Packet-Level Signatures for Smart Home Devices

Rahmadi Trimananda, Janus Varmarken, Athina Markopoulou, and Brian Demsky
Home
Smart Home

Smart Plugs
Smart Home

Smart Plugs

Light Bulbs
Smart Home

Smart Plugs
Light Bulbs
Thermostats
Smart Home

Smart Plugs

Light Bulbs

Thermostats

Cameras
Smart Home

- Smart Plugs
- Light Bulbs
- Thermostats
- Cameras
- Doorbells
Smart Home

LAN Traffic

Phone-Device
Smart Home
Smart Home
Smart Home

Device-Cloud

Phone-Device

Phone-Cloud
NOT-SO PRIVATE Home

Device-Cloud

Phone-Cloud

Phone-Device
WAN Sniffer
WAN Sniffer
WAN Sniffer
WAN Sniffer

1) Can look into TCP/IP packet
2) Can see IP address
3) Cannot see MAC address
Wi-Fi Sniffer
Wi-Fi Sniffer
Wi-Fi Sniffer
Wi-Fi Sniffer

1) Cannot look into TCP/IP packet
2) Cannot see IP address
3) Can see MAC address
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)\textsuperscript{Homonit} [CCS’18]
- Volume-based\textsuperscript{Apthorpe et al.} [PETS’19]
- ML-based approaches\textsuperscript{HomeSnitch} [WiSec’19]
- IoT datasets\textsuperscript{Ren et al.} [IMC’19], Alrawi et al. [S&P’19]
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)$^\text{Homonit [CCS’18]}$
- Volume-based$^\text{Apthorpe et al. [PETS’19]}$
- ML-based approaches$^\text{HomeSnitch [WiSec’19]}$
- IoT datasets$^\text{Ren et al. [IMC’19], Alrawi et al. [S&P’19]}$
State-of-the-Art

- **Specific protocols** (ZigBee/Z-Wave)\textsuperscript{Homonit [CCS’18]}
- **Volume-based**\textsuperscript{Aptthorpe et al. [PETS’19]}
- **ML-based approaches**\textsuperscript{HomeSnitch [WiSec’19]}
- **IoT datasets**\textsuperscript{Ren et al. [IMC’19], Alrawi et al. [S&P’19]}

![Graphs showing traffic data over time for Nest security camera and Belkin Wemo switch.](image)
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)\textsuperscript{Homonit [CCS’18]}
- Volume-based\textsuperscript{Apthorpe et al. [PETS’19]}
- ML-based approaches\textsuperscript{HomeSnitch [WiSec’19]}
- IoT datasets\textsuperscript{Ren et al. [IMC’19], Alrawi et al. [S&P’19]}

Volume spike is event
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)\textsuperscript{Homonit [CCS’18]}
- Volume-based\textsuperscript{Apthorpe et al. [PETS’19]}
- ML-based approaches\textsuperscript{HomeSnitch [WiSec’19]}
- IoT datasets\textsuperscript{Ren et al. [IMC’19], Alrawi et al. [S&P’19]}
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)\textsuperscript{Homonit [CCS’18]}
- Volume-based\textsuperscript{Apthorpe et al. [PETS’19]}
- ML-based approaches\textsuperscript{HomeSnitch [WiSec’19]}
- IoT datasets\textsuperscript{Ren et al. [IMC’19], Alrawi et al. [S&P’19]}

<table>
<thead>
<tr>
<th>Feature</th>
<th>Category</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. bytes from client per seq.</td>
<td>Throughput</td>
<td>0.213104</td>
</tr>
<tr>
<td>Avg. bytes from server per seq.</td>
<td>Throughput</td>
<td>0.072519</td>
</tr>
<tr>
<td>Aggregate server bytes sent for ADU</td>
<td>Throughput</td>
<td>0.105775</td>
</tr>
<tr>
<td>Aggregate client bytes sent to ADU</td>
<td>Throughput</td>
<td>0.117552</td>
</tr>
<tr>
<td>Min bytes from client for single seq.</td>
<td>Burstiness</td>
<td>0.038917</td>
</tr>
<tr>
<td>Min bytes from server for single seq.</td>
<td>Burstiness</td>
<td>0.038344</td>
</tr>
<tr>
<td>Max bytes from server for single seq.</td>
<td>Burstiness</td>
<td>0.079063</td>
</tr>
<tr>
<td>Max bytes from client for single seq.</td>
<td>Burstiness</td>
<td>0.135909</td>
</tr>
<tr>
<td>Stdev of bytes for server seq.</td>
<td>Burstiness</td>
<td>0.054491</td>
</tr>
<tr>
<td>Stdev of bytes for client seq.</td>
<td>Burstiness</td>
<td>0.050798</td>
</tr>
<tr>
<td>Server sequences per ADU</td>
<td>Synchronicity</td>
<td>0.013566</td>
</tr>
<tr>
<td>Client sequences per ADU</td>
<td>Synchronicity</td>
<td>0.016211</td>
</tr>
<tr>
<td>Total time of connection</td>
<td>Duration</td>
<td>0.063750</td>
</tr>
</tbody>
</table>

