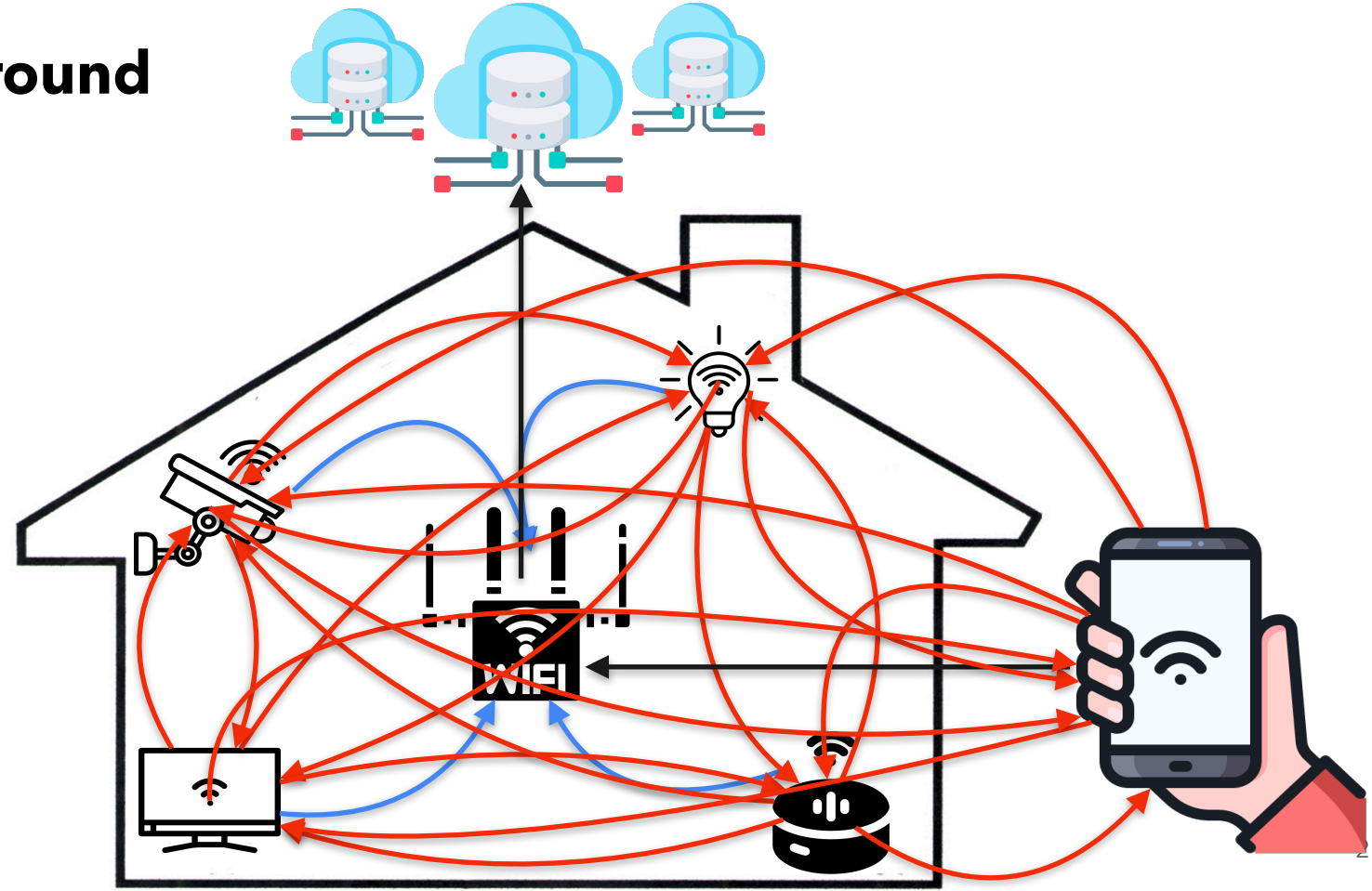
In the Room Where It Happens:
Characterizing Local Communication and Threats in Smart Homes

