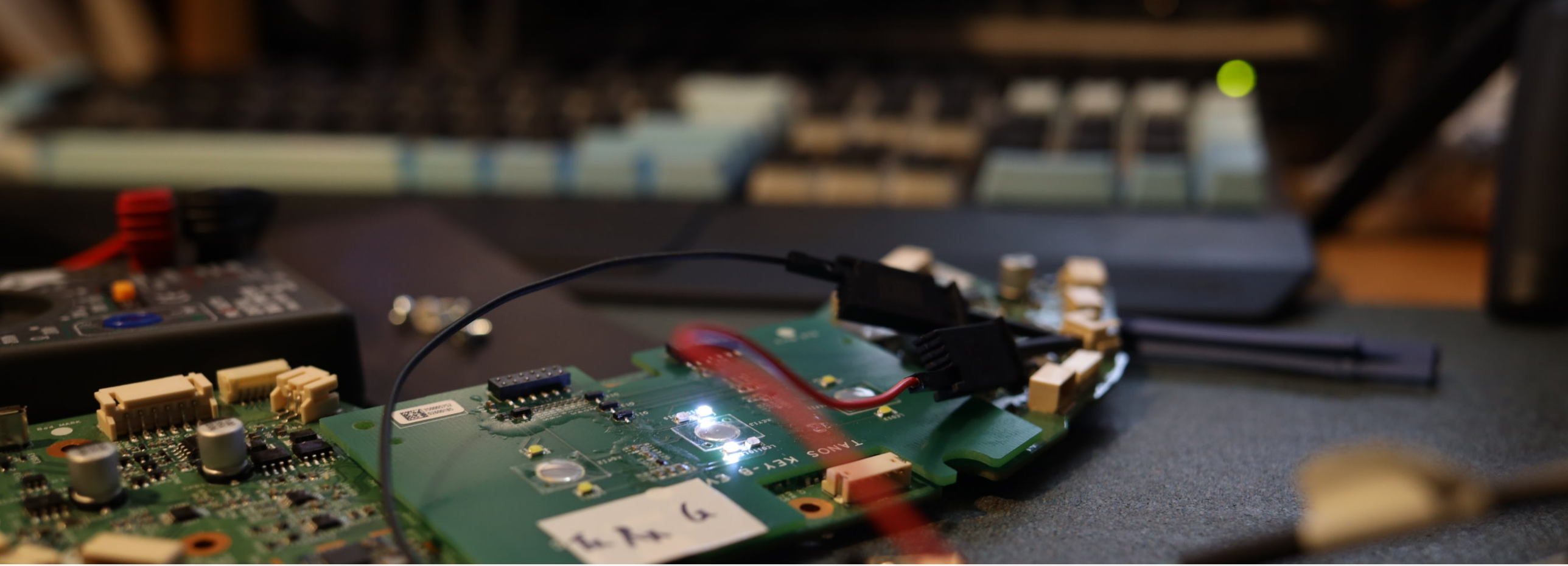


“Smart” Vacuum Cleaners

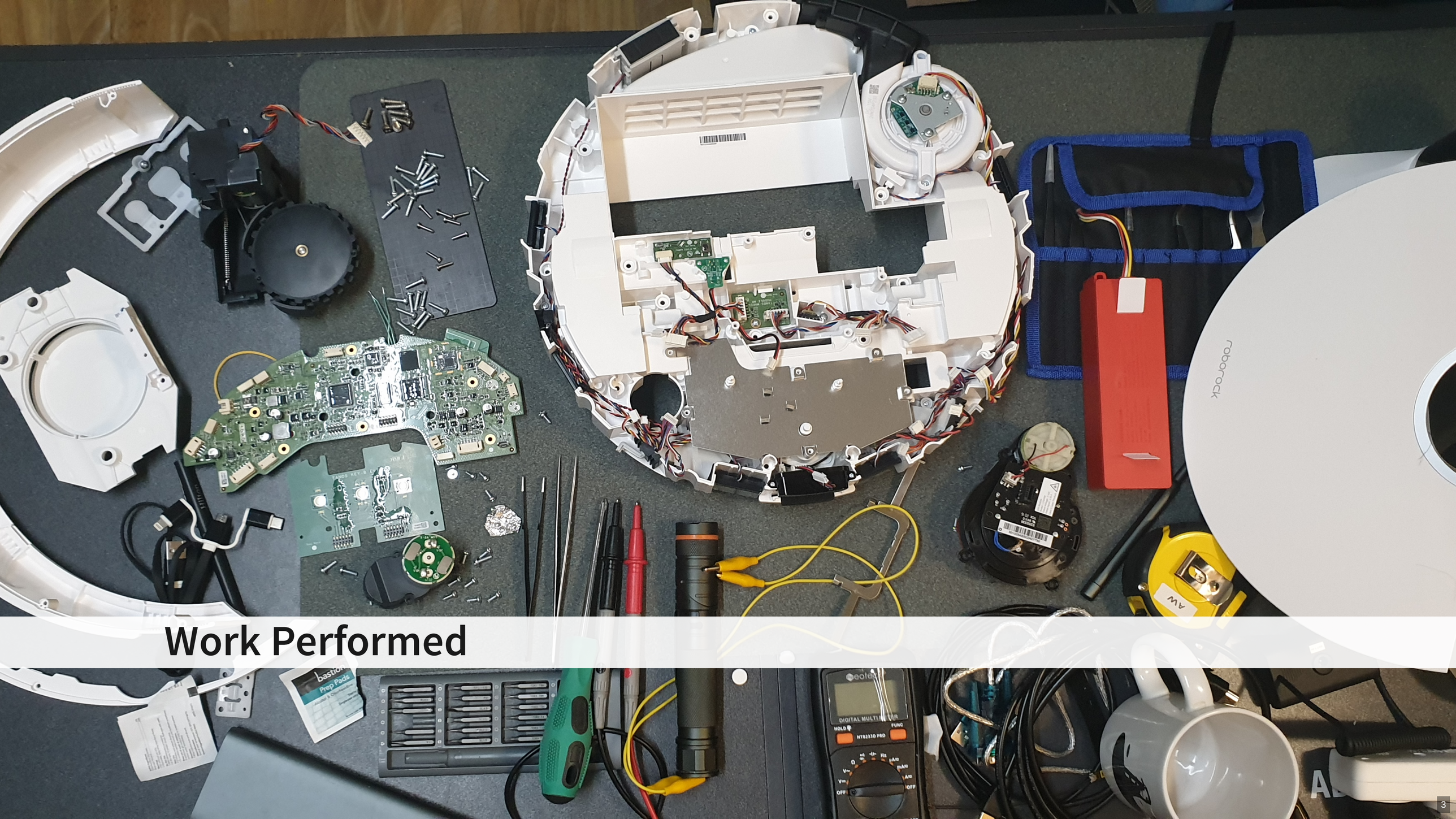
An Audit Into The Security and Integrity of IoT Systems

Andrew Wong | UNSW Sydney

