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
Smart Home
Smart Home

Phone - Cloud

WAN Traffic
Smart Home

Device-Cloud

Phone-Cloud

Phone-Device
Smart Home

Device-Cloud

Phone-Cloud

Phone-Device

NOT-SO PRIVATE
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

WAN Traffic

LAN Traffic

UCI University of California, Irvine
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** \( (\text{ZigBee/Z-Wave})^{\text{Homonit [CCS’18]}} \)
- **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{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]}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{example.png}
\caption{(a) Nest security camera – Video monitoring (b) Belkin Wemo switch – Appliance power cycle}
\end{figure}
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>
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]}

Network statistics as features

\begin{tabular}{|c|c|}
\hline
Feature & statistic \\
\hline
Avg. bytes from client per seq. & 0.105775 \\
Avg. bytes from server per seq. & 0.117552 \\
Aggregate server bytes sent for ADU & Burstiness 0.038917 \\
Aggregate client bytes sent to ADU & Burstiness 0.038344 \\
Min bytes from client for single seq. & Burstiness 0.079063 \\
Min bytes from server for single seq. & Burstiness 0.135909 \\
Max bytes from server for single seq. & Burstiness 0.054491 \\
Max bytes from client for single seq. & Burstiness 0.050798 \\
Std dev of bytes for server seq. & Synchronicity 0.013566 \\
Std dev of bytes for client seq. & Synchronicity 0.016211 \\
Server sequences per ADU & Duration 0.063750 \\
Client sequences per ADU & \\
Total time of connection & \\
\hline
\end{tabular}
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)
- Volume-based
- ML-based approaches
- IoT datasets

Device study
- Network traffic characteristics

Public datasets
- Mon(IoT)r
  https://moniotrlab.ccis.neu.edu/imc19/
- YourThings
  https://yourthings.info/

Public 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
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
Remote Phone

Toggle ON Plug

Phone-Cloud

WAN Traffic
Remote Phone

Toggle ON Plug

WAN Traffic

Phone

Remote Phone

Phone-Cloud

Remote

Plug
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

University of California, Irvine
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

Off

< C-556, S-1293 >

Device-Cloud

< C-557, S-1294 >

Device-Cloud
Ping-Pong in D-Link Plug

Phone ON Internet Host

Phone OFF Internet Host

1117 \(\langle C-1117, S-613\rangle\) Phone-Cloud

1118 \(\langle C-1118, S-613\rangle\) Phone-Cloud

613

613
Ping-Pong in SmartThings Plug

Phone | Internet Host 1 | Phone | Internet Host 1
---|---|---|---
| ON | 699 | | OFF | 700 |
| 511 | | 511 | |
| Internet Host 2 | 612 | Internet Host 2 | 616 |
| 777 | 136 | 780 | 136 |
| t | | t | |
Ping-Pong in SmartThings Plug

Phone-Cloud

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

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

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

Phone

\(\text{ON}\)

Internet Host 1

\(699\)

Internet Host 2

\(612\)

\(777\)

\(511\)

\(136\)

\(t\)

Phone

\(\text{OFF}\)

Internet Host 1

\(700\)

Internet Host 2

\(616\)

\(780\)

\(511\)

\(136\)

\(t\)

\(<S-780, C-136>\)

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

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

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

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

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

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
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

The PingPong System

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
- 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
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

1. Event Triggers
2. Device
3. Training
4. Data Collection
5. Network Trace
6. Trace Filtering
7. Pair Clustering
8. Signature Creation
9. Signature Validation

