POSTER: In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes

Aniketh Girish*
IMDEA Networks Institute /
Universidad Carlos III de Madrid

Tianrui Hu*
Northeastern University

Vijay Prakash
New York University

Daniel J. Dubois
Northeastern University

Srdjan Matic
IMDEA Software Institute

Danny Yuxing Huang
New York University

Serge Egelman
ICSI / University of California, Berkeley

Joel Reardon
University of Calgary / AppCensus

Juan Tapiador
Universidad Carlos III de Madrid

David Choffnes
Northeastern University

Narseo Vallina-Rodriguez
IMDEA Networks Institute / AppCensus

Abstract

The network communication between Internet of Things (IoT) devices on the same local network has significant implications for platform and device interoperability, security, privacy, and correctness. Yet, the analysis of local home Wi-Fi network traffic and its associated security and privacy threats have been largely ignored by prior literature, which typically focuses on studying the communication between IoT devices and cloud end-points, or detecting vulnerable IoT devices exposed to the Internet. In this paper, we present a comprehensive and empirical measurement study to shed light on the local communication within a smart home deployment and its threats. We use a unique combination of passive network traffic captures, protocol honeypots, dynamic mobile app analysis, and crowdsourced IoT data from participants to identify and analyze a wide range of device activities on the local network. We then analyze these datasets to characterize local network protocols, security and privacy threats associated with them. Our analysis reveals vulnerable devices, insecure use of network protocols, and sensitive data exposure by IoT devices. We provide evidence of how this information is exfiltrated to remote servers by mobile apps and third-party SDKs, potentially for household fingerprinting, surveillance and cross-device tracking. We make our datasets and analysis publicly available to support further research in this area.

Acknowledgment

This work has been published in *Proceedings of the 2023 ACM on Internet Measurement Conference*, IMC '23. DOI: https://doi.org/10.1145/3618257.3624830

References

[1] Aniketh Girish, Tianrui Hu, Vijay Prakash, Daniel J. Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David Choffnes, and Narseo Vallina-Rodriguez. In the room where it happens: Characterizing local communication and threats in smart homes. In *Proceedings of the 2023 ACM on Internet Measurement Conference*, IMC '23, page 437–456, New York, NY, USA, 2023. Association for Computing Machinery.

[*] The two lead authors contributed equally to this work.

ACM IMC 2023
MONTRÉAL
October 24 - 26

Published at IMC'23

In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes

Aniketh Girish*[1,2], **Tianrui Hu*[3]**, Vijay Prakash[5] , Daniel J. Dubois[3], Srdjan Matic[7], Danny Yuxing Huang[5], Serge Egelman[6], Joel Reardon[8], Juan Tapiador[2], David Choffnes[3], Narseo Vallina-Rodriguez[1,4]

[1] IMDEA Networks Institute, [3] Northeastern University, [8] University of Calgary, [5] New York University, [6] UC Berkeley / ICSI, [7] IMDEA Software Institute, [2] Universidad Carlos III de Madrid, [4] AppCensus

Motivation:

Local network communication and its associated threats within smart homes are poorly understood

Device broadcast PII (MAC, IDs, etc.)

Surveillance & Tracking

Broken local privacy protection

Cross-device tracking

Household fingerprinting

Socio-economic status inference

Identifying exploitable devices

Dave's Bedroom Apple TV 08:66:98:xx:xx:xx UUID: xx

Research Questions:

RQ1: What are the characteristics of smart home local network communication?

RQ2: What are the privacy & security threats?

RQ3: Is local network communication abused for fingerprinting and tracking?

Our Data/Testbeds:

Testbed with 93 smart home devices

+ Google Play android

Static, dynamic, and network analysis

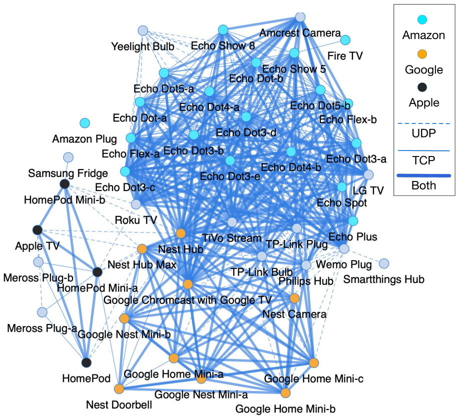
AppCensus

2K IoT and non-IoT mobile apps

+ IoT Inspector: crowdsourced data from 12,669 IoT devices in 3,860 households

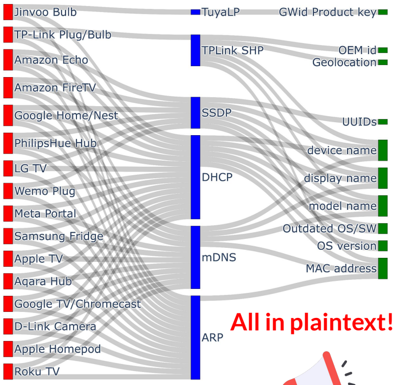
Contributions & Results:

① First Study of Smart Home Local Communication:



While only half of devices use unicast↑, most use broadcast/multicast protocols for discovery ↗②

② Sensitive Data Dissemination Through Discovery Protocols:



All in plaintext!

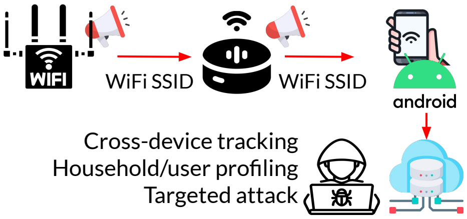
Check out our paper for more characteristics and security & privacy issues we found.

③ Information Harvesting:

Mobile apps and third-party SDKs can harvest data exposed by smart devices **without user consent.**

Several apps & SDKs collect local network data for advertising and tracking purposes.

Bypass Android runtime permission to access WiFi SSID/BSSID:
No user consent. Side-channel
Reported — acknowledged by Google



Cross-device tracking
Household/user profiling
Targeted attack

Potential in-LAN adversaries: Smart TV apps, IoT devices/manufacturers, visitors, roommates, compromised devices, etc.

④ Smart Home Fingerprintability:

Smart home households are easily fingerprinted, enabling cross-device tracking.

- **Data:** mDNS and SSDP from IoT Inspector crowdsourced data
- **3 identifiers:** MAC Address, Names, UUIDs
- **Metric:** Entropy
  Higher entropy → greater fingerprintability

# of Identifiers	Entropy
1	6.7
2	14.5
3	20.1

For Reference, entropy of HTTP User Agent: ~10.5

- Expose 3 identifiers makes your household **highly distinctive.**
- **94.2%** of households can be uniquely identified

institute imdea networks · Northeastern University · uc3m Universidad Carlos III de Madrid · NYU · institute imdea software · Berkeley University of California · ICSI · University of Calgary · AppCensus · ProperData · NSF

Scan QR code for our full paper, code, and datasets