

Acoustics in Computer Security

Ilia Shumailov

Me

- Ilia
- 4th year PhD student at University of Cambridge
- Security background
- Primary research interests:
 - Adversarial ML
 - Surveillance technology
 - Cybercrime

Acoustics

- Acoustics deal with **mechanical waves** in gases, liquids and solids
 - Vibration
 - Audible Sound
 - Ultrasound
 - Infrasound
- Humans primarily use acoustics for communications

Acoustics and Privacy

- Humans use acoustics to exchange information
- Surveillance is possible and is often easy
- Everything vibrates, often removing acoustic leakage requires active counter-measures



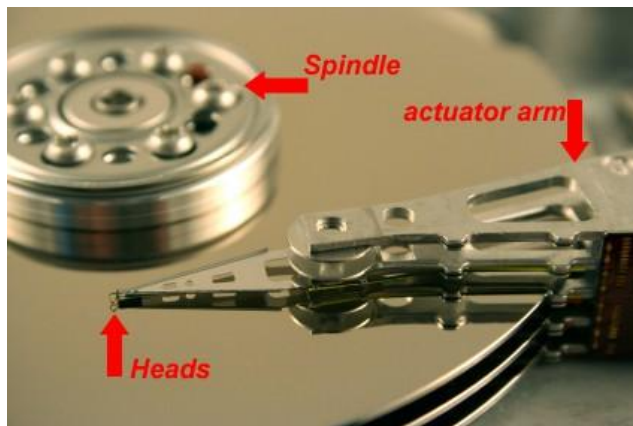
Hearing speech

Speech and Privacy: The Thing (1945)



“The **microphone** hidden inside **was passive** and only activated when the Soviets wanted it to be. They shot radio waves from a van parked outside into the ambassador's office and could then detect the changes of the microphone's diaphragm inside the resonant cavity. When Soviets turned off the radio waves it was virtually impossible to detect the hidden ‘bug.’ The Soviets were able to eavesdrop on the U.S. ambassador's conversations for **six years.**”

Speech and Privacy: Hard Drives (?)



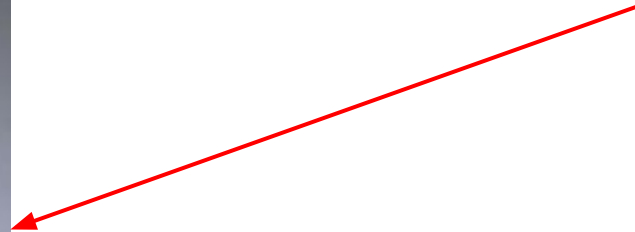
“The offset is referred to as the Positional Error Signal (PES) and hard drives monitor this signal to keep the read/write head in the optimal position for reading and writing data. PES measurements must be very fine because drive heads can only be off by a few nanometers before data errors arise. The sensitivity of the gear, however, means human speech is sufficient to move the needle, so to speak.”

PES has sampling rate of 34.56 kHz, essentially PCM encoded

DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise, Guri et al. 2016)

Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone (Kwong et al. 2019)

Speech and Privacy: Lasers and Coffee cups (?)



- Humans speak, air vibrates, windows vibrate
- Wave shifts can be detected
- Look at the reflection of the coffee cup, chips or stickers
- ``The witness claimed that he had been asked by Morales to place stickers in the windows to make it easier for the US to use lasers to listen to conversations in the embassy.``

Speech and Privacy: WIFI routers (2014)