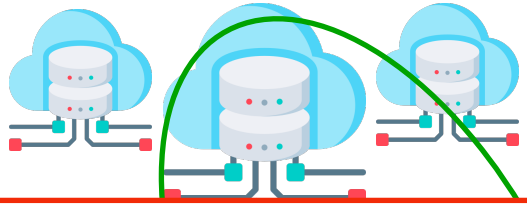
Aniketh Girish
IMDEA Networks Institute

RIPE 89, Prague, Czechia

Background

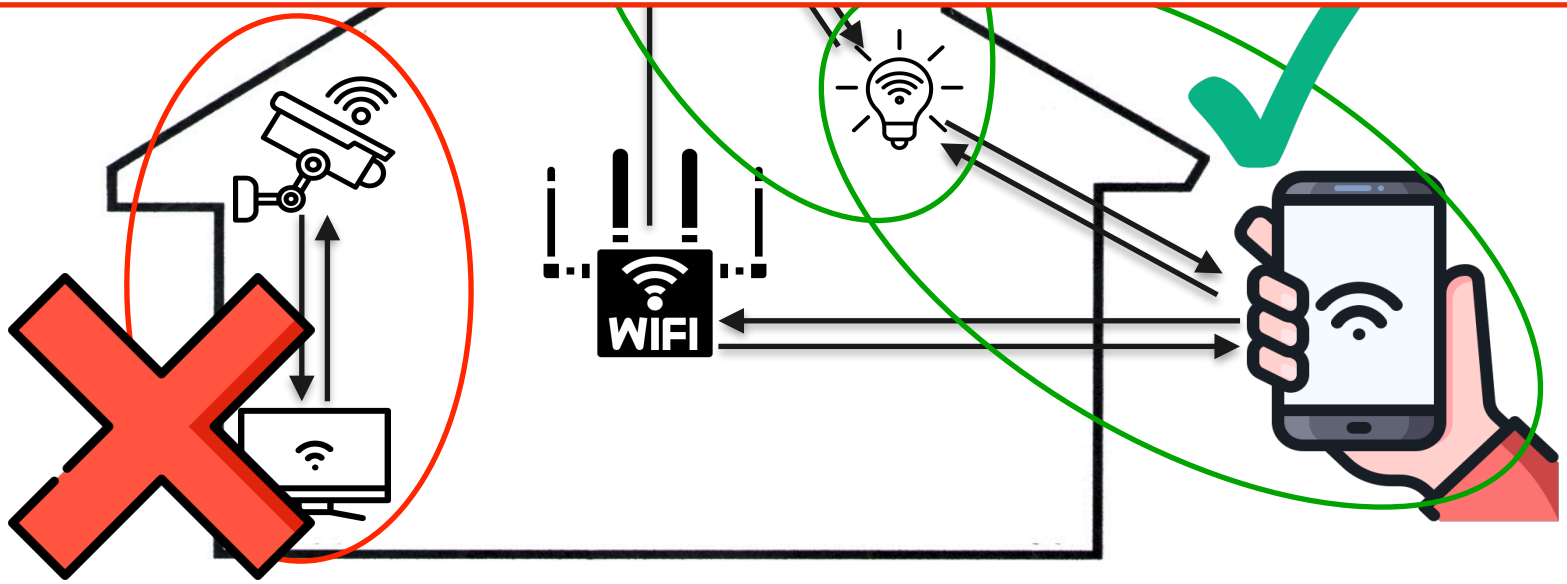


Background

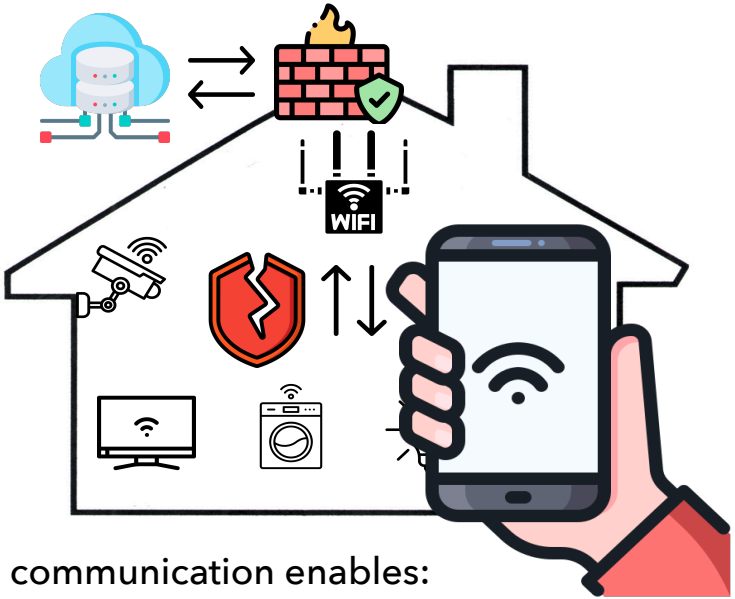


Local communication and its associated threats are poorly understood

Prior work: study the devices or how IoT devices interact with cloud services



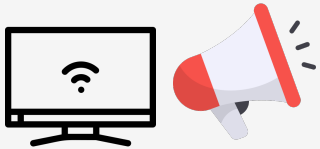
Background



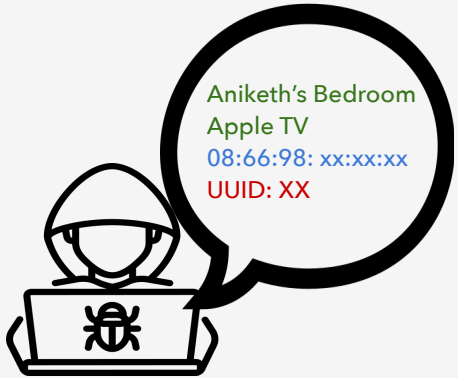
Local communication enables:

