BehavIoT: Measuring Smart Home IoT Behavior Using Network-Inferred Behavior Models

Tianrui Hu, Daniel J. Dubois, David Choffnes
Background

Internet-enabled smart home
Background

Internet-enabled smart home

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet
Background

Internet-enabled smart home

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Google admits its new smart speaker was eavesdropping on users
Background

Internet-enabled smart home

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Google admits its new smart speaker was eavesdropping on users

Amazon Outage Shuts Down IoT Vacuums, Doorbells, Fridges, Even Home Locks
Background

- Diverse security, privacy, and safety issues
- Due to attacks, malfunctions, misconfigurations, etc.

- Internet-enabled smart home
- The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet
- Google admits its new smart speaker was eavesdropping on users
- Amazon Outage Shuts Down IoT Vacuums, Doorbells, Fridges, Even Home Locks
Why is it hard to model IoT behavior?
Why is it hard to model IoT behavior?

Diversity
Why is it hard to model IoT behavior?

Diversity

Opaqueness
Why is it hard to model IoT behavior?

Diversity

Opaqueness

Hard to fully understand
- what is normal device behavior
- how it changes over time
Why is it hard to model IoT behavior?

Diversity

Opaqueness

Hard to fully understand
- what is normal device behavior
- how it changes over time

Key observation: IoT reveals behavior via network traffic
Why is it hard to model IoT behavior?

Diversity

Opaqueness

Hard to fully understand
- what is normal device behavior
- how it changes over time

Key observation: IoT reveals behavior via network traffic

Open question: Can we model IoT behavior based on this traffic?
Motivation

- Predictable network traffic patterns
Motivation

- **Predictable** network traffic patterns

Network Traffic:

Time

Bytes
Motivation

- **Predictable** network traffic patterns

Network Traffic: Bytes vs. Time

Decompose into periodic patterns:

- Status update, heartbeats, etc.
Motivation

- Predictable network traffic patterns

\[ \text{periodic} \rightarrow \text{correlate with the actual functions} \]

Network Traffic:

- Motion Detected
- Doorbell Rings

Time → Bytes

\[ \leftarrow \text{Status update, heartbeats, etc.} \]

They often have temporal correlation
Motivation

- **Predictable** network traffic patterns
  - Periodic
  - Correlate with the actual functions

Network Traffic:

- Bytes
- Time

Decompose into:

- Status update, heartbeats, etc.
- They often have temporal correlation

- Relatively simple — having a limited set of functionalities and states.
Research Questions
Research Questions

RQ1: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

RQ2: How do we measure and characterize behavior deviations of a smart home system?
Our Approach - BehavIoT

1. Capture IoT devices’ encrypted network traffic
Our Approach - BehavIoT

1. **Capture** IoT devices' encrypted network traffic

2. **Characterize** individual device behavior
Our Approach - BehavIoT

1. Capture IoT devices’ encrypted network traffic
2. Characterize individual device behavior
3. Characterize smart home system behavior
Our Approach - BehavIoT

1. Capture IoT devices' encrypted network traffic
2. Characterize individual device behavior
3. Characterize smart home system behavior
4. Measure and quantify behavior deviation
Our Approach - BehavIoT

Key advantages of the approach

- works across a **wide range of IoT devices**.
- requires **no privileged access** to devices or APIs. Deployable on routers.
- models behaviors of both **individual devices and a smart home system**
Testbed & Datasets

49 devices from a wide range of categories
Testbed & Datasets

- Controlled interactions (4,230 experiments): Capture device behaviors of actual functions.

49 devices from a wide range of categories
Testbed & Datasets

- **Controlled interactions** (4,230 experiments): Capture device behaviors of actual functions.
- **Idle experiments** (5 days): Capture device periodic background behaviors.

49 devices from a wide range of categories
Testbed & Datasets

- **Controlled interactions** (4,230 experiments):
  Capture device behaviors of actual functions.

- **Idle experiments** (5 days):
  Capture device periodic background behaviors.

- **Routines** (16 routines, 24 hours):
  Capture smart home system behaviors.

49 devices from a wide range of categories
Testbed & Datasets

- **Controlled interactions** (4,230 experiments): Capture device behaviors of actual functions.
- **Idle experiments** (5 days): Capture device periodic background behaviors.
- **Routines** (16 routines, 24 hours): Capture smart home system behaviors.
- **Uncontrolled interactions** (3 months, 40 participants, IRB-approved): Measure behavior deviation over time.

49 devices from a wide range of categories
Research Questions

RQ1: How do we measure and characterize the behaviors of smart home system from their mostly encrypted network traffic?