UCI University of California, Irvine
State-of-the-Art

- **Specific protocols** (ZigBee/Z-Wave)\(^\text{Homonit [CCS'18]}\)
- **Volume-based** Apthorpe et al. [PETS'19]
- **ML-based approaches** HomeSnitch [WiSec'19]
- **IoT datasets** Ren et al. [IMC'19], Alrawi et al. [S&P'19]

Network statistics as features
State-of-the-Art

● Specific protocols (ZigBee/Z-Wave)\(^{\text{Homonit [CCS'18]}}\)
● Volume-based\(^{\text{Apthorpe et al. [PETS'19]}}\)
● ML-based approaches\(^{\text{HomeSnitch [WiSec'19]}}\)
● IoT datasets\(^{\text{Ren et al. [IMC'19], Alrawi et al. [S&P'19]}}\)
State-of-the-Art

- Specific protocols (ZigBee/Z-Wave)
- Volume-based
- ML-based approaches
- IoT datasets

- Device study
  - Network traffic characteristics
- Public datasets
  - Mon(IoT)r
    - [Link to Mon(IoT)r]
  - YourThings
    - [Link to YourThings]

Public datasets

- Mon(IoT)r
- YourThings

IoT datasets

- Ren et al. [IMC'19], Alrawi et al. [S&P’19]
Outline

I. Background and Problem Statement

II. Key Observation: Packet-Level Signatures

III. The PingPong System

IV. Conclusion
Outline

I. Background and Problem Statement
II. Key Observation: Packet-Level Signatures
III. The PingPong System
IV. Conclusion
Smart Home

Device-Cloud

Phone-Cloud

Phone-Device
Local Phone

Toggle ON Plug

LAN Traffic

Phone-Device
Key Observation: Ping-Pong

Toggle ON Plug

Request PING!
Key Observation: Ping-Pong

Toggle ON Plug

Reply
PONG!
Key Observation

Toggle ON Plug

Device-Cloud

WAN Traffic
Key Observation

Toggle ON Plug

Request

Reply
Remote Phone

Toggle ON Plug
Remote Phone

Toggle ON Plug

Phone-Cloud

WAN Traffic

Remote Phone
Remote Phone

Toggle ON Plug
Remote Phone

Toggle ON Plug

Request

Reply
Home Automation

Toggle ON Plug
Home Automation

Toggle ON Plug
Home Automation

Toggle ON Plug

Request

Reply
Ping-Pong in TP-Link Plug
Ping-Pong in TP-Link Plug
Ping-Pong in TP-Link Plug
Ping-Pong in TP-Link Plug

Device - Cloud

ON

Internet Host

Phone

<556, S-1293>

Device-Cloud

OFF

Internet Host

Phone

<557, S-1294>

Device-Cloud

TCP
Ping-Pong in D-Link Plug

Phone

ON

Internet Host

ON

613

1117

C-1117, S-613

Phone-Cloud

613

1118

C-1118, S-613

Phone-Cloud
Ping-Pong in SmartThings Plug

Phone | Internet Host 1 | Phone | Internet Host 1
511  
612  
777  
---|---|---|---
699  
136  
136  
---|---|---|---
700  
616  
780  
136  
136  
t
Ping-Pong in SmartThings Plug

Phone-Cloud

\(<C-699, S-511>\)

\(<S-612, C-136>\)

\(<S-777, C-136>\)

Phone

ON

699

511

Internet Host 1

Internet Host 2

Phone

OFF

700

511

Internet Host 1

Internet Host 2

Phone-Cloud

\(<C-700, S-511>\)

\(<S-616, C-136>\)

\(<S-780, C-136>\)
Ping-Pong in SmartThings Plug

Packet-Level Signature of an Event

Sequences of request-reply packet pairs with unique and deterministic packet lengths and directions
Research Questions

