IoT Forensics Challenges and Opportunities for Digital Traces

Francesco Servida, Eoghan Casey
Outline

• Smart Devices
• Forensic Interest
• Methodology
• Results
• Discussion
Smart Devices

Security systems
- cameras
- door locks
- motion sensors
- smoke & CO detectors

Smart assistants
- audio
- video

Smart hubs

Smart:
- microwave, stove, grill, crock pot
- refrigerator
- grow system
- coffee maker
- television
- thermostat
- light bulbs
- plugs
- toys
- ...

Unil
Université de Lausanne
École des sciences criminelles
Forensic Interest

• Myriad of sensors
• Highly connected
• Low security

• Direct Targets
  – Sensitive Data
• Secondary targets
  – Alarm Systems
  – «Trojan Horses»
  – Botnets (eg. Mirai)
• Witnesses
IoT forensics approach

Enterprise IoT
- Proactive collection

Home IoT
- What to do on an “unprepared” crime scene?
Methodology
Methodology

- Literature review
- Existing Vulnerability Reports
- Home automation communities
Methodology

- Preliminary Analysis
- Testbed Setup
- Network Analysis
- Smartphone Application Artifacts
- Vulnerability Research
- Physical Analysis

Diagram:
- Samsung Galaxy Edge S6
- WAN (UNIL) - 130.223.0.0/16
- LAN - 10.20.30.0/24
- Raspberry Pi 10.20.30.1
- iSmartAlarm 10.20.30.18
- Nest Protect 10.20.30.19
- Amazon Echo (Gen1) 10.20.30.23
- WinkHub 10.20.30.22
- Netgear Arlo 10.20.30.17
- Nest Camera 10.20.30.13
- Qbee Camera 10.20.30.15
Methodology

Who?  How?  What?

Preliminary Analysis
Testbed Setup
Network Analysis
Smartphone Application Artifacts
Vulnerability Research
Physical Analysis

TCPDUMP & Libpcap
Wireshark

Nmap
Elasticsearch
Logstash
Kibana

© UNIL | Université de Lausanne
École des sciences criminelles
Methodology

What traces on a smartphone?

- Traditional Tools -> No parsers
- Manual investigation and correlation
- Plugin development
Methodology

- Builds on Network Analysis
  - Listening ports, Traffic Type, Traffic Content

- MITM
  - mitmproxy, SSLsplit

- Firmware Analysis
  - Binwalk, strings, hexdump…
Methodology

- Serial Connection
- Root Access
- (JTAG)
- (Chip Off)
- Physical Images
- NVRAM Settings
- Filesystem Images
Network Analysis

- Mostly TLS
- Only a minority is local traffic.
Network Analysis

- iSmartAlarm
  - «Encrypted» traffic with Android app \(^1\)
  - Unauthenticated diagnostic logs access (CVE-2018-16224)

- QBee
  - Cleartext traffic with Android app (CVE-2018-16225)
  - (UPnP port forwarding)

(1) [https://dojo.bullguard.com/dojo-by-bullguard/blog/burglar-hacker-when-a-physical-security-is-compromised-by-iot-vulnerabilities/]
Physical Analysis

- Memory Images
  - Arlo, iSmartAlarm Cube One

- Filesystem Images
  - Wink, Arlo (Partially)

- NVRAM Settings

- Settings & Events depending on device
# Smartphone Application Artifacts

- **Android Phone (Samsung Galaxy Edge S6)**

<table>
<thead>
<tr>
<th>iSmartAlarm</th>
<th>Arlo</th>
<th>Nest</th>
<th>QBee</th>
<th>Wink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Credentials</td>
<td>Cloud Credentials (token)</td>
<td>User Informations Dispositifs Liés Events Video Extracts</td>
<td>Cloud Credentials</td>
<td>User Info Linked Devices Events (Long term storage)</td>
</tr>
<tr>
<td>Events</td>
<td>Linked devices Thumbnails</td>
<td>Dispositifs Liés Events</td>
<td>video extracts</td>
<td>Dispositifs Liés Events (Long term storage)</td>
</tr>
<tr>
<td>UPnP discovered devices</td>
<td>MQTT Topic Infos</td>
<td>Dispositifs Liés Events</td>
<td>video extracts</td>
<td>Dispositifs Liés Events (Long term storage)</td>
</tr>
</tbody>
</table>

![Image of iSmartAlarmData.xml file]

![Image of a source file with XML code]

**UNIL | Université de Lausanne**
**École des sciences criminelles**
# Smartphone Application Artifacts

## Investigation

<table>
<thead>
<tr>
<th>Source File</th>
<th>Date Source</th>
<th>Tags</th>
<th>Event Type</th>
<th>Event Timestamp</th>
<th>Event Type</th>
<th>Device</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartAlarm.DBF</td>
<td>0x00, 0x00</td>
<td>Contact Sensor</td>
<td>Sensor Info</td>
<td>0x00</td>
<td>Contact Sensor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## App Decompilation

| Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 145    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 146    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 147    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 148    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 149    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 150    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 151    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
| 152    | 0x2110 | 0x00   | 0x00   | 1       | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   | 0x00   |
Cloud

Increased persistence

Access
- Reuse of credentials on smartphone
- Request to Service Provider

Arlo
- Recorded videos

DFRWS Challenge submissions
- Wink Hub - Devices & Events, iSmartAlarm - Members, Nest - Devices, Events & Clips
Freezing the IoT crime scene?

Live Data (Transmitted)

- Authentication Credentials (e.g. CVE-2018-16225)
- Current Events

Stored Data

- Not always persistent
- Sometimes accessible live (w/ previous knowledge of the device)
  - E.g. CVE-2018-16224

First responder activities generate IoT traces at scene

- Risk of data loss!
Discussion

Survey
Preservation
Examination
Documentation
Analysis
Integration
Evaluation

Which Traces? Where?

Proposed Methodology

Preliminary Analysis
Testbed Setup
Network Analysis
Smartphone Application Artifacts
Vulnerability Research
Physical Analysis

Developed Knowledge & Tools
Discussion

New devices

- Unknown meaning of the data, prone to error and misinterpretation

Controlled Environment Testing

- Share results (+ Peer Review)
- Better and more accepted knowledge of the meaning of the data
- Increased admissibility
Issues

• Smartphone artifacts not produced in background

• Physical:
  – Extraction methods
  – Volatility of traces

• Variety of protocols
Future Research

Study common smarthome IoT devices

Analyse IoT RF activities (e.g., Zigbee, Z-Wave)

Chip-off analysis
https://github.com/fservida/msc_autopsy_plugins

https://github.com/fservida/msc_thesis

https://francescoservida.ch

francesco.servida@unil.ch

Thank You.