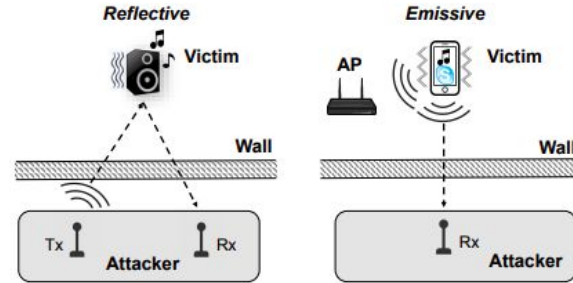
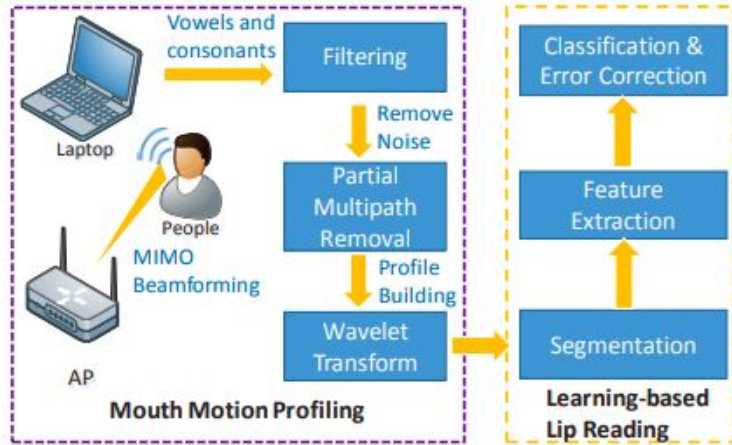
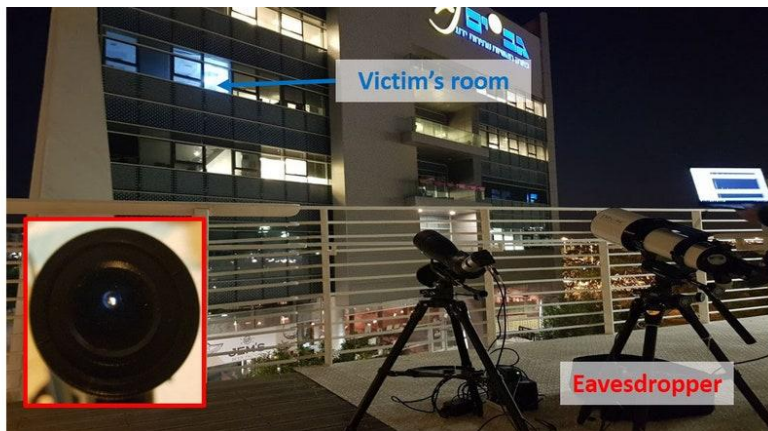


Figure 1: Two threat models based on wireless vibrometry: *Reflective* and *Emissive*.

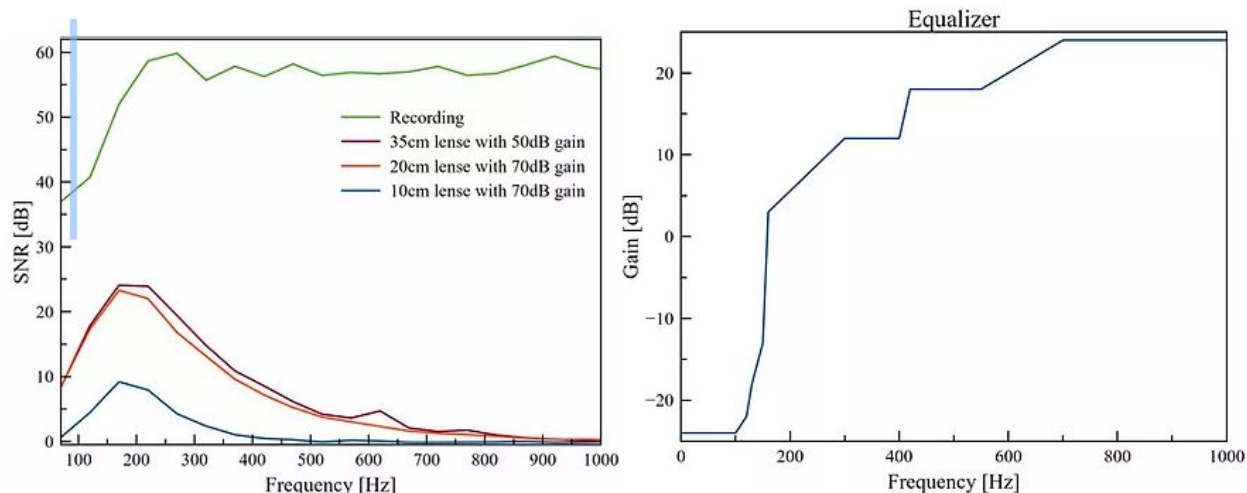
- Captures fine-grained radio reflections from mouth movements
- Work outside of line-of-sight!
- Wireless vibrometry
- Audio causes small vibrations of the antenna which can be decoded

Speech and Privacy: Light-bulbs (2020)



- Humans speak, Light-bulbs vibrate
- Light shifts can be detected
- Look at the changes in light

