IoTDI 2020

CHARACTERIZING SMART HOME IOT TRAFFIC IN THE WILD

M. Hammad Mazhar
@HmdMazhar

Zubair Shafiq
@zubair_shafiq

The University of Iowa

Smart Home IoT – A Target

Smart Home IoT – A Target

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Smart Home IoT – A Target

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

The New York Times

Somebody's Watching: Hackers Breach Ring Home Security Cameras

Smart Home IoT – A Target

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

The New York Times

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

Somebody's Watching: Hackers Breach Ring Home Security Cameras

Prior Work – Limitations and Challenges

Prior Work – Limitations and Challenges

- ***Fragmentation***

Prior Work – Limitations and Challenges

- ***Fragmentation***
  - Smart TVs [PETS '20], Alexa [AsiaCCS '19].

Prior Work – Limitations and Challenges

- *Fragmentation*
  - Smart TVs [PETS '20], Alexa [AsiaCCS '19].
- *Non-representative*

Prior Work – Limitations and Challenges

- *Fragmentation*
  - Smart TVs [PETS '20], Alexa [AsiaCCS '19].
- *Non-representative*
  - Testbed environments [IMC '19, S&P '19].

Prior Work – Limitations and Challenges

- *Fragmentation*
  - Smart TVs [PETS '20], Alexa [AsiaCCS '19].
- *Non-representative*
  - Testbed environments [IMC '19, S&P '19].
- *Scale*

Prior Work – Limitations and Challenges

- *Fragmentation*
  - Smart TVs [PETS '20], Alexa [AsiaCCS '19].
- *Non-representative*
  - Testbed environments [IMC '19, S&P '19].
- *Scale*
  - Limited number of devices [PETS '17, PETS '19].

Our Contributions

Our Contributions

- ***Fragmentation***
  - Leverage the ***home gateway*** as the vantage point.

Our Contributions

- *Fragmentation*
  - Leverage the ***home gateway*** as the vantage point.
- *Non-representative*
  - Study smart home IoT behavior ***in the wild***.

Our Contributions

- *Fragmentation*
  - Leverage the ***home gateway*** as the vantage point.
- *Non-representative*
  - Study smart home IoT behavior ***in the wild***.
- *Scale*
  - Study ***over 200*** homes.

Data Collection - Instrumentation

Data Collection - Instrumentation

- Collect Netflow-style flow records at WAN interface of home gateway.

Data Collection - Instrumentation

- Collect Netflow-style flow records at WAN interface of home gateway.

- Device identification using DHCP, SSDP and UPnP traffic.

Data Collection - Instrumentation

- Collect Netflow-style flow records at WAN interface of home gateway.
- Device identification using DHCP, SSDP and UPnP traffic.
- *Anonymized* data collection (no public IP addresses or device MAC addresses) with user consent.

Data Statistics

Data Statistics

- 1230 devices observed across 220 homes over 19-day period in February 2018.

Data Statistics

- 1230 devices observed across 220 homes over 19-day period in February 2018.
  - 240 IoT, 958 non-IoT.

Data Statistics

- 1230 devices observed across 220 homes over 19-day period in February 2018.
  - 240 IoT, 958 non-IoT.

- 66 unique IoT device types (make and model) across 8 categories.

Data Statistics

- 1230 devices observed across 220 homes over 19-day period in February 2018.
  - 240 IoT, 958 non-IoT.

- 66 unique IoT device types (make and model) across 8 categories.
  - Smart TVs, Cameras, Speakers, Assistants, Game Consoles, Home Automation, Work Appliances and Health/Wearables.

Characterizing Smart Home IoT traffic

Characterizing Smart Home IoT traffic

- Three dimensions:

Characterizing Smart Home IoT traffic

- Three dimensions:

Volumetric	Temporal	Destination

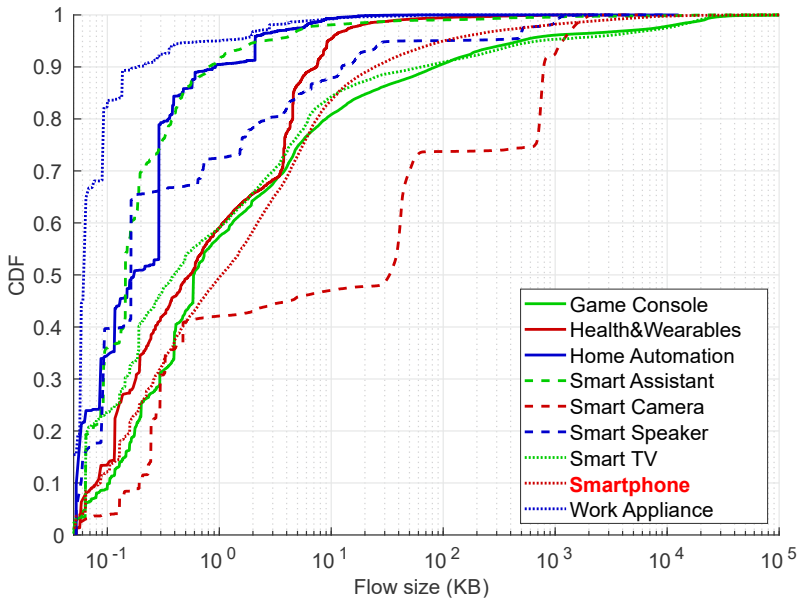
Characterizing Smart Home IoT traffic

- Three dimensions:

Volumetric

Temporal

Destination



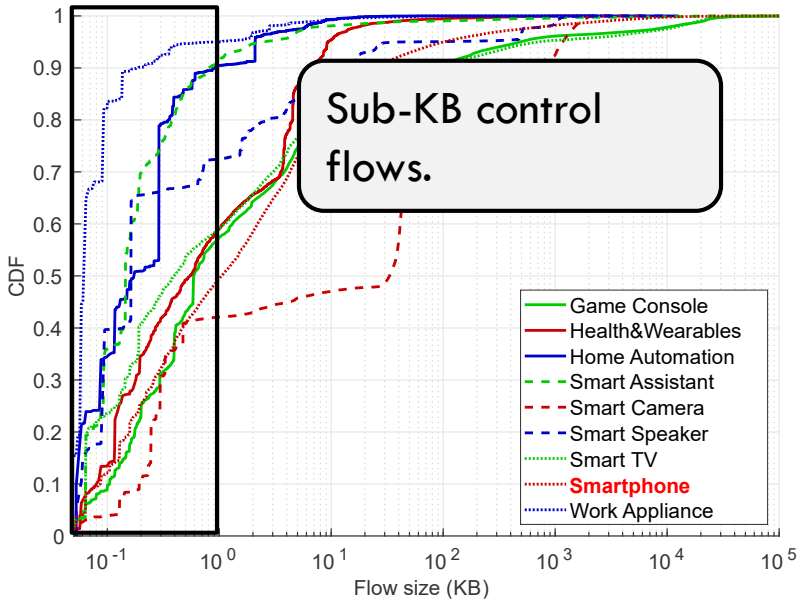
Characterizing Smart Home IoT traffic

- Three dimensions:

Volumetric

Temporal

Destination



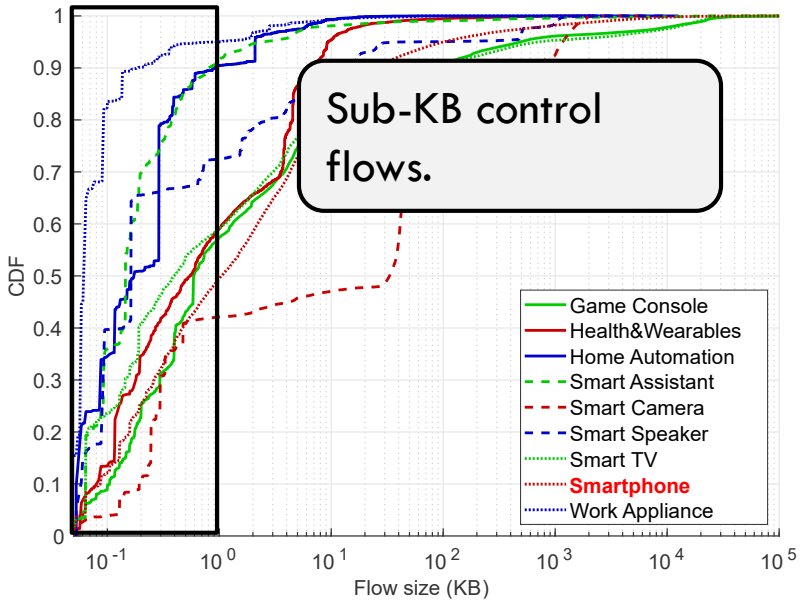
Characterizing Smart Home IoT traffic

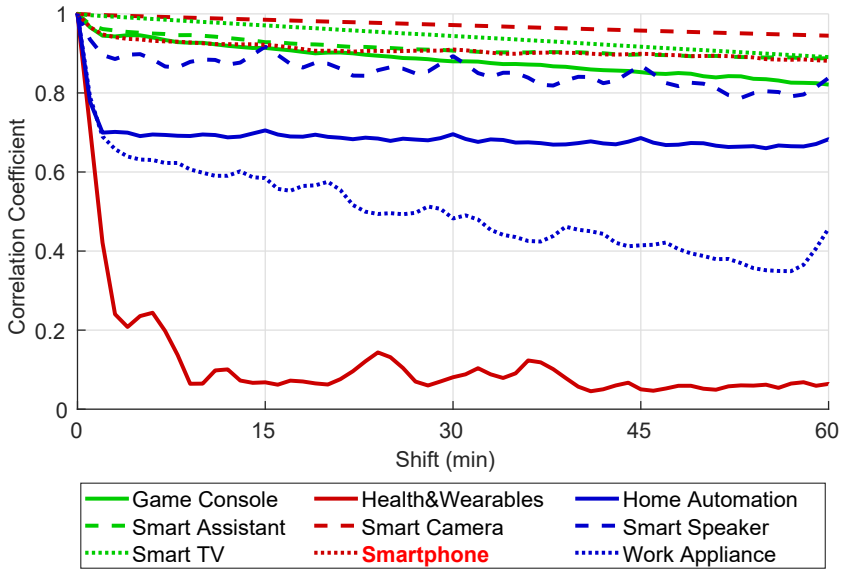
- Three dimensions:

Volumetric

Temporal

Destination

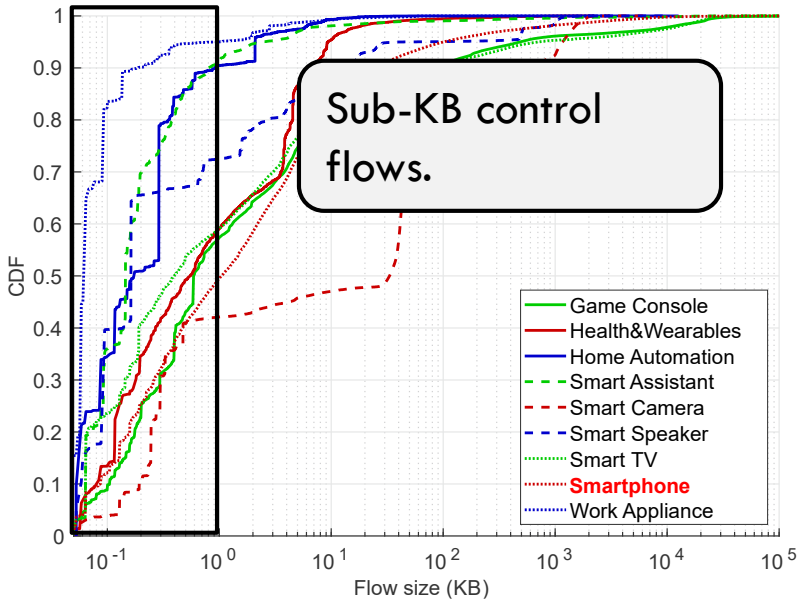




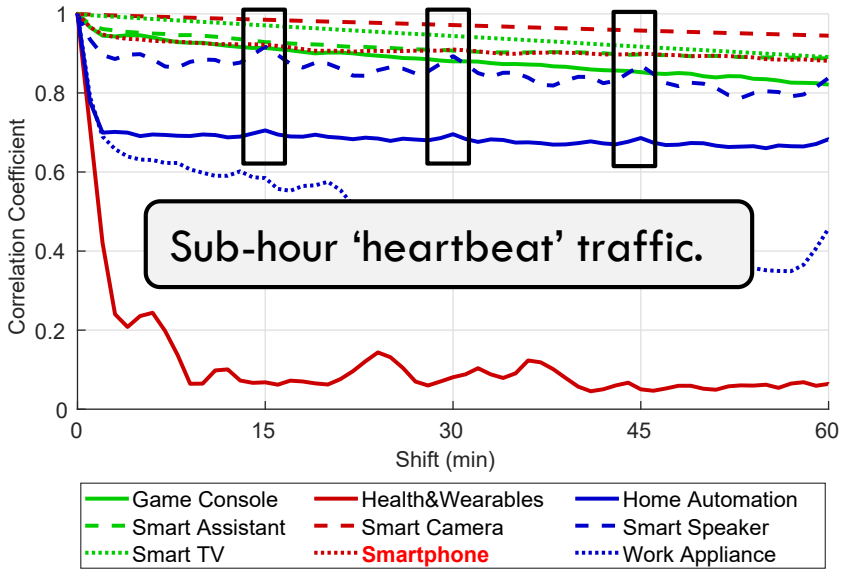
Characterizing Smart Home IoT traffic

- Three dimensions:

Volumetric



Temporal

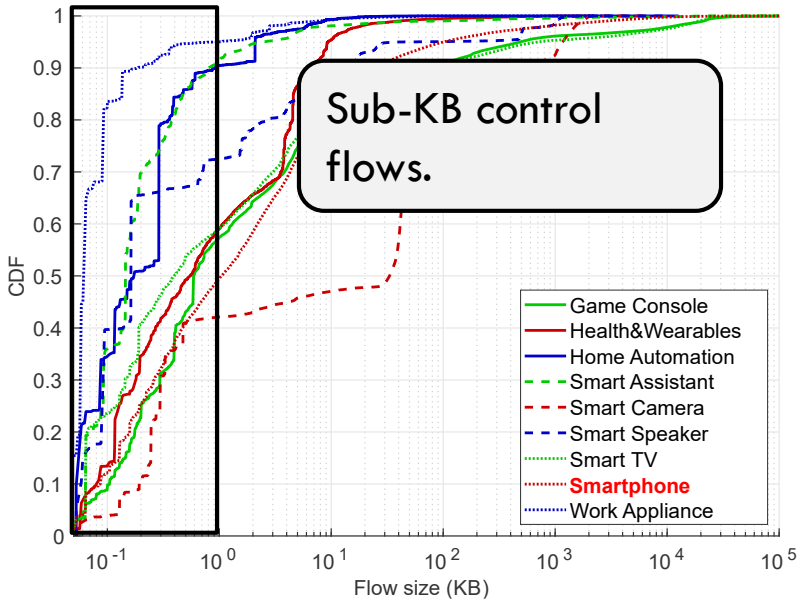


Destination

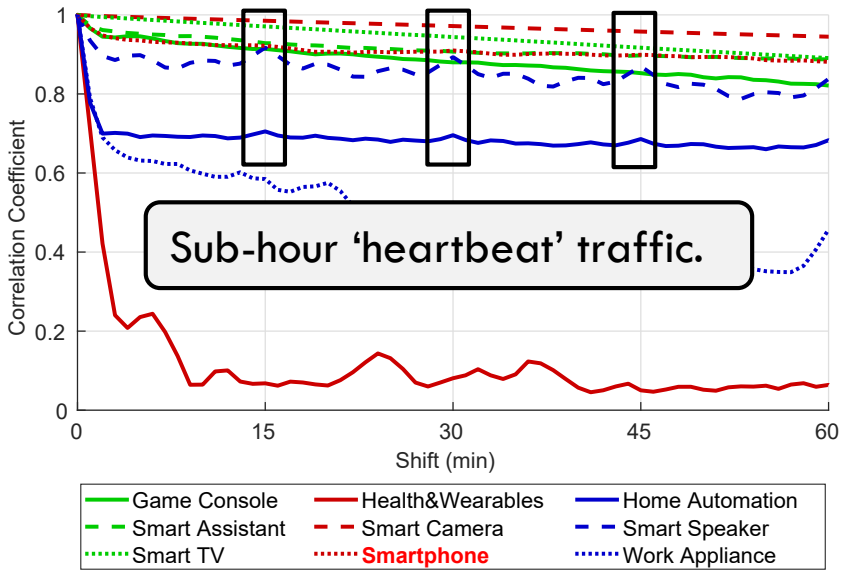
Characterizing Smart Home IoT traffic

- Three dimensions:

Volumetric



Temporal



Destination

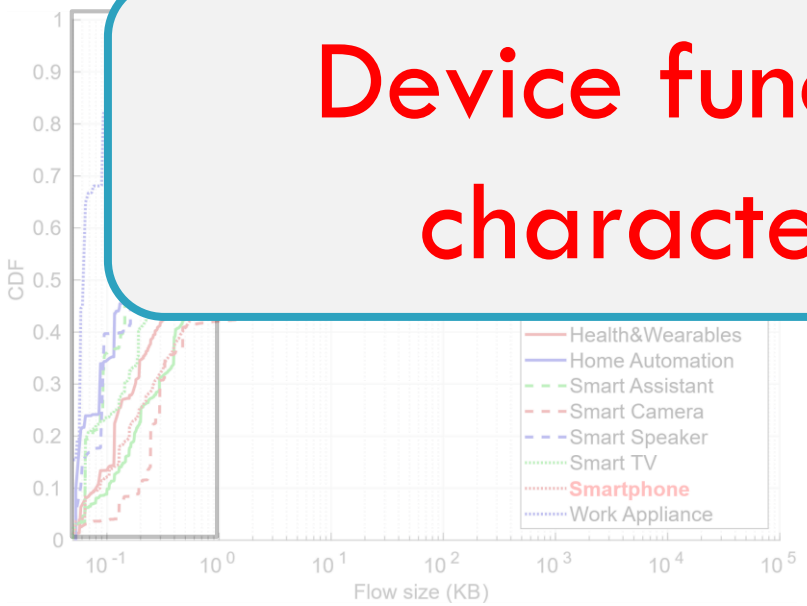
70-90% of traffic to Amazon, Google owned AS (higher backend centralization compared to 31% of overall Web).