● How to automatically extract packet-level signatures?
● How universal are packet-level signatures?
● How unique are packet-level signatures?
Research Questions

- How to automatically extract packet-level signatures?
- How universal are packet-level signatures?
- How unique are packet-level signatures?
I. Background and Problem Statement
II. Key Observation: Packet-Level Signatures
III. The PingPong System
IV. Conclusion
Automated Extraction

- Extract these pairs
- Form longest possible sequences
- Use them as a signature
PingPong Training

The PingPong System

Input

Event Triggers → Device
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace → Trace Filtering

UCI University of California, Irvine
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Pair Clustering
PingPong Training

The PingPong System

- Input
  - Event Triggers
  - Device

Training

- Data Collection
- Network Trace
- Trace Filtering
- Pair Clustering
- Signature Creation
PingPong Training

The PingPong System

Input

Event Triggers → Device

Data Collection → Network Trace

Training

Trace Filtering

Pair Clustering

Signature Creation

Signature Validation
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Pair Clustering

Signature Creation

Signature Validation

Signature
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Pair Clustering

Signature Creation

Signature Validation

Signature

C-556 S-1293

University of California, Irvine
PingPong Training

The PingPong System

Input
- Event Triggers
- Device

Training
- Data Collection
- Network Trace
- Trace Filtering
- Pair Clustering
- Signature Creation
- Signature Validation

Signature

C-556 S-1293

PingPong Training

The PingPong System

Input
- Event Triggers
- Device

Training
- Data Collection
- Network Trace
- Trace Filtering
- Pair Clustering
- Signature Creation
- Signature Validation

Output

C-556 S-1293

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]
Research Questions

● How to automatically extract packet-level signatures?

● How universal are packet-level signatures?

● How unique are packet-level signatures?
Research Questions

● How to **automatically** extract packet-level signatures?

● How **universal** are packet-level signatures?

● How **unique** are packet-level signatures?
Universal Signatures

- Three communications
Universal Signatures

● Three communications
Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- **Different triggers**
  - **Local-Phone**
Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices
### Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Signature</th>
<th>Communication</th>
<th>Matching (Per 100 Events)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WAN Snif.</td>
</tr>
<tr>
<td>Amazon plug</td>
<td>ON</td>
<td>S1: 8443-445 S2: C-1099 S-235</td>
<td>Device-Cloud</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: 8444-446 S2: C-1179 S-235 S3: C-1514 C-103 S-235</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>WeMo plug</td>
<td>ON/OFF</td>
<td>S1: PH-259 PH-473 D-246</td>
<td>Phone-Device</td>
<td>-</td>
</tr>
<tr>
<td>WeMo Insight plug</td>
<td>ON/OFF</td>
<td>S1: PH-259 PH-475 D-246</td>
<td>Phone-Device</td>
<td>-</td>
</tr>
<tr>
<td>TP-Link plug</td>
<td>ON</td>
<td>S1: C-556 S-1293</td>
<td>Device-Cloud</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-557 S-[1294-1295]</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>D-Link plug</td>
<td>ON/OFF</td>
<td>S1: S-91 S-1227 C-784 S2: C-1092 S-647</td>
<td>Device-Cloud</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>S1: C-[1109-1124] S-613</td>
<td>Phone-Cloud</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-[1110-1124] S-613</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SmartThings plug</td>
<td>ON</td>
<td>S1: C-699 S-511 S2: S-777 C-136</td>
<td>Phone-Cloud</td>
<td>92</td>
</tr>
</tbody>
</table>
## Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Signature</th>
<th>Communication</th>
<th>Matching (Per 100 Events)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sengled light bulb</td>
<td>ON</td>
<td>S1: S-[217-218] C-[209-210] S2: C-430 S3: C-466</td>
<td>Device-Cloud</td>
<td>97 0 - -</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: S-[217-218] C-[209-210] S2: C-430 S3: C-465</td>
<td>Phone-Cloud</td>
<td>93 0 97 0</td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>S1: C-211 S-1063 S2: S-1277</td>
<td>Device-Cloud</td>
<td>99 2 - -</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-211 S-1063 S-1276</td>
<td>Phone-Cloud</td>
<td>99 0 99 0</td>
</tr>
<tr>
<td>Hue light bulb</td>
<td>ON</td>
<td>S1: C-364 S2: D-88</td>
<td>Device-Cloud</td>
<td>- - - -</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-365 S2: D-88</td>
<td>Phone-Device</td>
<td>- - - -</td>
</tr>
<tr>
<td>TP-Link light bulb</td>
<td>ON</td>
<td>S1: PH-198 D-227</td>
<td>Phone-Device</td>
<td>- - 100 4</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: PH-198 D-244</td>
<td>Phone-Device</td>
<td>- - 100 0</td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: PH-[240-242] D-[287-289]</td>
<td>Phone-Device</td>
<td>- - 100 0</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>S1: PH-317 D-287</td>
<td>Phone-Device</td>
<td>- - 100 0</td>
</tr>
</tbody>
</table>
## Universal Signatures

