CRII: SaTC: Fingerprinting Encrypted Voice Traffic on Smart Speakers

Research Problems:

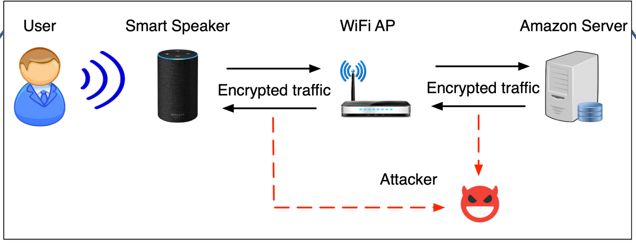
- Can an attacker reveal which voice command a user says to a smart speaker by analyzing encrypted network traffic?
- How can we protect user privacy against attackers?

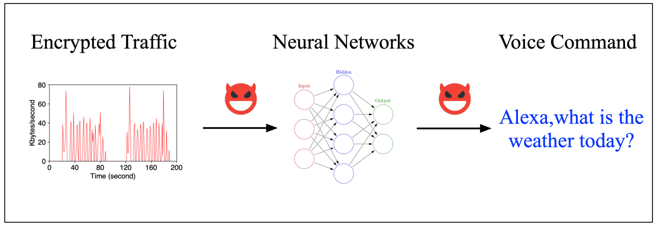
Solution:

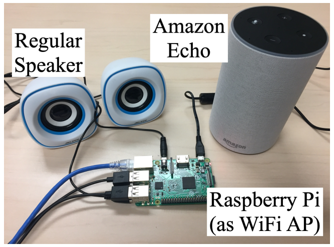
- Fingerprinting voice commands with deep neural networks
- Examine which packets are critical to privacy leakage
- Obfuscate network traffic with no delay

Award Number: CNS-1947913

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







Scientific Impact:

- Build large-scale datasets for research & reproducibility
- New approaches to protect privacy of network traffic in addition to encryption

Broader Impact:

- Identify new privacy leakage of smart speakers & AI-based voice services
- Datasets have been used by 6 universities
- 4 undergrads (1 underrepresented, 1 veteran) participating research