Commonwealth Cyber Initiative

University of Virginia

Synthesizing Inference Attacks and Defenses in Smart Home IoT Devices

Smart Home:

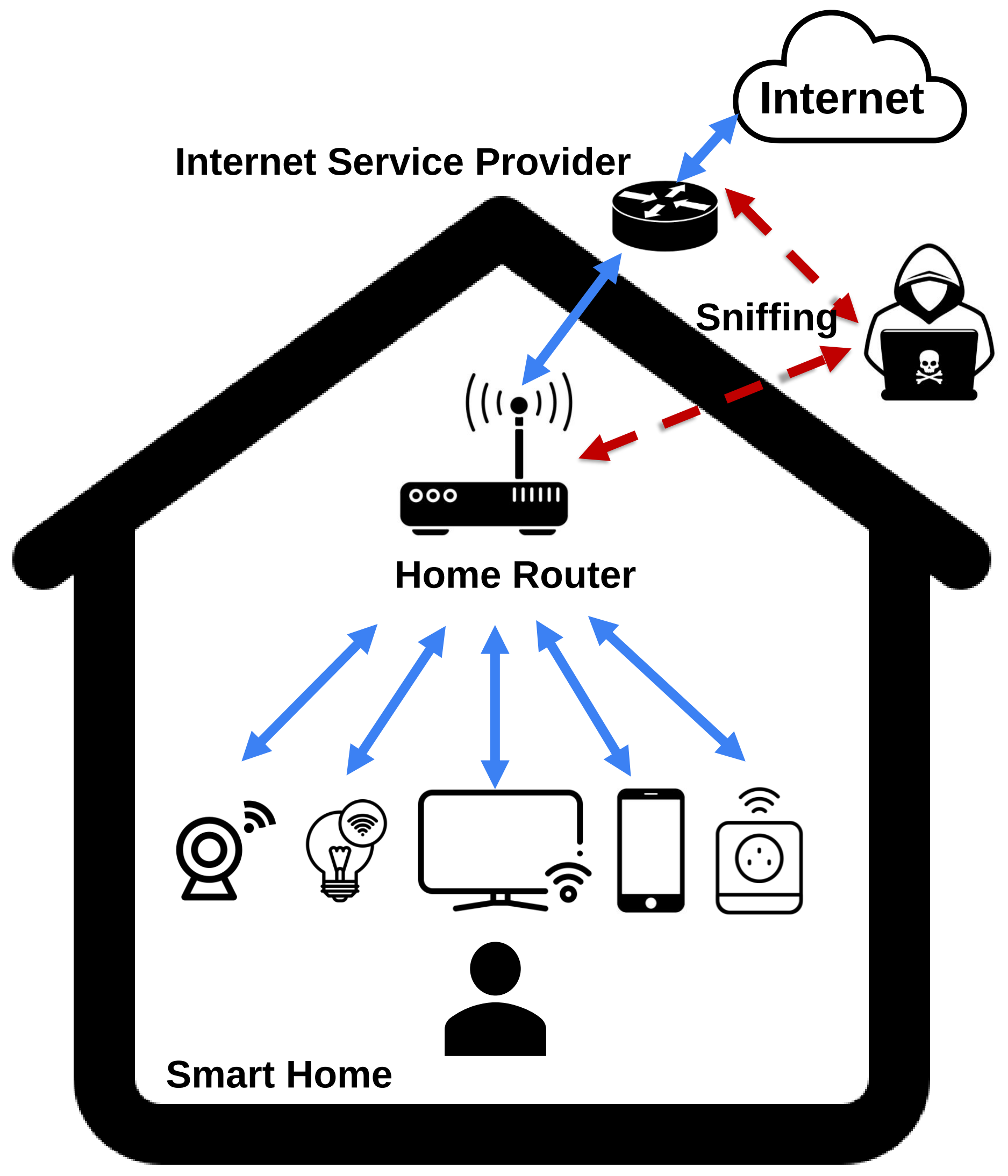
Smart homes, characterized by interconnected Internet of Things (IoT) devices, represent a modern paradigm of convenience and efficiency. These devices, spanning from smart thermostats to security cameras and voice assistants, collect and exchange data to automate tasks and enhance user experiences.

