NORWICH UNIVERSITY™

Welcome Pwn: Almond Smart Home Hub Forensics

Akshay Awasthi[1], Huw Read[1,2],
Konstantinos Xynos[4,2], Iain Sutherland[2,3]

[1]Norwich University, Northfield, Vermont, USA
[2]Noroff University College, 4068 Kristiansand S, Vest-Agder, Norway
[3]Security Research Institute, Edith Cowan University, Perth, Australia
[4]MycenX Consultancy, Germany

noroff UNIVERSITY COLLEGE

NORWICH UNIVERSITY

$ whoami

Akshay Awasthi (Student)

Qualifications:

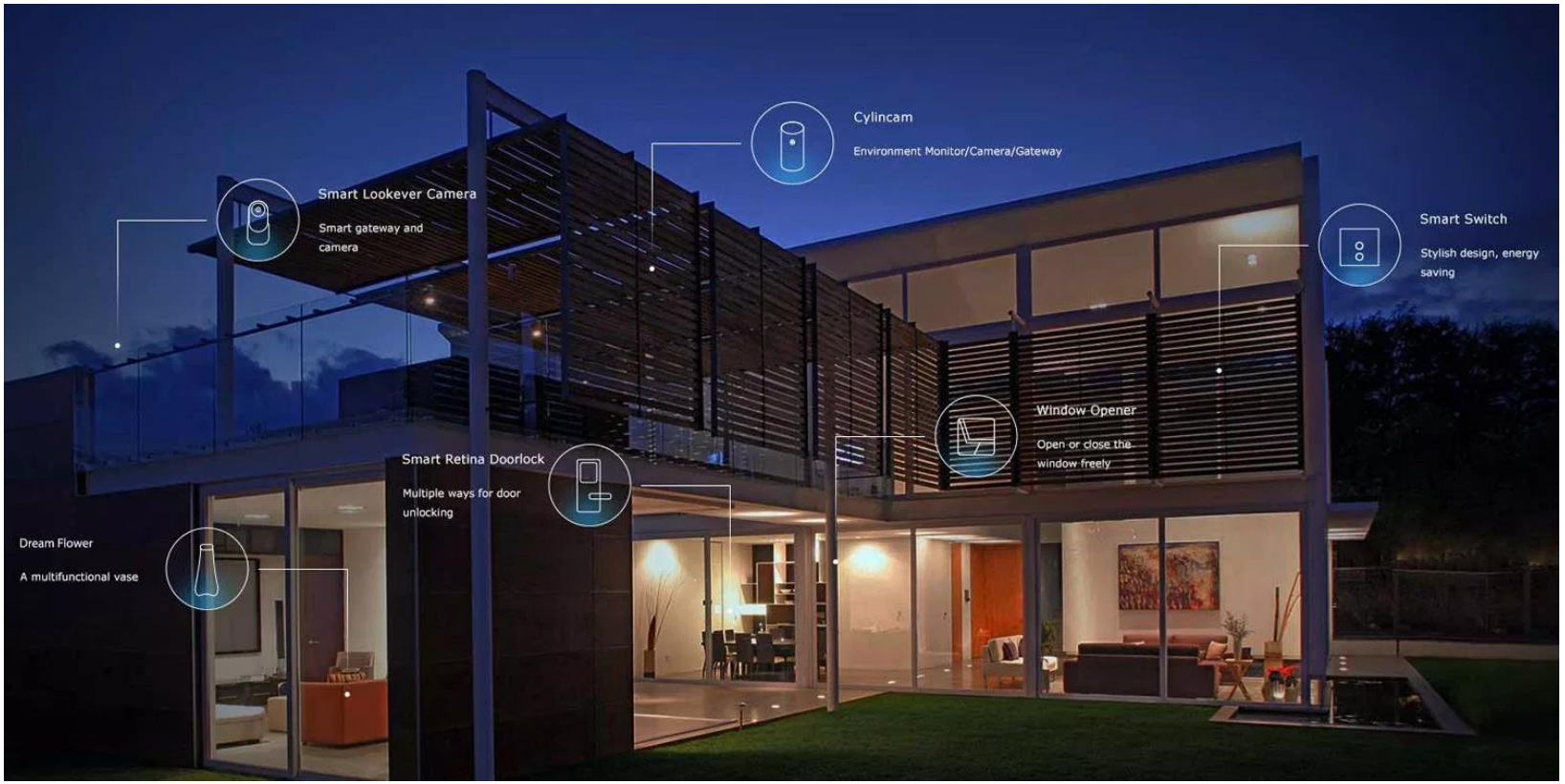
- Bachelor of Computer Application (BIT Mesra, 2016)
- B.S. Computer Security (Norwich, 2017)

Work:

- Norwich University, VT, USA
  - Research Lead, 2016-2017
  - PWC Cyber Specialist, 2016-2017

- The Estēe Lauder Companies, NY, USA
  - Senior Analyst, GIRS Investigations, 2018 - Present

Are ”smart homes” really that smart?



https://9to5mac.com/2018/07/09/smart-home-domestic-abuse-help/

noroff UNIVERSITY COLLEGE

NORWICH UNIVERSITY

Why look at the Almond+ Smart Home Hub?

