Your Smart Home Exchanged 3M Messages: Defining and Analyzing Smart Device Passive Mode

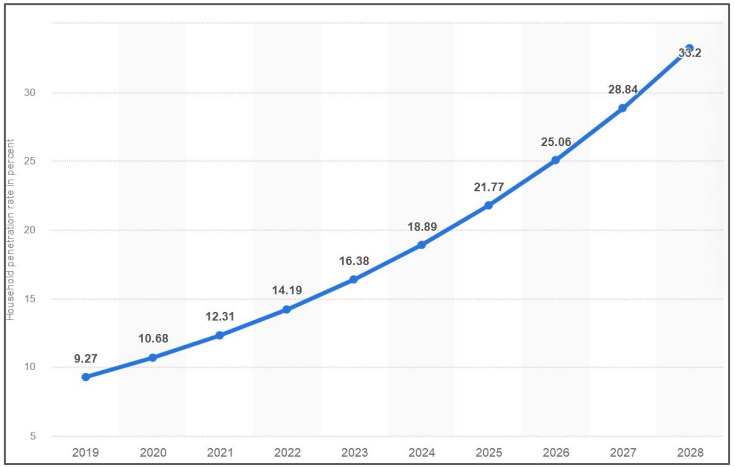
Christian Badolato[1], Kaur Kullman[1], Nikolaos Papadakis[2], Manav Bhatt[1], Georgios Bouloukakis[2], Don Engel[1], Roberto Yus[1]

[1] University of Maryland, Baltimore County

[2] Télécom SudParis, IP Paris

Internet of Things (IoT) in the Smart Home

- Adoption of smart home technology has doubled since 2019[1]
  - 70 million U.S. homes in 2024[2]
  - 1/3rd of households predicted to have some form of smart home IoT by 2028



(Image credit: Statista)

[1]Statista, " Penetration rate of the smart homes market worldwide from 2019 to 2028" 2025. https://www.statista.com/forecasts/887636/penetration-rate-of-smart-homes-in-the-world
[2]Oberlo.com, "US Smart Home Statistics (2019–2028)," 2024. https://www.oberlo.com/statistics/smart-home-statistics

Smart Home IoT Privacy

- Protecting smart home users' privacy is increasingly important
  - Even fully encrypted traffic can reveal sensitive information[1]

[1]Y. Wan et al., "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," INFOCOM, 2022.
[2]D. Dubois et al., "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," PoPETs, 2020.

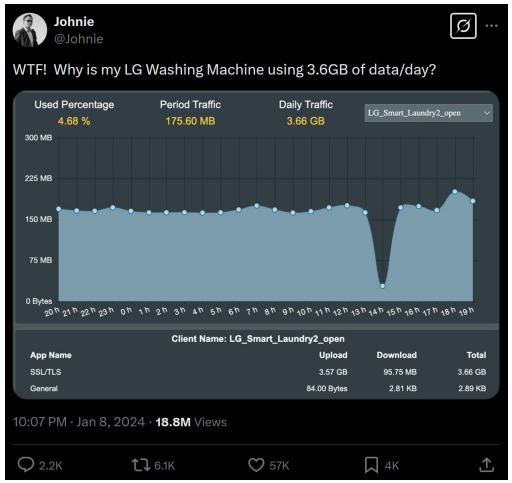
Smart Home IoT Privacy

- Protecting smart home users' privacy is increasingly important
  - Even fully encrypted traffic can reveal sensitive information[1]
- The "non-active" behavior of smart home devices is a topic of interest[2]

[1]Y. Wan et al., "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," INFOCOM, 2022.
[2]D. Dubois et al., "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," PoPETs, 2020.

Smart Home IoT Privacy

- Protecting smart home users' privacy is increasingly important
  - Even fully encrypted traffic can reveal sensitive information[1]
- The "non-active" behavior of smart home devices is a topic of interest[2]

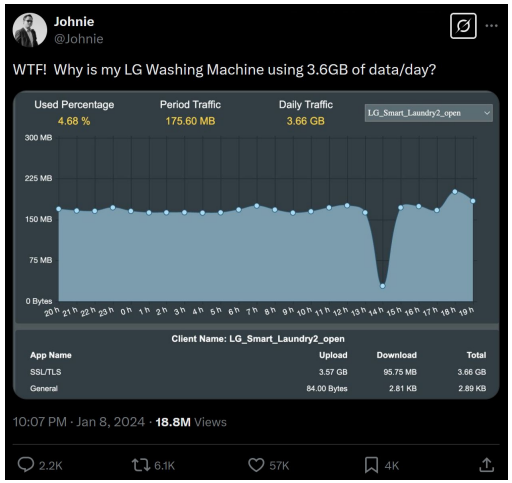


(Image credit: Johnie/X)

[1]Y. Wan et al., "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," INFOCOM, 2022.
[2]D. Dubois et al., "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," PoPETs, 2020.

Smart Home IoT Privacy

- Protecting smart home users' privacy is increasingly important
  - Even fully encrypted traffic can reveal sensitive information[1]
- The "non-active" behavior smart home devices is topic of interest for privacy[2]

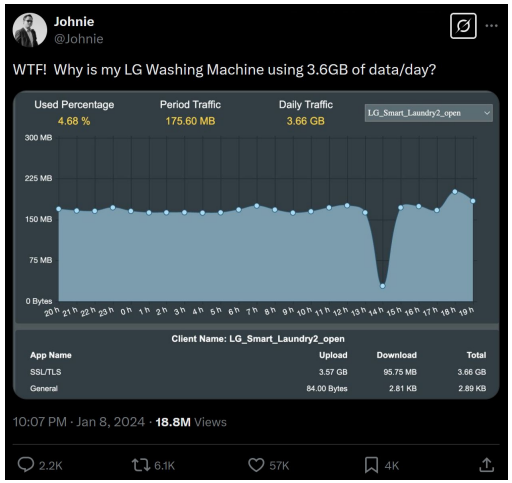


(Image credit: Johnie/X)

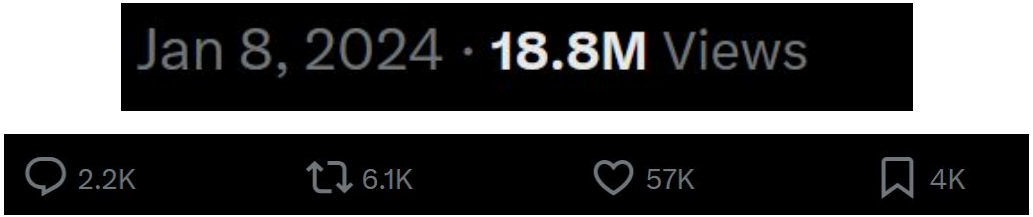
[1]Y. Wan et al., "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," INFOCOM, 2022.
[2]D. Dubois et al., "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," PoPETs, 2020.

Smart Home IoT Privacy

- Protecting smart home users' privacy is increasingly important
  - Even fully encrypted traffic can reveal sensitive information[1]
- The "non-active" behavior of smart home devices is a topic of interest[2]



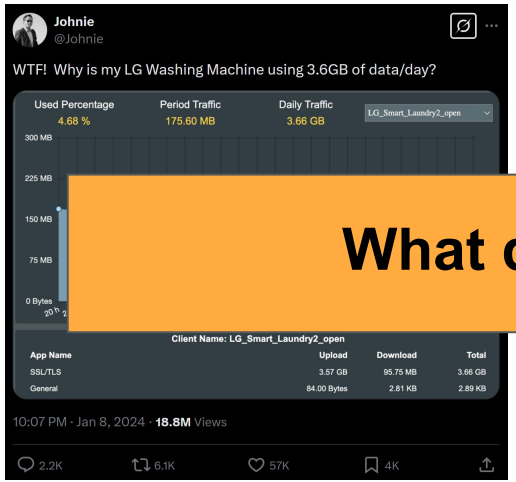
(Image credit: Johnie/X)



[1]Y. Wan et al., "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," INFOCOM, 2022.
[2]D. Dubois et al., "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," PoPETs, 2020.

Smart Home IoT Privacy

- Protecting smart home users' privacy is increasingly important
  - Even fully encrypted traffic can reveal sensitive information[1]
- The "non-active" behavior of smart home devices is a topic of interest[2]



What does "non-active" mean?

(Image credit: Johnie/X)

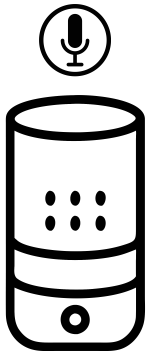
[1]Y. Wan et al., "IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes," INFOCOM, 2022.
[2]D. Dubois et al., "When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers," PoPETs, 2020.

Idle Smart Devices

Devices are often considered “idle” when not actively performing functions or processing commands, but are ready to respond to triggers

Idle Smart Devices

Devices are often considered “idle” when not actively performing functions or processing commands, but are ready to respond to triggers

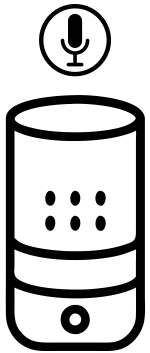


Smart speaker
waiting for command phrase

The Problem with “Idle”

Devices are often considered “idle” when not actively performing functions or processing commands, but are ready to respond to triggers

…but this is not granular enough to understand non-active device behaviors!

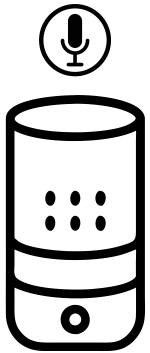


Smart speaker
waiting for command phrase

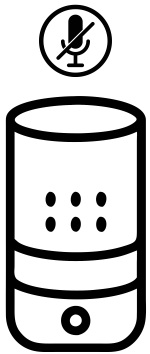
The Problem with “Idle”

Devices are often considered “idle” when not actively performing functions or processing commands, but are ready to respond to triggers

…but this is not granular enough to understand non-active device behaviors!