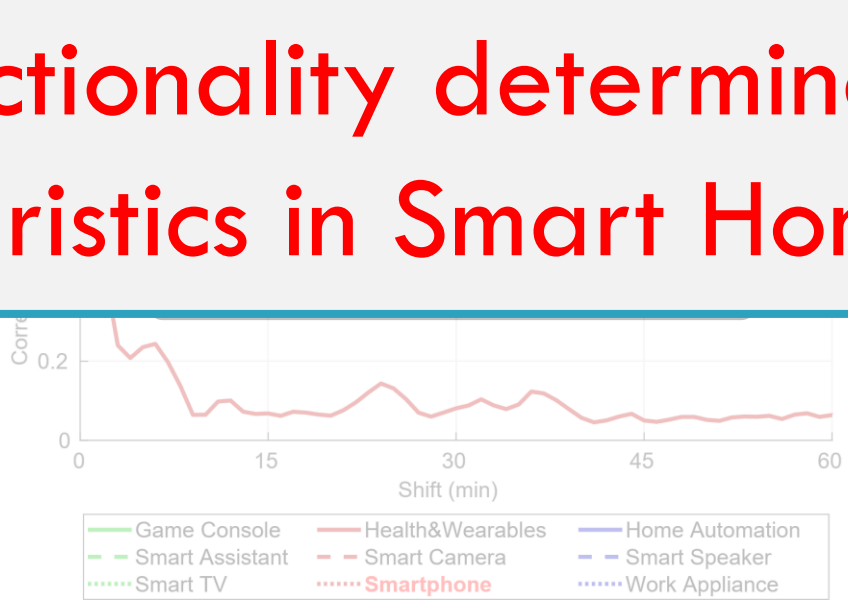
Characterizing Smart Home IoT traffic

- Three dimensions:

Volumetric | Temporal | Destination

Device functionality determines traffic characteristics in Smart Home IoT.





backend centralization compared to 31% of overall Web).

Security/Privacy Issues in Smart Home IoT

Security/Privacy Issues in Smart Home IoT

- Highlight current issues and their implications.

Security/Privacy Issues in Smart Home IoT

- Highlight current issues and their implications.
- 4 case studies:
  - **Security via Access Control.**
  - **Advertising/Tracking.**
  - Unencrypted Traffic – Devices vulnerable to HTTP snooping.
  - Use of public DNS services – use of Google DNS prevalent.

Security/Privacy Issues in Smart Home IoT

- Highlight current issues and their implications.
- 4 case studies:
  - **Security via Access Control.**
  - **Advertising/Tracking.**
  - Unencrypted Traffic – Devices vulnerable to HTTP snooping.
  - Use of public DNS services – use of Google DNS prevalent.

Securing Smart Home IoT via Access Control

Securing Smart Home IoT via Access Control

- Prior work recommends some form of Internet Access Control for smart home IoT.

Securing Smart Home IoT via Access Control

- Prior work recommends some form of Internet Access Control for smart home IoT.
- Manufacturer Usage Description (MUD – RFC 8520) by device manufacturers.

Securing Smart Home IoT via Access Control

- Prior work recommends some form of Internet Access Control for smart home IoT.
- Manufacturer Usage Description (MUD – RFC 8520) by device manufacturers.
- Research tools to build MUDs based on device traffic – MUDgee (IoTS&P '18).