Released 2015

- Promoted as an “ambitious product”
- One box to do it all.

Generally designed to control all the smart home appliances from one hub

- Only on-box interactive smart home hub.
- Supports both “zigbee” and ”zwave”

No-other smart home hub has a touch screen!

Related Work

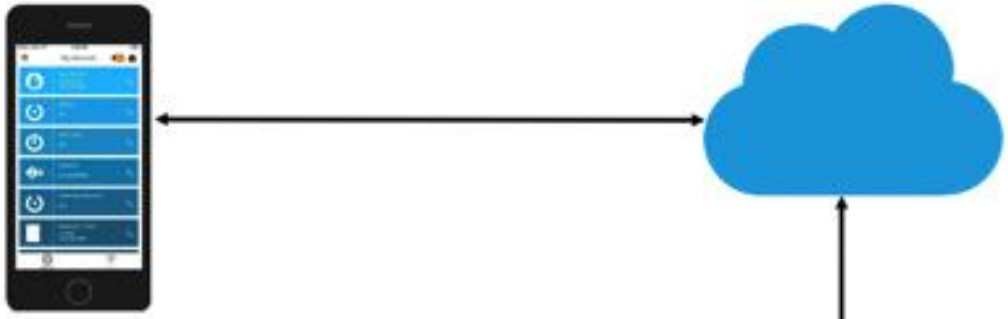
- Amazon Alexa (LCDI, 2016)
  - Extracting data via third party devices
- Apple Homekit (Cook, 2016)
  - Apple's strong encryption on smart home hubs.
- Google OnHub and Google Home (Google, 2017)
  - Google's contender for smart home hubs.

Forensic Value of the Almond+

Considerable given the device:

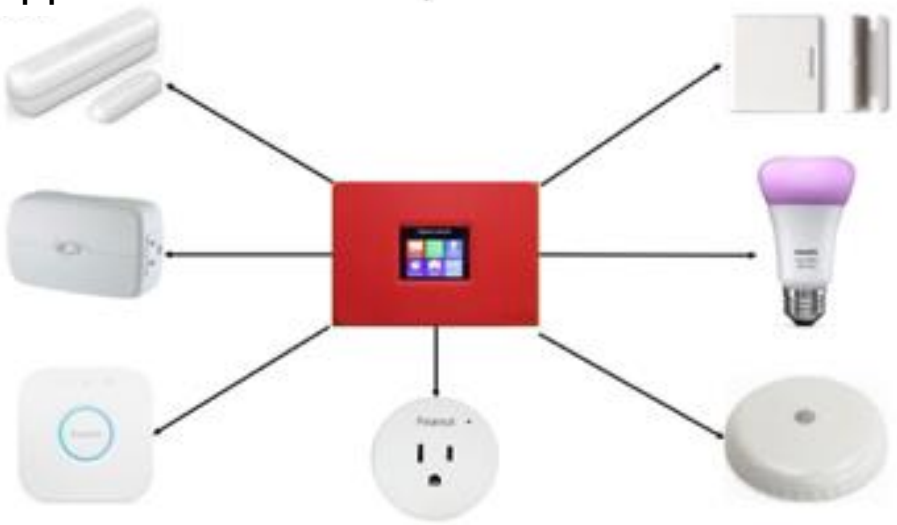
- Companion app (iOS/android)
- Web interface (local and cloud)
- On-device interface
- Linux OS
- wifi router
- wifi extender
- Smart Hub
- Third party device integration
- USB 3.0
- SSH capability

Almond+ Ecosystem



Almond+ Cloud

Almond iPhone / Android App



Connected Sensors

Challenges to Acquisition

- Evidence resides in volatile file system
  - Cannot be rebooted / reset
  - Evidence stored in tmpfs
- Cannot interact with the on-board touchscreen
  - Will create “log files” which will tamper the existing evidence
- Jailbreak / Circumventing Security
  - Acquire a logical copy of data
  - No effective method yet (at time of writing)

Considering forensic acquisition…

Data obtained at one of three levels:

- Companion App
- Web Interface
- File System

Increasing Preference

Observations

- Evidence is lost when the device is restarted, unplugged or reset.
- Interacting with touch screen interface modifies the evidence logs.
- Third party smart hubs (e.g. Amazon Alexa) if connected can also provide significant logs.
- USB drive can be used to generate an evidence dump
- “dd” command can be used via ssh to retrieve a forensically sound image.
- Cloud interface and companion apps maintain a significant log of the connected device activity.
- Can never delete the cloud account.