Smart speaker
waiting for command phrase

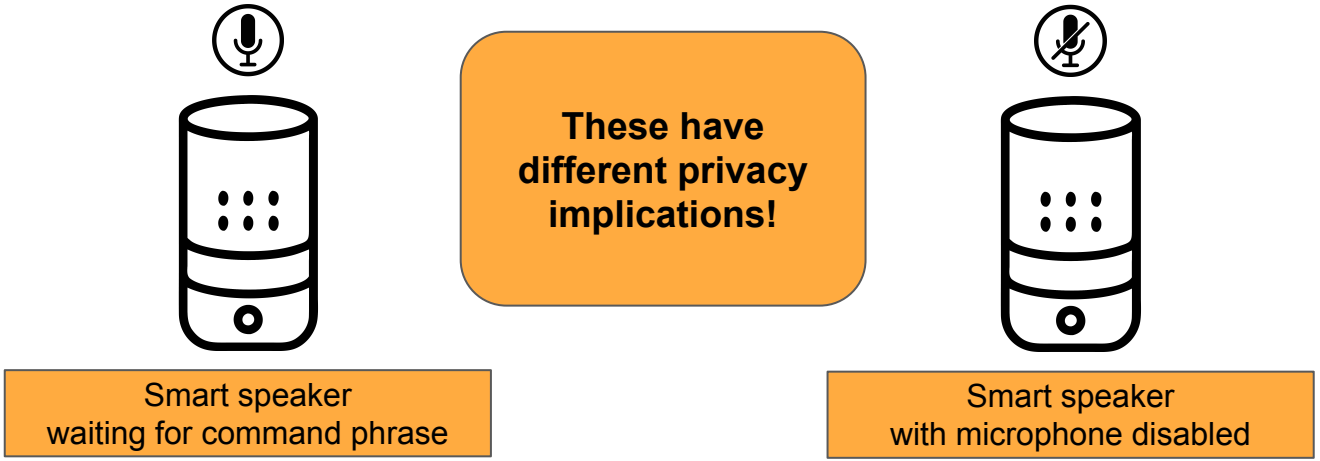


Smart speaker
with microphone disabled

The Problem with “Idle”

Devices are often considered “idle” when not actively performing functions or processing commands, but are ready to respond to triggers

…but this is not granular enough to understand non-active device behaviors!



Why is this a Problem?

Why is this a Problem?

Requires users be familiar with each individual device's privacy considerations

Why is this a Problem?

Requires users be familiar with each individual device's privacy considerations

Manufacturer-defined "privacy" modes vary

Why is this a Problem?

Requires users be familiar with each individual device's privacy considerations

Manufacturer-defined "privacy" modes vary

Hinders the ability to compare non-active behaviors

Why is this a Problem?

- **Requires users be familiar with each individual device's privacy considerations**
- **Manufacturer-defined "privacy" modes vary**
- **Hinders the ability to compare non-active behaviors**
- **Users may wish to behave differently when being observed**

Why is this a Problem?

Requi

Hinders

s vary

Users may wish to behave differently when being observed

S. Harding., “Everything you say to your Echo will be sent to Amazon starting on March 28,” arstechnica.com, 2025.

Introducing “Passive” Mode

We propose a new “passive” mode designation for smart home IoT devices to facilitate clear expectations of device behaviors with respect to privacy

Introducing “Passive” Mode

We propose a new “passive” mode designation for smart home IoT devices to facilitate clear expectations of device behaviors with respect to privacy

A device is considered to be in *passive mode* if either:

(1) The device is not actively performing its *primary* function(s), OR
(2) All data collection and reporting features of the device are disabled

Introducing “Passive” Mode

A device is considered to be in *passive mode* if either:

(1) The device is not actively performing its *primary* function(s), OR
(2) All data collection and reporting features of the device are disabled

This definition:

- Supports comparability w.r.t. privacy
- Understandable from a privacy-conscious end user’s perspective
- Ensures similar devices have equivalent passive modes
- Is robust to future device types

Determining Device-Specific Passive Modes

1. Constructed a two-tiered categorization based on an existing taxonomy[1]

TWO TIER CATEGORIZATION OF SMART HOME IOT DEVICES.

Category	Subcategory	Passive Mode Def.
Entertainment and Media	Smart TVs	A/V Presentation off
	Speakers and Audio	
	VR Devices	
	Streaming Devices	Media streaming not active
Ambient Sensors	Environmental	Environment sensing disabled
	Occupancy	
Security and Monitoring	Outdoor Cameras	Camera off AND Microphone off AND Motion sensor off
	Indoor Cameras	
	Doorbells	
	Locks and Keypads	(Prox. sensing disabled AND No command processing) OR Data monitoring disabled
	Alarms and Notifiers	No notifications active
	Hazard Sensors	Environment sensing disabled
	Contact Sensors	
	Security Hub	Data monitoring disabled AND No command processing
Lighting	Outdoor Lighting	Actuator off OR Data monitoring disabled
	Indoor Lighting	
	Lighting Control	No command processing
	Lighting Hub	Data monitoring disabled AND No command processing
Wardrobe and Hygiene	Hygiene Tools	Data monitoring disabled AND Main device purpose not active
	Clothing Storage	
	Bathing	
	Toilets	User not detected OR Data monitoring disabled
	Mirrors	A/V Presentation off
Wearables	Accessories	(Environment sensing disabled AND Health sensing disabled AND Smartphone connection not active) OR Device not worn
	Clothing	(Environment sensing disabled AND Health sensing disabled) OR Device not worn
	Glasses	A/V Presentation off OR Device not worn
Fitness	*N/A*	Main device purpose not active
Power and Energy	Switches	No command processing
	Plugs and Outlets	Actuator off OR Data monitoring disabled
	Energy Meters	Data monitoring disabled
Cleaning and Sanitation	Vacuum/Mop Robots	Main device purpose not active
	Trash Disposal	No command processing
	Laundry	Main device purpose not active OR Data monitoring disabled
Meal and Food	Ranges	Main device purpose not active OR Data monitoring disabled
	Dishwashers	
	Small Appliances	
	Refrigerators	A/V Presentation off OR Data monitoring disabled
Sleep	Sleep Trackers	Health sensing disabled OR User not detected
	Beds and Bedding	
	Alarm Clocks	No notifications active AND A/V Presentation off
Simple Actuators	*N/A*	Main device purpose not active AND No command processing
Gardening and Property Maintenance	Lawn Care Robots	Main device purpose not active
	Irrigation	Main device purpose not active OR Data monitoring disabled
	Weather Sensor	Environment sensing disabled
	Planters	Data monitoring disabled
HVAC and Water	Thermostats	No command processing AND Data monitoring disabled
	Water Meters	Data monitoring disabled
	Standalone Heating	Main device purpose not active OR Data monitoring disabled
	Standalone Cooling	
Hubs and Assistants	Voice Assistants	Microphone off AND Data processing not active
	IoT Protocol Hubs	No command processing AND Data monitoring disabled
	Status Displays	A/V Presentation off
Pet	Food/Water Bowls	Data monitoring disabled AND Main device purpose not active
	Waste management	Data monitoring disabled OR User not detected

[1]M. Schiefer, “Smart Home Definition and Security Threats,” IEE IMF, 2015.

Determining Device-Specific Passive Modes

1. Constructed a two-tiered categorization based on an existing taxonomy[1]

TWO TIER CATEGORIZATION OF SMART HOME IOT DEVICES.

Category	Subcategory	Passive Mode Def.
Entertainment and Media	Smart TVs	A/V Presentation off
	Speakers and Audio	
	VR Devices	
	Streaming Devices	Media streaming not active
Ambient Sensors	Environmental	Environment sensing disabled
	Occupancy	
Security and Monitoring	Outdoor Cameras	Camera off AND Microphone off AND Motion sensor off
	Indoor Cameras	
	Doorbells	
	Locks and Keypads	(Prox. sensing disabled AND No command processing) OR Data monitoring disabled
	Alarms and Notifiers	No notifications active
	Hazard Sensors	Environment sensing disabled
	Contact Sensors	
	Security Hub	Data monitoring disabled AND No command processing
Lighting	Outdoor Lighting	Actuator off OR Data monitoring disabled
	Indoor Lighting	
	Lighting Control	No command processing
	Lighting Hub	Data monitoring disabled AND No command processing
Wardrobe and Hygiene	Hygiene Tools	Data monitoring disabled AND Main device purpose not active
	Clothing Storage	
	Bathing	
	Toilets	User not detected OR Data monitoring disabled
	Mirrors	A/V Presentation off
Wearables	Accessories	(Environment sensing disabled AND Health sensing disabled AND Smartphone connection not active) OR Device not worn
	Clothing	(Environment sensing disabled AND Health sensing disabled) OR Device not worn
	Glasses	A/V Presentation off OR Device not worn
Fitness	*N/A*	Main device purpose not active

Category	Subcategory	Passive Mode Def.
Power and Energy	Switches	No command processing
	Plugs and Outlets	Actuator off OR Data monitoring disabled
	Energy Meters	Data monitoring disabled
Cleaning and Sanitation	Vacuum/Mop Robots	Main device purpose not active
	Trash Disposal	No command processing
	Laundry	Main device purpose not active OR Data monitoring disabled
Meal and Food	Ranges	Main device purpose not active OR Data monitoring disabled
	Dishwashers	
	Small Appliances	
	Refrigerators	A/V Presentation off OR Data monitoring disabled
Sleep	Sleep Trackers	Health sensing disabled OR User not detected
	Beds and Bedding	
	Alarm Clocks	No notifications active AND A/V Presentation off
Simple Actuators	*N/A*	Main device purpose not active AND No command processing
Gardening and Property Maintenance	Lawn Care Robots	Main device purpose not active
	Irrigation	Main device purpose not active OR Data monitoring disabled
	Weather Sensor	Environment sensing disabled
	Planters	Data monitoring disabled
HVAC and Water	Thermostats	No command processing AND Data monitoring disabled
	Water Meters	Data monitoring disabled
	Standalone Heating	Main device purpose not active OR Data monitoring disabled
	Standalone Cooling	
Hubs and Assistants	Voice Assistants	Microphone off AND Data processing not active
	IoT Protocol Hubs	No command processing AND Data monitoring disabled
	Status Displays	A/V Presentation off
Pet	Food/Water Bowls	Data monitoring disabled AND Main device purpose not active
	Waste management	Data monitoring disabled OR User not detected

[1]M. Schiefer, “Smart Home Definition and Security Threats,” IEE IMF, 2015.

Determining Device-Specific Passive Modes

1. Constructed a two-tiered categorization based on an existing taxonomy[1]
   - Category = Device Purpose
   - Subcategory = Device Type

Category	Subcategory	Passive Mode Def.
Entertainment and Media	Smart TVs	A/V Presentation off
	Speakers and Audio	
	VR Devices	
	Streaming Devices	Media streaming not active
Ambient Sensors	Environmental	Environment sensing disabled
	Occupancy	
Security and Monitoring	Outdoor Cameras	Camera off AND Microphone off AND Motion sensor off
	Indoor Cameras	
	Doorbells	
	Locks and Keypads	(Prox. sensing disabled AND No command processing) OR Data monitoring disabled
	Alarms and Notifiers	No notifications active
	Hazard Sensors	Environment sensing disabled
	Contact Sensors	
	Security Hub	Data monitoring disabled AND No command processing

[1]M. Schiefer, “Smart Home Definition and Security Threats,” IEE IMF, 2015.