- Applies to many devices
  - Our corpus: **18 devices**

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Signature</th>
<th>Communication</th>
<th>Matching (Per 100 Events)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WAN Sniff.</td>
</tr>
<tr>
<td>Nest thermostat</td>
<td>Fan ON</td>
<td>S1: C-891-894</td>
<td>Phone-Cloud</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Fan OFF</td>
<td>S1: C-858-860</td>
<td>Phone-Cloud</td>
<td>0</td>
</tr>
<tr>
<td>EcoBee thermostat</td>
<td>HVAC Auto</td>
<td>S1: S-1300 C-640</td>
<td>Phone-Cloud</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>HVAC OFF</td>
<td>S1: C-1299 C-640</td>
<td>Phone-Cloud</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Fan ON</td>
<td>S1: S-1387 C-640</td>
<td>Phone-Cloud</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Fan Auto</td>
<td>S1: C-1389 C-640</td>
<td>Phone-Cloud</td>
<td>0</td>
</tr>
<tr>
<td>Rachio sprinkler</td>
<td>Quick Run</td>
<td>S1: S-267 C-155</td>
<td>Device-Cloud</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>S1: C-496 C-155 C-395</td>
<td>Device-Cloud</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Standby/Active</td>
<td>S1: S-299 C-135 C-395</td>
<td>Device-Cloud</td>
<td>100</td>
</tr>
<tr>
<td>Blossom sprinkler</td>
<td>Quick Run</td>
<td>S1: C-326</td>
<td>Device-Cloud</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>S2: C-177 S-505</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>S1: C-726 S2: C-177 S-458 S3: C-238 C-56 S-388</td>
<td>Device-Cloud</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Quick Run</td>
<td>S1: C-649 S-459 C-574 S-507 S2: S-1135-139</td>
<td>Phone-Cloud</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>S1: C-617 S-431</td>
<td>Phone-Cloud</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Hibernate</td>
<td>S1: C-621 S-493</td>
<td>Phone-Cloud</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Active</td>
<td>S1: C-622 S-494 S2: S-599 C-566 C-554 C-566</td>
<td>Phone-Cloud</td>
<td>0</td>
</tr>
</tbody>
</table>

---

UCI University of California, Irvine
**Universal Signatures**

- Applies to many devices
  - Our corpus: 18 devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Signature</th>
<th>Communication</th>
<th>Matching (Per 100 Events)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring alarm</td>
<td>Arm</td>
<td>S1: S-99 S-2 C-99 S-181-183 C-99</td>
<td>Device-Cloud</td>
<td>98 0 95 0</td>
</tr>
<tr>
<td></td>
<td>Disarm</td>
<td>S1: S-99 S-235 C-99 S-181-183 C-99</td>
<td></td>
<td>0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>Stream OFF</td>
<td>S1: C-[445-449] S-442</td>
<td></td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>D-Link siren</td>
<td>ON</td>
<td>S1: C-1076 S-593</td>
<td>Phone-Cloud</td>
<td>100 0 98 0</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-1023 S-613</td>
<td></td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>Kwikset door lock</td>
<td>Lock</td>
<td>S1: C-699 S-511 S2: S-639 C-136</td>
<td>Phone-Cloud</td>
<td>100 0 100 0</td>
</tr>
<tr>
<td></td>
<td>Unlock</td>
<td>S1: C-701 S-511 S2: S-647 C-136</td>
<td></td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>Roomba robot</td>
<td>Clean</td>
<td>S1: S-[1014-1015] C-105 S-432 C-105</td>
<td>Phone-Cloud</td>
<td>91 0 94 0</td>
</tr>
<tr>
<td></td>
<td>Back-to-station</td>
<td>S1: S-440 C-105 S-[1018-1024]</td>
<td></td>
<td>0 0 0 0</td>
</tr>
</tbody>
</table>

