Stepping out of the MUD: contextual threat information for IoT devices with manufacturer-provided behavior profiles

Luca Morgese Zangrandi  TNO
Thijs van Ede  University of Twente
Tim Booij  TNO
Savio Sciancalepore  Technical University of Eindhoven
Luca Allodi  Technical University of Eindhoven
Andrea Continella  University of Twente
Motivation
Motivation

• Attackers actively compromise IoT devices
Motivation

• Attackers actively compromise IoT devices
• >50% devices deployed in home-like environments
Motivation

- Attackers actively compromise IoT devices
- >50% devices deployed in home-like environments
- No honeypots, monitors, intelligence
Motivation

• Attackers actively compromise IoT devices
• >50% devices deployed in home-like environments
• No honeypots, monitors, intelligence

→ Hard to gather threat information
Goal

MUDscope

→ Monitor for IoT threat activities at home-like environments
MUD profiles

- Manufacturer-provided allow-lists
- Manufacturer Usage Description (IETF RFC 8520)
MUD profiles

- Manufacturer-provided allow-lists
- Manufacturer Usage Description (IETF RFC 8520)
Key idea

ACSAC 22, Austin, Texas, USA
Key idea

MUD-rejected traffic

Cross-deployment MRT evolution correlation

- Home IoT lightbulb
- Cafe IoT lightbulb
- Offices thermostat
Key idea

MUD-rejected traffic

Cross-deployment MRT evolution correlation
Key idea
Approach
Approach

0. MUD enforced (we used MUDgee)

1. Collect MUD-rejected traffic (MRT)

Device A
Approach

0. MUD enforced (we used MUDgee)

1. Collect MUD-rejected traffic (MRT)
2. Describe MRT
1. Collect MUD-rejected traffic (MRT)
2. Describe MRT

Device A

Device B

Device C
Approach

1. Collect MUD-rejected traffic (MRT)
2. Describe MRT

Device A

Device B

Device C

3. Compare MRT from many devices
Approach – 1. Collect MRT
Approach – 2. Describe MRT
Approach – 2. Describe MRT

IoT device X / Y / Z

- MUD Rejected traffic (MRT)
- MRT NetFlow CSV
- Flows clustering
- MRT characterization
Approach – 2. Describe MRT

- IoT device X / Y / Z
- MUD rejected traffic (MRT)
- NetFlow CSV
- Flows clustering
- MRT characterization
- pcap
- pcap

[Diagram of data flow and analysis processes]
Approach – 2. Describe MRT
Approach – 2. Describe MRT
Approach – 2. Describe MRT
Approach – 2. Describe MRT

Clusters balance | clusters distances | Mutual/forward/backward matches | forward/backward agglomeration
Approach – 2. Describe MRT

<table>
<thead>
<tr>
<th>Clusters balance</th>
<th>clusters distances</th>
<th>Mutual/forward/backward matches</th>
<th>forward/backward agglomeration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Approach – 3. Compare MRT

<table>
<thead>
<tr>
<th>Clusters balance</th>
<th>clusters distances</th>
<th>Mutual/forward/backward matches</th>
<th>forward/backward agglomeration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Experiments
Experiments – same attacks
Experiments – same attacks
Experiments – same attacks

TNO
Den Haag

Attacker

OS scan

Honeywell T57RF2025
Eufy HomeBase 2
Hombli plug HBPP-0201
Hombli plug HBPP-0201
Foscam RM2
Foscam C1780P

IoT Lab TU/e Eindhoven
Experiments – same attacks

TNO
Den Haag

Attacker

Vuln. scan

Honeywell T57RF2025
Eufy HomeBase 2
Hombli plug HBPP-0201
Hombli plug HBPP-0201
Foscam C1780P
Foscam RM2

IoT Lab TU/e Eindhoven

5-9 December 2022

ACSAC 22, Austin, Texas, USA
Experiments – same attacks
Experiments – different attacks

TNO
Den Haag

Attacker

Honeywell T57RF2025
Eufy HomeBase 2
Hombli plug HBPP-0201
Hombli plug HBPP-0201
Foscam C1780P

IoT Lab TU/e Eindhoven

ACSAC 22, Austin, Texas, USA
Experiments – different attacks
Experiments – different attacks

TNO
Den Haag

Attacker

Telnet
SSH
scan

OS
scan

Vuln.
scan

Honeywell
T57RF2025

Eufy
HomeBase 2

Hombli plug
HBPP-0201

Hombli plug
HBPP-0201

Foscam
C1780P

IoT Lab TU/e
Eindhoven

Foscam
RM2
Experiments – different attacks

TNO
Den Haag

Attacker

Telnet
SSH
scan

OS
scan

Vuln.
scan

Honeywell
T57RF2025

Eufy
HomeBase 2

Hombli plug
HBPP-0201

Hombli plug
HBPP-0201

Foscam
C1780P

Foscam
RM2

IoT Lab TU/e
Eindhoven

5-9 December 2022

ACSAC 22, Austin, Texas, USA

38
Experiments – different attacks
Experiments – different attacks
Experiments – different attacks
Results
Results – detecting attacks

(= with clusters fluctuations)