Determining Device-Specific Passive Modes

1. Constructed a two-tiered categorization based on an existing taxonomy[1]
   - Category = Device Purpose
   - Subcategory = Device Type
2. Determined the primary function(s) and conditions which prevent data collection for each subcategory

Category	Subcategory	Passive Mode Def.
Entertainment and Media	Smart TVs	A/V Presentation off
	Speakers and Audio	
	VR Devices	
	Streaming Devices	Media streaming not active
Ambient Sensors	Environmental	Environment sensing disabled
	Occupancy	
Security and Monitoring	Outdoor Cameras	Camera off AND Microphone off AND Motion sensor off
	Indoor Cameras	
	Doorbells	
	Locks and Keypads	(Prox. sensing disabled AND No command processing) OR Data monitoring disabled
	Alarms and Notifiers	No notifications active
	Hazard Sensors	Environment sensing disabled
	Contact Sensors	
	Security Hub	Data monitoring disabled AND No command processing

[1]M. Schiefer, “Smart Home Definition and Security Threats,” IEE IMF, 2015.

Determining Device-Specific Passive Modes

1. Constructed a two-tiered categorization based on an existing taxonomy[1]
   - Category = Device Purpose
   - Subcategory = Device Type
2. Determined the primary function(s) and conditions which prevent data collection for each subcategory
3. Constructed boolean expressions using generalized conditions

Category	Subcategory	Passive Mode Def.
Entertainment and Media	Smart TVs	A/V Presentation off
	Speakers and Audio	
	VR Devices	
	Streaming Devices	Media streaming not active
Ambient Sensors	Environmental	Environment sensing disabled
	Occupancy	
Security and Monitoring	Outdoor Cameras	Camera off AND Microphone off AND Motion sensor off
	Indoor Cameras	
	Doorbells	
	Locks and Keypads	(Prox. sensing disabled AND No command processing) OR Data monitoring disabled
	Alarms and Notifiers	No notifications active
	Hazard Sensors	Environment sensing disabled
	Contact Sensors	
	Security Hub	Data monitoring disabled AND No command processing

[1]M. Schiefer, “Smart Home Definition and Security Threats,” IEE IMF, 2015.

Passive Mode for a Smart Lock / Keypad

Primary functions:

- Proximity sensing
- Processing keypad command
- Locking/Unlocking the door

Data collection disabled if:

- No entry logging

Passive Mode for a Smart Lock / Keypad

Primary functions:

- Proximity sensing
- Processing keypad command
- Locking/Unlocking the door

Data collection disabled if:

- No entry logging

Boolean Definition

(Prox. sensing disabled AND not processing keypad command AND not locking/unlocking)
OR (entry logging disabled)

Passive Mode for a Smart Lock / Keypad

Primary functions:

- Proximity sensing
- Processing keypad command
- Locking/Unlocking the door

Data collection disabled if:

- No entry logging

Boolean Definition

(Prox. sensing disabled AND not processing keypad command AND not locking/unlocking)
OR (entry logging disabled)

Final Boolean Definition

(Prox. sensing disabled AND No command processing) OR (Data monitoring disabled)

Composability of Passive Modes

Combined smart TV and security system hub?

Composability of Passive Modes

Combined smart TV and security system hub?

Smart TV passive mode

A/V presentation off

Security Hub passive mode

Data monitoring disabled AND

No command processing

Composability of Passive Modes

Combined smart TV and security system hub?

Smart TV passive mode

A/V presentation off

Security Hub passive mode

Data monitoring disabled AND

No command processing

Device passive mode

(A/V presentation off) **AND** (Data monitoring disabled AND No command processing)

Investigating Current Passive Behaviors

***Goal*: Use Network Traffic Analysis (NTA) to answer the following questions**

Investigating Current Passive Behaviors

***Goal*: Use Network Traffic Analysis (NTA) to answer the following questions**

RQ1: Do smart home devices communicate through the network while passive and to what degree?

Investigating Current Passive Behaviors

***Goal*: Use Network Traffic Analysis (NTA) to answer the following questions**

RQ1: Do smart home devices communicate through the network while passive and to what degree?

RQ2: What type of communications take place in passive modes and what are the implications?

Investigating Current Passive Behaviors

***Goal*: Use Network Traffic Analysis (NTA) to answer the following questions**

RQ1: Do smart home devices communicate through the network while passive and to what degree?

RQ2: What type of communications take place in passive modes and what are the implications?

RQ3: With whom do the devices communicate in passive modes and to what degree?

Investigating Current Passive Behaviors

***Goal*: Use Network Traffic Analysis (NTA) to answer the following questions**

RQ1: Do smart home devices communicate through the network while passive and to what degree?

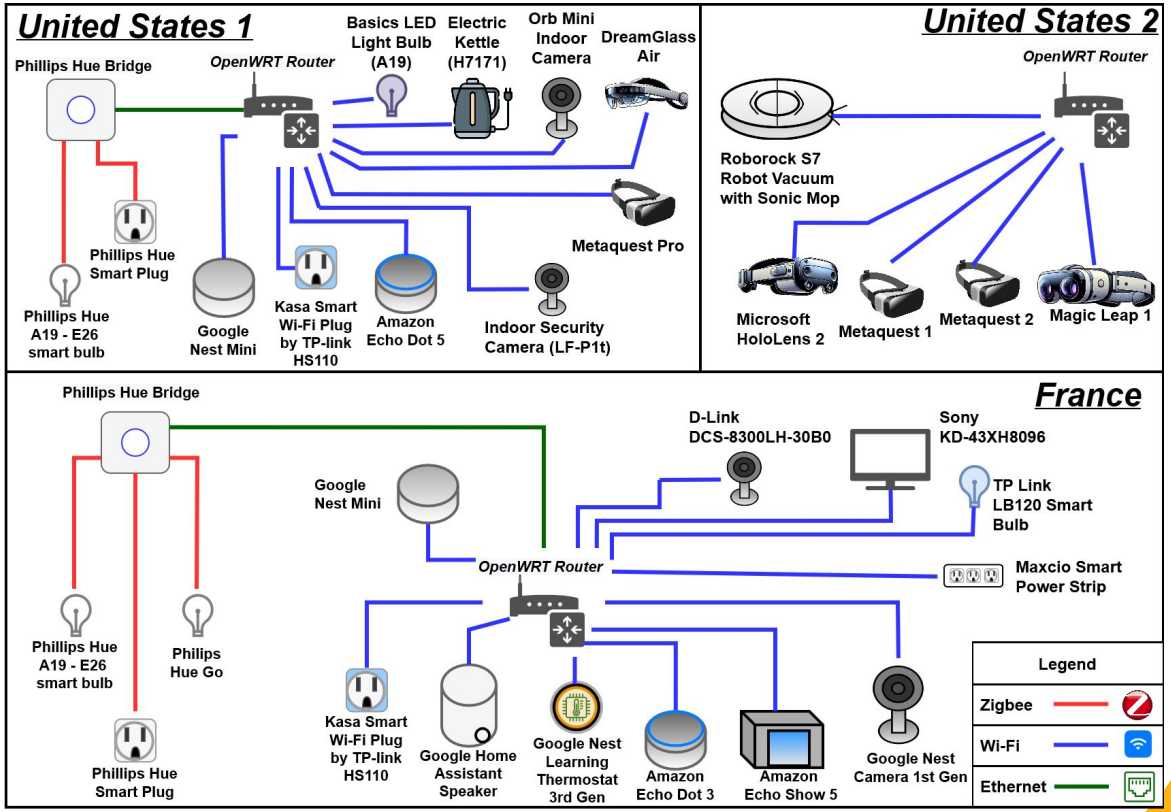
RQ2: What type of communications take place in passive modes and what are the implications?

RQ3: With whom do the devices communicate in passive modes and to what degree?

RQ4: Are there differences in passive communication behavior between US and EU-located devices?

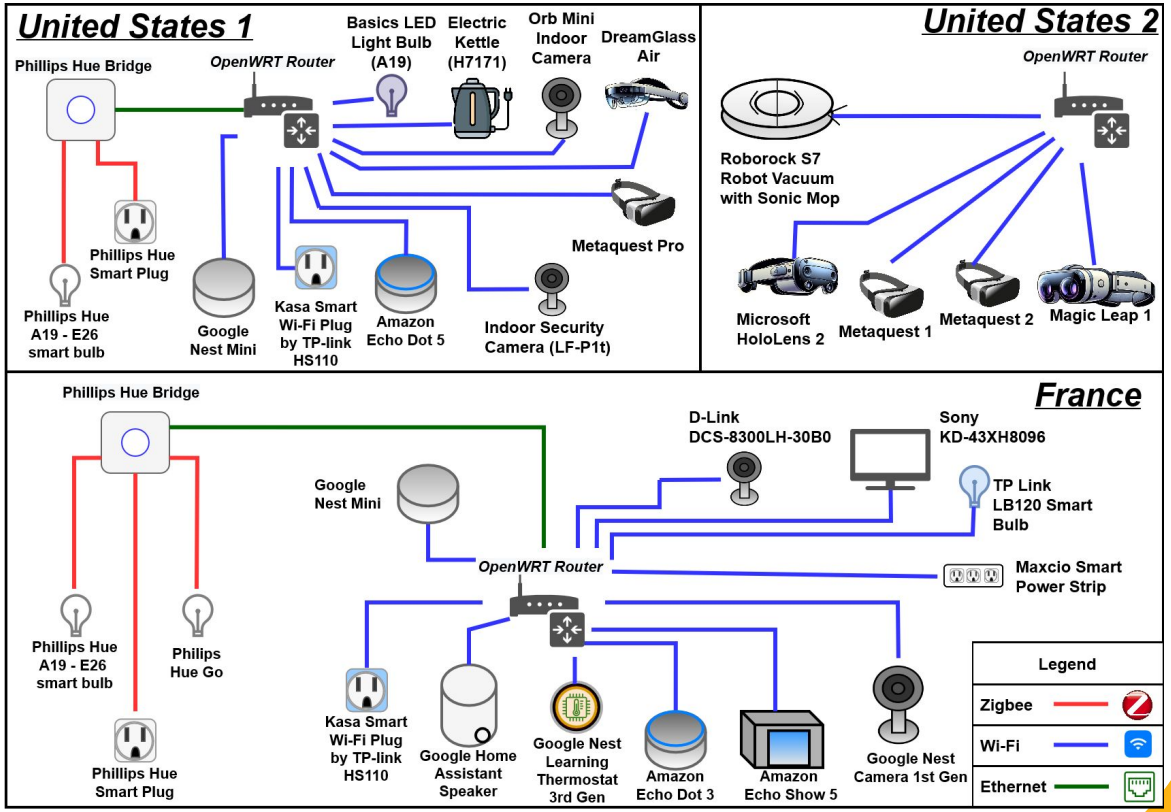
Testbench Setup

- Analyzed 32 devices
  - 11 subcategories
  - 15 manufacturers
- 3 testbenches
  - 2 in the US (US1, US2)
  - 1 in France (FR)