Traffic Sniffing:

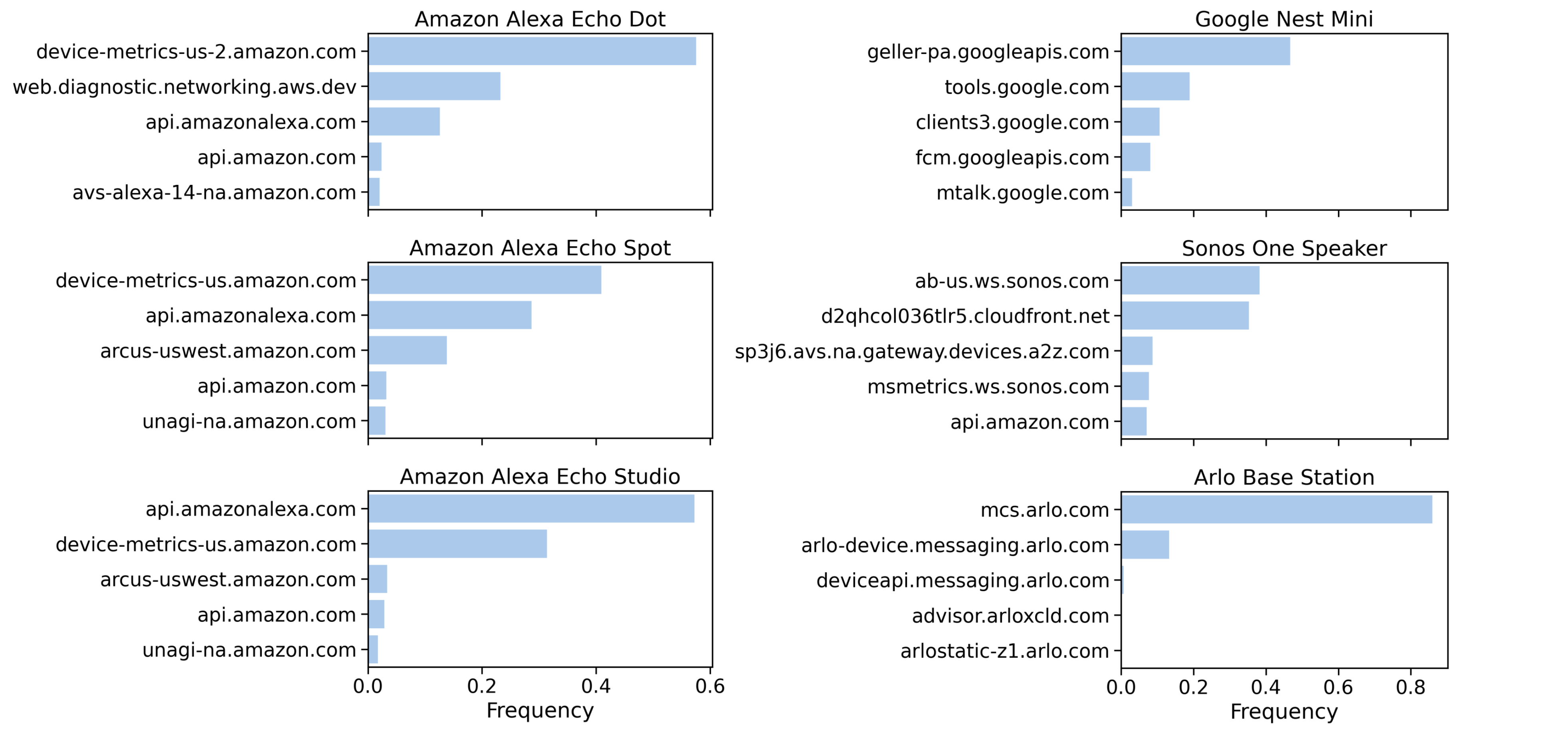
Traffic sniffing involves intercepting and analyzing data packets as they traverse the network, providing attackers with insights into the communication between devices and backend servers.

Inference Attacks:

By analyzing patterns in the network data, attackers can deduce personal habits and routines, potentially compromising the privacy and security of smart home occupants. As the adoption of IoT devices continues to expand, addressing the threat of inference attacks caused by traffic sniffing becomes crucial to safeguarding the confidentiality of user data and preserving trust in smart home technologies.



