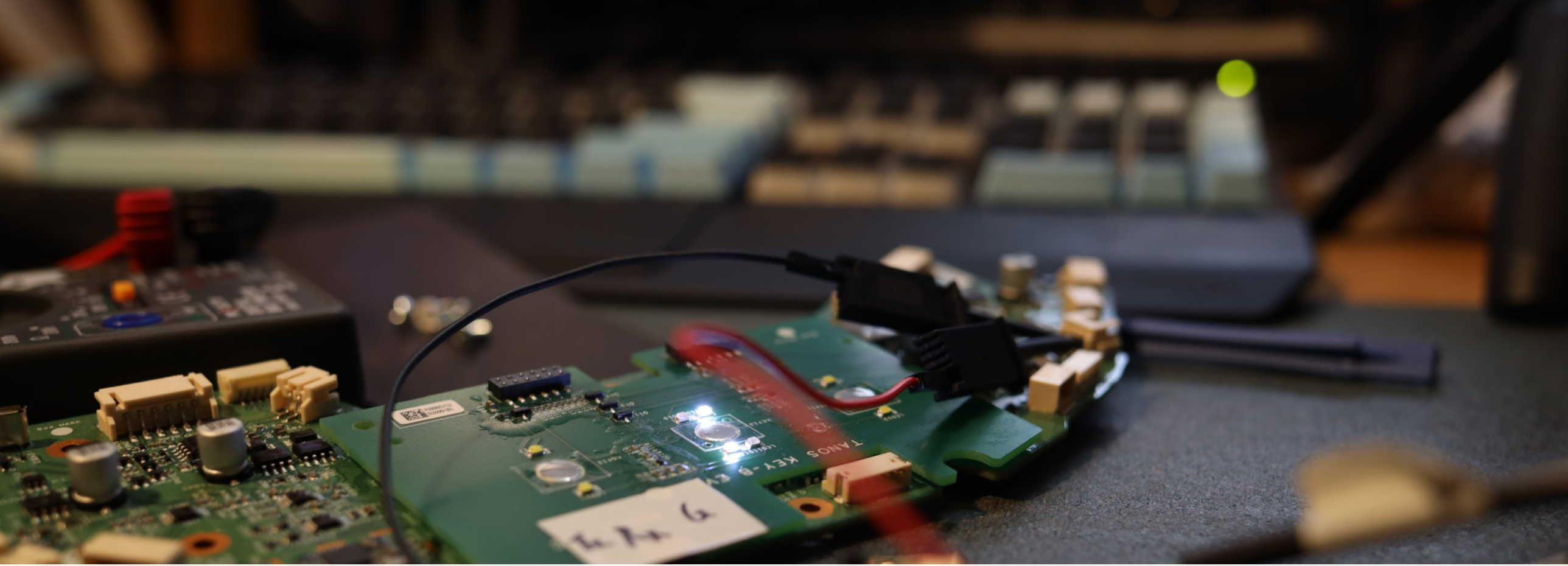


“Smart” Vacuum Cleaners

An Audit Into The Security and Integrity of IoT Systems

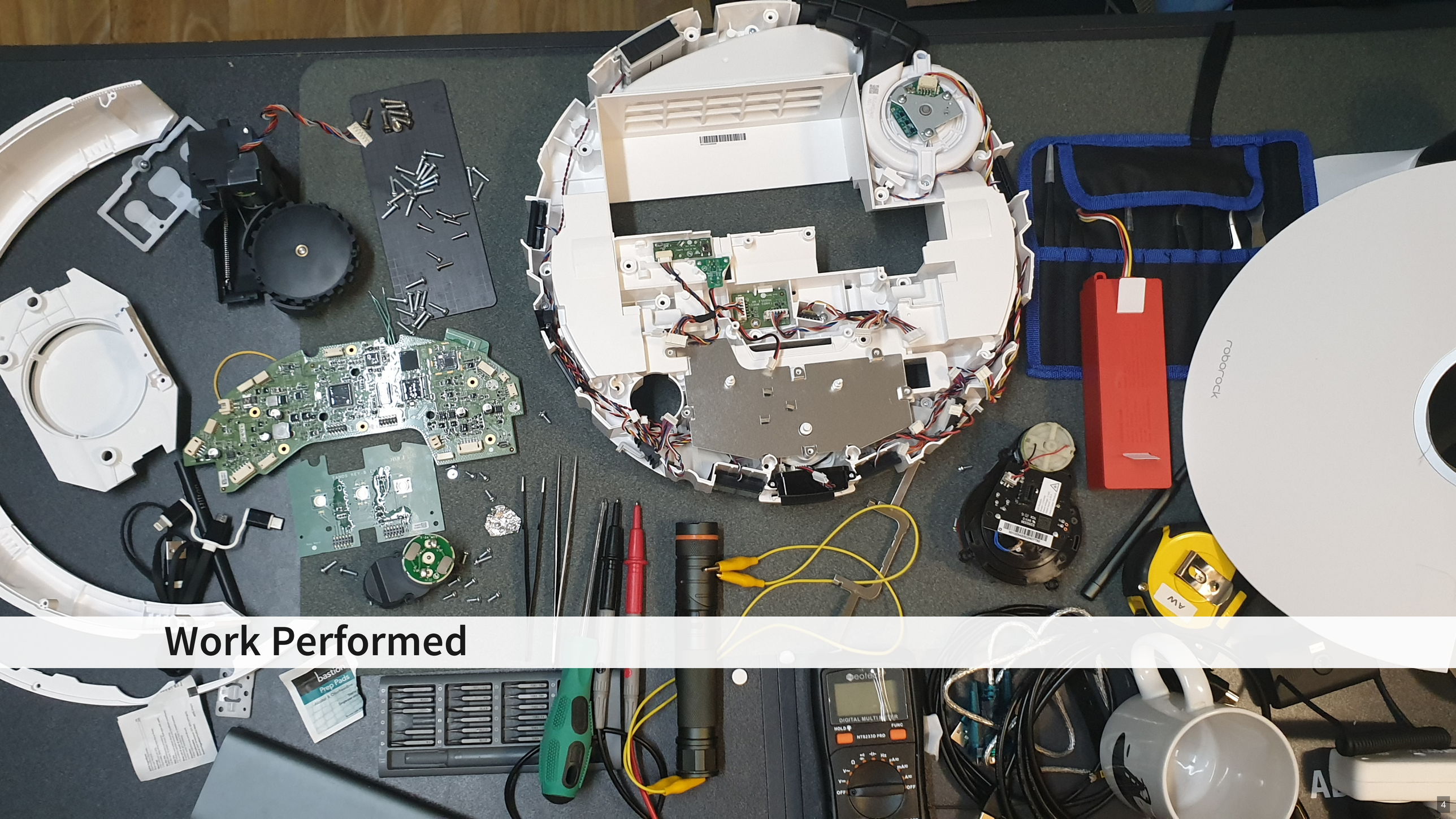
Andrew Wong | UNSW Sydney

Today’s Agenda

Statement

How have manufacturers of IoT / smart home devices addressed the increasing concerns of digital privacy and product security?

- Digital Privacy - Investigate the nature of network data (i.e. content, frequency, destination) and how the data is used.
- Product Security - Investigate potential security vulnerabilities and assess the effectiveness of current security fortifications.



Work Performed

Fingerprinting

System

```
[ 0.340]U-Boot 2011.09-rc1-dirty (Mar 25 2020 - 20:45:43) Allwinner Technology
[ 0.000000] Linux version 3.4.39 (rockrobo@apimg) (gcc version 4.8.4 (Ubuntu/Linaro 4.8
[ 0.000000] CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=10c5387d
[ 0.000000] Machine: sun8i
...
```

CPU: Allwinner R16 (ARM Cortex-A7) - ARMv7l / armhf

ACU: STM32F103VCT6 (ARM Cortex-M3)

Roborock Firmware version: 3.5.4_1558

Operating system: Ubuntu 14.04.3 LTS

Fingerprinting

Users

root@192.168.8.1:22

```
root@rockrobo:~# ~/z5206677/bat /etc/passwd
```

File: **/etc/passwd**
Size: **1.1 KB**

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/bin/false
```

root@192.168.8.1:22

```
root@rockrobo:~# ~/z5206677/bat /etc/shadow
```

File: **/etc/shadow**
Size: **679 B**

```
root:$6$mptOwWOW$DpR0O/CdKUfpapA3rEGl/4m6WZOkRYC5LSaCJSYKj9iHuZp2PUzfolgrGVeHW5tMtRSYlBWSlonusy67027JF/::0:99999:7:::
daemon:*:16652:0:99999:7:::
bin:*:16652:0:99999:7:::
sys:*:16652:0:99999:7:::
sync:*:16652:0:99999:7:::
games:*:16652:0:99999:7:::
man:*:16652:0:99999:7:::
lp:*:16652:0:99999:7:::
mail:*:16652:0:99999:7:::
news:*:16652:0:99999:7:::
uucp:*:16652:0:99999:7:::
proxy:*:16652:0:99999:7:::
www-data:*:16652:0:99999:7:::
backup:*:16652:0:99999:7:::
list:*:16652:0:99999:7:::
irc:*:16652:0:99999:7:::
gnats:*:16652:0:99999:7:::
nobody:*:16652:0:99999:7:::
libuuid:!:16652:0:99999:7:::
syslog:*:16652:0:99999:7:::
sshd:*:16799:0:99999:7:::
dnsmasq:*:16799:0:99999:7:::
```

No additional users

```
root@rockrobo:~# ls /home
ruby
```

`/home/ruby` exists but no user `ruby`, though exists in `/etc/passwd`~

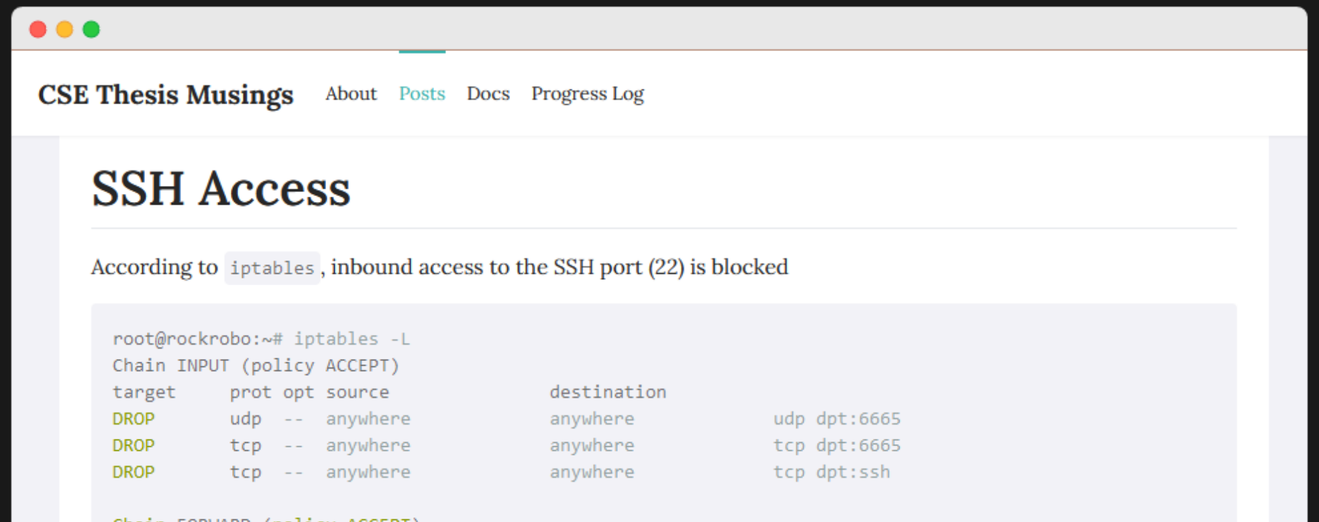
Fingerprinting

Processes

- Everything is running as root

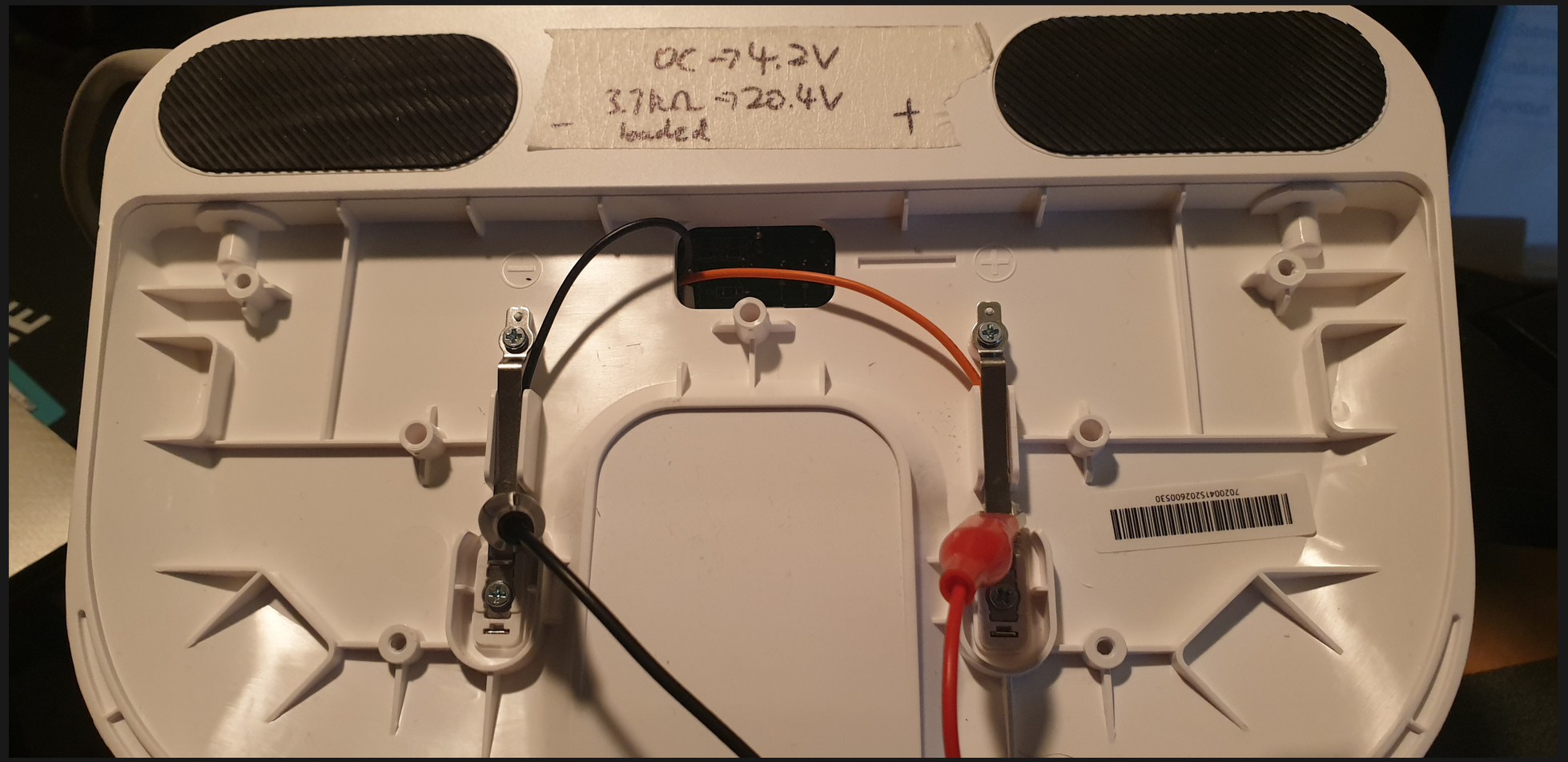
Fingerprinting

Going wireless - establishing SSH



Trivial Power Analysis

Batteries dont’t last forever!



What if I unplug the battery?

- No change in output during boot
- But device will turn off after around 20 seconds

See 2-wire log, 4-wire log

File System Imaging

The eMMC only has 4GB of storage, so we can’t (also shouldn’t) image the flash onto itself… but we can image it remotely!

```
IP=10.10.10.8
for partition in `ssh root@$IP "ls /dev/mmcblk0?* -1"`
do
    ssh root@$IP "sudo dd if=$partition bs=1M" | dd of=$(basename $partition).img
done
```

File System Structure

partition	label	description
mmcblk0p1	UDISK	user data
mmcblk0p2	boot-res	bootloader stuff
mmcblk0p5	env	
mmcblk0p6	app (RO)	device data
mmcblk0p7	recovery	stock firmware
mmcblk0p8	system_a	Main OS (boot)
mmcblk0p9	system_b	Backup OS
mmcblk0p10	Download	Update temp
mmcblk0p11	reserve	blackbox???

Recovery Reset

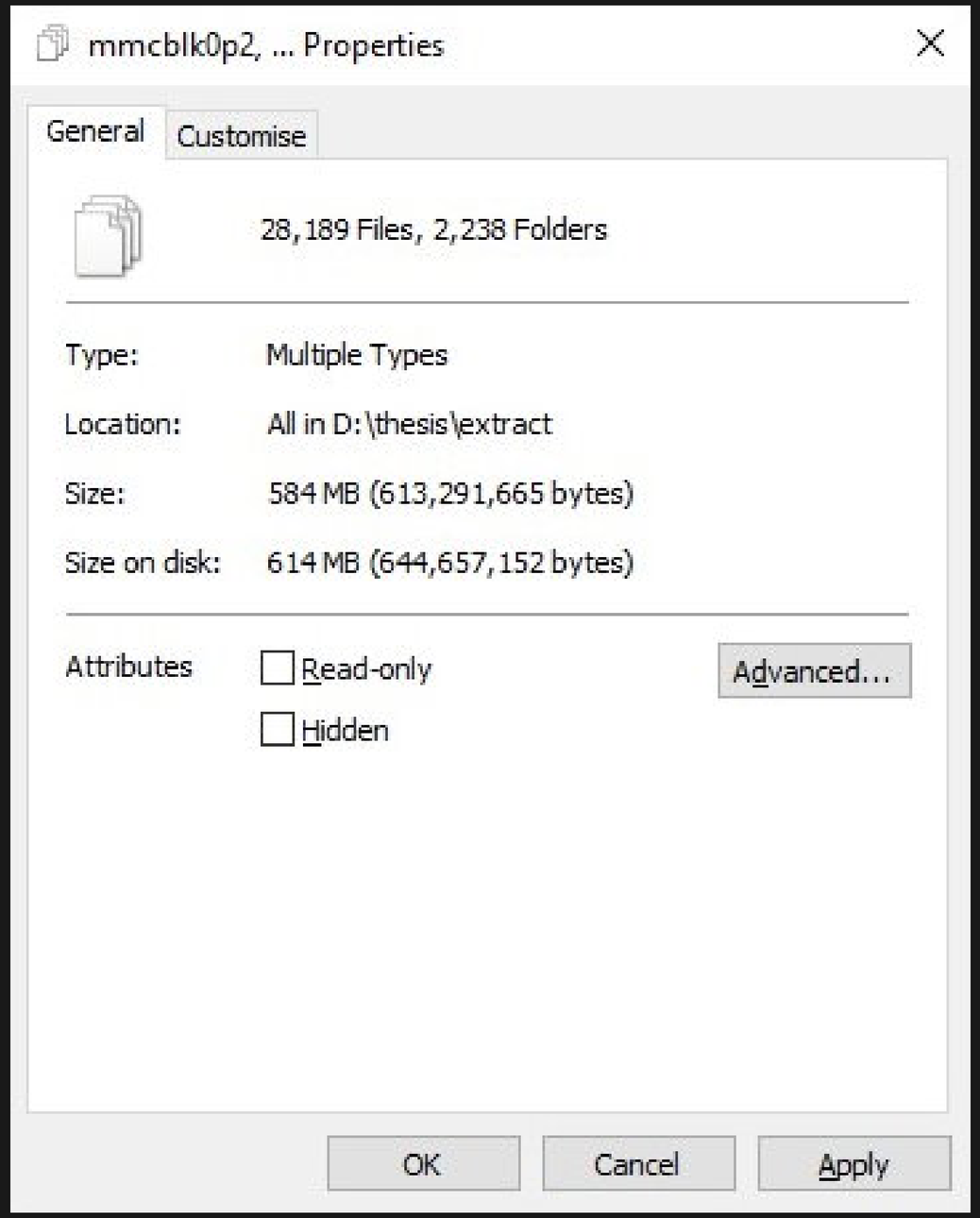
Recovery supposedly resets `system_a`, `system_b`, `UDISK` and `Download`

```
flag a=2,flag b=4,will be recover system
play opt/rockrobo/resources/sounds/en/bl_recovery_bootfailed.wav
Loading file "opt/rockrobo/resources/sounds/en/bl_recovery_bootfailed.wav" from mmc device 2:7
195238 bytes read
sunxi codec request dma 0x5ebb47b4
rr_recovery_pre_check:716:found recovery num 3
Loading file "/boot/zImage" from mmc device 2:7
3882616 bytes read
part recovery valid
recovery from "recovery" to "system_a"
cover init begin
found recovery
set src start=0,src_size=0
found system_a
set dest start=645922816,dest_size=536870912
real_cover:141:total size=536870912,block=1048576

