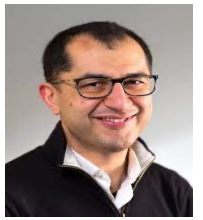
PowerCut and **Obfuscator**: An Exploration of the Design Space for Privacy-Preserving Interventions for Voice Assistants

Varun Chandrasekaran, Suman Banerjee, Bilge Mutlu, Kassem Fawaz






WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

Voice Assistants: A Blessing!

Home automation

Music

Third party apps

Weather

Timer

Information bank

News

Lists

Shopping

So What's the Problem?

Passive Threats

Amazon's Alexa Never Stops Listening to You. Should You Worry?

'Alexa, are you invading my privacy?' – the dark side of our voice assistants

July 2, 2021
11:43 AM EDT
Last Updated 16 days ago

Technology

Google must face Voice Assistant privacy lawsuit -U.S. judge

U.S.

Healthcare Workers Sue Amazon Over Potential HIPAA Violations With Alexa Device

BY EMMA MAYER ON 7/2/21 AT 5:01 PM EDT

Active Threats

BackDoor: Making Microphones Hear Inaudible Sounds

Nirupam Roy, Haitham Hassanieh, Romit Roy Choudhury

University of Illinois at Urbana-Champaign

Inaudible Voice Commands: The Long-Range Attack and Defense

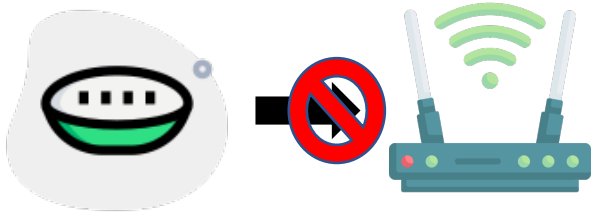
Nirupam Roy, Sheng Shen, Haitham Hassanieh, Romit Roy Choudhury
University of Illinois at Urbana-Champaign

IMPERIO: Robust Over-the-Air Adversarial Examples for Automatic Speech Recognition Systems

Lea Schönherr, Thorsten Eisenhofer, Steffen Zeiler, Thorsten Holz, and Dorothea Kolossa
Ruhr University Bochum
{lea.schoenherr,thorsten.eisenhofer,steffen.zeiler,thorsten.holz,dorothea.kolossa}@rub.de

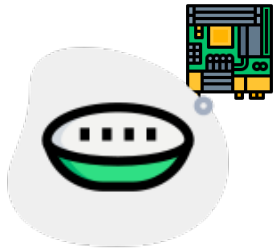
Strawman Solutions

Network Traffic Interception



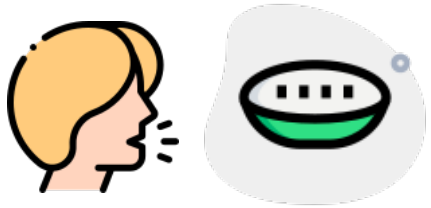
- Hard to understand
- Susceptible to passive & active threats
- Encrypted traffic