---

[Image: University of California, Irvine]
Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices
Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices
  - Public dataset Mon(IoT)r
    - Extraction for 21 new devices
Universal Signatures

- Applies to many devices
- Public dataset

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Signature</th>
<th>Duration (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon camera</td>
<td>Week</td>
<td>SU: S127/S141 S129/S134</td>
<td>207.7 ± 261.7</td>
</tr>
<tr>
<td>Blink light bulb</td>
<td>On</td>
<td>OFF</td>
<td>4.7 ± 4.78</td>
</tr>
<tr>
<td>Amazon Echo Dot</td>
<td>Voice</td>
<td>SI: C195/S190 S196/S195</td>
<td>217 ± 430.0</td>
</tr>
<tr>
<td>Amazon Echo Plus</td>
<td>Voice</td>
<td>SI: C178/S180 C185/S187</td>
<td>1,551 ± 2,009</td>
</tr>
<tr>
<td>Amazon Echo Spot</td>
<td>Voice</td>
<td>SI: C184/S183 C185/S187</td>
<td>1,220 ± 765.1</td>
</tr>
<tr>
<td>Google Home</td>
<td>Voice</td>
<td>SI: C134/S136 S135/S136</td>
<td>977 ± 1.57</td>
</tr>
<tr>
<td>Harmon Kardon Invoke speaker</td>
<td>Voice</td>
<td>SI: S149/S148 C149/C150</td>
<td>2,109 ± 2,065</td>
</tr>
<tr>
<td>TV</td>
<td>Power</td>
<td>SI: S148/S148 S149/S149</td>
<td>223 ± 567.7</td>
</tr>
<tr>
<td>Honeywell thermostat</td>
<td>ON</td>
<td>SI: S127/S137 S128/S138</td>
<td>1,097 ± 1,269</td>
</tr>
<tr>
<td>Sennheiser TV</td>
<td>On</td>
<td>SI: C127/S129 C128/S130</td>
<td>2.7 ± 2.7</td>
</tr>
<tr>
<td>Realtime SDK</td>
<td>Set</td>
<td>SI: C149/C149</td>
<td>377 ± 109.7</td>
</tr>
<tr>
<td>Samsung fridge</td>
<td>Set</td>
<td>SI: C149/C149</td>
<td>377 ± 109.7</td>
</tr>
<tr>
<td>Motorola (Satellite)</td>
<td>Set</td>
<td>SI: C149/C149</td>
<td>377 ± 109.7</td>
</tr>
<tr>
<td>Other Types of Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Universal Signatures

- Applies to many devices
  - Our corpus: 18 devices
  - Public dataset Mon(IoT)r
    - Extraction for 21 new devices
    - Comparison for 5 common devices
Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- **Different triggers**
  - **Local-Phone**
Universal Signatures

- **Three** communications
- **Two** adversaries
  - WAN and Wi-Fi sniffers
- **Different triggers**
  - Local-Phone
  - Remote-Phone, and
  - Home Automation
## Universal Signatures

- **Three communications**
  - Two adversaries
    - WAN and Wi-Fi sniffers
- **Different triggers**
  - Local
  - Remote
  - Home Automation

### Device Signatures

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Device-Cloud Signature</th>
<th>Matching (Per 100 Events)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>WAN Sniffer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plugs</td>
<td></td>
</tr>
<tr>
<td>WeMo plug</td>
<td>ON/OFF</td>
<td>S1: S-146</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-210 S-134 S-286 C-294</td>
<td></td>
</tr>
<tr>
<td>WeMo Insight plug</td>
<td>ON</td>
<td>S1: S-146</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-210 S-134 S-286 C-294</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: S-146</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-210 S-134 S-350 C-294</td>
<td></td>
</tr>
<tr>
<td>TP-Link plug</td>
<td>ON</td>
<td>S1: C-592 S-1234 S-100</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-503 S-723 S-100</td>
<td>93</td>
</tr>
<tr>
<td>D-Link plug</td>
<td>ON/OFF</td>
<td>S1: C-256</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-1020 S-647</td>
<td></td>
</tr>
<tr>
<td>Hue light bulb</td>
<td>ON</td>
<td>S1: [827-229] [857-859] C-355</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: [827-230] [857-860] C-366</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: [257-240] [895-899]</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: [1378-3759]</td>
<td></td>
</tr>
<tr>
<td>TP-Link light bulb</td>
<td>ON</td>
<td>S1: [348-349] C-199-400</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: [348-349] C-418-419</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: [348-442] C-396-400</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>S1: [386-388] C-397-399</td>
<td>99</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rachio sprinkler</td>
<td>Quick Run</td>
<td>S1: S-267 C-155</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>S1: C-661</td>
<td>95</td>
</tr>
<tr>
<td>Arlo camera</td>
<td>Start Recording</td>
<td>S1: C-704 S-215</td>
<td>100</td>
</tr>
<tr>
<td>D-Link siren</td>
<td>ON</td>
<td>S1: [899-100] C-616</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-216</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>98.4</td>
</tr>
</tbody>
</table>
Universal Signatures