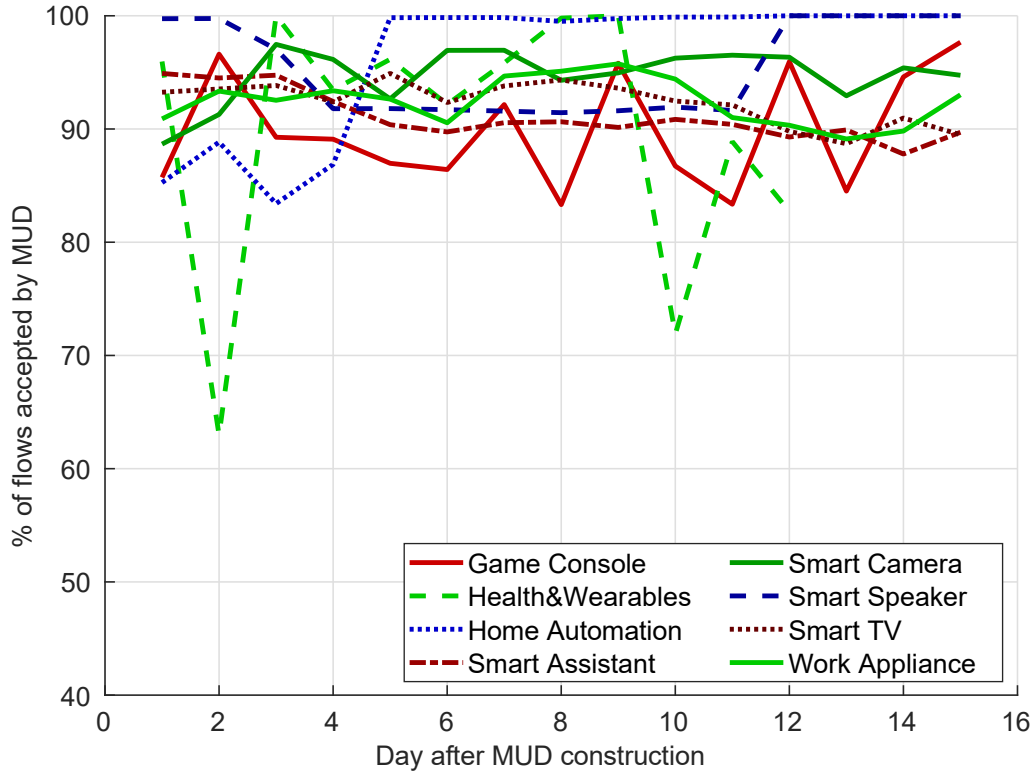
Securing Smart Home IoT via Access Control

Securing Smart Home IoT via Access Control

- First 72 hours of traffic to build MUD, then test for acceptance.

Securing Smart Home IoT via Access Control

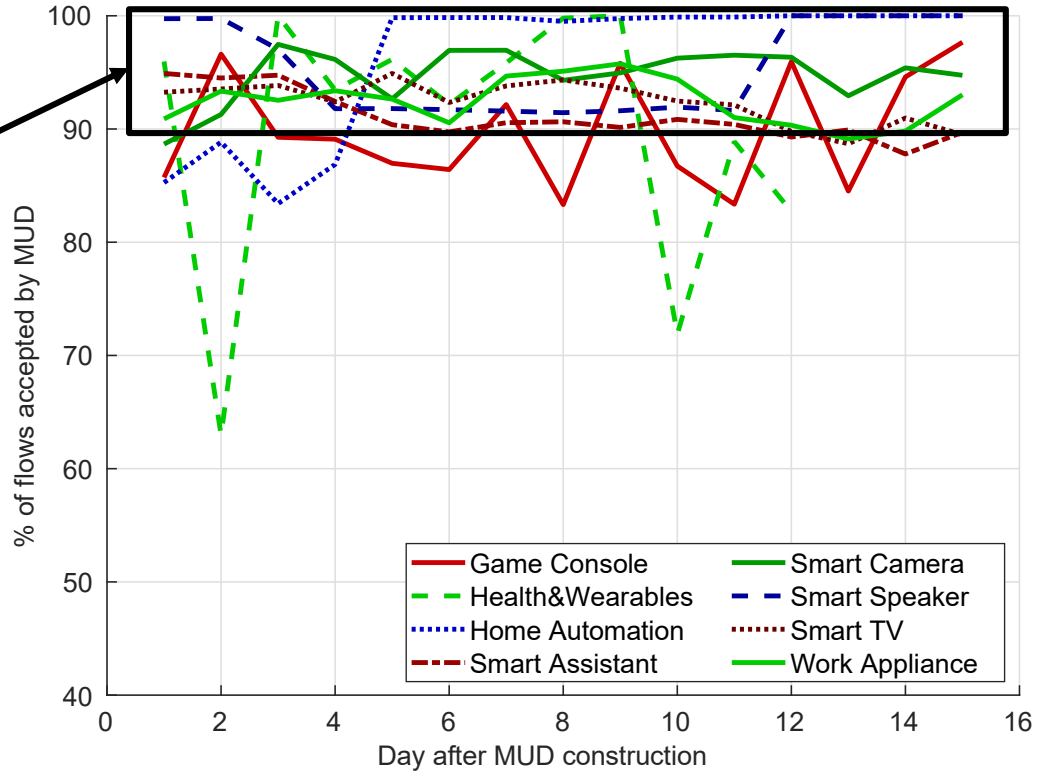
- First 72 hours of traffic to build MUD, then test for acceptance.