- **cross-device tracking**
- **unique household fingerprinting**
- **socio-economic status inference**

Broken local privacy protection



Device broadcast PII (MAC address, device IDs)



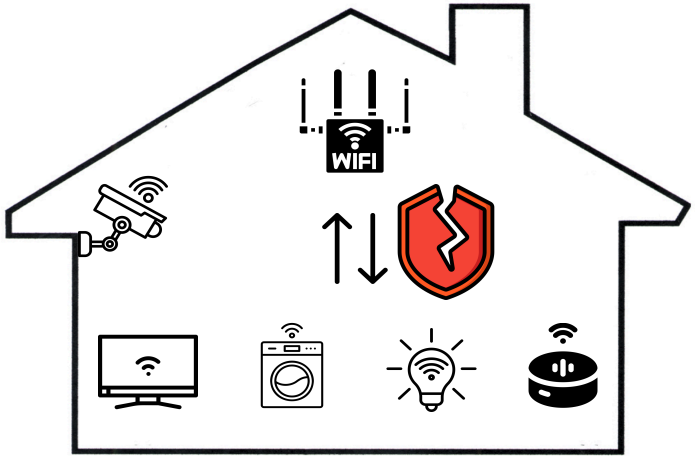
Surveillance & Tracking

Research Questions

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

RQ2: What are the privacy and security threats?

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



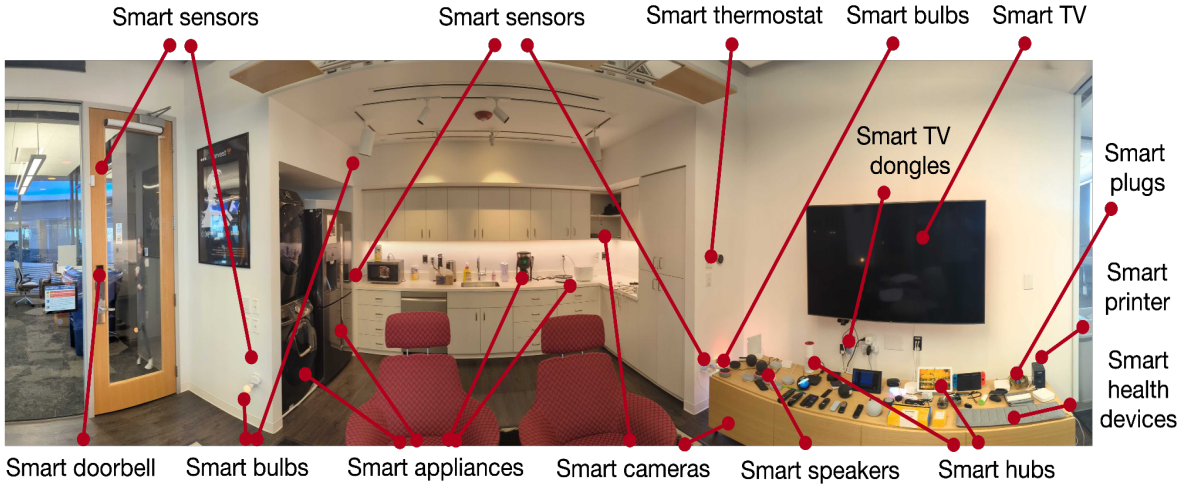
Our Testbed & Datasets

Devices: 93 consumer IP-based smart home devices.

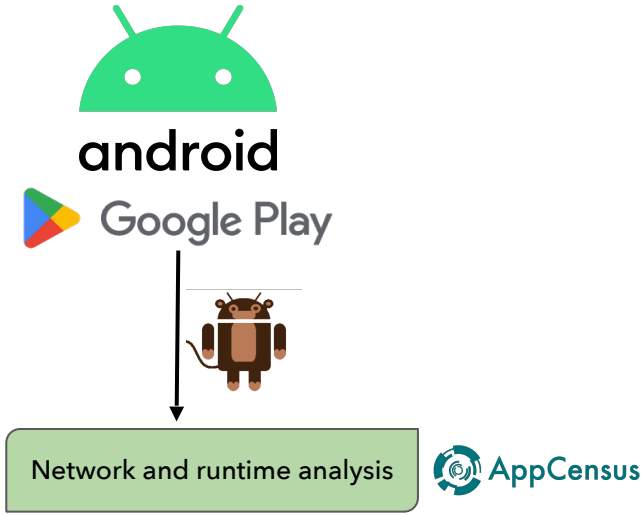
Traffic: We capture all LAN traffic during interactions with IoT devices, and during idle periods.