MMC read: dev # 2, block # 253952, count 8192 ... 8192 blocks read: OK

MMC write: dev # 2, block # 1302528, count 8192 ... 8192 blocks write: OK
```

What about the other partitions? If we want to plant malicious software, can put it in `recovery` and `system_a`?



TODO: Recovery partition is modifiable

28,189 files…

Well there's for sure a lot of files to look at…

I did a thing - Commentree

Plain-text annotation / commentary tool

Interesting Files

mmcblk0p1/miio/device.token=utnevRELra5sqef3 mmcblk0p1/miio/device.uid=1738271950 mmcblk0p1/rockrobo/ mmcblk0p11\endpoint.bin - AWS address + key? mmcblk0p7\boot\zImage - bootloader vinda usage

passwords syslogs

```
Look for IPs, emails, host/domains, passwords, keys
Check where DID and UID is used
Dummy data to check if it’s logged
```

What other files were changed?

compare against base ubuntu system?

miio mmcblk0p7\opt\rockrobo rrlog rriot

ADB

adb

/usr/sbin/tcpdump

```
root@rockrobo:/var/log# cat dpkg.log | grep "install "
2016-04-25 09:58:30 install libpcap0.8:armhf <none> 1.5.3-2
2016-04-25 09:58:31 install tcpdump:armhf <none> 4.5.1-2ubuntu1.2
2016-05-03 12:06:01 install pigz:armhf <none> 2.3-2
2016-05-23 09:41:25 install lsof:armhf <none> 4.86+dfsg-1ubuntu2
2016-06-23 15:02:26 install gcc-6-base:armhf <none> 6.1.1-3ubuntu11~14.04.1
2016-06-23 15:06:01 install gcc-5-base:armhf <none> 5.3.0-3ubuntu1~14.04
root@rockrobo:/var/log#
```

mmcblk0p7\usr\sbin\tcpdump

/var/log/apt/history.log

```
Start-Date: 2016-01-25  11:18:05
Commandline: /usr/bin/apt-get install rsync
Install: rsync:armhf (3.1.0-2ubuntu0.2)
End-Date: 2016-01-25  11:18:11

Start-Date: 2016-04-05  12:30:59
Commandline: /usr/bin/apt-get install ccrypt
Install: ccrypt:armhf (1.10-4)
End-Date: 2016-04-05  12:31:01

Start-Date: 2016-04-25  09:58:29
Commandline: /usr/bin/apt-get install tcpdump
Install: tcpdump:armhf (4.5.1-2ubuntu1.2), libpcap0.8:armhf (1.5.3-2, automatic)
End-Date: 2016-04-25  09:58:33
```

Static binaries

```
./htop --sort-key=PID -C
```

Thesis consideration - some thoughts and discussions

How have manufacturers of IoT / smart home devices addressed the increasing concerns of digital privacy and product security?