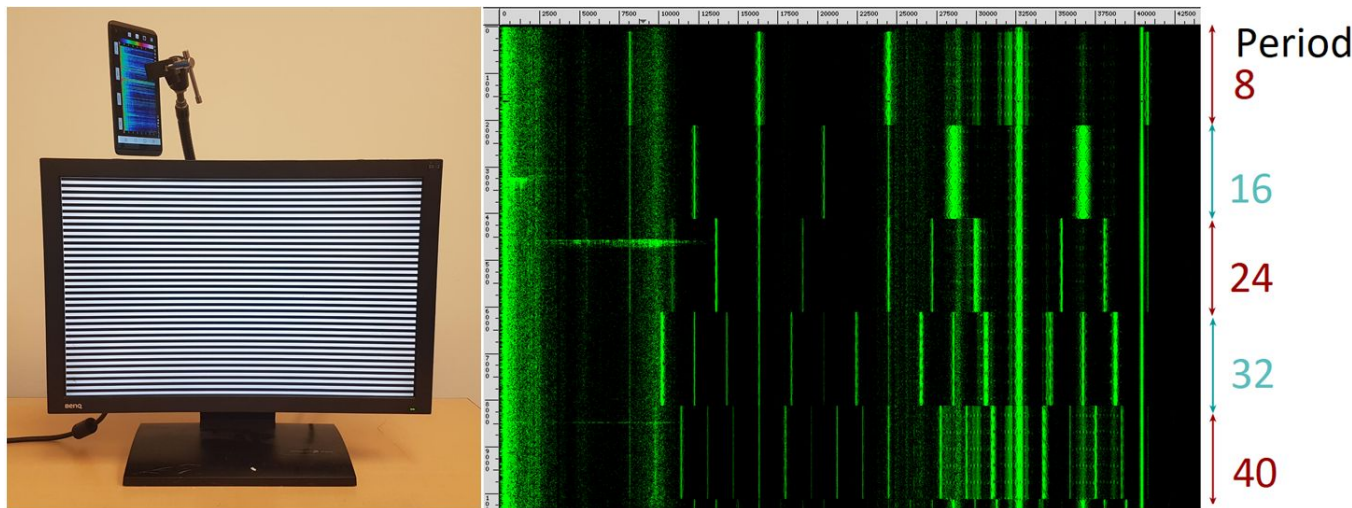
Speech and Privacy: Light-bulbs (2020)



- Electro-optical sensor is sampled at rate of 2-4 kHz
- Can actually run shazam over it

Hearing monitors

Monitor and Privacy: something vibrates



- Electronic components vibrate
- With enough sampling rate one can recover what is being shown

Monitor and Privacy: something vibrates

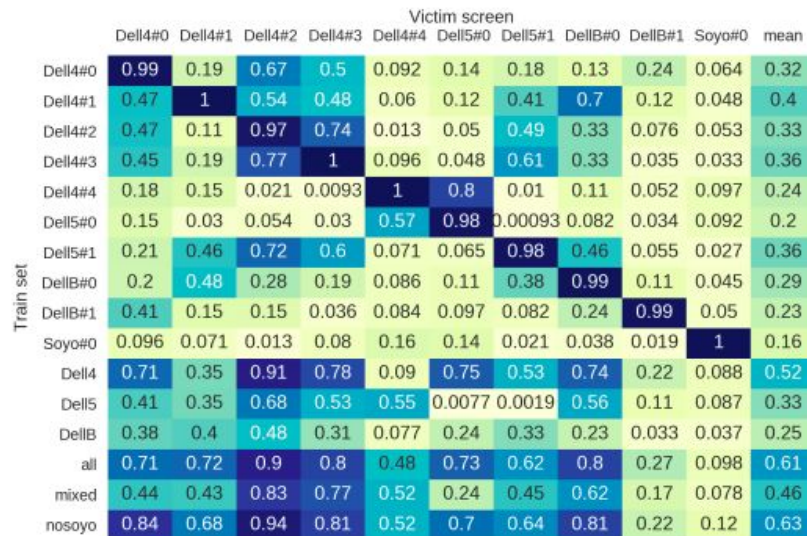


Figure 7.1: Cross-screen classification accuracy.

- Electronic components are shared by multiple monitors
- Transferability of attacks

Hearing printers

Printer and Privacy: sounds of a printing head

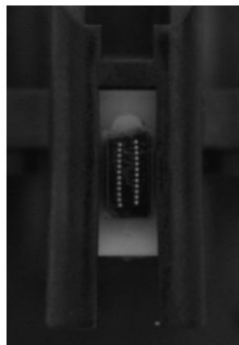


Figure 2: Print-head of an Epson LQ-300+II dot-matrix printer, showing the two rows of needles.