File System

```
BusyBox v1.22.1 (2015-03-11 10:48:25 IST) built-in shell (ash)
Enter 'help' for a list of built-in commands.


 _____  _      __  __  _____  __   _  ____      __
|  ___| | |    |  \/  | |  _ | |  \ | | |  \    |__| |__
| |__| | | |    |      | | |_| | |   \| | | |\ \  |  |  |
|  __  | | |__  | |\/| | | |_| | | |\   | | |/ /  |__|  |__
|_|  |_| |____| |_|  |_| |_____| |_| \__| |____/     |__|

S E C U R I F I  Home Automation
root@AlmondPlus:~# df -h
Filesystem                Size      Used Available Use% Mounted on
rootfs                   30.0M     30.0M         0 100% /
/dev/root                30.0M     30.0M         0 100% /rom
tmpfs                   211.6M      2.9M    208.7M   1% /tmp
tmpfs                   512.0K         0    512.0K   0% /dev
/dev/mtdblock7           16.0M    748.0K     15.3M   5% /overlay
mini_fo:/overlay         30.0M     30.0M         0 100% /
/dev/mtdblock11           5.0M    432.0K      4.6M   8% /hadata
mini_fo:/hadata          30.0M     30.0M         0 100% /data
root@AlmondPlus:~#
```

Forensic Extraction – Almond+

1. Investigate the Almond+ first.
2. Do not touch the screen.
3. Connect to Wi-Fi (if password available) or LAN on Almond+ from forensic workstation.
4. Connect via SSH.
5. Create a backup of the device.
6. Analyse log files (next slide) from Almond+.

Artefacts - Significant locations

Source	Location	Significance
Securifi Almond+	/tmp/connected_home.log	Entries created when smart devices are used on Almond+
Securifi Almond+	/tmp/association.log	Identified when smart device is added to hub
Securifi Almond+	/tmp/CloudDaemon.log	Detailed log of data sent/received from Cloud
Securifi Almond+	/tmp/autoip.json	Almond + geographical information and weather data
iPhone App	<root>/Documents/tool-kit_devicelogs.db	Record of all network devices (dis)associating with Almond+
iPhone App	<root>/Documents/tool-kit_notifications.db	Record of all smart devices which have alerts explicitly set
iPhone App	<root>/Library/Caches/Sna-pshots/ com.securifi.al-mond/*@2x.png	Screenshot of most recent user-interaction in app
Android App	/data/data/com.securi-fi.almondplus/ databases/not-ifications.db	Record of smart devices which have alerts explicitly set and network devices (dis)associating with Almond+
Cloud/Web	connect.securifi.com	Current Wi-Fi settings, list of all networked devices (highlights connected), firmware version

Forensic Extraction – Companion App

1. Ensure device data is copied using standard operating procedures
2. Assess ability of forensic imaging tools to extract data.
3. If device is iOS-based and jailbreaking is an option, evaluate impact of jailbreak to be able to defend actions in a court of law
4. Install Filza or iFile from the Cydia App Store onto device, manually extract data described in section data extraction.
5. Analyse files of forensic importance (previous slide).
6. If jailbreaking (iOS) or rooting (Android) are not an option, start video recorder and begin capture.
7. Perform hand-scroll of Almond+ companion app paying particular attention to any Alerts - once viewed their status will change to "seen".

   (a) Bell icon - provides timeline of alerts (for those explicitly setup by user)

   (b) Devices icon-"ViewHistory" provides presence-based (i.e. within range) artefacts (note - only useful with Cloud connectivity enabled)

Forensic Extraction - Cloud

If the Cloud password is known:

1. Login at https://connect.securifi.com
2. Obtain router and device sensor via print screen and/or saving web pages.

Sample – Log of state changes

devicename	devicetype	value_index	value_indexname	indexvalue	viewed	notiCat
Filter	Filter	Filter	Filter	Filter	...	...
Peanut Plug	50	1	SWITCH BINARY	false	1	0
Peanut Plug	50	1	SWITCH BINARY	true	1	0
motion sensor	60	6	HUMIDITY	44	1	0
motion sensor	60	6	HUMIDITY	45	1	0
motion sensor	60	6	HUMIDITY	46	1	0
hr nyce	12	1	STATE	true	1	0
hr nyce	12	1	STATE	false	1	0
motion sensor	60	1	*NULL*	false	1	0
motion sensor	60	1	*NULL*	true	1	0
hr nyce	12	1	STATE	false	1	0

Summary

- Forensic extraction methodology provides investigators with a useful guide for investigating an Almond+ smart home hub.
- Can be used to track an individual's daily activity.
- Weak security posture enables a future possibility of breach of a ”smart home”.

The Future…

- Investigate latest model, Almond 3S, Almond 3
  - Experiments conducted on original Almond+ with periodic firmware updates
  - Reassess methodology
- GUI visualization tool for replaying actions in a simulated environment

Questions ?