Honeypot: Issues authentic responses to scan from IoT devices.

Active scan: nmap and Nessus.



Our Testbed & Datasets



2,335 Android mobile apps:

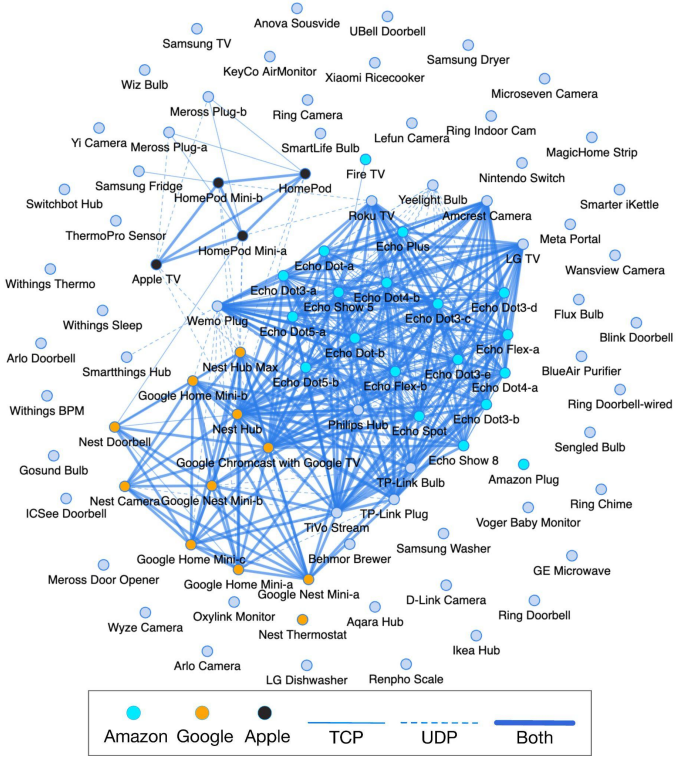
- 987 IoT specific apps (e.g., companion apps).
- 1,348 randomly selected "regular" apps.

IoT Inspector

Crowdsourced IoT network traffic:

- 12,669 IoT devices from 3,860 households.
- 264 products from 165 vendors.
- mDNS and SSDP responses.

How do these devices interact with each other?



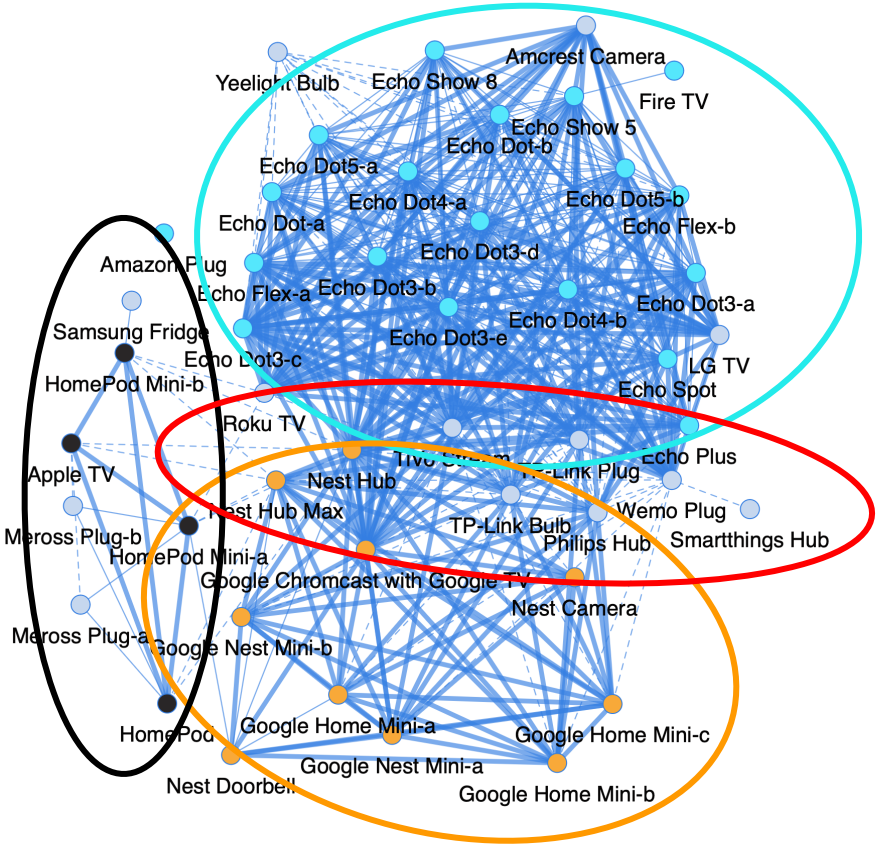
35 different protocols!