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

```
[ 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
...
```

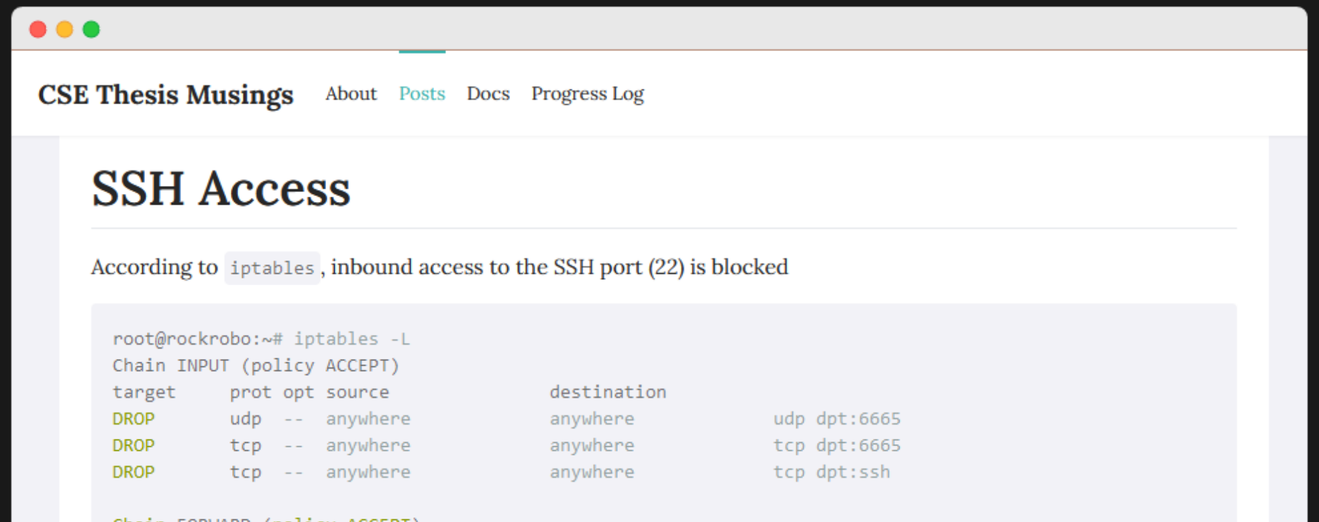
CPU: Allwinner R16 (ARM Cortex-A7)