<table>
<thead>
<tr>
<th>Attack</th>
<th>MRT entries</th>
<th>Anomalous entries</th>
<th>TP</th>
<th>TN</th>
<th>FP</th>
<th>FN</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/SSH port scan</td>
<td>130</td>
<td>15</td>
<td>15</td>
<td>115</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>OS scan</td>
<td>217</td>
<td>26</td>
<td>26</td>
<td>191</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>Vulnerability scan</td>
<td>310</td>
<td>48</td>
<td>45</td>
<td>259</td>
<td>3</td>
<td>0</td>
<td>98.06%</td>
<td>93.75%</td>
<td>100.00%</td>
<td>96.77%</td>
</tr>
<tr>
<td>TCP SYN flood DoS</td>
<td>170</td>
<td>22</td>
<td>16</td>
<td>142</td>
<td>6</td>
<td>0</td>
<td>96.47%</td>
<td>72.73%</td>
<td>100.00%</td>
<td>84.21%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>827</strong></td>
<td><strong>111</strong></td>
<td><strong>102</strong></td>
<td><strong>707</strong></td>
<td><strong>9</strong></td>
<td><strong>0</strong></td>
<td><strong>98.90%</strong></td>
<td><strong>91.89%</strong></td>
<td><strong>100.00%</strong></td>
<td><strong>95.77%</strong></td>
</tr>
</tbody>
</table>
## Results – detecting attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>MRT entries</th>
<th>Anomalous entries</th>
<th>TP</th>
<th>TN</th>
<th>FP</th>
<th>FN</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/SSH port scan</td>
<td>130</td>
<td>15</td>
<td>15</td>
<td>115</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>OS scan</td>
<td>217</td>
<td>26</td>
<td>26</td>
<td>191</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>Vulnerability scan</td>
<td>310</td>
<td>48</td>
<td>45</td>
<td>259</td>
<td>3</td>
<td>0</td>
<td>98.06%</td>
<td>93.75%</td>
<td>100.00%</td>
<td>96.77%</td>
</tr>
<tr>
<td>TCP SYN flood DoS</td>
<td>170</td>
<td>22</td>
<td>16</td>
<td>142</td>
<td>6</td>
<td>0</td>
<td>96.47%</td>
<td>72.73%</td>
<td>100.00%</td>
<td>84.21%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>827</strong></td>
<td><strong>111</strong></td>
<td><strong>102</strong></td>
<td><strong>707</strong></td>
<td><strong>9</strong></td>
<td><strong>0</strong></td>
<td><strong>98.90%</strong></td>
<td><strong>91.89%</strong></td>
<td><strong>100.00%</strong></td>
<td><strong>95.77%</strong></td>
</tr>
</tbody>
</table>

FPs because of non manufacturer’s MUD
## Results – identifying same attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>Total signatures</th>
<th>Expected matches</th>
<th>TP</th>
<th>TN*</th>
<th>FP</th>
<th>FN</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/SSH port scan</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>N/A*</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>OS scan</td>
<td>5</td>
<td>10</td>
<td>6</td>
<td>N/A*</td>
<td>0</td>
<td>4</td>
<td>60.00%</td>
<td>100.00%</td>
<td>60.00%</td>
<td>75.00%</td>
</tr>
<tr>
<td>Vulnerability scan</td>
<td>5</td>
<td>10</td>
<td>8</td>
<td>N/A*</td>
<td>0</td>
<td>2</td>
<td>80.00%</td>
<td>100.00%</td>
<td>80.00%</td>
<td>88.89%</td>
</tr>
<tr>
<td>TCP SYN flood DoS</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>N/A*</td>
<td>1</td>
<td>0</td>
<td>50.00%</td>
<td>50.00%</td>
<td>100.00%</td>
<td>66.67%</td>
</tr>
<tr>
<td>Total</td>
<td>17</td>
<td>31</td>
<td>25</td>
<td>N/A*</td>
<td>1</td>
<td>6</td>
<td>78.13%</td>
<td>96.15%</td>
<td>80.65%</td>
<td>87.72%</td>
</tr>
</tbody>
</table>

\[\text{same attacks identified as same}\]
Results – identifying same attacks - example

DoS experiment

Clusters balance

MRT entry #
## Results – discerning different attacks

<table>
<thead>
<tr>
<th>Test</th>
<th>Device(s)</th>
<th>Compared MRT feeds</th>
<th>Incorrect matches</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Expected</td>
<td>Worst</td>
</tr>
<tr>
<td>1</td>
<td>Eufy home-kit doorbell</td>
<td></td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Honeywell thermostat</td>
<td>Scans</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Homblì plug 1</td>
<td>(Telnet/SSH, OS,</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Homblì plug 2</td>
<td>Vulnerabilities)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Foscam camera C1780P</td>
<td>All</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Eufy, Honeywell, Homblì, Foscam</td>
<td>All</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Overall</td>
<td></td>
<td>0</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Matches correctly discarded</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comparisons correctly discarded
Results – identifying different attacks

![Graph showing different types of attacks](image-url)
Conclusions
Conclusions - results

Novel approach to gain visibility of IoT threats at home-like environments

95.77% F1 score for detection of attacks
96.15% of same attack cases identified as same
94.44% of different attack cases identified as different
Conclusions – discussion

Main limitations:
- MUD attack surface
- Low-volume attacks
Conclusions – discussion

Main limitations:
- MUD attack surface
- Low-volume attacks

Main future work:
- Distributed scenario → Test at-scale events
Conclusions – discussion

Main limitations:
- MUD attack surface
- Low-volume attacks

Main future work:
- Distributed scenario → Test at-scale events

Use-case:
- Security monitoring for vendors
Conclusions – open source!

MUDscope tool and Dataset

https://github.com/lucamrgs/MUDscope
Thank you

Stepping out of the MUD: contextual threat information for IoT devices with manufacturer-provided behavior profiles

https://github.com/lucamrgs/MUDscope

luca.morgese@tno.nl

Luca Morgese Zangrandi

Questions?