Nearly half (43/93) devices communicate via unicast

(mostly) Discovery protocols

- **93% of devices use broadcast**-based protocols e.g., ARP, XID/LLC, DHCP.
- **73% of devices use multicast** ones e.g., mDNS, ICMPv6, SSDP, DHCPv6, IGMPv2/v3, CoAP.

How do these devices interact with each other?



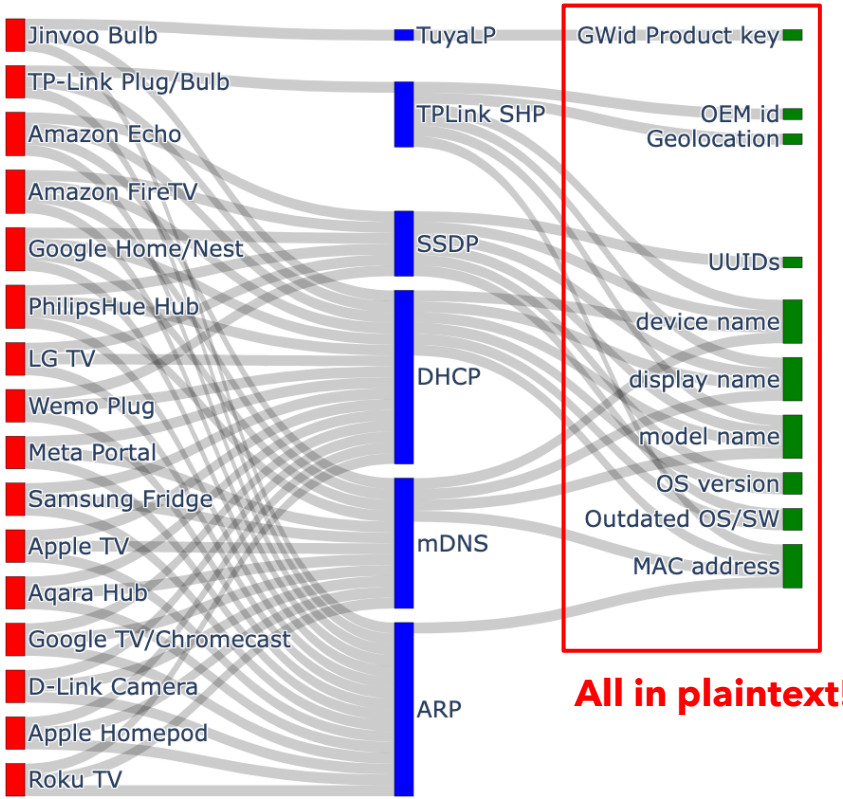
Intra-vendor communication across devices in Amazon, Google, and Apple's ecosystem.

Inter-vendor communication across devices offering interoperable features (e.g., casting, using open-source protocols)

What are the privacy and security threats?

Dissemination of sensitive device and network information through discovery protocols

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



Do advertising and tracking services collect network and device information in the Android platform?

Android Apps and SDKs can scan the local network and collect information exposed by smart devices using only the INTERNET permission (automatically granted at install time).

No user consent required.

Bypass runtime permission to access WiFi SSID/BSSID

Side-channel

Local network scanning is constrained in iOS

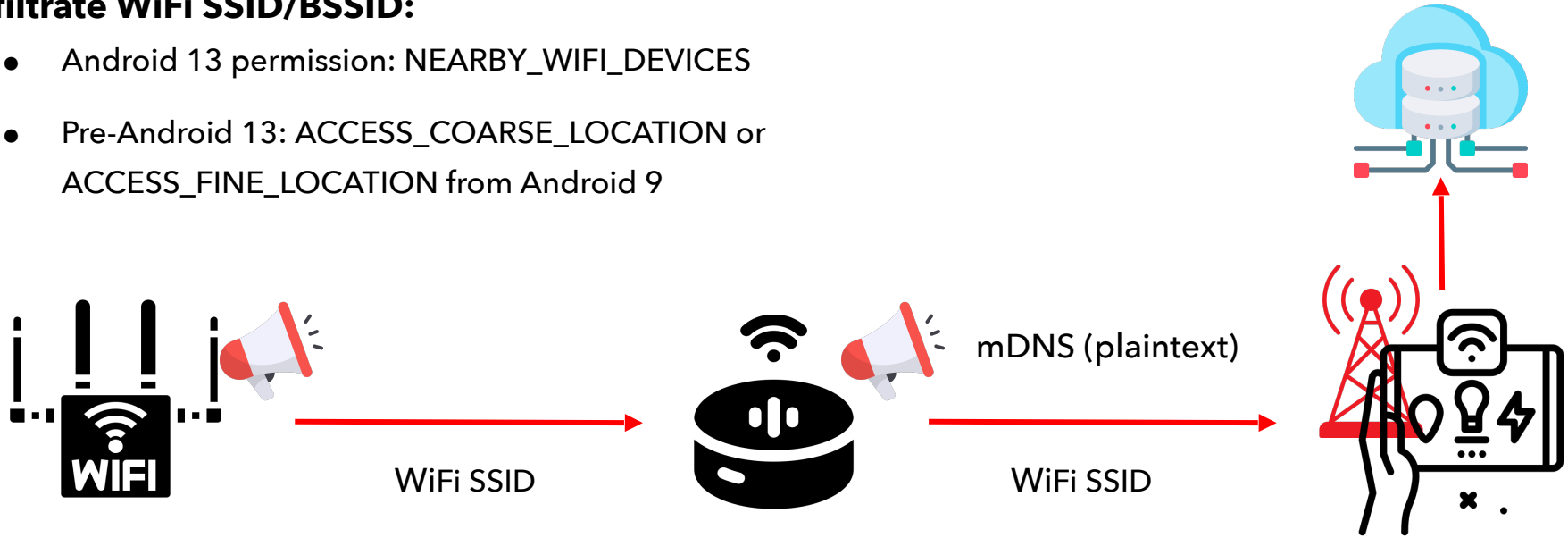
- Developers need **explicit approval from Apple** to access multicast sockets.
- **Permission required**: NSLocalNetworkUsageDescription.