Securing Smart Home IoT via Access Control

- First 72 hours of traffic to build MUD, then test for acceptance.

High acceptance rates for MUD-based ACL

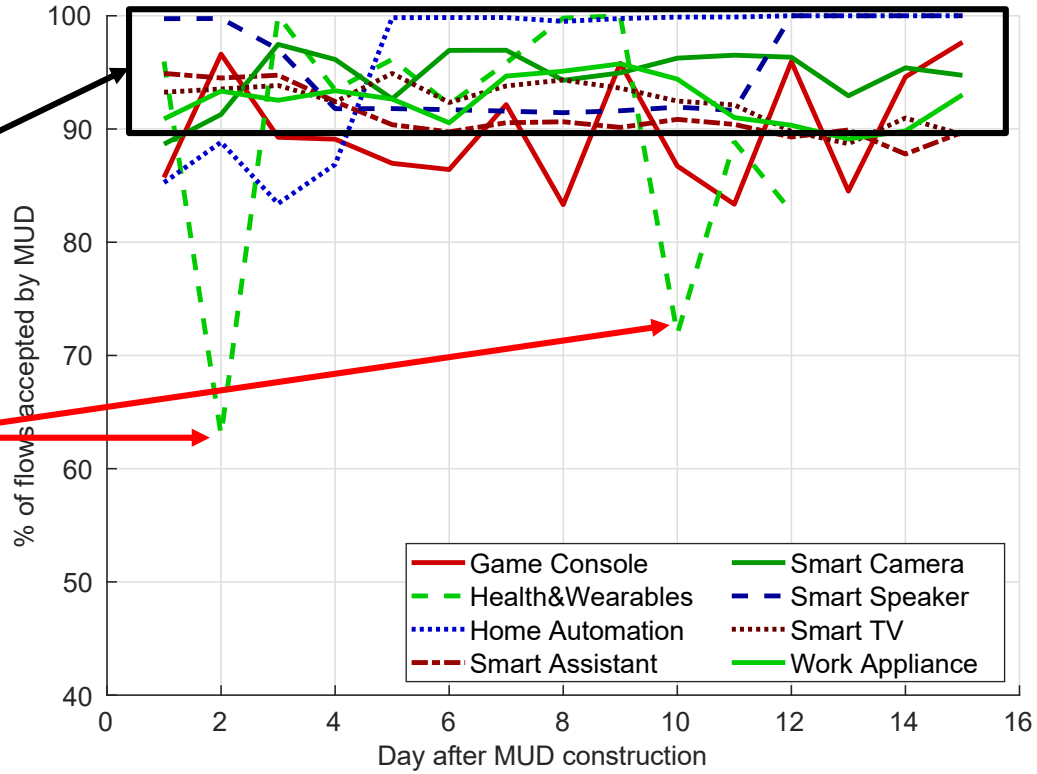


Securing Smart Home IoT via Access Control

- First 72 hours of traffic to build MUD, then test for acceptance.