ACU: STM32F103VCT6 (ARM Cortex-M3)

Roborock Firmware version: 3.5.4_1558

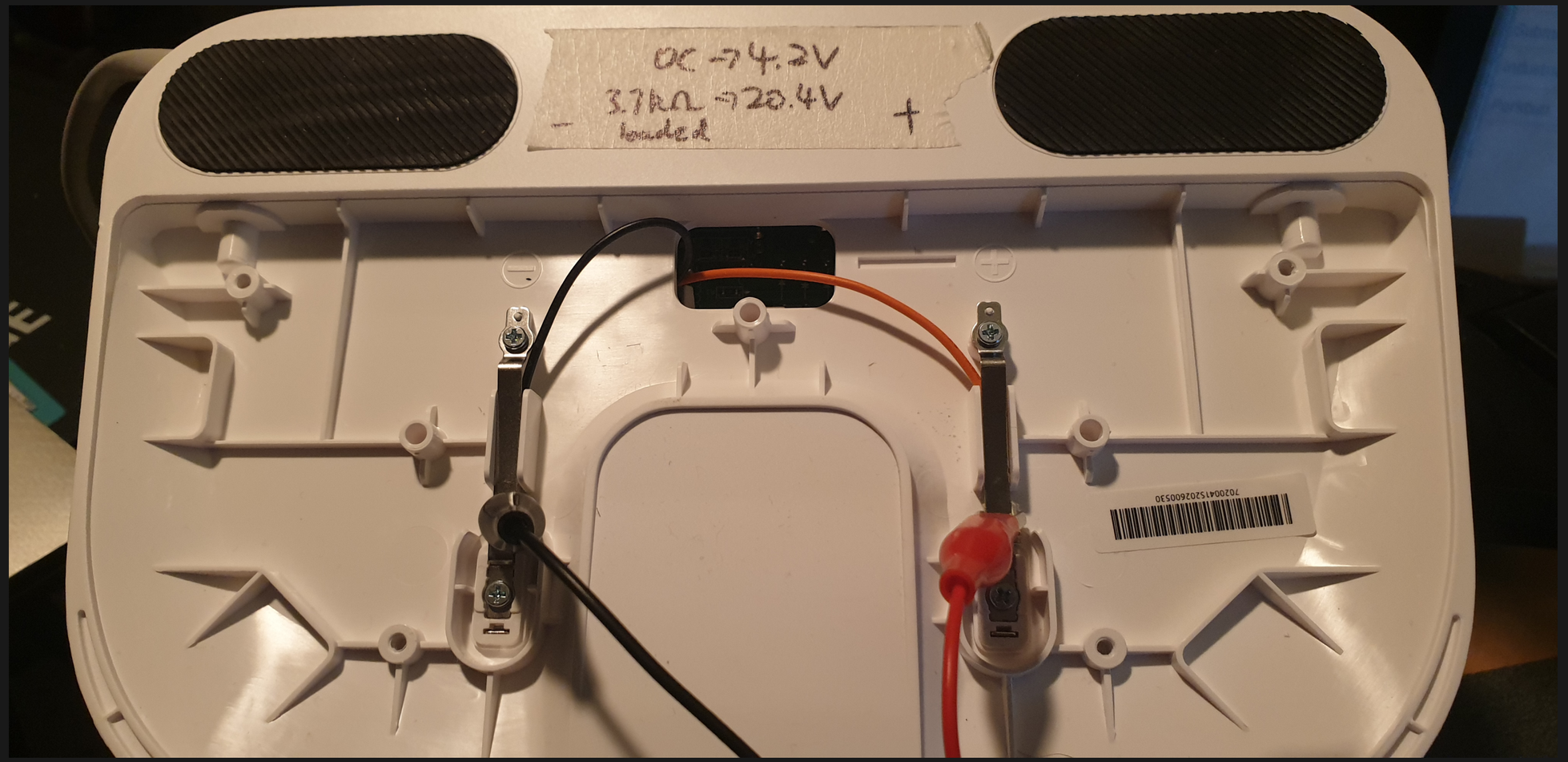
Operating system: Ubuntu 14.04.3 LTS

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

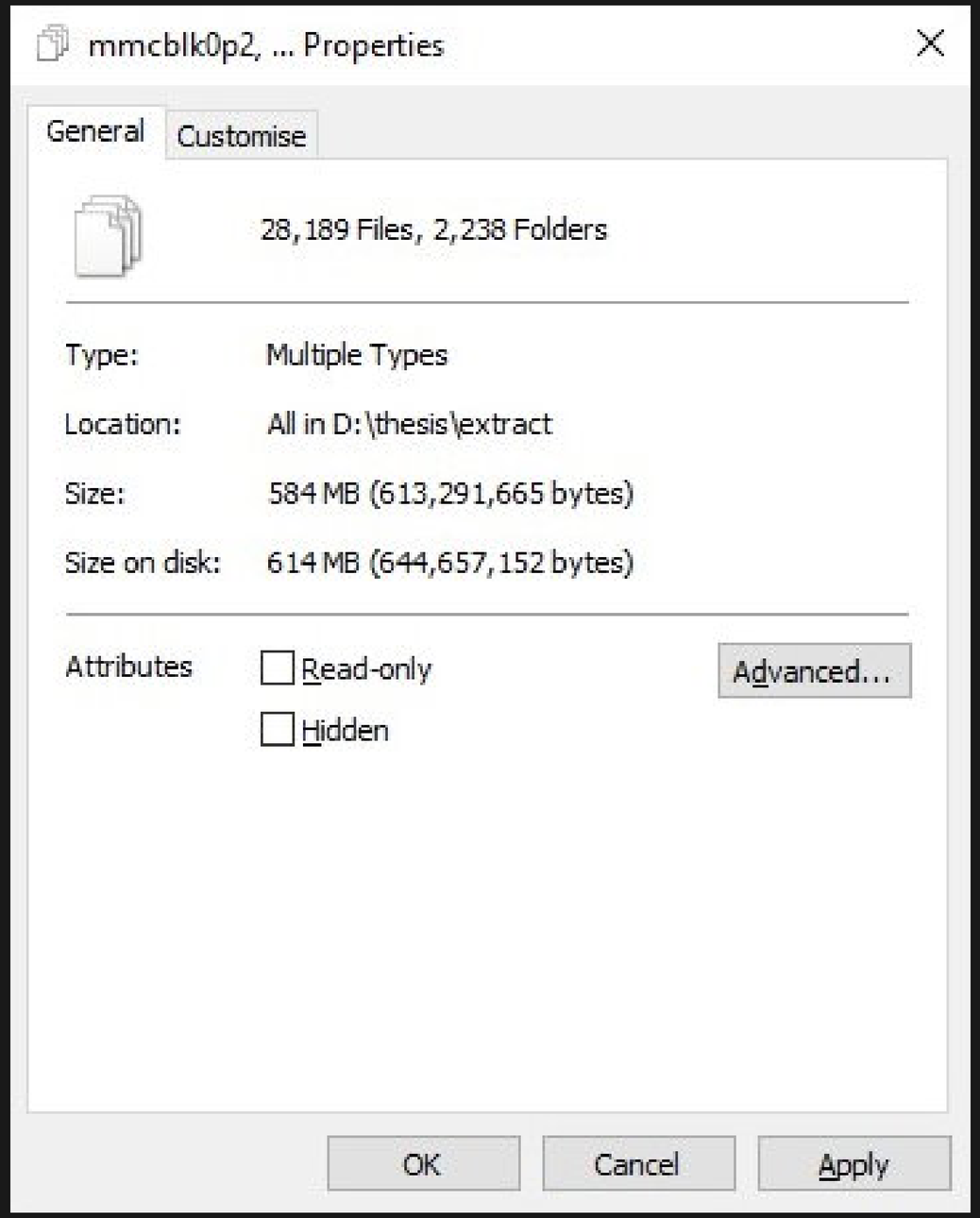
Recovery supposedly resets `system_a`, `system_b`, `UDISK` and `Download`

```
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`?



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

device.token=utnevRELra5sqef3 device.uid=1738271950
mmcblk0p1/rockrobo/

```
mmcblk0p11\endpoint.bin
    AWS address + key?
mmcblk0p6\adb.conf
    adb_lock=1
mmcblk0p7\boot\zImage
mmclbk0p7\etc\init\adbd.conf
vinda usage
mmcblk0p7\opt\rockrobo
adb
mmcblk0p7\usr\sbin\tcpdump
mmcblk0p8\var\log\upstart\adbd.log
    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?