Input

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

- **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>
<th>WAN Sniff.</th>
<th>FPR</th>
<th>Wi-Fi Sniff.</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon plug</td>
<td>ON</td>
<td>S1: (443-445)</td>
<td>Device-Cloud</td>
<td></td>
<td>98</td>
<td>0</td>
<td>99</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: (444-446)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-1099 S-235</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: 1110-1104</td>
<td></td>
<td></td>
<td></td>
<td></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>
<td>-</td>
<td>-</td>
<td>100</td>
<td>0</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>
<td>-</td>
<td>-</td>
<td>99</td>
<td>0</td>
</tr>
<tr>
<td>TP-Link plug</td>
<td>ON</td>
<td>S1: C-556 S-1293</td>
<td>Device-Cloud</td>
<td></td>
<td>99</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-557 S-[1294-1295]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>S1: PH-112 D-115</td>
<td>Phone-Device &amp;</td>
<td></td>
<td>-</td>
<td>-</td>
<td>99</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-556 S-1293</td>
<td>Device-Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>S1: PH-112 D-115</td>
<td></td>
<td></td>
<td>95</td>
<td>0</td>
<td>95</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-1092 S-647</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D-Link plug</td>
<td>ON/OFF</td>
<td>S1: S-91 S-1227 C-784</td>
<td>Device-Cloud</td>
<td></td>
<td>98</td>
<td>0</td>
<td>98</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-1092 S-647</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SmartThings plug</td>
<td>ON</td>
<td>S1: C-699 S-511</td>
<td>Phone-Cloud</td>
<td></td>
<td>92</td>
<td>0</td>
<td>92</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: S-777 C-136</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-700 S-511</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-780 C-136</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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><strong>WAN Snif.</strong></td>
</tr>
<tr>
<td>Sengled light bulb</td>
<td>ON</td>
<td>S1: S-[217-218] C-[209-210]</td>
<td>Device-Cloud</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-430</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S3: C-466</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: S-[217-218] C-[209-210]</td>
<td>Device-Cloud</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-430</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S3: C-465</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ON</td>
<td>S1: C-211 S-1063</td>
<td>Phone-Cloud</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: S-1277</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-211 S-1063 S-1276</td>
<td>Device-Cloud</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: S-[216-220] C-[208-210]</td>
<td>Device-Cloud</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S1: C-[215-217] S-[1275-1277]</td>
<td>Phone-Cloud</td>
<td>-</td>
</tr>
<tr>
<td>Hue light bulb</td>
<td>ON</td>
<td>S1: C-364</td>
<td>Device-Cloud &amp; Phone-Device</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: D-88</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-365</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: D-88</td>
<td></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>-</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: PH-198 D-244</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: PH-[240-242] D-[287-289]</td>
<td>Phone-Device</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>S1: PH-317 D-287</td>
<td>Phone-Device</td>
<td>-</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 Snif.</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>93</td>
</tr>
<tr>
<td></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>100</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>100</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>100</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 S2: C-177 S-505</td>
<td>Device-Cloud</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>S1: C-326 S2: C-177 S-458 S3: C-238 C-56 S-388</td>
<td>Phone-Cloud</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Quick Run</td>
<td>S1: C-649 S-459 C-574 S-507 S2: S-135-139</td>
<td>Phone-Cloud</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td>S1: C-617 S-431</td>
<td>Phone-Cloud</td>
<td>95</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>95</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>Ring alarm</td>
<td>Arm</td>
<td>S1: S-99 S-2 S-8 C-99 S-181 S-183 C-99</td>
<td>Device-Cloud</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Disarm</td>
<td>S1: S-99 S-255 C-99 S-181 S-183 C-99</td>
<td>Phone-Cloud</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Stream OFF</td>
<td>S1: C-[445-449] S-442</td>
<td>Phone-Cloud</td>
<td>100</td>
</tr>
<tr>
<td>D-Link siren</td>
<td>ON</td>
<td>S1: C-1076 S-593</td>
<td>Phone-Cloud</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: C-1023 S-613</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kwikset door lock</td>
<td>Lock</td>
<td>S1: C-639 S-511 S2: S-647 C-136</td>
<td>Phone-Cloud</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Unlock</td>
<td>S1: C-701 S-511 S2: S-647 C-136</td>
<td>Phone-Cloud</td>
<td>100</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</td>
</tr>
<tr>
<td></td>
<td>Back-to-station</td>
<td>S1: S-440 C-105 S-[1018-1024] C-105</td>
<td>Phone-Cloud</td>
<td>91</td>
</tr>
</tbody>
</table>
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
- Our corpus: 18 devices
- Public dataset Mon(IoT)r
- Extraction for 21 new devices
- Appliance: Universal Signatures

<table>
<thead>
<tr>
<th>Device</th>
<th>Event</th>
<th>Signature 1</th>
<th>Duration (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Echo Dot</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Amazon Echo Plus</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Amazon Echo Spot</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Google Home</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Harman Kardon Invoke</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Smart TV</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Pay TV</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>LG TV</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Rekai TV</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</td>
</tr>
<tr>
<td>Samsung TV</td>
<td>Voice</td>
<td>C-105-B-300</td>
<td>147.107,195</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

19
Universal Signatures

- Three communications
  - Two adversaries
    - WAN and Wi-Fi sniffer
- Different triggers
  - Local - Phone
  - Remote - Phone, and
  - Home Automation

<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>Plugs</td>
<td></td>
<td></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></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>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-593 S-7235 S-100</td>
<td></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>Light Bulbs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hue light bulb</td>
<td>ON</td>
<td>S1: S-[227-229] C-[857-859] C-365</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: S-[237-240] C-[895-899]</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-[1378-375]</td>
<td></td>
</tr>
<tr>
<td>TP-Link light bulb</td>
<td>ON</td>
<td>S1: S-[348-349] C-[399-400]</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>S1: S-[348-349] C-[418-419]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>S1: S-[348-442] C-[396-400]</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>S1: S-[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></td>
</tr>
<tr>
<td></td>
<td></td>
<td>S2: C-155</td>
<td></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: S-[989-1003] 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**
  - **Event type:** binary and non-binary
- **Same-vendor devices**