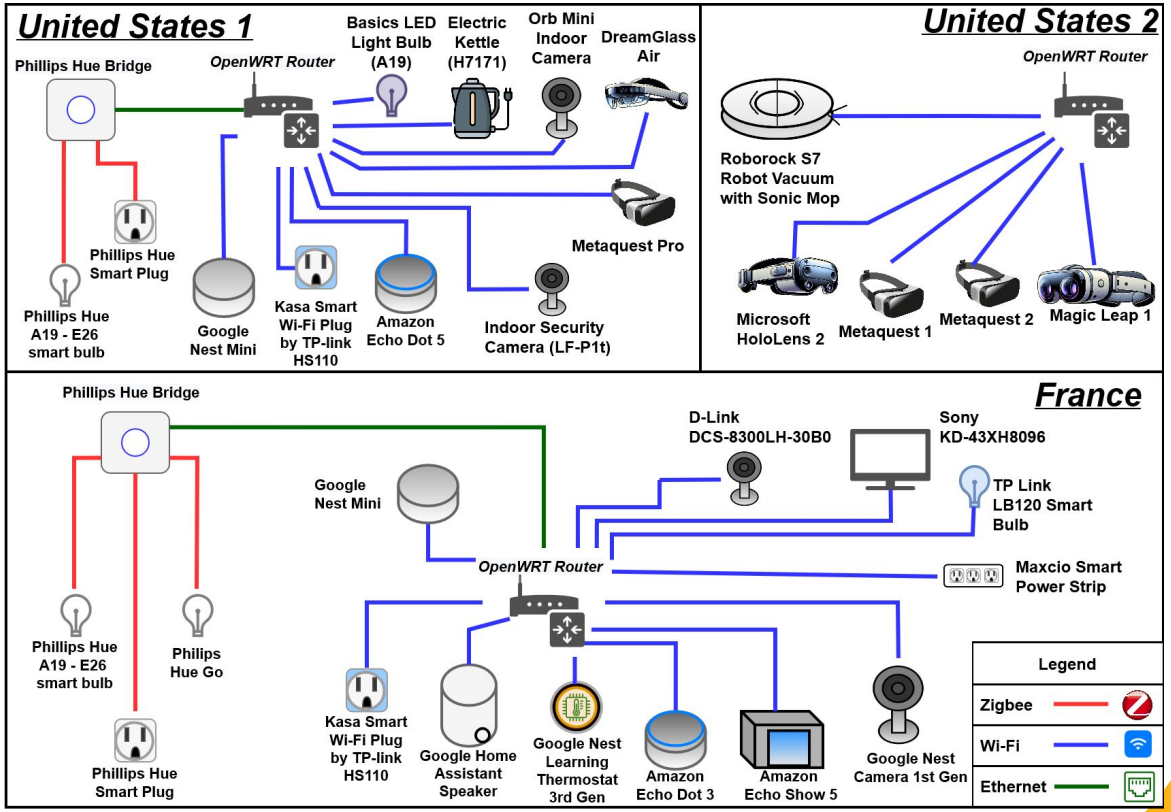
Testbench Setup

- Analyzed 32 devices
  - 11 subcategories
  - 15 manufacturers
- 3 testbenches
  - 2 in the US (US1, US2)
  - 1 in France (FR)
- 6 devices overlaped between US1 and FR



Testbench Setup

- Analyzed 32 devices
  - 11 subcategories
  - 15 manufacturers
- 3 testbenches
  - 2 in the US (US1, US2)
  - 1 in France (FR)
- 6 devices overlaped between US1 and FR
- OpenWRT[1] routers captured device traffic



[1]R. Brown, “Welcome to the OpenWrt Project,” 2016. https://openwrt.org/start

Network Traffic Analysis Approach

- Analyzed between 71 and 168 hours of passive traffic per device

Network Traffic Analysis Approach

- Analyzed between 71 and 168 hours of passive traffic per device
- Removed local network administration traffic (e.g. DHCP / ICMP), as well as TCP errors and retransmissions
    - Network administration traffic primarily existed between LAN devices and the router

Network Traffic Analysis Approach

- Analyzed between 71 and 168 hours of passive traffic per device
- Removed local network administration traffic (e.g. DHCP / ICMP), as well as TCP errors and retransmissions
  - Network administration traffic primarily existed between LAN devices and the router
- DNS used to identify endpoints, but not included in metrics

Network Traffic Analysis Approach

- Analyzed between 71 and 168 hours of passive traffic per device
- Removed local network administration traffic (e.g. DHCP / ICMP), as well as TCP errors and retransmissions
  - Network administration traffic primarily existed between LAN devices and the router
- DNS used to identify endpoints, but not included in metrics

Network Entities of Concern:

- Remote First Parties
- Remote Support Parties
- Remote Third Parties
- Network Infrastructure Parties
- Local Smart Devices

Network Traffic Analysis Approach

- Analyzed between 71 and 168 hours of passive traffic per device
- Removed local network administration traffic (e.g. DHCP / ICMP), as well as TCP errors and retransmissions
  - Network administration traffic primarily existed between LAN devices and the router
- DNS used to identify endpoints, but not included in metrics

Network Entities of Concern:

- Remote First Parties
- Remote Support Parties
- Remote Third Parties
- Network Infrastructure Parties
- Local Smart Devices

Metrics

- Traffic Volume and Variation
- Protocol Types
- Protocol Distributions
- Usage of Protocol-Level Encryption
- WAN Endpoint Types
- LAN Endpoints

RQ1: Volume and Variation

- Vastly different traffic patterns across devices
  - From less than 100 packets and 0.5KB per hour to nearly 40,000 packets and 55.8MB

HOURLY AVERAGE VOLUME AND VARIANCE OF TRAFFIC.

Device Name	Packet		Byte	
	Average	CoV	Average	CoV
Metaquest 1 (US2)	39,364	9.45	55838.9KB	10.75
Echo Show 5 (FR)	19,781	0.05	3159.5KB	0.33
Echo Dot 3 (FR)	19,324	0.02	2323.7KB	0.13
Google Speaker (FR)	17,559	0.28	2398.5KB	0.50
Nest Mini (FR)	15,860	0.25	2475.8KB	0.57
Metaquest Pro (US1)	5112	0.53	3370.3KB	2.01
Hue Bridge (FR)	3581	0.15	947.0KB	0.21
Hue Bridge (US1)	3065	0.62	677.5KB	1.12
Nest Mini (US1)	2554	0.22	600.4KB	0.79
Echo Dot 5 (US1)	2359	0.70	1139.4KB	4.34
Netvue Camera (US1)	2078	0.92	425.4KB	0.95
Sony TV (FR)	2074	0.23	752.1KB	0.68
Litokam Camera (US1)	1309	0.02	246.6KB	0.02
Metaquest 2 (US2)	1126	1.02	662.1KB	1.42
Roborock S7 (US2)	1120	0.09	133.4KB	0.22
Nest Thermostat (FR)	1057	1.00	428.1KB	1.06
Nest Camera (FR)	929	0.09	98.5KB	0.14
D-Link Camera (FR)	870	4.60	746.2KB	5.54
Maxcio Power Strip (FR)	665	0.23	96.0KB	0.31
DreamGlass Air (US1)	614	4.56	268.4KB	5.10
TP-Link Light (FR)	573	0.32	239.8KB	0.34
TP-Link Plug (FR)	472	0.14	156.7KB	0.28
HoloLens 2 (US2)	358	1.47	130.9KB	3.17
Govee Kettle (US1)	187	0.42	20.9KB	2.38
Amazon Light (US1)	94	0.15	15.2KB	0.29
TP-Link Plug (US1)	50	0.20	5.9KB	0.57
MagicLeap (US2)	22	6.97	8.4KB	7.62
TOTAL	142,157	N/A	77365.6KB	N/A

[1]D. Ahmed et al., “Analyzing the Feasibility and Generalizability of Fingerprinting Internet of Things Devices,” PoPETs, vol. 2022.

RQ1: Volume and Variation

- Vastly different traffic patterns across devices
  - From less than 100 packets and 0.5KB per hour to nearly 40,000 packets and 55.8MB

HOURLY AVERAGE VOLUME AND VARIANCE OF TRAFFIC.

Device Name	Packet		Byte	
	Average	CoV	Average	CoV
Metaquest 1 (US2)	39,364	9.45	55838.9KB	10.75
Echo Show 5 (FR)	19,781	0.05	3159.5KB	0.33
Echo Dot 3 (FR)	19,324	0.02	2323.7KB	0.13
Google Speaker (FR)	17,559	0.28	2398.5KB	0.50
Nest Mini (FR)	15,860	0.25	2475.8KB	0.57
Metaquest Pro (US1)	5112	0.53	3370.3KB	2.01
Hue Bridge (FR)	3581	0.15	947.0KB	0.21
Hue Bridge (US1)	3065	0.62	677.5KB	1.12
Nest Mini (US1)	2554	0.22	600.4KB	0.79
Echo Dot 5 (US1)	2359	0.70	1139.4KB	4.34
Netvue Camera (US1)	2078	0.92	425.4KB	0.95
Sony TV (FR)	2074	0.23	752.1KB	0.68
Litokam Camera (US1)	1309	0.02	246.6KB	0.02
Metaquest 2 (US2)	1126	1.02	662.1KB	1.42
Roborock S7 (US2)	1120	0.09	133.4KB	0.22
Nest Thermostat (FR)	1057	1.00	428.1KB	1.06
Nest Camera (FR)	929	0.09	98.5KB	0.14
D-Link Camera (FR)	870	4.60	746.2KB	5.54
Maxcio Power Strip (FR)	665	0.23	96.0KB	0.31
DreamGlass Air (US1)	614	4.56	268.4KB	5.10
TP-Link Light (FR)	573	0.32	239.8KB	0.34
TP-Link Plug (FR)	472	0.14	156.7KB	0.28
HoloLens 2 (US2)	358	1.47	130.9KB	3.17
Govee Kettle (US1)	187	0.42	20.9KB	2.38
Amazon Light (US1)	94	0.15	15.2KB	0.29
TP-Link Plug (US1)	50	0.20	5.9KB	0.57
MagicLeap (US2)	22	6.97	8.4KB	7.62
TOTAL	142,157	N/A	77365.6KB	N/A

> 50% of packets were FR Voice Assistants

[1]D. Ahmed et al., “Analyzing the Feasibility and Generalizability of Fingerprinting Internet of Things Devices,” PoPETs, vol. 2022.