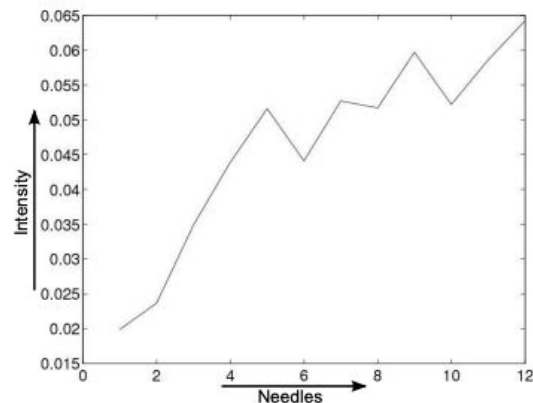
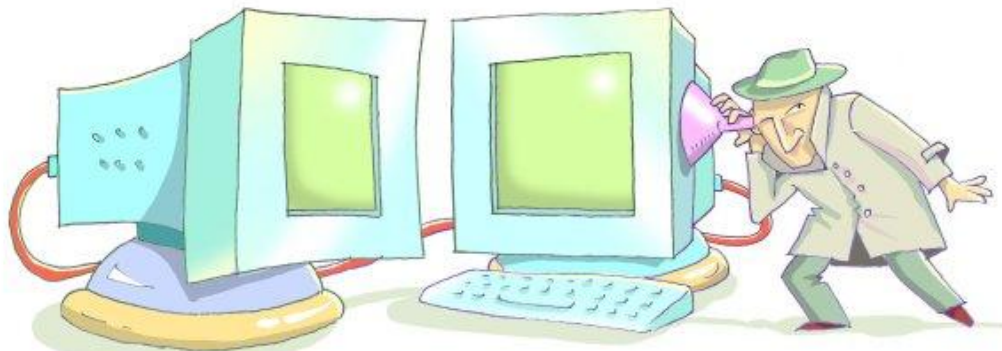


Figure 3: Graph showing the correlation between the number of needles striking the ribbon and the measured acoustic intensity.

- Printing head vibrates and uses different number of needles
- Attacker can recover printed text with a high probability

Hearing cryptography

Crypto and Privacy: something vibrates



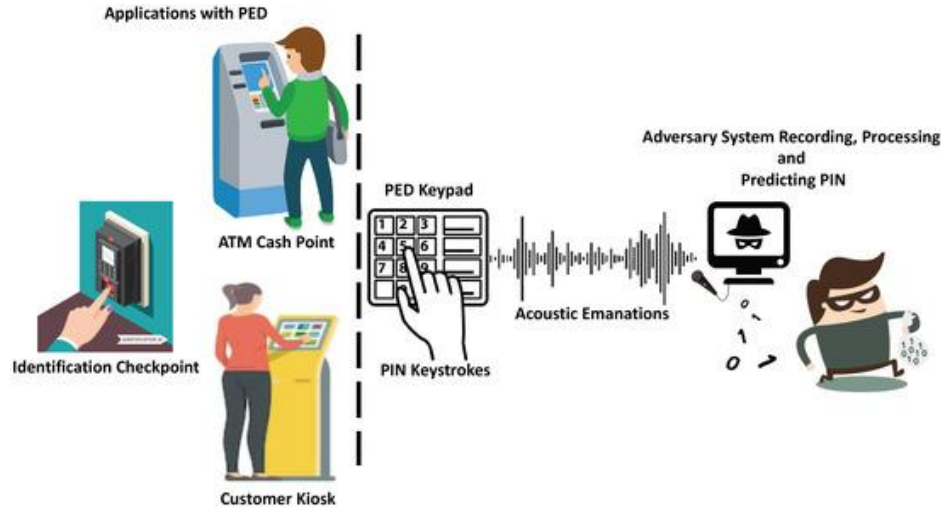
- Electronic components vibrate, in a CCA one can recover information
- Can and has been used to recover cryptographic keys

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis (Genkin et al. 2013)

<https://www.independent.co.uk/news/people/obituary-peter-wright-1617351.html>

Hearing typed PINs and text

PIN-pad and Privacy: keys vibrate



- Physical keys have their own signatures
- Can easily be picked up and deciphered
- A very simple problem

Physical keyboard and Privacy: keys vibrate

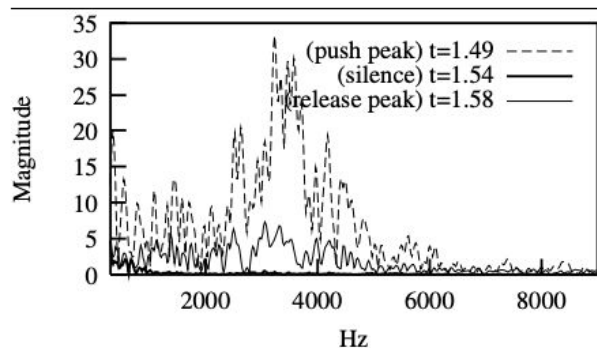


Figure 2. Frequency spectrums corresponding to the push peak, a silence interval, and the release peak.

