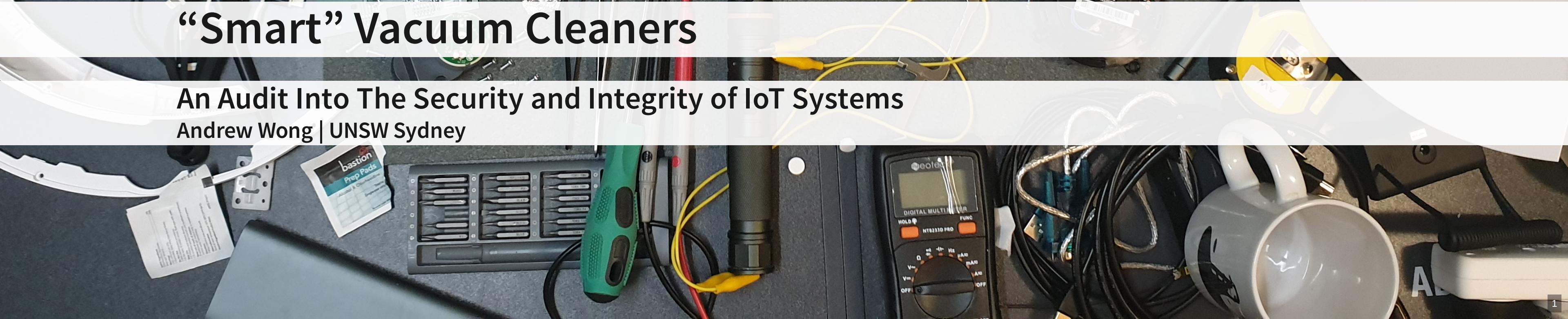


“Smart” Vacuum Cleaners

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?

Proposal

Digital Privacy

Investigate the nature of network data (i.e. content, frequency, destination) from the Roborock S6, and how the data is used.

Product Security

Investigate potential security vulnerabilities of the Roborock S6, and assess the effectiveness of current security fortifications.

Work

Current Findings

Relate back to the question about security / privacy.

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
```

<https://en.wikipedia.org/wiki/Linaro>

ROBOROCK_VERSION=3.5.4_1558

Ubuntu 14.04.3 LTS

Commentree

Documentation tool

The screenshot shows the Commentree application interface. On the left is a file browser window titled "Files" showing a directory structure with various files. The main area is a code editor displaying a configuration file named "rrwatchdoge.conf". The code is annotated with comments in the right margin:

```
File: D:\thesis\extract\mmcblk0p7\opt\rockrobo\watchdog\rrwatchdoge.conf
Comments
40 # Directory for saving downloaded update package and related files
41 env UPDPKG_DIR=/mnt/data/.temp
42
43 # Full path for update info file
44 env UPDPKG_INFO_PATH=/mnt/data/.temp
45 env UPDPKG_INFO_NAME=Update.pkg.inf
46
47 # HWDOG reboot option
48 # 1 = REBOOT_SYSTEM      2 = ONLY_INTERRUPT
49 env HWDOG_OPTION=1
50
51 # crash detect, if robot did not crash after "CRASH_IGNORE_MIN" minutes, then clear the o
52 env CRASH_IGNORE_MIN=600
53
54 pre-start script
55 #   key_service
56 #     ip_server 2>/dev/null &
57     mkdir -p $RR_UDATA/rockrobo/rrlog
58     mkdir -p $RR_UDATA/rockrobo/devtest
59     mkdir -p $RR_UDATA/rockrobo/noupload
60     mkdir -p $RR_UDATA/rockrobo/map
61     mkdir -p $RR_UDATA/wlan
62     mkdir -p $RR_UDATA/mio
63     ldconfig
64     iptables -I INPUT -j DROP -p tcp --dport 22
65     iptables -I INPUT -j DROP -p tcp --dport 6665
66     iptables -I INPUT -j DROP -p udp --dport 6665
67     $RR_ROOT/scripts/provision.sh
68     $RR_ROOT/scripts/pipes.sh
69     # $RR_ROOT/scripts/cpu.sh ondemand
70     ip6tables -P INPUT DROP
71     ip6tables -P FORWARD DROP
72     ip6tables -P OUTPUT DROP
73 end script
74
75 script
76     export RR_ROOT
77     export RR_UDATA
78     export RR_DEFAULT
79     export RR_RESERVE
80     export WIFI_START_PATH
81     export WIFI_START_NAME
82     export WIFI_CONF_PATH
83     export WIFI_CONF_NAME
84     export WIFI_ENABLE_PATH
85     export WIFI_ENABLE_NAME
86     export MIO_RECV_LINE
87     export MIO_SEND_LINE
```

Annotations in the margin:

- Line 41: Save dir
- Line 64: This line creates an IP table rule to drop SSH

Persistence!

Copying the password is annoying (don't want to change it either)

```
ssh-copy-id -i ~/.ssh/id_rsa root@10.10.10.8
```

```
-----fastboot partitions-----
-total partitions:9-
-name-      -start-      -size-
boot-res    : 1000000    800000
env         : 1800000   1000000
app (ro)    : 2800000   4000000
recovery    : 6800000  20000000
system_a    : 26800000 20000000
system_b    : 46800000 20000000
Download    : 66800000 21000000
reserve     : 87800000 1000000
UDISK       : 88800000 0
-----
```

```
root@rockrobo:/home# fdisk -l
```

```
Disk /dev/mmcblk0: 3959 MB, 3959422976 bytes
1 heads, 16 sectors/track, 483328 cylinders, total 7733248 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

Device	Boot	Start	End	Blocks	Id	System
/dev/mmcblk0p1	*	4513792	7782399	1634304	b	W95 FAT32
/dev/mmcblk0p2		73728	90111	8192	6	FAT16
/dev/mmcblk0p3		1	4423680	2211840	5	Extended
/dev/mmcblk0p5		90112	122879	16384	83	Linux
/dev/mmcblk0p6		122880	253951	65536	83	Linux
/dev/mmcblk0p7		253952	1302527	524288	83	Linux
/dev/mmcblk0p8		1302528	2351103	524288	83	Linux
/dev/mmcblk0p9		2351104	3399679	524288	83	Linux
/dev/mmcblk0p10		3399680	4481023	540672	83	Linux
/dev/mmcblk0p11		4481024	4513791	16384	83	Linux

```
root@rockrobo:/# cat /etc/fstab
# UNCONFIGURED FSTAB FOR BASE SYSTEM
tmpfs /tmp tmpfs size=30m 0 0
tmpfs /run/shm tmpfs size=100m 0 0
/dev/mmcblk0p1      /mnt/data/          ext4 defaults 0 0
/dev/mmcblk0p6      /mnt/default/       ext4 ro 0 0
/dev/mmcblk0p10     /mnt/updbuf/        ext4 defaults 0 0
/dev/mmcblk0p11     /mnt/reserve/       ext4 defaults 0 0
```

app (/mnt/default) is ro system_a ->

Behaviour

The battery ()

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

[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