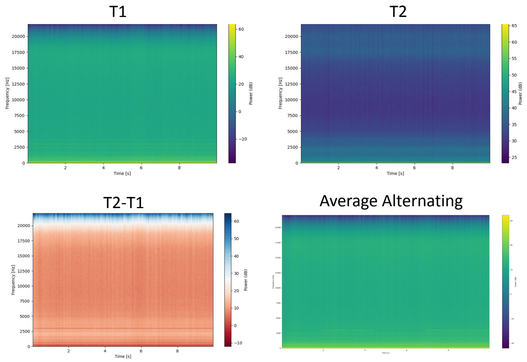
Microphones on Laptops Leak Information Remotely Over VoIP

Lent an Ear
Reproducing the work of Lend Me Your Ear

PRESENTER: **Domenic Lo Iacono**

ADVISOR: **Billy Bob Brumley**

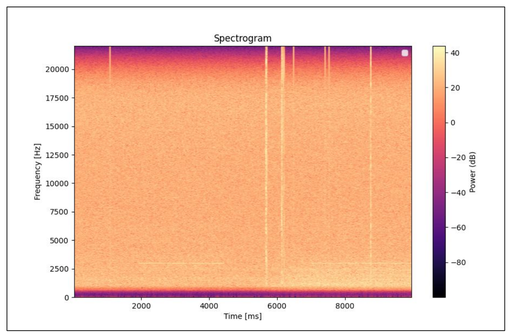
Main Finding: Passive remote side channel attacks targeting VoIP calls are accessible and effective



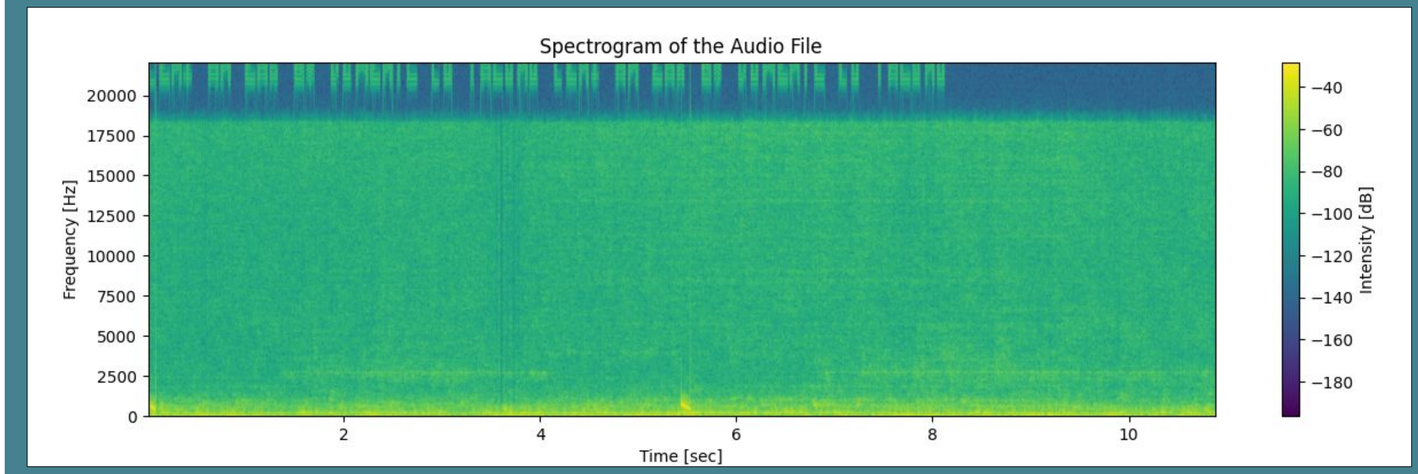
Local Experiment: Difference of Means with CPU tasks

- Used to isolate leakage patterns
- T1 is with no added CPU load
- T2 is with CPU load via a test program
- The differential is T2-T1
- Alternating a single CPU process and taking the average results in a clear differential as well

Remote Experiment: Show the same patterns through a VoIP call utilizing Mumble. Zoom, Discord, Google Meet, and other popular solutions are impacted as well



RIT | Golisano College of Computing and Information Sciences
Department of Computing Security