IoT Device Visualization



Features:

Volume based:

These features characterize the amount of data transferred between IoT devices and network servers during a given time window.

Domain based:

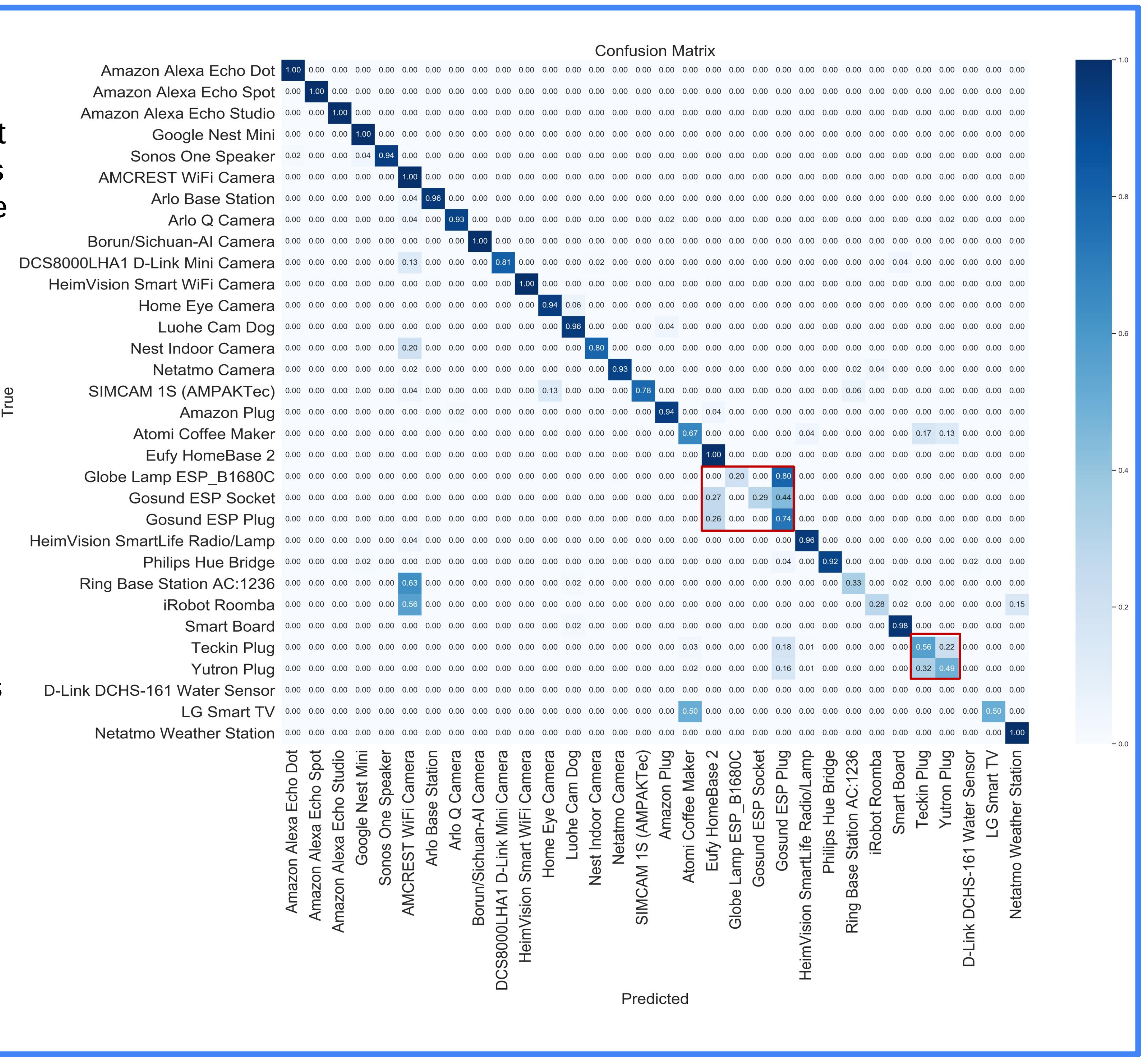
These features capture the most popular domains sent by IoT devices within a specified time window.

Ciphersuites based:

Ciphersuites refer to the combination of cryptographic algorithms used for securing communication channels between IoT devices and servers. These features capture the ciphersuites negotiated during the establishment of secure connections.