- **Three** communications
- **Two** adversaries
  - **WAN** and **Wi-Fi** sniffers
- **Different triggers**
  - **Local-Phone**
  - **Remote-Phone**, and
  - **Home Automation**
- **Matching with recall** > 97%
Unique Signatures

- Distinguish
  - Device type
  - Event type: binary and non-binary
  - Same-vendor devices
## Unique Signatures

### Distinguish

- **Device type:**
  - Same-vendor devices

- **Event type:**
  - Binary and non-binary

### Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Model</th>
<th>Event</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing TP-Link Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TP-Link plug</td>
<td>HS-110</td>
<td>ON</td>
<td>S1: PH-172 D-115</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S2: C-592 S-1234 S-100</td>
</tr>
<tr>
<td>TP-Link light bulb</td>
<td>LB-130</td>
<td>ON</td>
<td>S1: PH-258 D-288</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S2: C-593 S-1235 S-100</td>
</tr>
<tr>
<td><strong>Newly Added TP-Link Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TP-Link two-outlet plug</td>
<td>HS-107</td>
<td>ON</td>
<td>S1: PH-219 D-103</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S2: C-300 C-711 S-1413 S-88</td>
</tr>
<tr>
<td>TP-Link power strip</td>
<td>HS-300</td>
<td>ON</td>
<td>S1: PH-219 D-103</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S2: C-301 C-1412 S-[1405-1406] S-88</td>
</tr>
<tr>
<td>TP-Link white light bulb</td>
<td>KL-110</td>
<td>ON</td>
<td>S1: C-[414-415] C-[331-332]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S2: C-648 S-[1279-1280] S-88</td>
</tr>
<tr>
<td>TP-Link camera</td>
<td>KC-100</td>
<td>ON</td>
<td>S1: PH-256 D-162 PH-624 D-256 PH-72 D-111 PH-608 D-371 PH-97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S2: C-1288 S-[1161-1162] S-100</td>
</tr>
</tbody>
</table>
Unique Signatures

- **Distinguish**
  - Device type
  - Event type: binary and non-binary
  - Same-vendor devices

- **Negative control experiment**
  - Three public datasets: >440 million packets
    - YourThings, UNSW, UNB
  - FPR: one FP per 40 million packets
Packet-Level Signatures

- Can distinguish event types

[Checkmark symbol]
Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓
Packet-Level Signatures

- Can distinguish event types ✓
- Minimal set of traffic features ✓
- Two adversaries ✓
Packet-Level Signatures

- Can distinguish event types
- Minimal set of traffic features
- Two adversaries
- Applicable to many devices
Packet-Level Signatures

- Can distinguish event types ✔
- Minimal set of traffic features ✔
- Two adversaries ✔
- Applicable to many devices ✔
- Resilient to traffic shaping & VPN encryption ✔
- Defended against by packet padding ✔
Packet-Level Signatures

- Can distinguish event types
- Minimal set of traffic features
- Two adversaries
- Applicable to many devices
- Resilient to traffic shaping & VPN encryption
- Defended against by packet padding
- Profiling and network monitoring
Limitations

- Need device to train
- Signatures may vary over time
- Apply to 95% of devices
  - UDP-based
  - Repetitive pairs for an event
Outline

I. Background and Problem Statement
II. Key Observation: Packet-Level Signatures
III. The PingPong System
IV. Conclusion
Conclusions

- Packet-level signatures
  - Request-reply pattern
  - Packet lengths and directions
- Automation: PingPong
  - Extraction and detection
- Signatures are universal and unique
Thank You!

- **Paper**
  

- **Software and datasets**
  
  http://plrg.ics.uci.edu/pingpong/
Additional Slides
Signature Variations

- Signatures with no variation
- Signatures with ranges
- Signatures that vary
  - Signature evolution
  - Signatures that vary in certain packets
    - App’s username and password
      - C-556  S-1293
      - C-339  S-329  C-[364-365]  S-[1061-1070]
      - C-[271-273]  S-[499-505]
PingPong Training

The PingPong System

Input

Event Triggers → Device

Toggle ON for TP-Link Plug
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Toggle ON for TP-Link Plug

tcpdump

UCI University of California, Irvine
PingPong Training

The PingPong System

- Event Triggers ➔ Device
- Training ➔ Data Collection ➔ Network Trace

Toggle ON for TP-Link Plug

adb

tcpdump

UCI University of California, Irvine
PingPong Training

The PingPong System

Event Triggers → Device

Training

Data Collection → Network Trace

Toggle ON for TP-Link Plug

adb

Toggle-ON
11/08/2018
01:28:23 PM

event
dump
PingPong Training

The PingPong System

- Event Triggers
- Device

Training

- Data Collection
- Network Trace
- Trace Filtering

Input

Toggle ON for TP-Link Plug

PCAP file

... 
... C-123 S-456 ... C-234 S-567 ... C-345 S-678 ...
... C-556 S-1293 ... C-238 S-826 ... C-129 S-123 ...
... C-123 S-456 ... C-234 S-567 ... C-345 S-678 ...
...
PingPong Training

The PingPong System

Input
- Event Triggers
  - Device

Training
- Data Collection
  - Network Trace
  - Trace Filtering

Toggle ON for TP-Link Plug

PCAP file

Toggle-ON
11/08/2018 01:28:23 PM

... C-123 S-456 ... C-234 S-567 ... C-345 S-678 ...
... C-556 S-1293 ... C-238 S-826 ... C-129 S-123 ...
... C-123 S-456 ... C-234 S-567 ... C-345 S-678 ...
...

UCI University of California, Irvine
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Toggle ON for TP-Link Plug

PCAP file

Toggle-ON
11/08/2018 01:28:23 PM

C-123 S-456 ... C-234 S-567 ...
C-345 S-678 ...

... C-556 S-1293 ... C-238 S-826 ...
C-129 S-123 ...

... C-123 S-456 ... C-234 S-567 ...
C-345 S-678 ...

...
PingPong Training

The PingPong System

Input

Event Triggers -> Device

Training

Data Collection -> Network Trace

Trace Filtering

Toggle ON for TP-Link Plug

... C-556 S-1293 ... C-238 S-826 ... C-129 S-123 ...
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Toggle ON for TP-Link Plug

... C-556 S-1293 ... C-238 S-826
... C-129 S-123 ...

TCP Conn.1 ... C-556 S-1293 ...
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Toggle ON for TP-Link Plug

TCP Conn.1 → C-556 S-1293

TCP Conn.2 → C-238 S-826

TCP Conn.3 → C-129 S-123

Training Data Collection

Input Event Triggers → Device

Network Trace

Trace Filtering

TCP Conn.1 → C-556 S-1293

TCP Conn.2 → C-238 S-826

TCP Conn.3 → C-129 S-123
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

TCP Conn.1 → C-556 S-1293 → C-238 S-826

TCP Conn.2 → C-556 S-1293 → C-238 S-826

TCP Conn.3 → C-129 S-123

Toggle ON for TP-Link Plug

UCI University of California, Irvine
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Trace Filtering

Packet Pairs

Toggle ON for TP-Link Plug

... C-556 S-1293 ... C-238 S-826 ... C-129 S-123 ...

<...,..> <C-556, S-1293> <...,..>

<...,..> <C-238, S-826> <...,..>

<...,..> <C-129, S-123> <...,..>
PingPong Training

The PingPong System:

Input
- Event Triggers
- Device

Training
- Data Collection
  - Network Trace
    - Trace Filtering
    - Pair Clustering
    - Signature Creation

Packet Pairs:
- (<...>, <C-556, S-1293>, <...>)
- (<...>, <C-238, S-826>, <...>)
- (<...>, <C-129, S-123>, <...>)

Toggle ON for TP-Link Plug

UCI University of California, Irvine
PingPong Training

The PingPong System

Input
- Event Triggers
- Device

Training
- Data Collection
- Network Trace
  - Trace Filtering
  - Pair Clustering
  - Signature Creation

Packet Pairs
- <..., C-556, S-1293>, <..., >
- <..., C-238, S-826>, <..., >
- <..., C-129, S-123>, <..., >

Toggle ON for TP-Link Plug

Phone

TCP

Internet Host

Device

1293

556
PingPong Training

(a) TP-Link Plug

Pair Clustering

C→S
556, 1293
f: 50

S→C
[238-240], [826-830]
f: 98

<......> <C-556, S-1293> <......>

<......> <C-238, S-826> <......>

<......> <C-129, S-123> <......>
PingPong Training

Pair Clustering

Pairs 1

C→S

556, 1293
f: 50

S→C

[230-240], [826-830]
f: 98

(a) TP-Link Plug
PingPong Training

Pair Clustering

Signature Creation

(a) TP-Link Plug
PingPong Training

Pair Clustering

Sequences 1

Pairs 1

S->C
[238-240], [826-830]
f: 98

C->S
556, 1293
f: 50

Signatures Creation

(a) TP-Link Plug
PingPong Training

Pair Clustering

Sequence 1

Pairs 1

C→S

556, 1293

f: 50

S→C

238-240, 826-830

f: 98

(a) TP-Link Plug

Signature Creation

Sequences 1

1

C

556

1293

C

S

Pair 1.1

Sequence 1.1

2

C

556

1293

S

Pair 1.2

50

C

556

1293

S

Pair 1.50

UCI University of California, Irvine
PingPong Training

Pair Clustering

- C→S: Pair 1
  - 556, 1293
  - f: 50

- S→C: Sequence 1
  - [238-240], [826-830]
  - f: 98

Signature Creation

- Pair 1.1
  - C
  - 556
  - 1293

- Sequence 1.1
  - C

- Pair 1.2
  - C
  - 556
  - 1293

- Pair 1.50
  - C
  - 556

C-556 S-1293

(a) TP-Link Plug
PingPong Training

(b) Arlo Camera
PingPong Training

(b) Arlo Camera
PingPong Training
PingPong Training

(b) Arlo Camera
PingPong Training
PingPong Training

(b) Arlo Camera

UCI University of California, Irvine
PingPong Training
PingPong Training

C–[271–273]  S–[499–505]
PingPong Training

List of Packet Sequence Sets (= Packet-level signature)

PingPong Training

● Run detection
  ○ Same PCAP file

● Valid signature iff
  ○ \( n \) detected events
  ○ \( n \) triggered events
  ○ Matching timestamps
PingPong Detection
PingPong Detection

Signature

Network Trace

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

...
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

C-339  S-329  C-[364-365]  S-[1061-1070]
C-[271-273]  S-[499-505]

... C-339

UCI University of California, Irvine
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

Range-based Matching

C-339  S-329  C-[364-365]  S-[1061-1070]
C-[271-273]  S-[499-505]

... C-339  S-329  C-365
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

Range-based Matching

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
PingPong Detection

The PingPong System

Detection

Match Packet

Match Sequence

Signature

Network Trace

First Sequence Matched

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

Match Sequence

Range-based Matching


C–[271–273] S–[499–505]

... C–339 S–329 C–365 S–1065

... C–272
PingPong Detection

The PingPong System

- Signature
- Network Trace
- Detection
  - Match Packet
  - Match Sequence

Range-based Matching
- C-339 S-329 C-[364-365] S-[1061-1070]
- C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
... C-272 S-500

UCI University of California, Irvine
PingPong Detection

The PingPong System

- Signature
- Network Trace

Detection
- Match Packet
- Match Sequence

Second Sequence Matched
- C-339 S-329 C-[364-365] S-[1061-1070]
- C-[271-273] S-[499-505]
- ... C-339 S-329 C-365 S-1065
- ... C-272 S-500
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

Match Sequence

Event 1

Matched Events

Event Match

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
... C-272 S-500
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet

Match Sequence

Event 1 ... Event n

Matched Events

Event Match

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
... C-272 S-500
PingPong Detection

The PingPong System

Detection

Signature

Network Trace

Match Packet

Match Sequence

Event 1 ... Event n

Matched Events

Event Match

C-339 S-329 C-[364-365] S-[1061-1070]
C-[271-273] S-[499-505]

... C-339 S-329 C-365 S-1065
... C-272 S-500

See paper for more detail

UCI University of California, Irvine
Possible Defenses

● Seemingly not effective defense
  ○ VPN
  ○ Traffic injection and shaping
Possible Defenses

- **Seemingly not effective defense**
  - VPN
  - Traffic injection and shaping

- **More effective defense**
  - Packet padding
    - Obfuscate packet lengths
Possible Defenses

● **Not too effective defense**
  ○ VPN
  ○ Traffic injection and shaping

● **More effective defense**
  ○ Packet padding
    ■ Obfuscate packet lengths

● **See paper for detail**