- Physical keys have their own signatures
- Can easily be picked up and deciphered

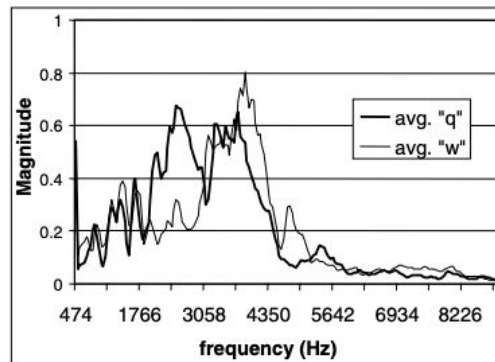
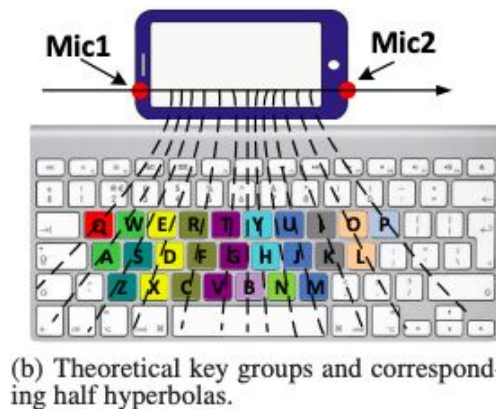
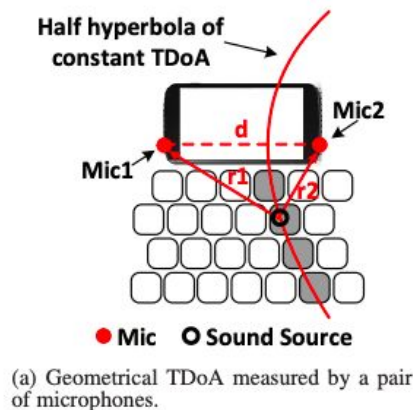


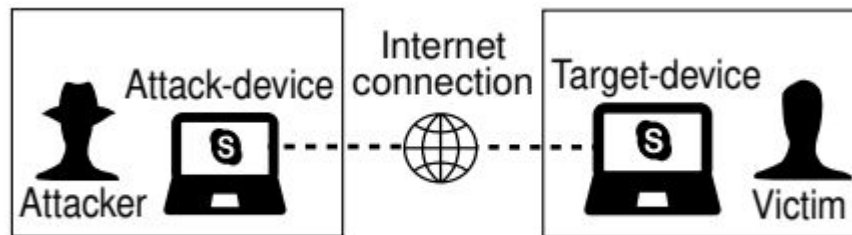
Figure 5. Comparison of the normalized average spectra (extracted from touch peaks of the clicks).

Physical keyboard and Privacy: keys are fixed



- Physical keyboards are fixed
- Key location can be found geometrically
 - with two mics you get an angle
 - with three+ precise location

Physical keyboard and Privacy: works over skype



- Physical keyboard artifacts survive fancy encoding techniques
- No need to have annotations, language has underlying frequency
- You can hear what people type over Zoom and Skype

Physical keyboard and Privacy: virtual keys vibrate

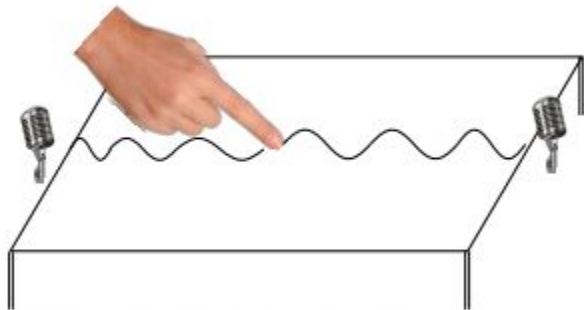


Figure: Screen is a fixed plate that vibrates upon pressure

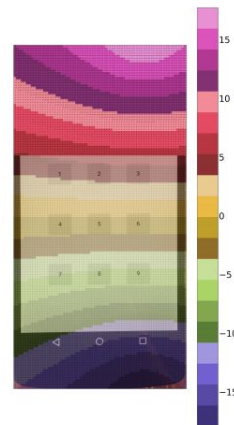


Figure: Theoretical recognisability for Nexus 5 phone. From Microphone 1 to Microphone 2 the difference is about 32 samples.