Port based:

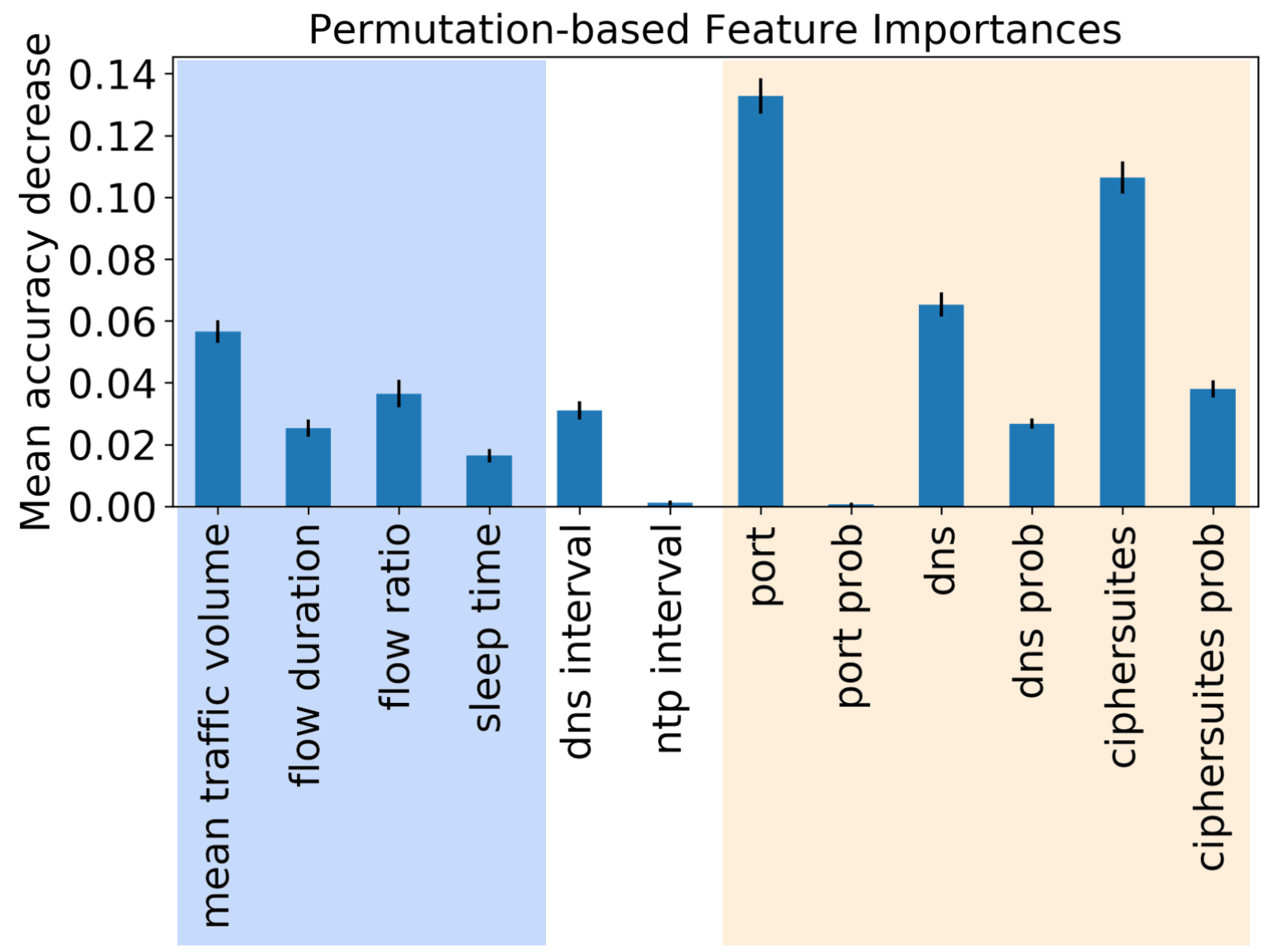
These features capture the most popular port used by IoT devices within a specified time window.



Do Defenses Against Inference Attacks Truly Stand Up?

