Welcome Pwn: Almond Smart Home Hub Forensics

Akshay Awasthi¹, Huw Read¹,², Konstantinos Xynos⁴,², Iain Sutherland²,³

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

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 iPhone / Android App

Connected Sensors

Almond+ Cloud
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.

```
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

<table>
<thead>
<tr>
<th>Source</th>
<th>Location</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securifi Almond+</td>
<td>/tmp/connected_home.log</td>
<td>Entries created when smart devices are used on Almond+</td>
</tr>
<tr>
<td>Securifi Almond+</td>
<td>/tmp/association.log</td>
<td>Identified when smart device is added to hub</td>
</tr>
<tr>
<td>Securifi Almond+</td>
<td>/tmp/CloudDaemon.log</td>
<td>Detailed log of data sent/received from Cloud Almond + geographical information and weather data</td>
</tr>
<tr>
<td>Securifi Almond+</td>
<td>/tmp/autoip.json</td>
<td>Record of all network devices (dis)associating with Almond +</td>
</tr>
<tr>
<td>iPhone App</td>
<td>&lt;root&gt;/Documents/tool-kit_device_logs.db</td>
<td>Record of all smart devices which have alerts explicitly set</td>
</tr>
<tr>
<td>iPhone App</td>
<td>&lt;root&gt;/Library/Caches/Snap-shots/</td>
<td>Screenshot of most recent user-interaction in app</td>
</tr>
<tr>
<td>iPhone App</td>
<td>com.securifi.almond/+*@2x.png</td>
<td></td>
</tr>
<tr>
<td>Android App</td>
<td>/data/data/com.securifi.almondplus/</td>
<td>Record of smart devices which have alerts explicitly set and network devices (dis)associating with Almond +</td>
</tr>
<tr>
<td></td>
<td>databases/notifications.db</td>
<td></td>
</tr>
<tr>
<td>Cloud/Web</td>
<td>connect.securifi.com</td>
<td>Current Wi-Fi settings, list of all networked devices (highlights connected), firmware version</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>devicename</th>
<th>devicetype</th>
<th>value_index</th>
<th>value_indexname</th>
<th>indexvalue</th>
<th>viewed</th>
<th>notiCat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peanut Plug</td>
<td>Filter</td>
<td>1</td>
<td>SWITCH BINARY</td>
<td>false</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Peanut Plug</td>
<td>Filter</td>
<td>1</td>
<td>SWITCH BINARY</td>
<td>true</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>motion sensor</td>
<td>Filter</td>
<td>6</td>
<td>HUMIDITY</td>
<td>44</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>motion sensor</td>
<td>Filter</td>
<td>6</td>
<td>HUMIDITY</td>
<td>45</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>motion sensor</td>
<td>Filter</td>
<td>6</td>
<td>HUMIDITY</td>
<td>46</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>hr nyce</td>
<td>Filter</td>
<td>1</td>
<td>STATE</td>
<td>true</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>hr nyce</td>
<td>Filter</td>
<td>1</td>
<td>STATE</td>
<td>false</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>motion sensor</td>
<td>Filter</td>
<td>1</td>
<td>NULL</td>
<td>false</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>motion sensor</td>
<td>Filter</td>
<td>1</td>
<td>NULL</td>
<td>true</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>hr nyce</td>
<td>Filter</td>
<td>1</td>
<td>STATE</td>
<td>false</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
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 ?