```
root@rockrobo:/proc# cat misc
 48 android_adb
 49 mali
 50 network_throughput
 51 network_latency
 52 cpu_dma_latency
 53 xt_qtaguid
 54 leds
236 device-mapper
130 watchdog
200 tun
 55 lds_motor
 56 jiffies
 57 uart_lds
 58 uart_mcu
237 loop-control
 59 sw_sync
 60 cuse
229 fuse
 61 sunxi-reg
 62 cachefiles
 63 ion
```

- Can I plant software (y)

- Why is netcat installed but not curl, wget?
- TODO: Check what gets cleared during a format / update

Current Challenges - Equipment

- Electricity is dangerous
- Using personal equipment is not a good idea for a test-bench
- Thank you Gigabyte for having ESD-protected USB ports

Unfinished Work

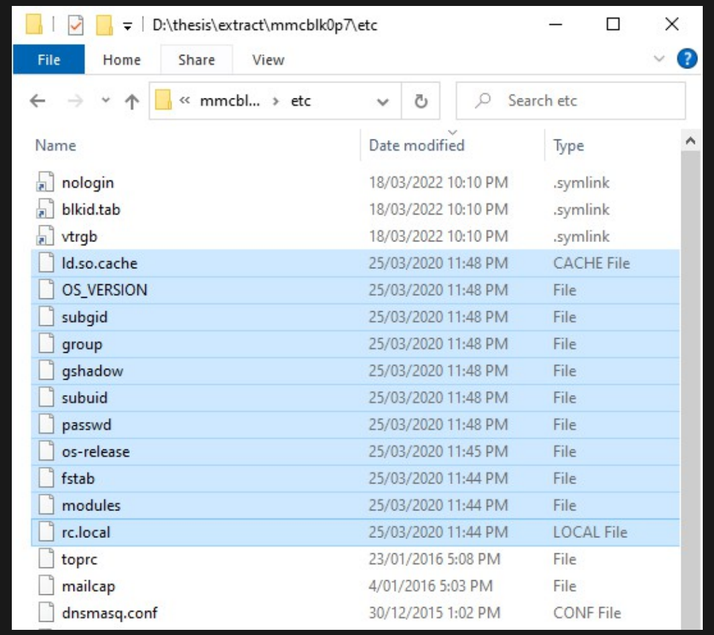
- Still a lot of files to look at
- Need to figure out which files are worthwhile to inspect

Unfinished Work

- Still a lot of files to look at
- Need to figure out which files are worthwhile to inspect

Approach 1 - Filter by date modified

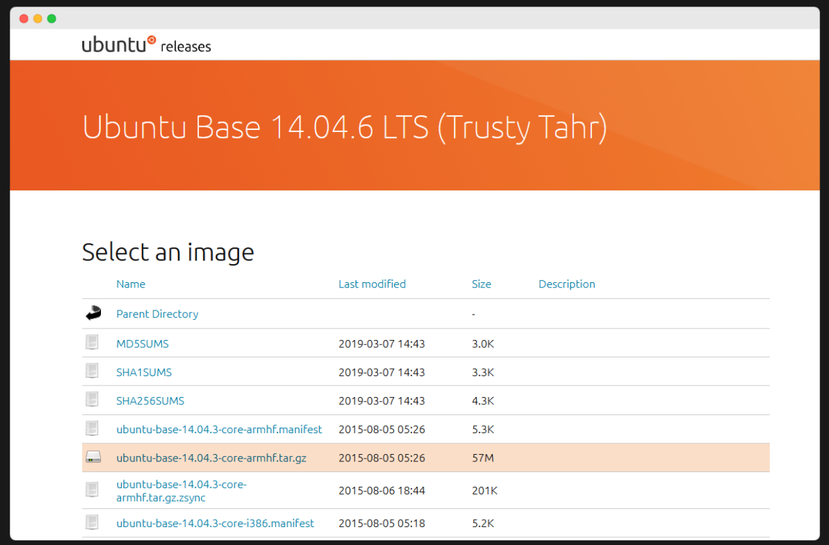
> *Ubuntu 14.04.3 LTS was released back in 2014, any changes would have a later timestamp*



Unfinished Work

- Still a lot of files to look at
- Need to figure out which files are worthwhile to inspect

Approach 2 - File Comparisons



Compare executable files and find differences in binary function

bindiff, binwalk, ssdeep, sdhash

As seen in A Large-Scale Analysis of the Security of Embedded Firmwares - Andrei C, Jonas Z, Aur'elien F, Davide B

Retrospective

- Time management / busy / other work
- Could have done more work

Project Timeline

Thesis A

- Initial research and research environment setup
- Teardown and initial hands-on of Roborock S6

Thesis B - Binary Assessment

- Disassembly and analysis of firmware binaries to identify vulnerabilities
  - inc. ADB binary functionality
- Search for unsecured secrets, logs, configurations

Thesis C - Connectivity Assessment

- Inspection of outbound internet traffic - security, PII, etc
- Inspection of local network traffic
- Inspection of interaction with nearby devices
- Protocol analysis

[Static] Binary assessment

In the mean time

Findings

Project Plan

Revised Project Plan

Next Steps

- Dump the firmware and begin RE / forensics
- Redo (and further investigate) live system analysis
  - i.e. Properly capture *all* network traffic

Any Questions?

Andrew Wong

w: featherbear.cc/UNSW-CSE-Thesis

e: andrew.j.wong@student.unsw.edu.au