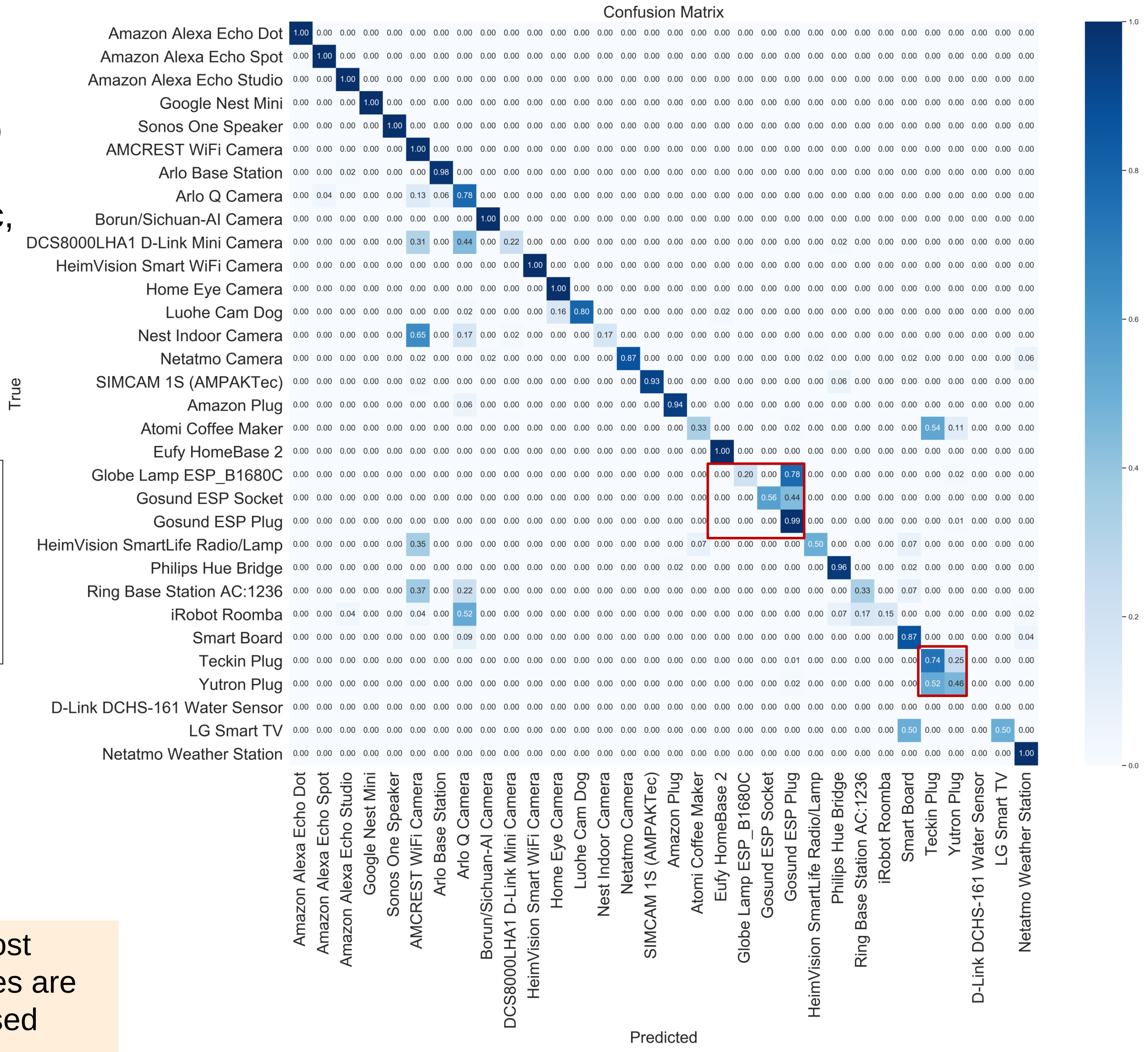
Traffic morphing:

The most popular defending techniques used in cybersecurity to evade inference attacks by altering the characteristics of network traffic, such as adding delays between packets padding packet, and inserting dummy packets.



Most defenses focus on volume-based features.

However, the most important features are specific to the used software stack.



Inference attack without any volume-based features.

Title: Synthesizing Inference Attacks and Defenses in Smart Home IoT Devices

Authors: Yizhe Zhang, Guancheng Tu, Yixin Sun

Affiliation: University of Virginia

cyberinitiative.org