Hardware Modifications



- Hard to understand
- Susceptible to passive & active threats

Wake Word Change



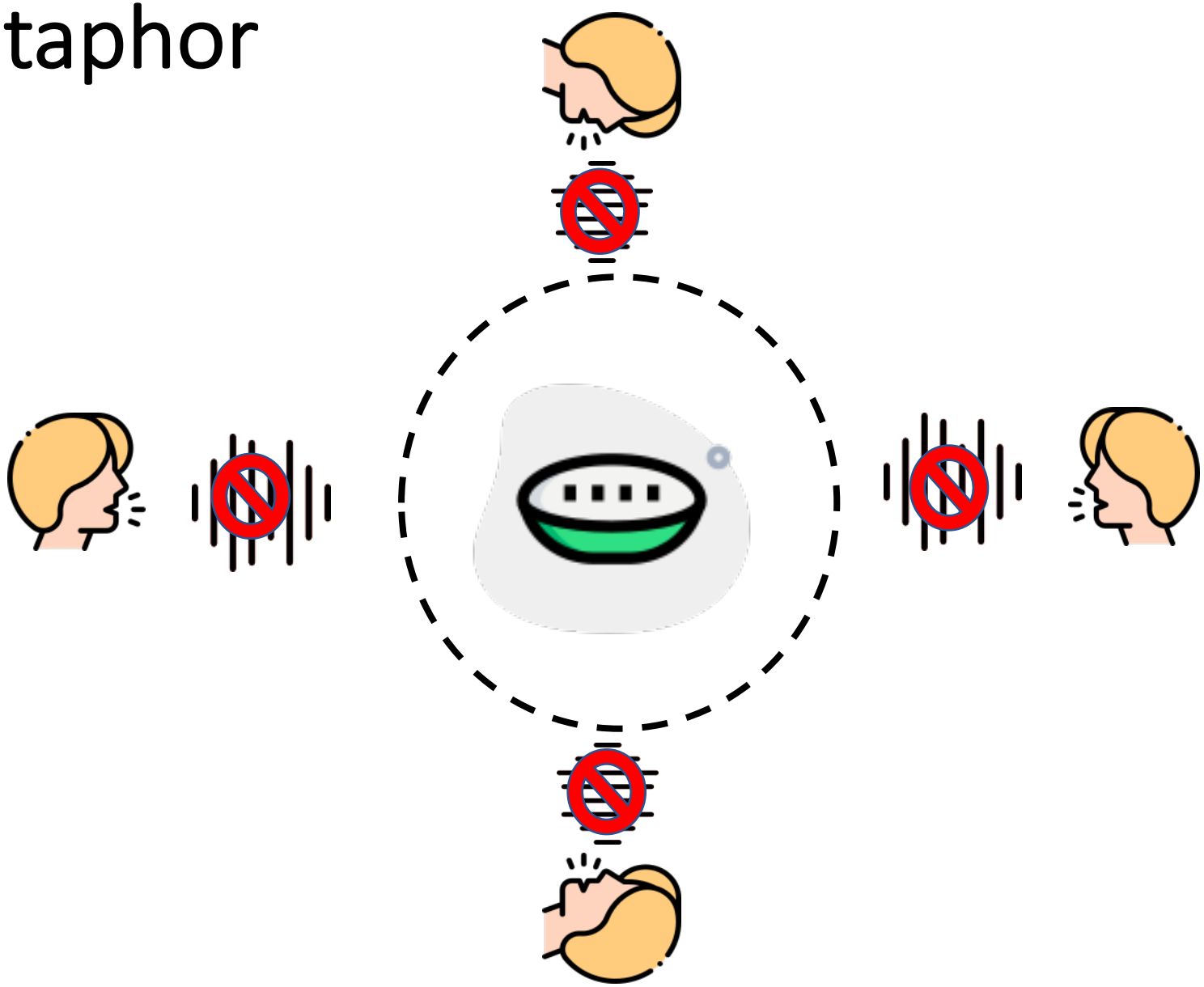
+ Simple to perform & follow
- Susceptible to active threats