RQ1: Volume and Variation

- Vastly different traffic patterns across devices
  - From less than 100 packets and 0.5KB per hour to nearly 40,000 packets and 55.8MB
- The degree and variability of the traffic makes fingerprinting attacks likely to succeed[1]

HOURLY AVERAGE VOLUME AND VARIANCE OF TRAFFIC.

Device Name	Packet		Byte	
	Average	CoV	Average	CoV
Metaquest 1 (US2)	39,364	9.45	55838.9KB	10.75
Echo Show 5 (FR)	19,781	0.05	3159.5KB	0.33
Echo Dot 3 (FR)	19,324	0.02	2323.7KB	0.13
Google Speaker (FR)	17,559	0.28	2398.5KB	0.50
Nest Mini (FR)	15,860	0.25	2475.8KB	0.57
Metaquest Pro (US1)	5112	0.53	3370.3KB	2.01
Hue Bridge (FR)	3581	0.15	947.0KB	0.21
Hue Bridge (US1)	3065	0.62	677.5KB	1.12
Nest Mini (US1)	2554	0.22	600.4KB	0.79
Echo Dot 5 (US1)	2359	0.70	1139.4KB	4.34
Netvue Camera (US1)	2078	0.92	425.4KB	0.95
Sony TV (FR)	2074	0.23	752.1KB	0.68
Litokam Camera (US1)	1309	0.02	246.6KB	0.02
Metaquest 2 (US2)	1126	1.02	662.1KB	1.42
Roborock S7 (US2)	1120	0.09	133.4KB	0.22
Nest Thermostat (FR)	1057	1.00	428.1KB	1.06
Nest Camera (FR)	929	0.09	98.5KB	0.14
D-Link Camera (FR)	870	4.60	746.2KB	5.54
Maxcio Power Strip (FR)	665	0.23	96.0KB	0.31
DreamGlass Air (US1)	614	4.56	268.4KB	5.10
TP-Link Light (FR)	573	0.32	239.8KB	0.34
TP-Link Plug (FR)	472	0.14	156.7KB	0.28
HoloLens 2 (US2)	358	1.47	130.9KB	3.17
Govee Kettle (US1)	187	0.42	20.9KB	2.38
Amazon Light (US1)	94	0.15	15.2KB	0.29
TP-Link Plug (US1)	50	0.20	5.9KB	0.57
MagicLeap (US2)	22	6.97	8.4KB	7.62
TOTAL	142,157	N/A	77365.6KB	N/A

> 50% of packets were FR Voice Assistants

[1]D. Ahmed et al., “Analyzing the Feasibility and Generalizability of Fingerprinting Internet of Things Devices,” PoPETs, vol. 2022.

RQ1: Volume and Variation

- Vastly different traffic patterns across devices
  - From less than 100 packets and 0.5KB per hour to nearly 40,000 packets and 55.8MB
- The degree and variability of the traffic makes fingerprinting attacks likely to succeed[1]
- **Current passive modes do not preclude unexpected traffic**

HOURLY AVERAGE VOLUME AND VARIANCE OF TRAFFIC.

Device Name	Packet		Byte	
	Average	CoV	Average	CoV
Metaquest 1 (US2)	39,364	9.45	55838.9KB	10.75
Echo Show 5 (FR)	19,781	0.05	3159.5KB	0.33
Echo Dot 3 (FR)	19,324	0.02	2323.7KB	0.13
Google Speaker (FR)	17,559	0.28	2398.5KB	0.50
Nest Mini (FR)	15,860	0.25	2475.8KB	0.57
Metaquest Pro (US1)	5112	0.53	3370.3KB	2.01
Hue Bridge (FR)	3581	0.15	947.0KB	0.21
Hue Bridge (US1)	3065	0.62	677.5KB	1.12
Nest Mini (US1)	2554	0.22	600.4KB	0.79
Echo Dot 5 (US1)	2359	0.70	1139.4KB	4.34
Netvue Camera (US1)	2078	0.92	425.4KB	0.95
Sony TV (FR)	2074	0.23	752.1KB	0.68
Litokam Camera (US1)	1309	0.02	246.6KB	0.02
Metaquest 2 (US2)	1126	1.02	662.1KB	1.42
Roborock S7 (US2)	1120	0.09	133.4KB	0.22
Nest Thermostat (FR)	1057	1.00	428.1KB	1.06
Nest Camera (FR)	929	0.09	98.5KB	0.14
D-Link Camera (FR)	870	4.60	746.2KB	5.54
Maxcio Power Strip (FR)	665	0.23	96.0KB	0.31
DreamGlass Air (US1)	614	4.56	268.4KB	5.10
TP-Link Light (FR)	573	0.32	239.8KB	0.34
TP-Link Plug (FR)	472	0.14	156.7KB	0.28
HoloLens 2 (US2)	358	1.47	130.9KB	3.17
Govee Kettle (US1)	187	0.42	20.9KB	2.38
Amazon Light (US1)	94	0.15	15.2KB	0.29
TP-Link Plug (US1)	50	0.20	5.9KB	0.57
MagicLeap (US2)	22	6.97	8.4KB	7.62
TOTAL	142,157	N/A	77365.6KB	N/A

> 50% of packets were FR Voice Assistants

[1]D. Ahmed et al., “Analyzing the Feasibility and Generalizability of Fingerprinting Internet of Things Devices,” PoPETs, vol. 2022.

RQ1: Volume and Variation

- Vastly different traffic patterns across devices
  - From less than 100 packets and 0.5KB per hour to nearly 40,000 packets and 55.8MB
- The degree and variability of the traffic makes fingerprinting attacks likely to succeed[1]
- **Current passive modes do not preclude unexpected traffic**

HOURLY AVERAGE VOLUME AND VARIANCE OF TRAFFIC.

Device Name	Packet		Byte	
	Average	CoV	Average	CoV
Metaquest 1 (US2)	39,364	9.45	55838.9KB	10.75
Echo Show 5 (FR)	19,781	0.05	3159.5KB	0.33
Echo Dot 3 (FR)	19,324	0.02	2323.7KB	0.13
Google Speaker (FR)	17,559	0.28	2398.5KB	0.50
Nest Mini (FR)	15,860	0.25	2475.8KB	0.57
Metaquest Pro (US1)	5112	0.53	3370.3KB	2.01
Hue Bridge (FR)	3581	0.15	947.0KB	0.21
Hue Bridge (US1)	3065	0.62	677.5KB	1.12
Nest Mini (US1)	2554	0.22	600.4KB	0.79
Echo Dot 5 (US1)	2359	0.70	1139.4KB	4.34
Netvue Camera (US1)	2078	0.92	425.4KB	0.95
Sony TV (FR)	2074	0.23	752.1KB	0.68
Litokam Camera (US1)	1309	0.02	246.6KB	0.02
Metaquest 2 (US2)	1126	1.02	662.1KB	1.42
Roborock S7 (US2)	1120	0.09	133.4KB	0.22
Nest Thermostat (FR)	1057	1.00	428.1KB	1.06
Nest Camera (FR)	929	0.09	98.5KB	0.14
D-Link Camera (FR)	870	4.60	746.2KB	5.54
Maxcio Power Strip (FR)	665	0.23	96.0KB	0.31
DreamGlass Air (US1)	614	4.56	268.4KB	5.10
TP-Link Light (FR)	573	0.32	239.8KB	0.34
TP-Link Plug (FR)	472	0.14	156.7KB	0.28
HoloLens 2 (US2)	358	1.47	130.9KB	3.17
Govee Kettle (US1)	187	0.42	20.9KB	2.38
Amazon Light (US1)	94	0.15	15.2KB	0.29
TP-Link Plug (US1)	50	0.20	5.9KB	0.57
MagicLeap (US2)	22	6.97	8.4KB	7.62
TOTAL	142,157	N/A	77365.6KB	N/A

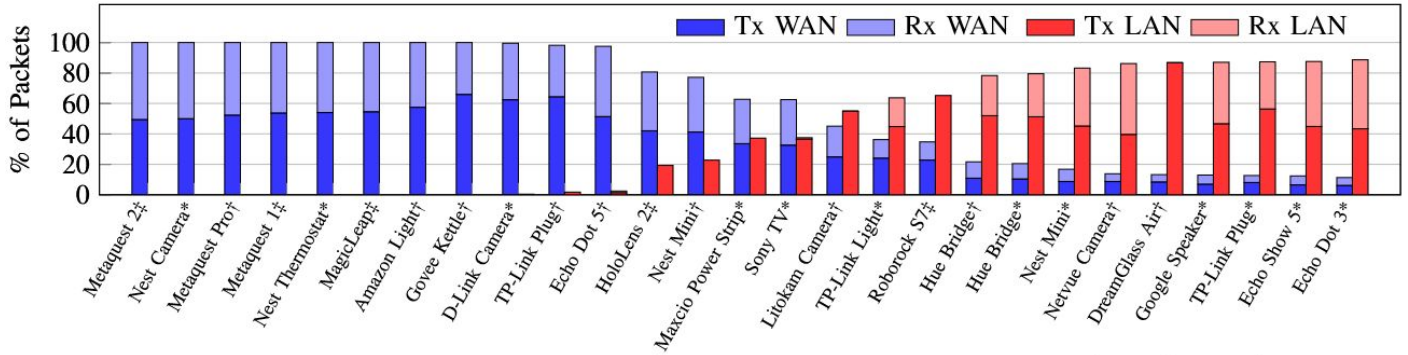
> 50% of packets were FR Voice Assistants

~3.4 million packets and ~1.86GB in 24 hours

[1]D. Ahmed et al., "Analyzing the Feasib
Fingerprinting Internet of Things Device

RQ2: Traffic Type

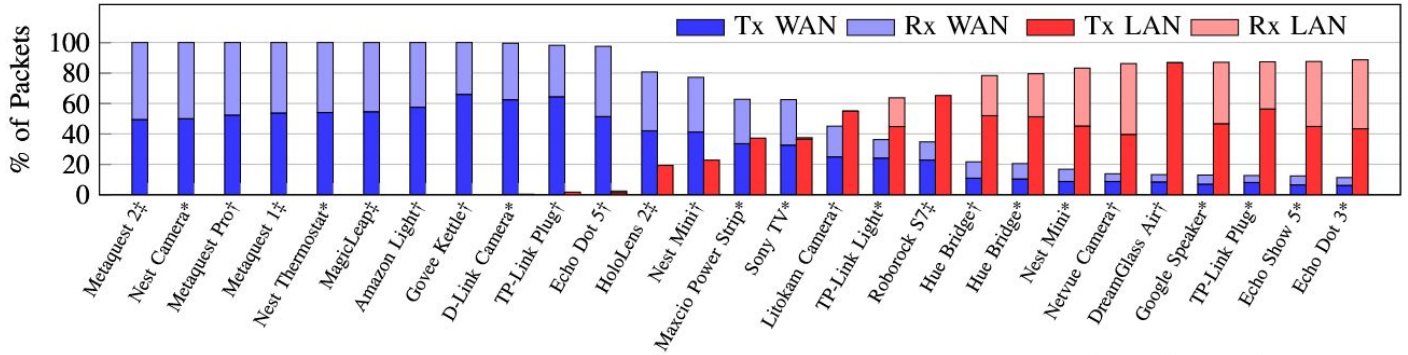
- LAN traffic accounted for 50.4% of the traffic
  - Observed in 19 devices



Packet-wise WAN vs. LAN distribution for each device ordered by % of LAN packets (*FR - †US1 - ‡US2).

RQ2: Traffic Type

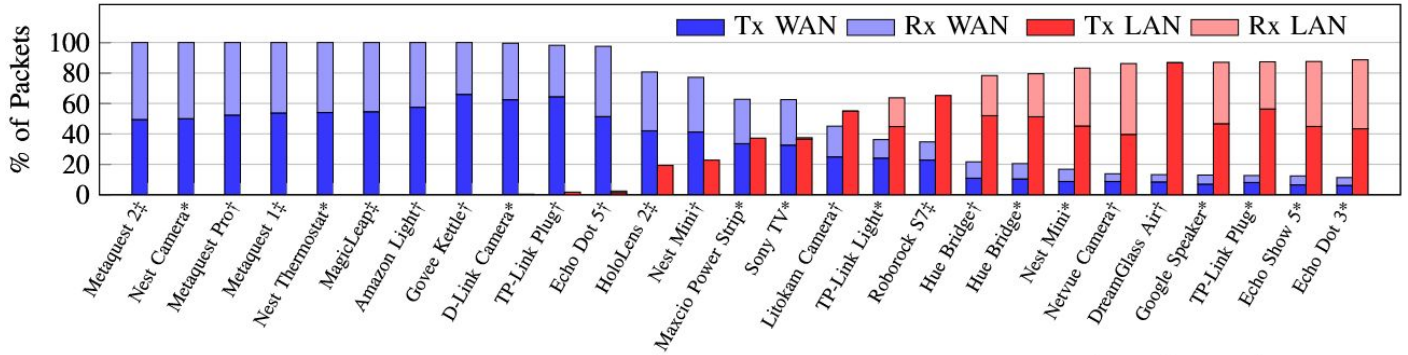
- LAN traffic accounted for 50.4% of the traffic
  - Observed in 19 devices
- Similar device types did not always have common LAN behavior
  - US1 cameras primarily communicated over LAN, FR cameras rarely did



Packet-wise WAN vs. LAN distribution for each device ordered by % of LAN packets (*FR - †US1 - ‡US2).

RQ2: Traffic Type

- LAN traffic accounted for 50.4% of the traffic
  - Observed in 19 devices
- Similar device types did not always have common LAN behavior
  - US1 cameras primarily communicated over LAN, FR cameras rarely did
- **Lack of common behavior for passive devices**



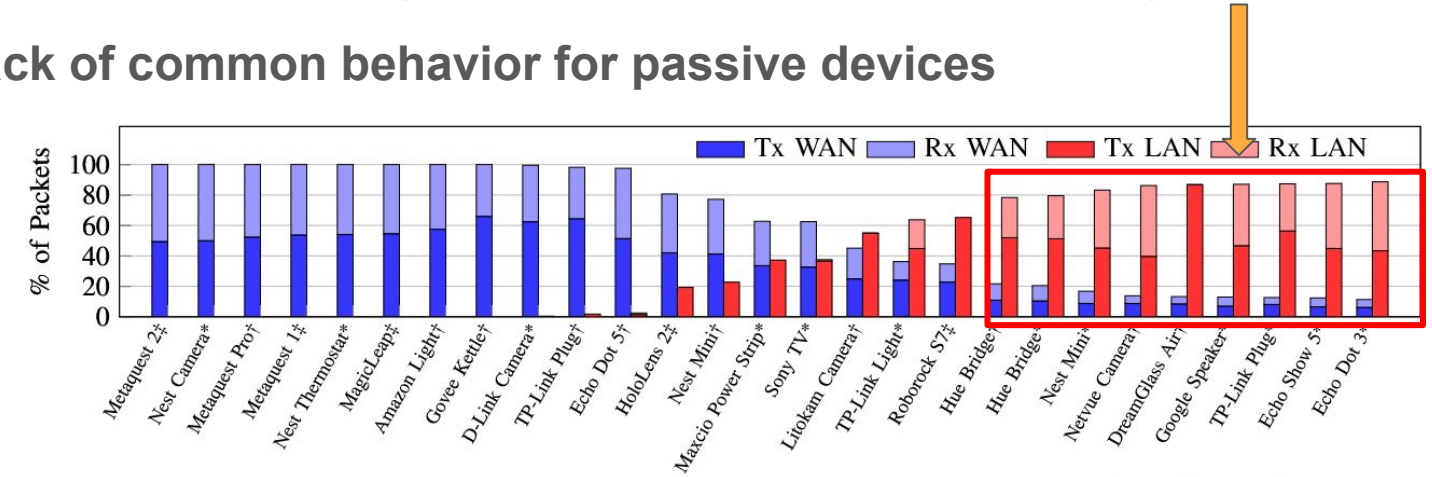
Packet-wise WAN vs. LAN distribution for each device ordered by % of LAN packets (*FR - †US1 - ‡US2).

[1]A. Girish et al., “In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes,” IMC, 2023.

RQ2: Traffic Type

- LAN traffic accounted for 50.4% of the traffic
  - Observed in 19 devices
- Similar device types did not always have common
  - US1 cameras primarily communicated over LAN, FR camera
- **Lack of common behavior for passive devices**

> 75% of traffic was LAN for 9 devices

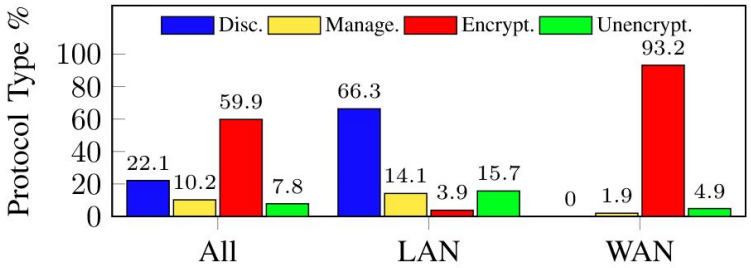


Packet-wise WAN vs. LAN distribution for each device ordered by % of LAN packets (*FR - †US1 - ‡US2).

[1]A. Girish et al., “In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes,” IMC, 2023.

RQ2: Protocols

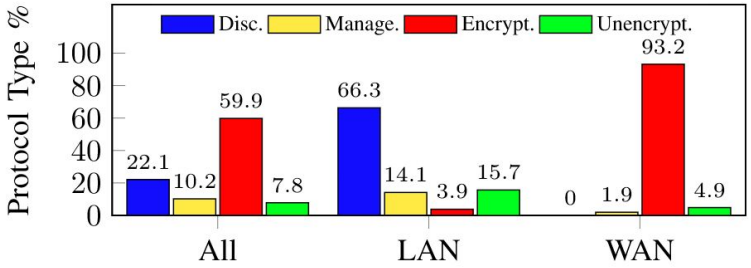
- Observed 31 application-layer protocols
  - 4 management
  - 7 discovery
  - 12 encrypted application-specific
  - 8 unencrypted application-specific



Distribution of packet-wise application protocol types.

RQ2: Protocols

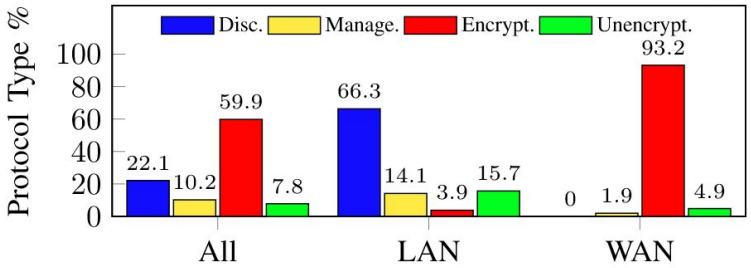
- Observed 31 application-layer protocols
  - 4 management
  - 7 discovery
  - 12 encrypted application-specific
  - 8 unencrypted application-specific
- 11 protocols were for unknown purposes
  - 6 encrypted - 5 unencrypted
  - 7 LAN
  - 9 used by Google devices



Distribution of packet-wise application protocol types.

RQ2: Protocols

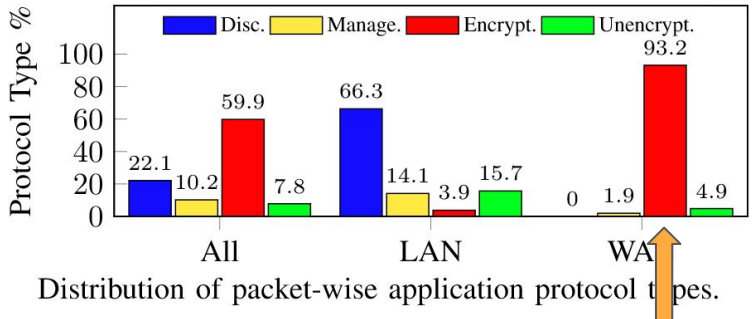
- Observed 31 application-layer protocols
  - 4 management
  - 7 discovery
  - 12 encrypted application-specific
  - 8 unencrypted application-specific
- 11 protocols were for unknown purposes
  - 6 encrypted - 5 unencrypted
  - 7 LAN
  - 9 used by Google devices
- High use of protocol encryption on WAN



Distribution of packet-wise application protocol types.

RQ2: Protocols

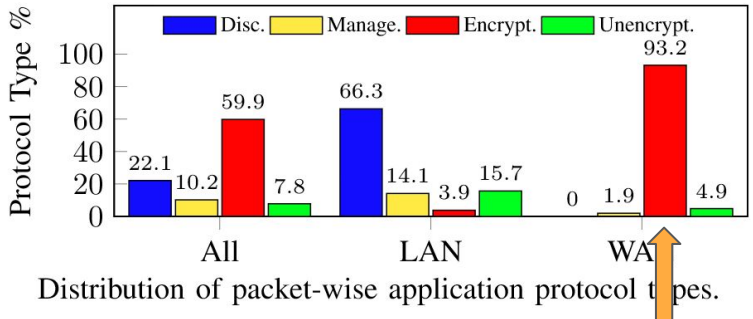
- Observed 31 application-layer protocols
  - 4 management
  - 7 discovery
  - 12 encrypted application-specific
  - 8 unencrypted application-specific
- 11 protocols were for unknown purposes
  - 6 encrypted - 5 unencrypted
  - 7 LAN
  - 9 used by Google devices
- High use of protocol encryption on WAN



WAN traffic almost entirely encrypted

RQ2: Protocols

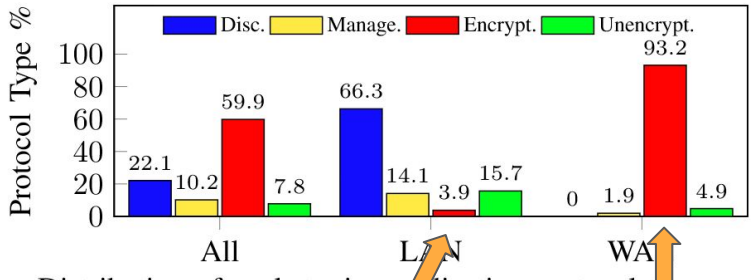
- Observed 31 application-layer protocols
  - 4 management
  - 7 discovery
  - 12 encrypted application-specific
  - 8 unencrypted application-specific
- 11 protocols were for unknown purposes
  - 6 encrypted - 5 unencrypted
  - 7 LAN
  - 9 used by Google devices
- High use of protocol encryption on WAN
- Very low use of protocol encryption on LAN



WAN traffic almost entirely encrypted

RQ2: Protocols

- Observed 31 application-layer protocols
  - 4 management
  - 7 discovery
  - 12 encrypted application-specific
  - 8 unencrypted application-specific
- 11 protocols were for unknown purposes
  - 6 encrypted - 5 unencrypted
  - 7 LAN
  - 9 used by Google devices
- High use of protocol encryption on WAN
- Very low use of protocol encryption on LAN



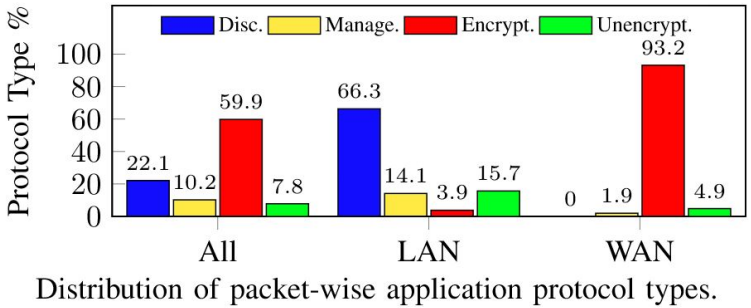
Distribution of packet-wise application protocol types.

Only 3.9% of LAN traffic was encrypted

WAN traffic almost entirely encrypted

RQ2: Protocols

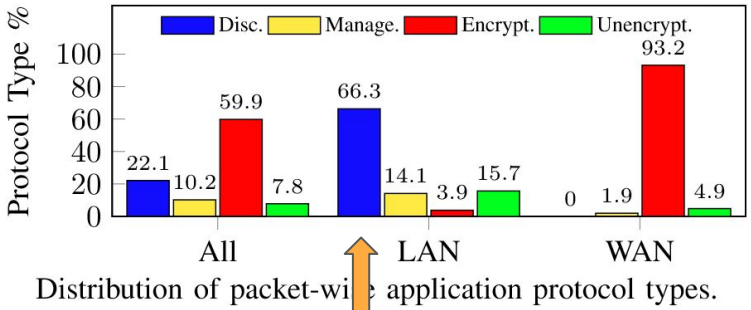
- Discovery protocols were used by 18 device
  - Including by unpaired devices



Distribution of packet-wise application protocol types.

RQ2: Protocols

- Discovery protocols were used by 18 device
  - Including by unpaired devices

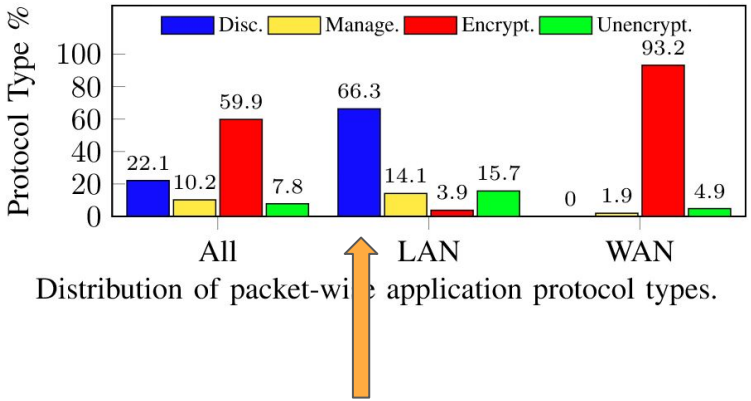


Distribution of packet-wi application protocol types.

~2/3rds of LAN traffic is discovery

RQ2: Protocols

- Discovery protocols were used by 18 device
  - Including by unpaired devices
- **Discovery protocols may allow local devices to share identifying information[1]**



~2/3rds of LAN traffic is discovery

[1]A. Girish et al., “In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes,” IMC, 2023.

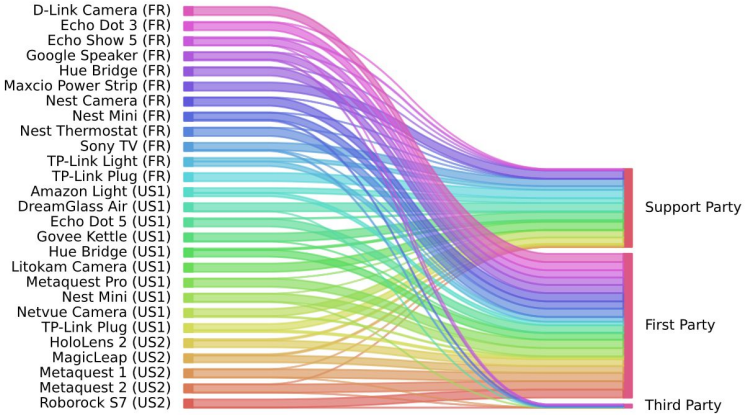
RQ2: Protocols

- TP-Link Plug shared precise location data freely over LAN
  - Also observed by Girish et al.[1]

[1]A. Girish et al., “In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes,” IMC, 2023.

RQ3: Endpoints - WAN

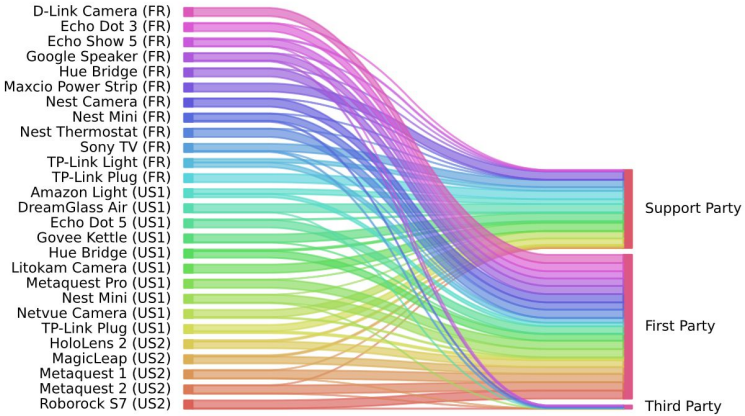
- Devices preferred either first or support parties
  - 18 devices showed >80% first party traffic, 7 showed >80% support party



Target entities for outgoing (Tx) device traffic.

RQ3: Endpoints - WAN

- Devices preferred either first or support parties
  - 18 devices showed >80% first party traffic, 7 showed >80% support party
- Support parties for non-management traffic were largely content delivery networks
  - This can reveal sensitive information to these parties through profiling or traffic monitoring[1]

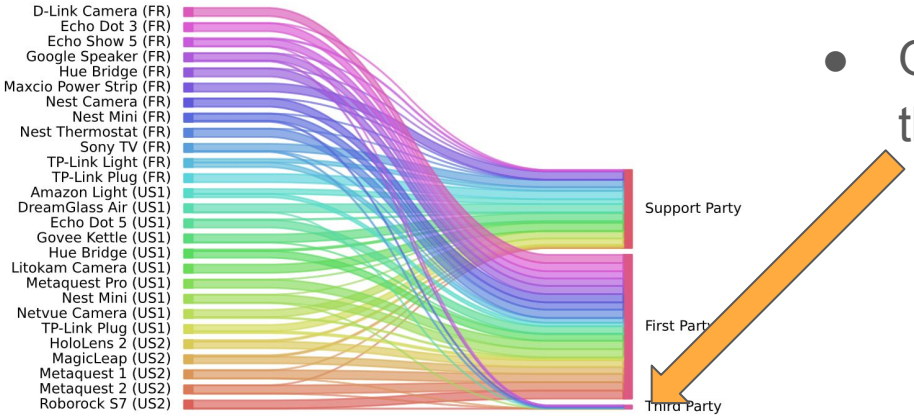


Target entities for outgoing (Tx) device traffic.

[1]M. Ghaznavi et al., “Content Delivery Network Security: A Survey,” IEEE Communications Surveys & Tutorials, vol. 23, 2021.

RQ3: Endpoints - WAN

- Devices preferred either first or support parties
  - 18 devices showed >80% first party traffic, 7 showed >80% support party
- Support parties for non-management traffic were largely content delivery networks
  - This can reveal sensitive information to these parties through profiling or traffic monitoring[1]



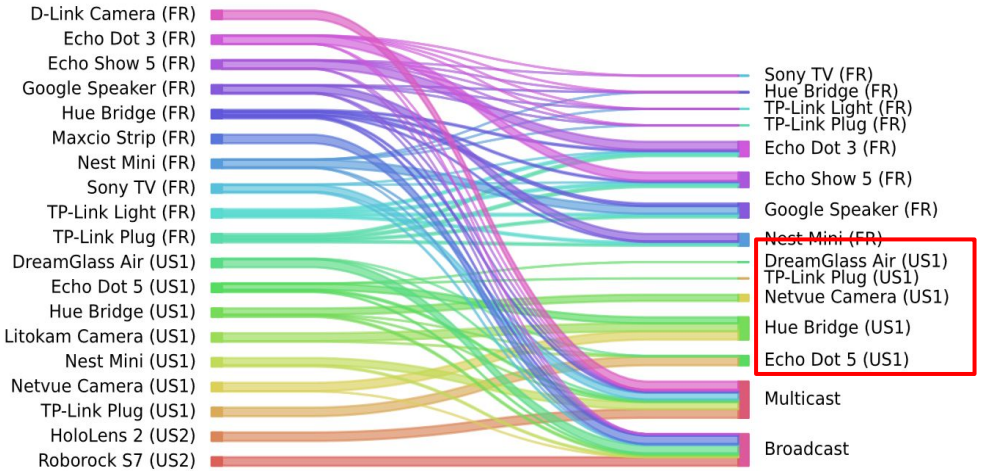
Target entities for outgoing (Tx) device traffic.