- Virtual keys have their own signatures:
 - Screen vibrates, waves bounce off sides and superpose
 - Each microphone gets unique to symmetry signature
- Can easily be picked up and deciphered

Physical keyboard and Privacy: virtual keys vibrate

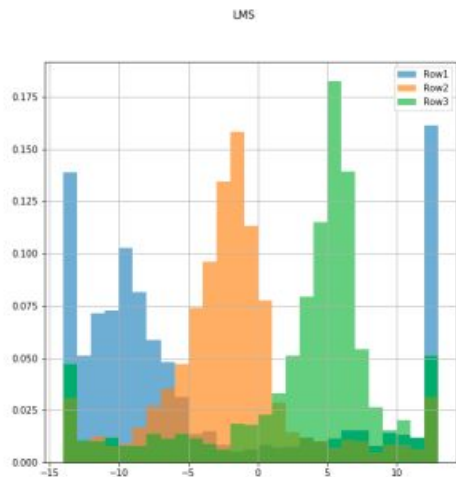


Figure: In practice the best we can do is recognise taps on different pin rows.

- Geometric solutions also work
- TDoA can tell which row the pin is entered in
- No noise because of the multi-mic setup
- Recovers both PIN-codes and texts
- Microphones provide comparable accuracy to existent side channel attacks, despite being a lot noisier.

Hearing your touch: A new acoustic side channel on smartphones (Shumailov et al, 2017)

Physical keyboard and Privacy: active sonar

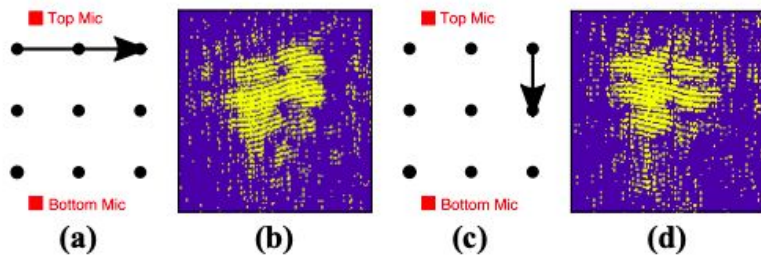


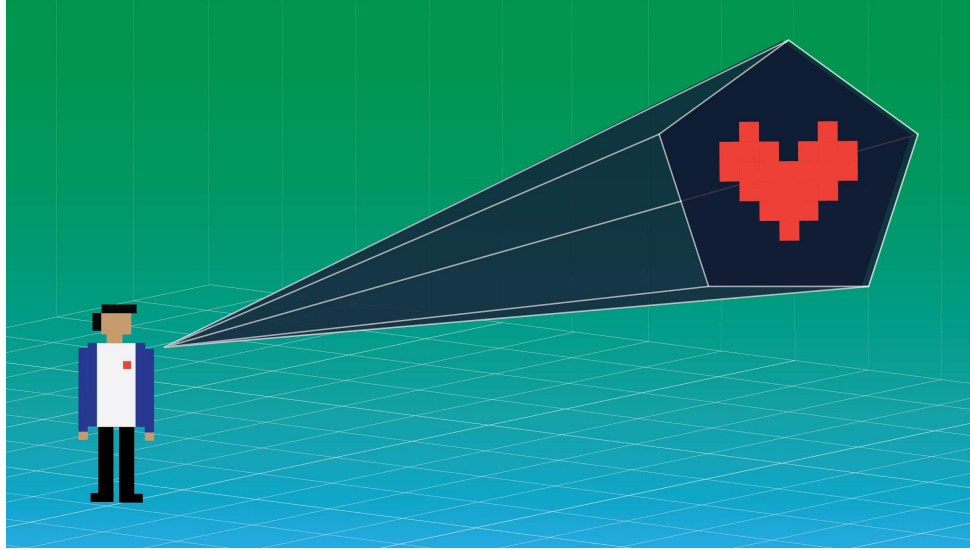
Fig. 6 Two strokes with different direction information. **a** A stroke that is moving away from the bottom microphone. **b** Connected components (CC) of the stroke shown in *a* extracted from the bottom microphone. It shows an ascending trend. **c** A stroke that is moving towards the bottom microphone. **d** CC of the stroke in *c* extracted from the bottom microphone. It shows a descending trend

- Can turn a smartphone into an active sonar
- Fingers introduce doppler effect
- Can recover swiping PIN-codes

SonarSnoop: active acoustic side-channel attacks (Cheng et al, 2020)