Smart Speaker Discarding

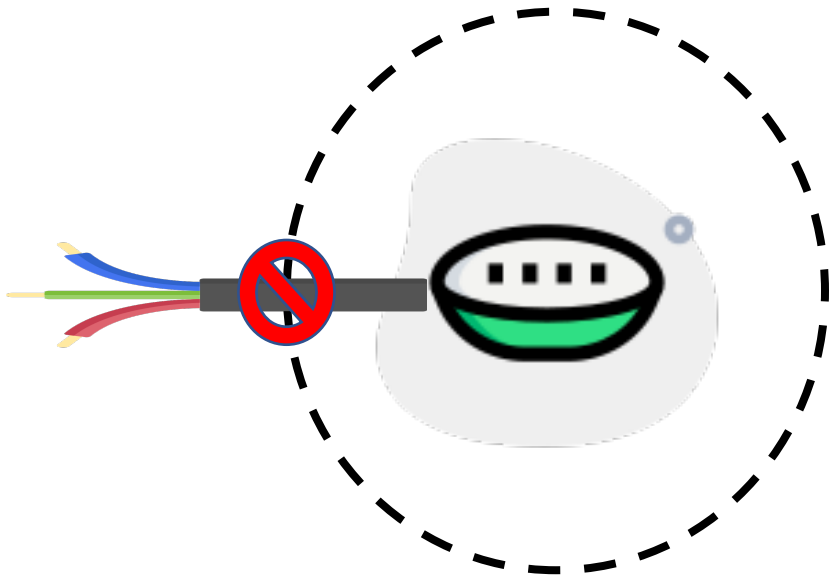
+ Perfect privacy!
- No utility

Privacy Metaphor

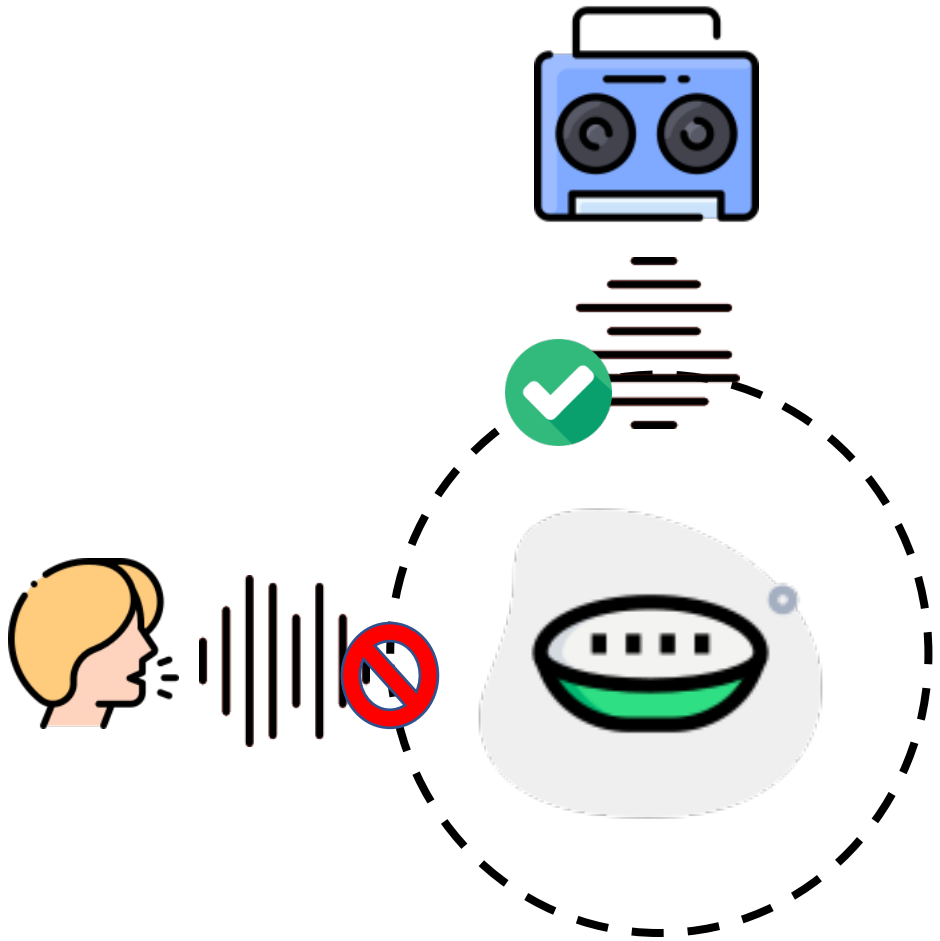
“Virtual Veil”



Metaphor Realizations



Cut the Power



Jam the Command

Our Proposals

Baseline: In-built Mute button

PowerCut

+ Familiarity
+ Inexpensive
+ Intuitive guarantee
- Slow boot-up times
- Form factor

Obfuscator

+ Customizable
+ Inexpensive
+ Provable guarantee
- Form factor
- Non-intuitive

Study Details

- **Tech probe study**

- 30 participants (24 families)
  - 15 males, 15 females; 12-67 years of age
  - 40 USD, IRB approved

- 2 years
  - Phase 1: 2018, Phase 2: 2019

- 2 independent coders
  - Cohen's Kappa = 0.57
  - 200 informal codes, 88 informal codes, 15 axial codes

Findings

Trust in technology:
Business model should be different

Multi-functionality:
Privacy protection is secondary function

Cost:
Cheaper than smart speaker

Ease of deployment:
Located conveniently for fixing issues

Informative cues:
State of operation must be clear

Ease of understanding:
Relatable privacy metaphor

Aesthetics & Physical footprint:
Customizable & Integrate with home decor

Mode of interaction:
Hands-free

Fine-grained privacy control: Customizable per-user privacy control

Thanks for listening!
Questions?

Varun Chandrasekaran

chandrasekaran@cs.wisc.edu

VarunChandrase3

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON