Mixed Reality Visualization of IoT Devices

Jad Al Aaraj[1], Isabela Figueira[1], Athina Markopoulou[1]
[1]University of California, Irvine


Jad Al Aaraj


Isabela Figueira

Introduction & Motivation

- IoT devices collect and transmit a lot of data, and often without the user's knowledge.
- IoT traffic is vast in quantity and not easily viewable for consumers.
- Information may be shared with many parties that users are unaware of.
- Users don't have an easy way to find out with whom their IoT devices are communicating.
- Mixed Reality (MR) involves increased user interaction

Contribution

- Mixed Reality (MR) experience for visualizing IoT traffic
- A toolkit to uncover the vast amount of IoT data transmitted over the web to help people realize the privacy implications of these devices.

System

The Raspberry Pi is running the traffic collection program and Pihole. It is also running the backend server for the website and MR app.

All traffic of devices connected to the Raspberry Pi will be logged into a database so that it is fetched later and used for visualization.

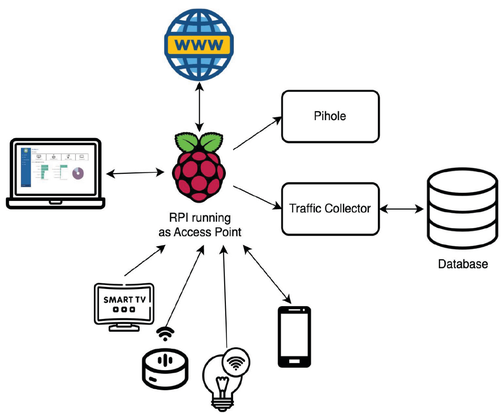
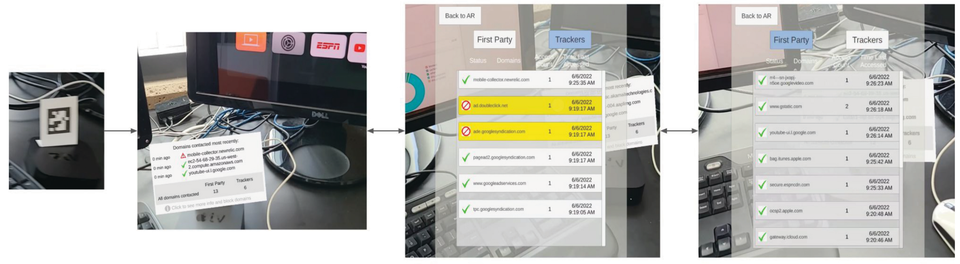


Figure 1: System Diagram

Mobile Application

- ***Traffic Visualization***: Users can view traffic per device. Traffic is classified into trackers and non trackers. The user can see the most recent domains contacted and will be warned of tracker domains. ⚠ The Recent Information Panel also shows the number of times each domain was contacted and the time last contacted.
- ***Mixed Reality Interaction***: Users can interact with the virtual Recent Information Panel within MR and with the traffic by blocking/unblocking tracker domains.



(a) (b) (c) (d)

Figure 2: Flow of the MR application. (a) The ArUco marker to be detected. (b) The Recent Information Panel is overlaid in the environment once the marker is detected. The user may click on the Recent Information Panel to see more information regarding (c) Trackers and (d) First Party domains.

Website

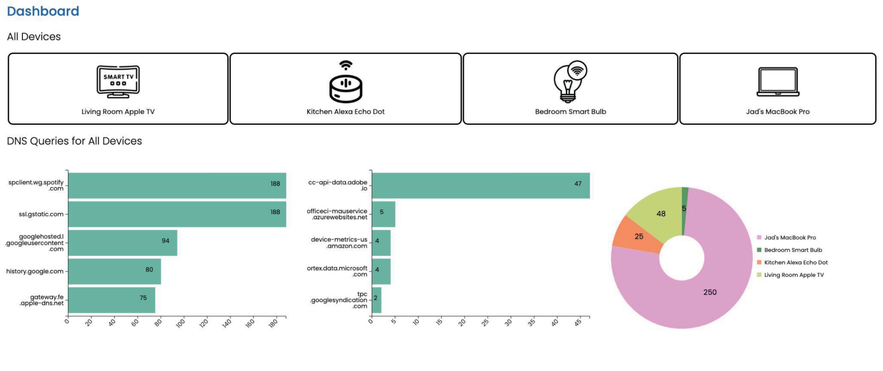


Figure 3: Website dashboard shows all registered devices on the network. The bar graphs show the domains and trackers most contacted. The pie chart shows the domains contacted per device. The user can also click on the devices to more detailed information for that device.

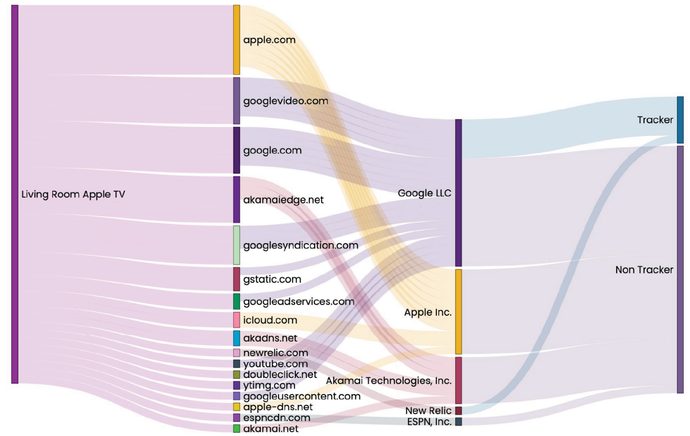


Figure 4: Display traffic flow starting from the device to domain, then categorizing what organizations the devices are contacting, and finally whether these domains are deemed trackers or not.

Conclusion & Future Work

- We delivered methods to collect and analyze IoT traffic and to block and unblock domains from being contacted.
- We also delivered an MR visualization of the IoT traffic that is interactive, user friendly, and provides a clean user interface that keeps information overload in check.
- This MR visualization has the potential to increase awareness of privacy risks in IoT as well as give users the opportunity to engage with their IoT devices' communications.
- This project has opportunity for future work in network traffic analysis and MR.

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]