Requests explicit user consent.

Apps and SDKs harvest local network information

Exfiltrate WiFi SSID/BSSID:

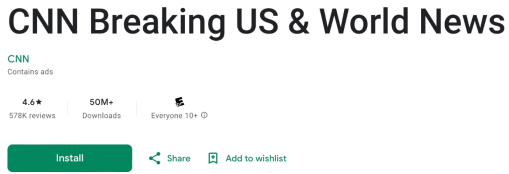
- Android 13 permission: NEARBY_WIFI_DEVICES
- Pre-Android 13: ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION from Android 9



IoT devices relay sensitive information from other devices in local network to mobile apps

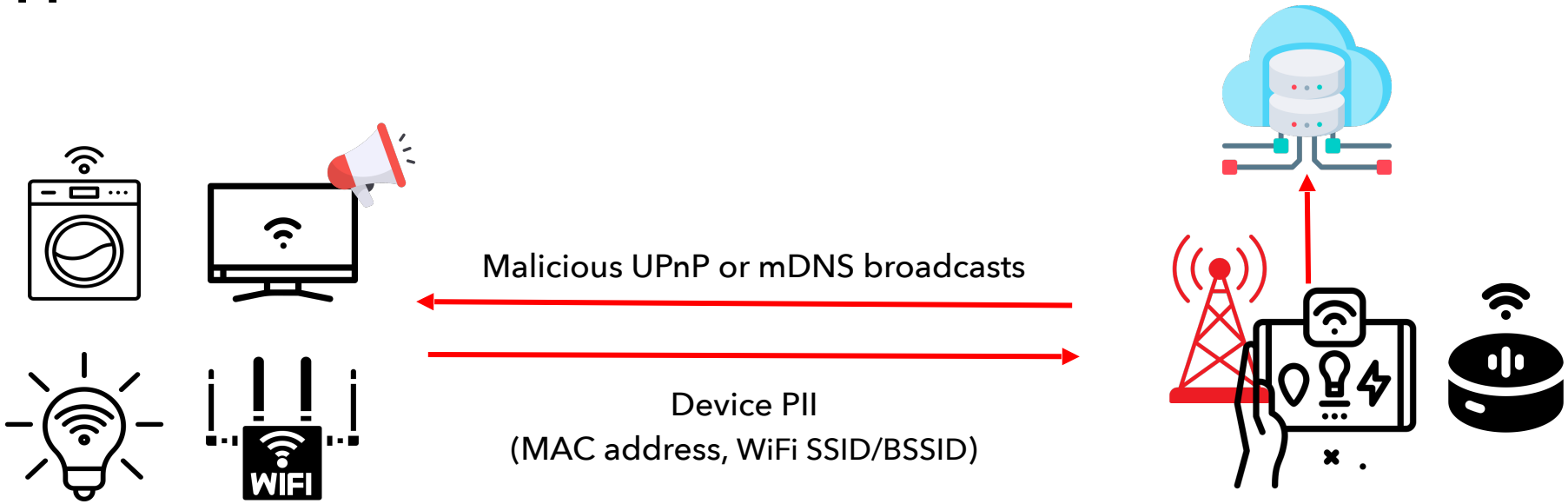
Apps and SDKs harvest local network information for advertising & tracking purposes

- **AppDynamics analytics and profiling SDK** collect device information in SSDP/UPnP messages.




```
HTTP/1.1 200 OK
SERVER: Linux, UPnP/1.0, Private UPnP SDK
...
<?xml version="1.0" ?>
<friendlyName>AMC020SC43PJ749D66</friendlyName>
<serialNumber>9c:8e:cd:0a:33:1b</serialNumber>
<UDN>uuid:device_3_0-AMC020SC43PJ749D66</UDN>
<serviceList>
<service>
```

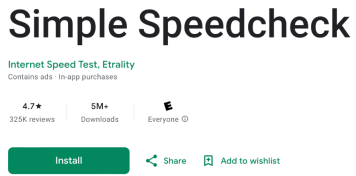
Apps and SDKs harvest local network information



IoT and regular apps & SDK scan and collect MAC address, and WiFi SSID

Apps and SDKs harvest local network information for advertising & tracking purposes

- **Umlaut InsightCore monetization SDK** collects the list of SSDP/UPnP connected devices.



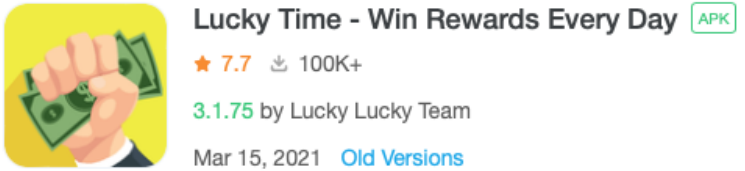

```
    const-string v3, "M-SEARCH * HTTP/1.1\r\nHost: 239.255.255.250:1900
\"ssdp:discover\"\r\nMX: 1\r\nST: urn:schemas-upnp-
org:device:InternetGatewayDevice:1\r\n"

    invoke-virtual {v3}, Ljava/lang/String;→getBytes()[B
    new-instance v5, Ljava/net/DatagramPacket;
    const-string v7, "239.255.255.250"

    invoke-static {v7}, Ljava/net/InetAddress;-
>getByName(Ljava/lang/String;)Ljava/net/InetAddress;
```

Apps and SDKs harvest local network information for advertising & tracking purposes

NetBIOS

- **Innosdk, a third-party anti-cheat and advertising library**

  It sends NetBIOS requests to every IP in the *192.168.0.0/24* prefix and sends local network info to *gw.innotechworld.com* endpoint.



All apps with this SDK have been removed from the Google Play Store

Household fingerprinting

Can exposed local network and device information be used for household fingerprinting?

IoT Inspector dataset: mDNS and SSDP responses from 12k devices from 3.8k households

3 types of identifiers:
(1) Names, (2) UUIDs, (3) MAC Address

Metric: entropy to measure fingerprintability defined by the Electronic Frontier Foundation (EFF)

Higher entropy indicates greater fingerprintability

For reference, entropy of HTTP User Agent: **~10.5**

# of Identifiers	Entropy
1	6.7
2	14.5
3	20.1

Exposing all three identifiers makes your household **highly distinctive**

2,814 households exposed UUIDs; 94.2% of these households can be uniquely identified.

Disclosure & Responses from vendors

- We reported the Android side channel issue to Google.
- We provided a list of misbehaving Android apps to Google.
- We sent reports to 19 IoT vendors regarding potential security issues.
- We contacted regulators in relevant jurisdictions regarding potential privacy issues.

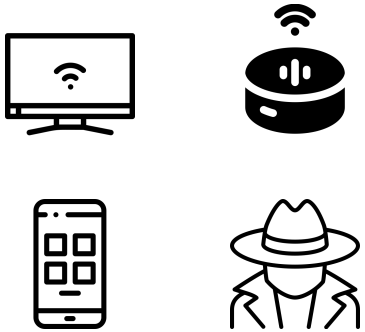
Signify/Hue: new identifier selected at random to replace the current UUID

Google acknowledges this is a real issue and harms users' privacy. Mitigations: **new permissions** in the Android OS, **app review** processes, and general **IoT standardization** efforts.

This attack vector is also exploitable by other in-network adversaries

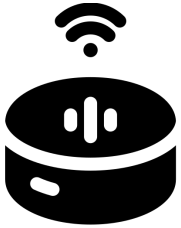
Potential in-LAN adversaries:

- IoT devices (IoT manufacturers, and providers)
- Routers, network service providers
- Smart TV apps
- Visitors, roommates, AirBnB users
- Compromised devices
- …



More (and continuous) research and tooling is needed!
IoT devices are very hard and expensive to test!

Lines of Action



Vendor

- Consider device metadata and identifiers as a sensitive piece of information.
- Privacy by design in local networks protocols and E2E encryption
- Transparency and usable interfaces for control.
- Secure-by-design firmware and timely updates
- Supply chain hardening

Policy

- Regulation: GDPR; EU cyber resilience Act
- Third-party auditing and certification process
- Standardization efforts (CRA, IETF)

Researchers

- Investigate security and privacy threats resulting from integrating elements.
- Testing methods for assisting vendors and independent auditors.
- Design more effective and usable security and privacy controls

Conclusion

- **First characterization:** *local* communication for 93 smart home IoT devices and mobile apps.
- **Sensitive information dissemination**: found in local traffic, including unique IDs, other PII.
- **Fingerprintability and information harvesting**:
  - we demonstrate households are easily fingerprinted, enabling cross-device tracking.
  - we find mobile apps and third-party SDKs harvesting local network information.
- **Disclosure**: We identified responsible parties, ongoing efforts for remediation.

Thank you!

Aniketh Girish
aniketh.girish@imdea.org

The paper. Datasets and code available here: https://github.com/Android-Observatory/IoT-LAN

Extras

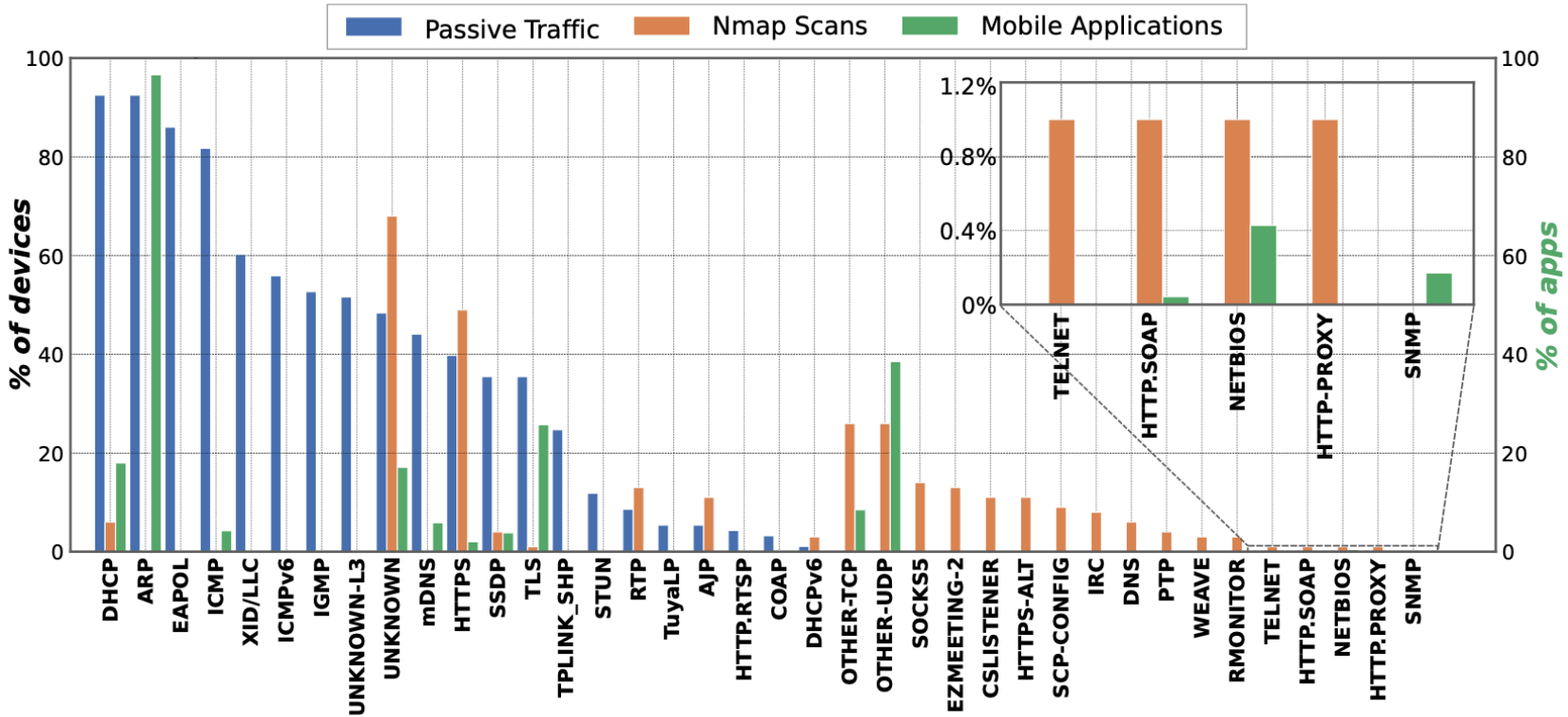


Figure 2: Percentage of protocols observed across the 93 devices deployed in our IoT devices, passively and with the active scans. We report the protocols observed when integrating 2,335 IoT and regular mobile apps. The y-axis values for the mobile app category refer to the number of tested apps observed using these protocols (N=2,335), rather than the number of IoT devices (N=93). The inset zooms into the long tail of the distribution.