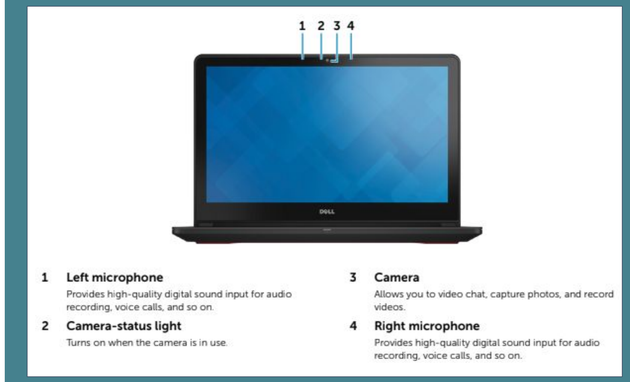
Side-channel analysis targets the physical leakage of information such as power consumption, electromagnetic emissions, and timing.

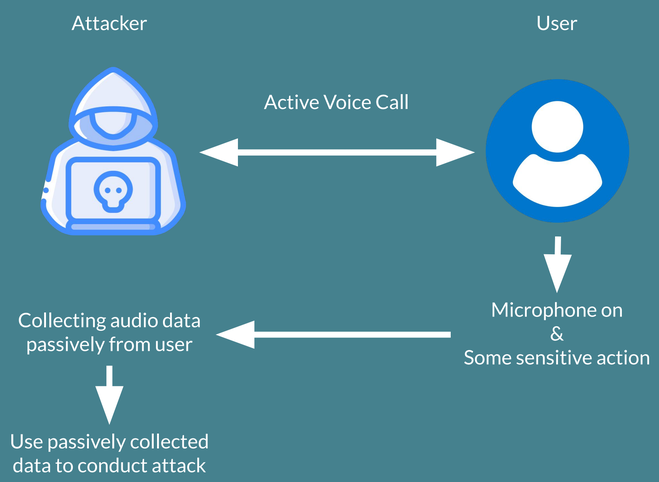
Most consider physical proximity required for this class of attacks.

Lent an Ear and Lend Me Your Ear are an exception to this as they leverage the physical leakage being sent over Voice Over IP calls from the device's internal microphone.

This leakage is electromagnetic in nature which allows it to be picked up by the microphone across a wide array of frequencies across normal human hearing of 20 to 20,000 Hz.

Note: you can't hear electromagnetic interference as it is not a mechanical wave like sound waves.



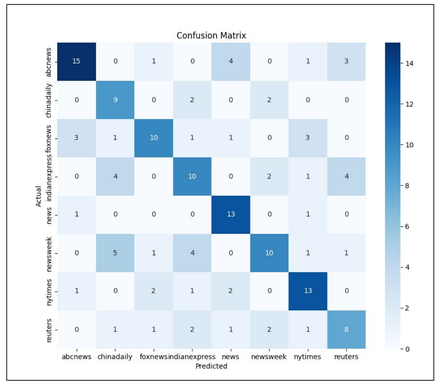


FAQs:

- Is my device vulnerable to this attack?
  - If your device has a built in microphone, most likely yes.
- What about external microphones?
  - A related work, "Synthesia" shows that a variety of microphones including phones and Google Home devices can pick up acoustic leakage from monitors. Further testing for the techniques in Lend Me Your Ear is needed.
- What mitigations can be put into place?
  - Restrict access to the microphone and ensure trust between all parties connected to the VoIP call, including group meetings!

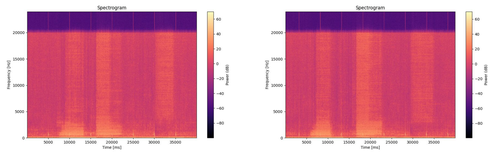
Website Fingerprinting

Main Finding: User activity can be inferred from remote leakage patterns



Experiment: Capture audio recordings 40 seconds each of a browser opening a news website and attempt to associate each CPU timing pattern with the site

- Utilized a CNN
- This technique is known as *profiling*
- Below are two spectrograms from the same website exhibiting a pattern



Future work: The authors of Lend Me Your Ear showed two additional attack vectors

1. A CPU timing attack against ECDSA nonces
2. A game hacking scenario against CSGO

Further work includes testing cross device profiling, external microphone testing, and integrating keystroke identification from audio data.

View the Github repository for more information and the full paper.