CRII: SaTC: Fingerprinting Encrypted Voice Traffic on Smart Speakers (CNS-1947913)

PI: Dr. Boyang Wang (boyang.wang@uc.edu)

Project web: https://homepages.uc.edu/~wang2ba/nsf_crii.html

UNIVERSITY OF Cincinnati

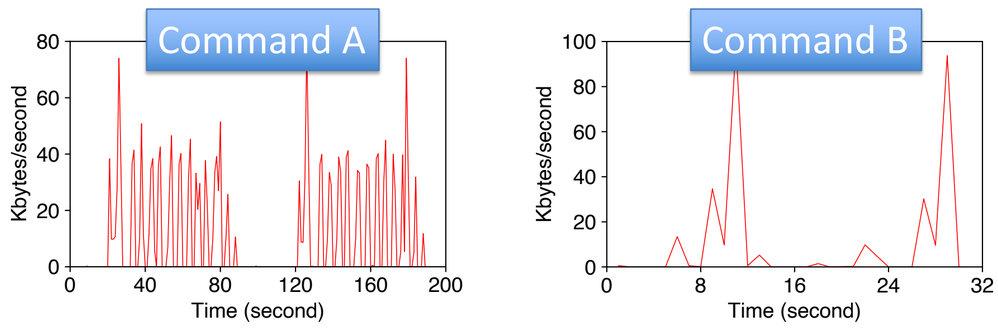
Program Overview: This project investigates the privacy leakage of smart speakers under voice command fingerprinting attacks over encrypted traffic and develops effective defenses against fingerprinting attacks on encrypted traffic. Voice command fingerprinting attacks infer which voice command a user says to a smart speaker by eavesdropping side-channel information (e.g., direction, size, and time intervals) of encrypted network packets.

Main Thrusts:

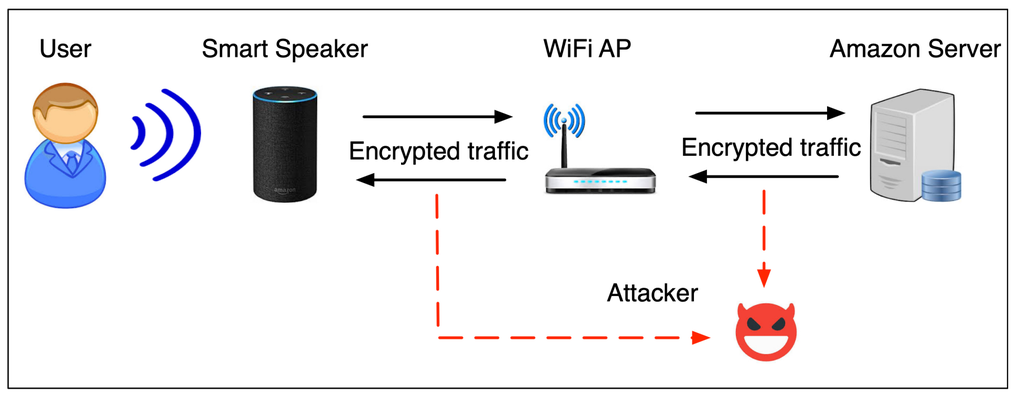
- Produce large-scale datasets for research
- Fingerprint with high accuracy using deep neural networks
- Build efficient defense by finding which packets' side-channel info are significant
- Develop effective defense with on-the-fly adversarial examples

Why Is The Attack Feasible?

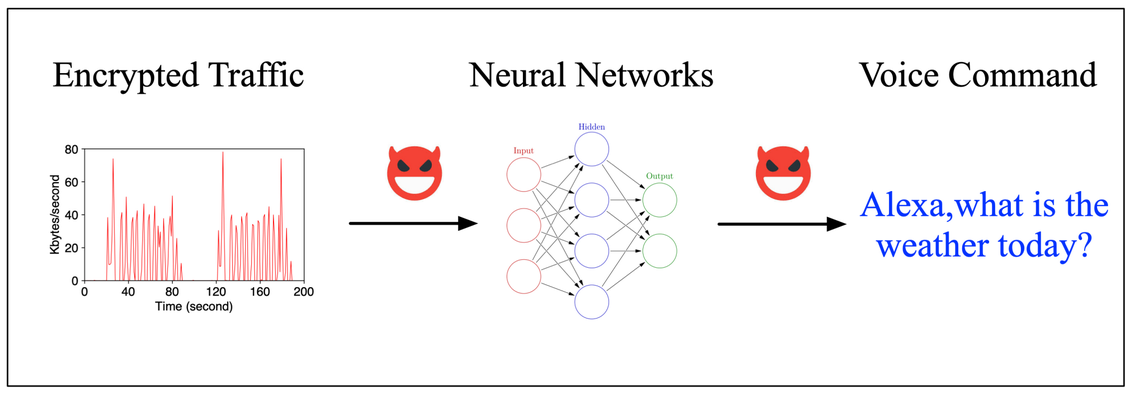
- Each command generates a unique network traffic pattern due to relatively deterministic responses generated by AI on the server



Threat Model:

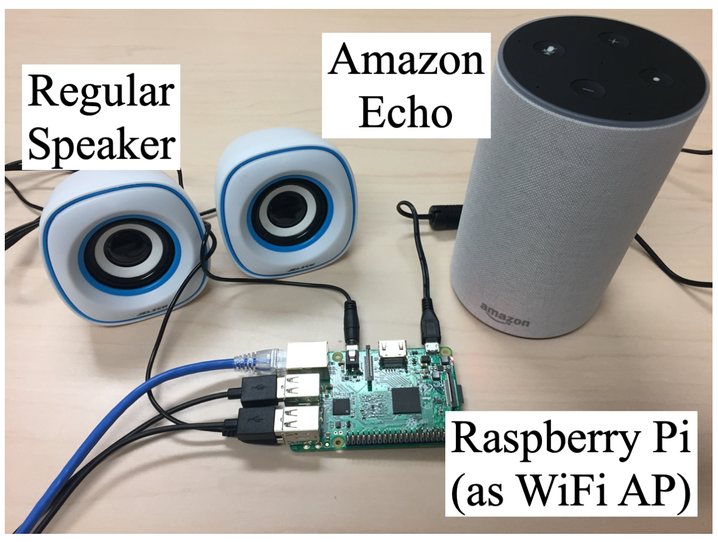


Attack Flow:



Main Results and Findings:

- An automatic tool for collecting voice traffic
- A large-scale dataset (5 voices, 100 voice commands, 1,500 traces/command, Amazon Echo & Google Home, 60 GBs)
- Attacker can achieve 89% accuracy using CNNs
- Proposed effective defense can reduce accuracy to 32%
- Expand studies to stream fingerprinting (YouTube traffic) and website fingerprinting (Tor traffic)
- Demonstrate transfer learning can overcome discrepancies between training & test and reduce the size of training data



Broader Impacts:

- Code and datasets available on GitHub
- Datasets have been utilized by researchers from 6 universities
- 4 REU students are supported through REU supplements.
- 6 presentations at local meetups and conferences

Main Publications:

- H. Liu et al. "AdvTraffic: Obfuscating Encrypted Traffic with Adversarial Examples," IEEE/ACM IWQoS 2022
- H. Li et al. "Cache Shaping: An Effective Defense against Cache-Based Website Fingerprinting," ACM CODASPY 2022
- C. Wang et al. "Fingerprinting Encrypted Voice Traffic on Smart Speakers with Deep Learning," ACM WiSec 2020