Acoustics and humans

Society and Privacy: humans vibrate



- Human hearts beat uniquely
- Can use lasers to identify people by how they sound

Society and Privacy: humans vibrate

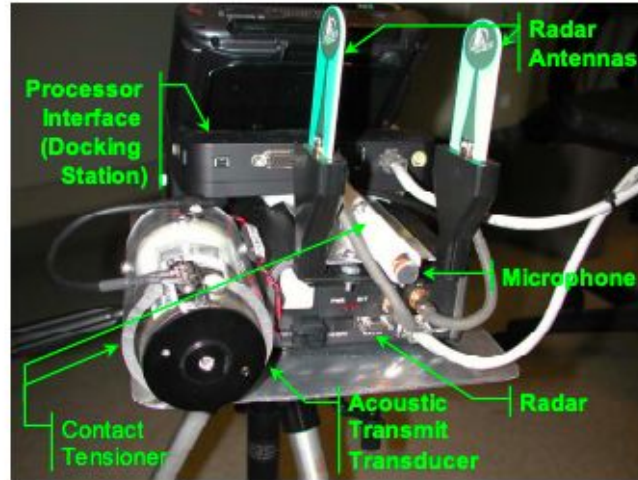
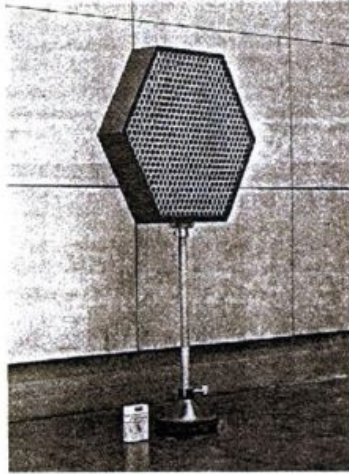


Figure 9: Photograph of Front of Assembled Unit, Sonar and Radar.

- People move around and always vibrate
- Already in use by law enforcement
- Can find movements through walls

Society and Privacy: humans can hear voices



- Parametric array allows combining high-frequencies to produce low-frequency signal
- Can make only certain people hear voices

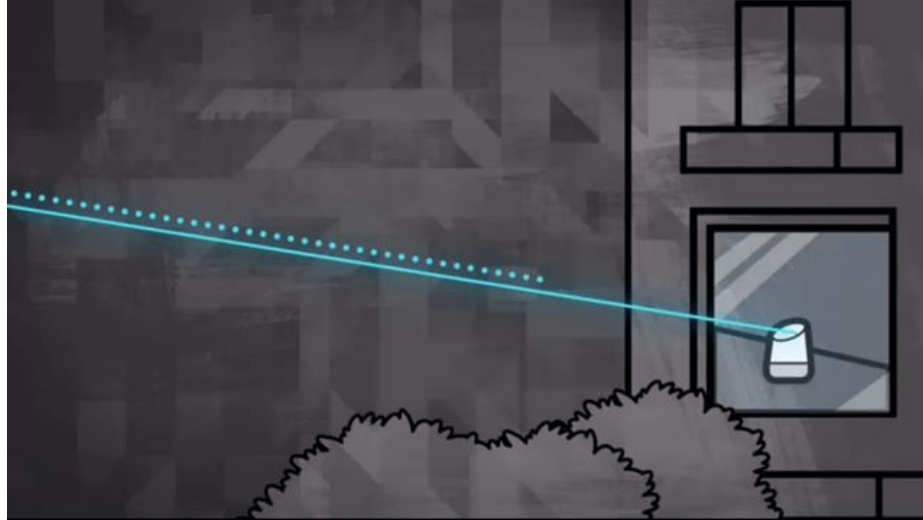
Society and Privacy: humans and sonic weapons



- Some success with sonic weapons
- Mob Excess Deterrent Using Silent Audio and Long Range Acoustic Devices
- Ultrasonic attacks on diplomats

Attacks on microphones

Microphone integrity: mics are sensitive



- Photoacoustic Effect
- Light is heating the microphone and causes it to vibrate
- Modulated by beam intensity

Microphone integrity: mics are sensitive

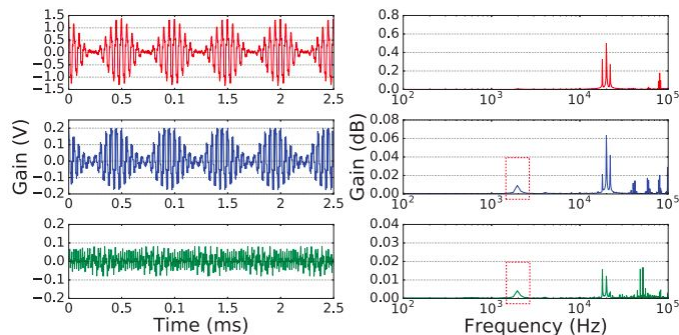


Figure 4: Evaluation of the nonlinearity effect. The time and frequency domain plots for the original signal, the output signal of the MEMS microphone, and the output signal of the ECM microphone. The presence of baseband signals at 2 kHz shows that nonlinearity can demodulate the signals.