Relate back to the question about security / privacy

- Wifi password in plain text
  - wpa_supplicant –> underlying linux framework How easy is it for someone to attack the system?
- netcat?
- There is an SSH server running (though restricted via iptables)
  - Why?
- Hands-on access a system = game over
  - But should it be?
- Some logs are encrypted locally

Are there any backdoors?

```
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
```

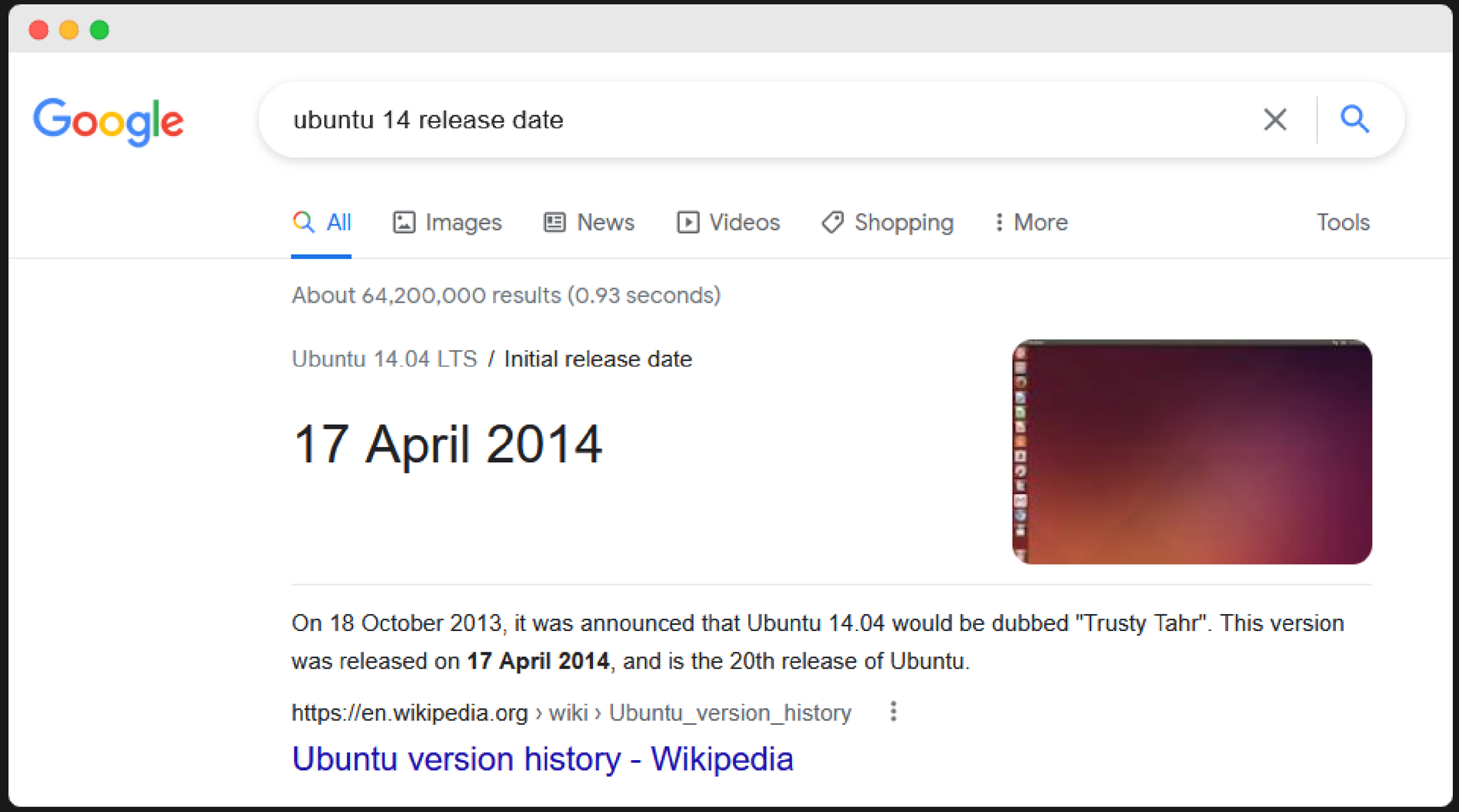
- Can I plant software (y)

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

Current Challenges

Electricity is dangerous. Thank you Gigabyte for having ESD-protected USB ports

Still a lot of files



[Static] Binary assessment

Retrospective of this term

- Time management
- Work
- COVID-19

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