- Only 5 devices exhibited more than 1% third party traffic
  - 3 of these were the Google voice assistants

[1]M. Ghaznavi et al., “Content Delivery Network Security: A Survey,” IEEE Communications Surveys & Tutorials, vol. 23, 2021.

RQ3: Endpoints - LAN

- Several devices communicated directly with each other despite never being paired or configured to advertise their presence
  - Discovery was not limited to multicast or broadcast for these devices



Summary of LAN Traffic.

RQ4: EU vs. US

- Very few differences were noted
- LAN variation was more dependent on the number of local devices
- FR devices were equally eager to share discovery information
  - The only notable difference being a less precise location for the TP-Link Plug
- No noticeable differences to account for differing privacy legislation
  - E.g. the General Data Protection Regulation (GDPR)

Key Findings

Key Findings

- **Current “passive” modes do not adequately describe non-active states**
  - Ambiguous privacy expectations
  - Users must assume constant data capture

Key Findings

- **Current “passive” modes do not adequately describe non-active states**
  - Ambiguous privacy expectations
  - Users must assume constant data capture
- **Idle does not imply “passive”**
  - Excessive amounts of discovery and other LAN traffic
  - Lack of transparency as to the purpose of passive mode network traffic

Key Findings

- **Current “passive” modes do not adequately describe non-active states**
  - Ambiguous privacy expectations
  - Users must assume constant data capture
- **Idle does not imply “passive”**
  - Excessive amounts of discovery and other LAN traffic
  - Lack of transparency as to the purpose of passive mode network traffic
- **Passive devices often probe the LAN, even when unpaired**
  - Can enable tracking and device fingerprinting attacks

Key Findings

- **Current “passive” modes do not adequately describe non-active states**
  - Ambiguous privacy expectations
  - Users must assume constant data capture
- **Idle does not imply “passive”**
  - Excessive amounts of discovery and other LAN traffic
  - Lack of transparency as to the purpose of passive mode network traffic
- **Passive devices often probe the LAN, even when unpaired**
  - Can enable tracking and device fingerprinting attacks
- **Outgoing traffic is encrypted, internal not so much**
  - 93% of WAN traffic was encrypted, but only 3.9% of LAN traffic was encrypted
  - Can leak information (such as location) to other LAN devices

Future Work

Future Work

- **Geolocation of Endpoints**
  - Difficult due to CDNs
  - Current work involves machine learning approaches

Future Work

- **Geolocation of Endpoints**
  - Difficult due to CDNs
  - Current work involves machine learning approaches
- **Deeper Network Traffic Analysis**
  - More devices overall
  - More common devices (US vs. EU)
  - Decrypt (if needed) and analyze the 11 unknown protocols
  - More detailed metrics (e.g. entropy)

Future Work

- **Geolocation of Endpoints**
  - Difficult due to CDNs
  - Current work involves machine learning approaches
- **Deeper Network Traffic Analysis**
  - More devices overall
  - More common devices (US vs. EU)
  - Decrypt (if needed) and analyze the 11 unknown protocols
  - More detailed metrics (e.g. entropy)
- **User study**
  - What are users' expectations when a device isn't in use
  - How would users define "not in use"
  - Is the passive mode designation intuitive to non-technical users

UMBC

PerCom Pervasive Computing 2025

All code and datasets are publicly available online at:

Smart Home IoT Passive Mode Analysis

https://github.com/DAMSlabUMBC/Passive-Mode-Study

Includes instructions and scripts for analyzing custom-made datasets and adding them to the repository

Code

Code Reviewed

Dataset Reviewed

Paper

Supplementary Slides

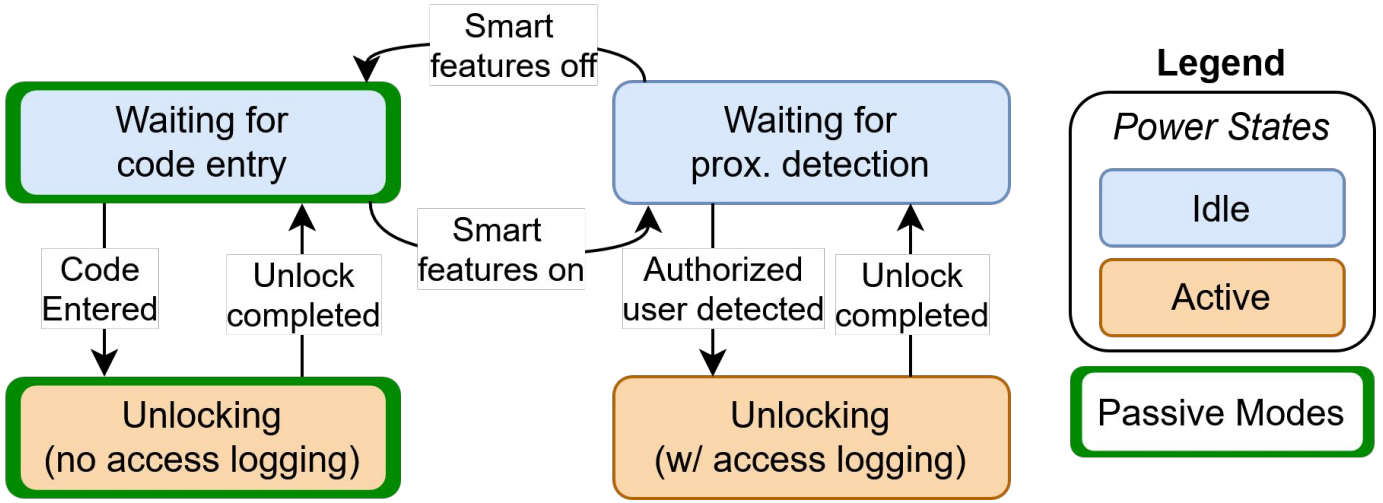
Privacy Policies

- **Many policies were not straightforward to locate**
  - Many policies were not specific as to if they applied to a device or just an online storefront
  - The Litokam camera's policy was only available after downloading the companion app
- **Many policies apply to a large range of devices and services**
  - Prevalent among large manufacturers like Google, Amazon, and Meta
  - Makes it difficult for users to determine the data a specific device processes
- **Enumerate diverse data types, but do not give temporal information**
  - The types of data collected is well defined, but not when the devices collect the data
  - No policies clarified under what modes the data was collected or if the collection does not occur under certain conditions
  - For instance, it is unclear if the Sony TV continues to send location data when in standby mode
- **Privacy-conscious users can only assume the data is constantly collected**

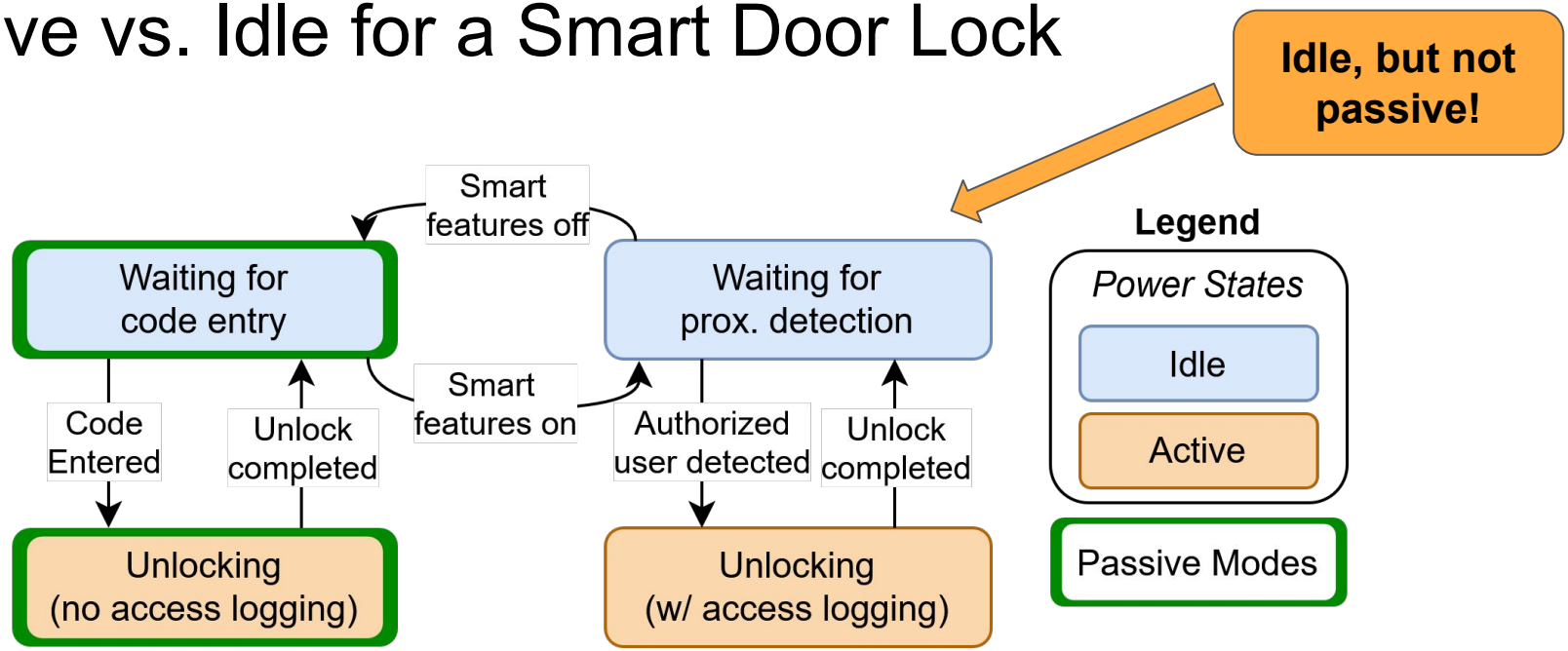
Preliminary User Study

- **21 Responses from Computer Science students UMBC**
- **77% expected low device communication frequency while passive**
  - No more than a few times an hour
  - This is unique to passive modes, 73% expected constant communication when active
- **33.5% preferred passive devices to only be capable of receiving data**
- **7 of the 8 respondents who were interested in “Smart Appliances” were uncomfortable with network communication more than “a few times a day”**
- **Most respondents indicated they were comfortable with LAN traffic**

Passive vs. Idle for a Smart Door Lock



Passive vs. Idle for a Smart Door Lock



Passive vs. Idle for a Smart Door Lock