### Table of Signatures

<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></td>
<td>S2: C-592 S-1234 S-100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S1: PH-172 D-115</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-593 S-1235 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>S1: PH-258 D-305</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S1: PH-[240-242] D-[287-289]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S1: PH-737 D-287</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></td>
<td>S2: C-300 C-710 S-1412 S-88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S1: PH-219 D-103</td>
</tr>
<tr>
<td></td>
<td></td>
<td></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></td>
<td>S2: C-301 C-1412 S-[1405-1406] S-88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S1: PH-219 D-103</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-301 C-1413 S-[1406-1407] S-88</td>
</tr>
<tr>
<td>TP-Link white light bulb</td>
<td>KL-110</td>
<td>ON</td>
<td>S1: S-[414-415] C-[331-332]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-648 S-[1279-1280] S-88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S1: S-[414-415] C-[350-351]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-649 S-[1280-1281] S-88</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S1: S-[479-483] C-[339-332]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-[654-656] S-[1285-1286] 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PH-608 D-371 PH-97</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-1288 S-[1161-1162] S-100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>S1: PH-256 D-162 PH-624 D-256 PH-72 D-111</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PH-614 D-371 PH-97</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2: C-1289 S-[1162-1163] 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 ✓
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
      - 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]
        - C-592 S-1234 S-100
        - C-605 S-1213 S-100

2018

2019
PingPong Training

The PingPong System

Event Triggers → Device

Input

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

Input

Event Triggers → Device

Training

Data Collection → Network Trace

Toggle ON for TP-Link Plug

adb

tcpdump
PingPong Training

The PingPong System

Event Triggers → Device

Input

Training

Data Collection → Network Trace

Toggle ON for TP-Link Plug

adb

event

tcpdump

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

The PingPong System

Input
- Event Triggers
- Device

Training
- Data Collection
- Network Trace
- Trace Filtering

PCAP file
- C-123 S-456 ...
- 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 ...
- ...

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

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

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

Training Data

Event Triggers → Device

Network Trace → Trace Filtering

Data Collection → Training

Toggle ON for TP-Link Plug

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

The PingPong System
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

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

... C-129 S-123 ...

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

- TCP Conn.1 → C-556 S-1293
- TCP Conn.2 → C-238 S-826
- ... C-556 S-1293 ...
- ... C-129 S-123 ...

Training Data Collection

Trace Filtering

Network Trace

Event Triggers

Device
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 → C-238 S-826
TCP Conn.2 → C-129 S-123
TCP Conn.3 → C-129 S-123

Training Data Collection
Trace Filtering Network Trace
Event Triggers → Device

UCI
University of California, Irvine
PingPong Training

The PingPong System

Input

Event Triggers → Device

Training

Data Collection → Network Trace → Trace Filtering

Packet Pairs

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

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

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
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
PingPong Training

Pair Clustering

(a) TP-Link Plug

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

(a) TP-Link Plug
PingPong Training

Pair Clustering

(Pairs 1) C->S
● 556, 1293
f: 50

S->C

[238-240], [826-830]
f: 98

(a) TP-Link Plug

Signature Creation

1
C
556
1293
S

2
C
556
1293
S

Pair 1.1

... 50
C
556
S

Pair 1.50

1293
PingPong Training

Pair Clustering

Signature Creation

(a) TP-Link Plug
PingPong Training

Pair Clustering
- Pair 1: C→S, 556, 1293, f: 50
- S→C, [238-240], [826-830], f: 98

Signature Creation
- Sequence 1.1: C→S→C, Pair 1.1: 556
- Sequence 1.2: C→S→C, Pair 1.2: 1293
- Sequence 1.50: C→S→C, Pair 1.50: 1293

(a) TP-Link Plug

UCI University of California, Irvine
PingPong Training

Pair Clustering

- C→S
  - Pairs 1
  - 556, 1293
  - f: 50
- S→C
  - [230-240], [829-830]
  - f: 98

Sequences 1

(a) TP-Link Plug

Signature Creation

- Sequence 1.1
  - Pair 1.1
  - 556
  - 1293

- Pair 1.2
  - 556
  - 1293

- Pair 1.50
  - 556
  - 1293

UCI University of California, Irvine

C-556 S-1293
PingPong Training

(b) Arlo Camera
PingPong Training
PingPong Training

(b) Arlo Camera
PingPong Training

(b) Arlo Camera

UCI University of California, Irvine
PingPong Training
PingPong Training

Sequences 1

Pair 1.1
C 339
S 329

Pair 2.1
C 365
S 1067

Sequences 2

Pair 3.1
C 272
S 502

Pair 3.2
C 273
S 503

(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)

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

- Run detection
  - Same PCAP file
- Valid signature iff
  - $n$ detected events
  - $n$ triggered events
  - Matching timestamps
PingPong Detection

Signature

Arlo Camera

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

Signature

Network Trace

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

UCI University of California, Irvine
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet


... C-339
PingPong Detection

The PingPong System

Signature

Network Trace

Detection

Match Packet
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

Signature

Network Trace

Detection

Match Packet

Match Sequence

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–[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

Event 1

Matched Events

Event Match


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

The PingPong System

- Signature
- Network Trace
- Match Packet
- Match Sequence

Event Match

  C–[271–273] S–[499–505]
  C–[272–500]
PingPong Detection

The PingPong System

Detection

Signature

Network Trace

Match Packet

Match Sequence

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

Event 1 ... Event n

Matched Events

See paper for more detail
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