High acceptance rates for MUD-based ACL

Drops due to unseen traffic

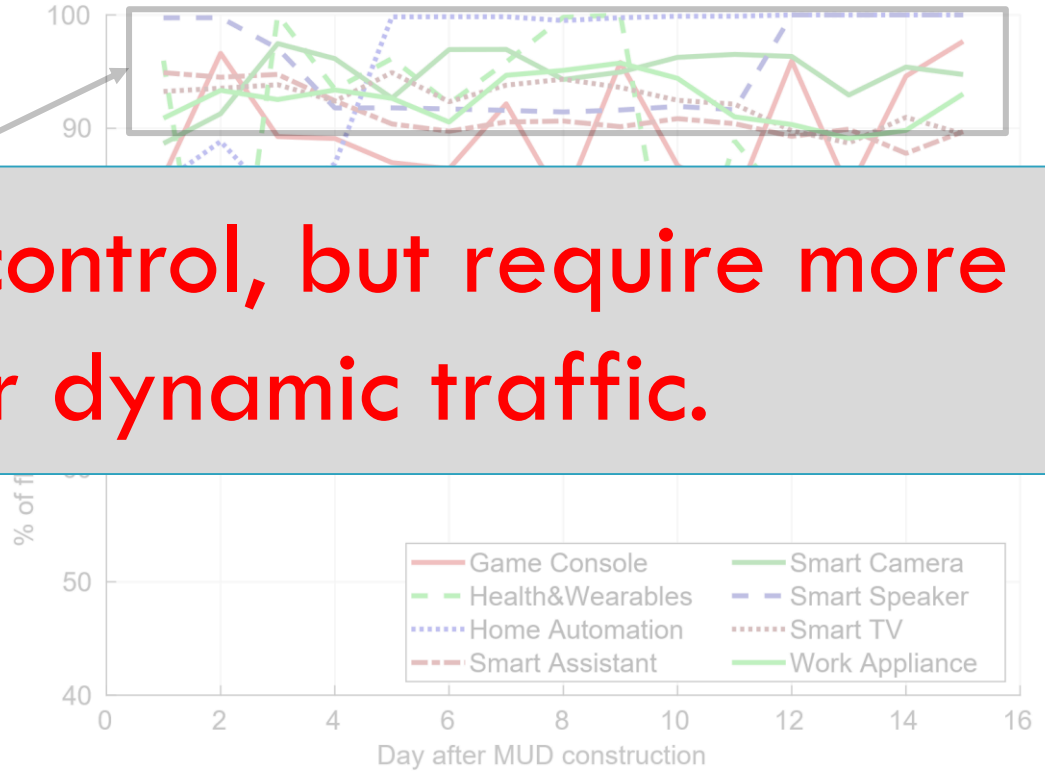


Securing Smart Home IoT via Access Control

- First 72 hours of traffic to build MUD, then test for acceptance.

High acceptance rates

traffic



MUDs can help in access control, but require more work to account for dynamic traffic.

Security/Privacy Issues in Smart Home IoT

- Highlight current issues and their implications.
- 4 case studies:
  - **Security via Access Control** – Feasible, account for dynamic traffic
  - **Advertising/Tracking**
  - Unencrypted Traffic – Devices vulnerable to HTTP snooping.
  - Use of public DNS services – use of Google DNS prevalent.

Security/Privacy Issues in Smart Home IoT

- Highlight current issues and their implications.
- 4 case studies:
  - **Security via Access Control** – Feasible, account for dynamic traffic
  - **Advertising/Tracking**
  - Unencrypted Traffic – Devices vulnerable to HTTP snooping.
  - Use of public DNS services – use of Google DNS prevalent.

Advertising/Tracking in Smart Home IoT

Advertising/Tracking in Smart Home IoT

- Detect ad/tracking hosts using Pi-Hole's block lists.

Advertising/Tracking in Smart Home IoT

- Detect ad/tracking hosts using Pi-Hole's block lists.

- 5.9% of Smart TVs unique hosts were ads/tracking, followed by 3.1% of Game Consoles and 2.9% Smart Assistants.

Advertising/Tracking in Smart Home IoT

- Detect ad/tracking hosts using Pi-Hole's block lists.
- 5.9% of Smart TVs unique hosts were ads/tracking, followed by 3.1% of Game Consoles and 2.9% Smart Assistants.
- DoubleClick and Google Syndication domains prominent.

Advertising/Tracking in Smart Home IoT

- Detect ad/tracking hosts using Pi-Hole's block lists.

Online Tracking has reached smart home IoT and requires more study into its effects.

- DoubleClick and Google Syndication domains prominent.

Security/Privacy Issues in Smart Home IoT

- Highlight current issues and their implications.
- 4 case studies:
  - **Security via Access Control** – Feasible, account for dynamic traffic
  - **Advertising/Tracking** – Present in certain devices, major players.
  - Unencrypted Traffic – Devices vulnerable to HTTP snooping.
  - Use of public DNS services – use of Google DNS prevalent.

Conclusions and Implications

Conclusions and Implications

- Device functionality influences traffic behavior.
  - Device identification, activity identification.

Conclusions and Implications

- Device functionality influences traffic behavior.
  - Device identification, activity identification.
- Smart Home IoT backend centralization.
  - Market monopolization, surveillance, single point of failure.

Conclusions and Implications

- Device functionality influences traffic behavior.
  - Device identification, activity identification.
- Smart Home IoT backend centralization.
  - Market monopolization, surveillance, single point of failure.
- Advertising and Tracking in Smart Home IoT.
  - Requires more study, solutions catered to smart home IoT.

Questions

- Twitter: @HmdMazhar
- Email: muhammadhammad-mazhar@uiowa.edu
- Website: cs.uiowa.edu/~mmazhar