RQ2: How do we measure and characterize behavior deviations of a smart home system?
Methods

Traffic Capture → Device Behavior Modeling → System Behavior Modeling → Behavior Deviation Measuring
Methods

→ periodic

Event Inference:
Classify traffic → events
Methods

→ periodic
→ correlate with device functionality

Event Inference:
Classify traffic → events

Traffic Capture → Device Behavior Modeling → System Behavior Modeling → Behavior Deviation Measuring

Periodic events
User events

Network traffic
Methods

→ periodic
→ correlate with device functionality

Event Inference:
Classify traffic → events
DFT + Autocorrelation
ML (Clustering & Random Forest)
Methods

→ periodic
→ correlate with device functionality

Event Inference:
Classify traffic → events
DFT + Autocorrelation
ML (Clustering & Random Forest)

Network traffic

Periodic events
User events
Unclassified traffic
Methods

→ periodic
→ correlate with device functionality

Event Inference:
Classify traffic → events
DFT + Autocorrelation
ML (Clustering & Random Forest)

Model generation:
Annotate with labels

Periodic events → Periodic models
User events → User-action models
Unclassified traffic

Traffic Capture → Device Behavior Modeling → System Behavior Modeling → Behavior Deviation Measuring
Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their network traffic?
The vast majority of IoT (mostly encrypted) traffic (99.3%) can be modeled.
Key Takeaways

**RQ1:** How do we measure and characterize the behaviors of smart home system from their network traffic?

The vast majority of IoT (mostly encrypted) traffic (99.3%) can be modeled.

The vast majority of IoT traffic (97.8%) is **periodic**.

A small portion of traffic (0.675%) cannot be modeled — most from devices running complex software.
Methods

Key insight: can be modeled as a finite state machine

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:15:10</td>
<td>Echo Spot Voice</td>
</tr>
<tr>
<td>09:15:12</td>
<td>TP-Link Plug On</td>
</tr>
<tr>
<td>09:16:13</td>
<td>Echo Spot Voice</td>
</tr>
<tr>
<td>09:16:15</td>
<td>TP-Link Plug Off</td>
</tr>
<tr>
<td>......</td>
<td></td>
</tr>
</tbody>
</table>
Methods

Key insight: can be modeled as a finite state machine

1. Combine temporally **correlated user events into traces**

09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
......
Methods

Key insight: can be modeled as a finite state machine

1. Combine temporally correlated user events into traces

```
09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
```

......
Methods

Key insight: can be modeled as a finite state machine

1. Combine temporally **correlated user events into traces**

2. Generate a **probabilistic finite state machine (PFSM) model from traces** using Synoptic [1]

   - State: user activity
   - Transition: probability

---

Methods

Key insight: can be modeled as a finite state machine

1. Combine temporally correlated user events into traces

2. Generate a probabilistic finite state machine (PFSM) model from traces using Synoptic [1]

- State: user activity
- Transition: probability

Key Takeaways

**RQ1**: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?
Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

- Capture both
  - programmed behaviors introduced by automations

Automation: turn on light if motion is detected
Key Takeaways

**RQ1:** How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

- Capture both
  - programmed behaviors introduced by automations
  - non-programmed behaviors introduced by human interactions

![Diagram showing automation and co-located motion sensors]
Research Questions

RQ1: How do we measure and characterize the behaviors of smart home system from their mostly encrypted network traffic?

RQ2: How do we measure and characterize behavior deviations of a smart home system?
Methods

Identify significant changes in behavior
Methods

Identify significant changes in behavior

- Deviation metrics that quantify the amount of behavior change
- Thresholds to capture statistically significant deviations
Methods

Identify significant changes in behavior

- **Deviation metrics** that quantify the amount of behavior change
- Thresholds to capture **statistically significant deviations**
Methods

Identify significant changes in behavior

- **Deviation metrics** that quantify the amount of behavior change
- Thresholds to capture statistically significant deviations
Methods

Identify significant changes in behavior

- Deviation metrics that quantify the amount of behavior change
- Thresholds to capture statistically significant deviations
Key Takeaways

RQ2: How do we measure and characterize behavior deviations of a smart home system?

- Our metrics identify significant deviations from real-world examples
Key Takeaways

RQ2: How do we measure and characterize behavior deviations of a smart home system?

● Our metrics identify significant deviations from real-world examples
Key Takeaways

- Our metrics identify significant deviations from real-world examples

RQ2: How do we measure and characterize behavior deviations of a smart home system?
Key Takeaways

- Our metrics identify significant deviations from real-world examples
  - Device malfunctions and misconfiguration
  - Misactivation
  - Network outages
  - Change of device positions
  - Change of user habits, etc.

RQ2: How do we measure and characterize behavior deviations of a smart home system?
Behavior Model Applications

- Create IoT profiles (MUD RFC8520) and verify compliance to existing profiles.
- Behavior triage to help with auditing such as security, regulatory, and privacy.
- Allocate attention to significant behavior deviation
Conclusion

● **Characterize IoT device and system behaviors:**
  ○ Most smart home devices are *amenable to modeling* through network traffic.
  ○ 97% of traffic is periodic; 2.33% is due to user actions; 0.68% is unmodelable.

● **Measure behavior deviation over time:**
  ○ Detect and quantify a range of behavior deviations.
  ○ Behavior was relatively stable during a longitudinal study

● **BehavIoT benefits:** creating IoT profiles, triage behaviors and deviation

Thank you! Datasets and code available here:
https://moniotrlab.khoury.northeastern.edu/behaviot/