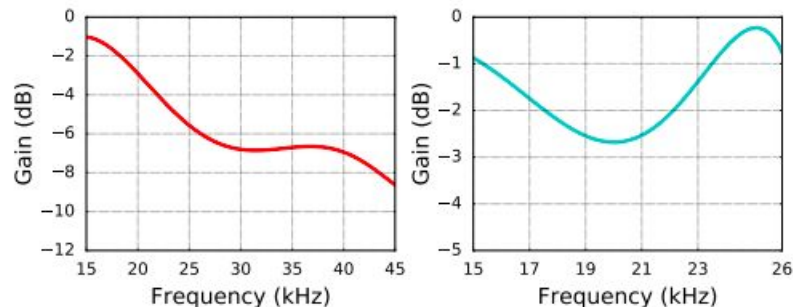
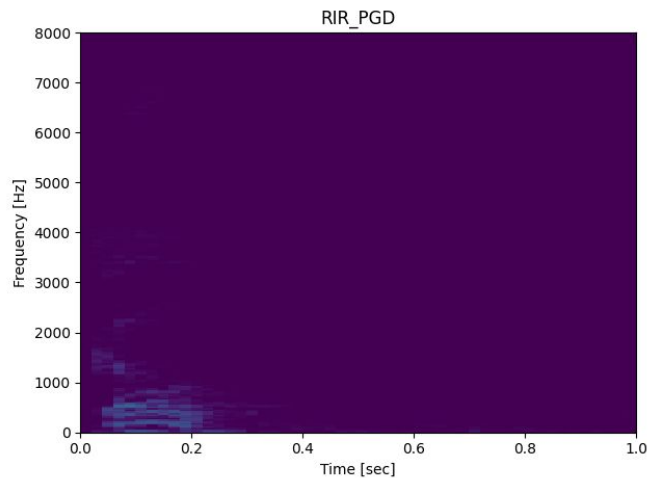
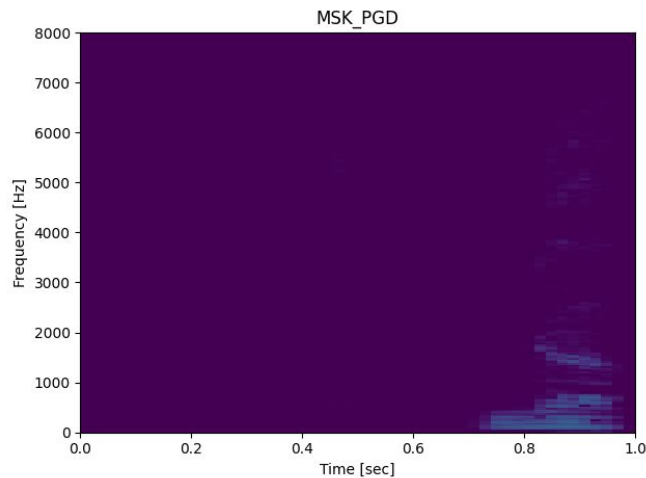


Figure 10: The frequency responses of the ADMP401 MEMS microphone (left) and the Samsung Galaxy S6 Edge speaker (right).

- Dolphin attacks, totally inaudible
- Exploit non-linearity in amplifiers
- Not removed by LPF in the pipeline because amplified beforehand!

Adversarial ML and acoustics

Adversarial ML in Acoustics: ASR and KWS



- ASR and KWS systems can be attacked
- Can target specific acoustic setups
- Adversarial samples can be hidden with different masking techniques
 - Echo masking
 - Frequency masking

Conclusions

- Acoustics can be used to launch a **variety of attacks**
 - Very few of the attacks are stoppable
- **Mechanical waves** are everywhere and are **hard to get rid of**
 - Unclear **how to protect against** a capable attacker
- **ML** has **enabled attacks** that were not possible before
- Sensors are **getting better**, attacks improve with them
- **Microphones** can be easily **manipulated**
- **Acoustic ML** is **exploitable**
- **No forward secrecy**
 - Tomorrow people will decode recordings from the past
 - Huawei has all recordings in the world, what will they do with them?