# Eavesdropping on Black-Box Mobile Devices via Audio Amplifier's EMR

Huiling Chen, Wenqiang Jin \*, Yupeng Hu\*, Zhenyu Ning, Kenli Li, Zheng Qin, Mingxing Duan, Yong Xie, Daibo Liu, and Ming Li

Hunan University
Nanjing University Posts of Telecommunications
The University of Texas at Alington







# Mobile Device's Speaker

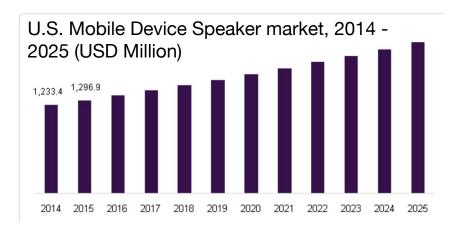


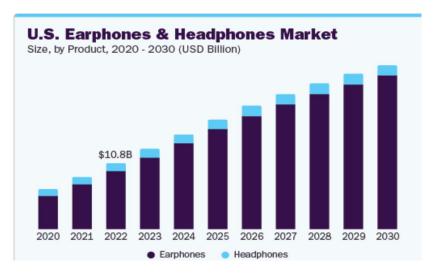




Earphones



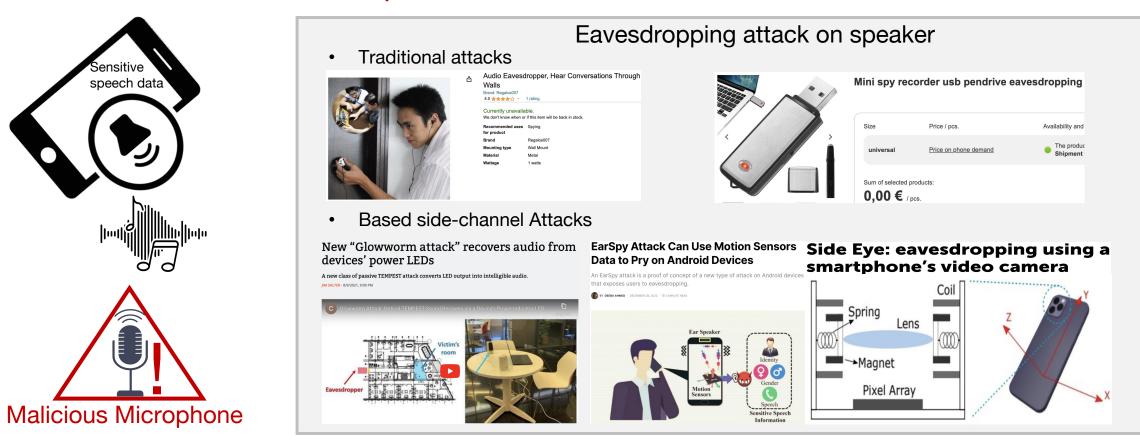




Speaker is an essential component for audio interaction on mobile devices.

#### **Audio Eavesdropping Attack**

The private audio played by the user can potentially be eavesdropped on by hidden malicious microphones.



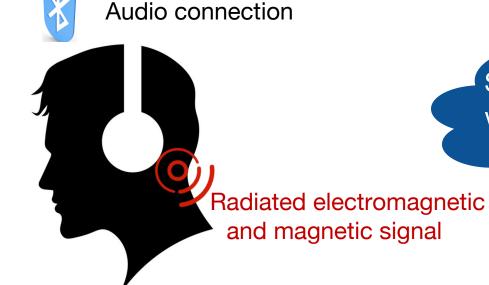
Protecting users' private audios is critical and we aim to explore the feasibility of eavesdropping on a mobile device via side channel attack when it is connected to headphones (microspeaker).

#### **Related Work**



[1] Choi et al., CCS 2020

[2] Liao et al., MobiSys 2022



Victim with wireless headphone

Side channel leakage from wireless headphones' microspeaker

We aim to investigate eavesdropping threats of headphone-plugged mobile device.

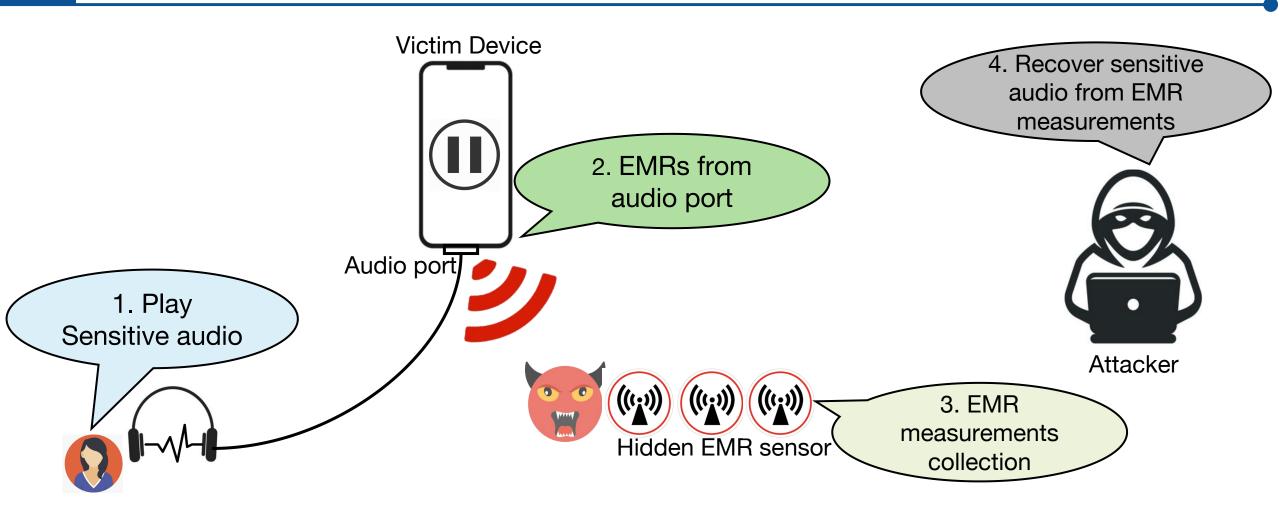
#### **Our Goals**

O To evaluate the new eavesdropping threat of headphone-plugged mobile devices.

To mitigate the security risk of using headphone-plugged mobile device to listen to private audio.



#### **Our Attack**



Attacker exploits EMRs of headphone-plugged mobile device to recover victim's sensitive audio.

# Challenges

Signal Acquisition: Which types of EM sensors can be used to measure a device's EMR in daily mobile usage scenarios?

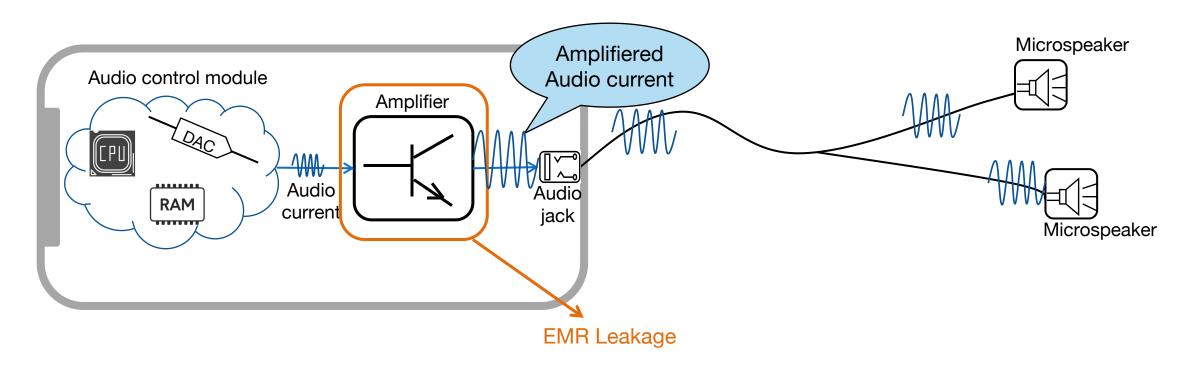


Audio recovery: How to recover intelligible audio from EMRs when the attacker has no prior knowledge about the target device?



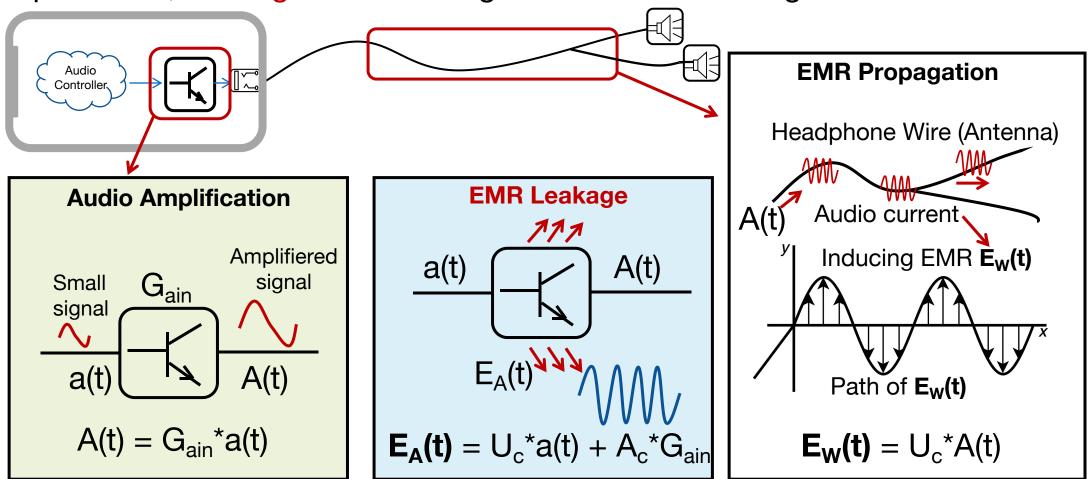
# **Working Principle of Wired Headphones**

- Wired headphones are powered by the mobile device's audio control module to produce sound.
- The amplifier plays a role in amplifying the generated audio current.



# **Amplifier's EMR Leakage**

Intense fluctuations in current occur when the amplifier processes the input audio, leading to electromagnetic radiation leakage.



EM signal E(t) is proportional to the input audio a(t), therefore, they have the same signal pattern.

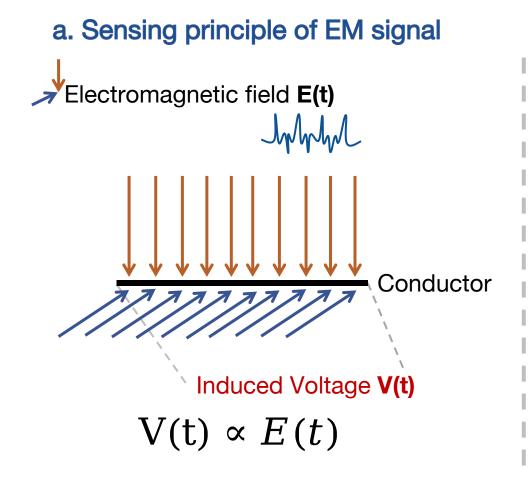
# **Attack Design**

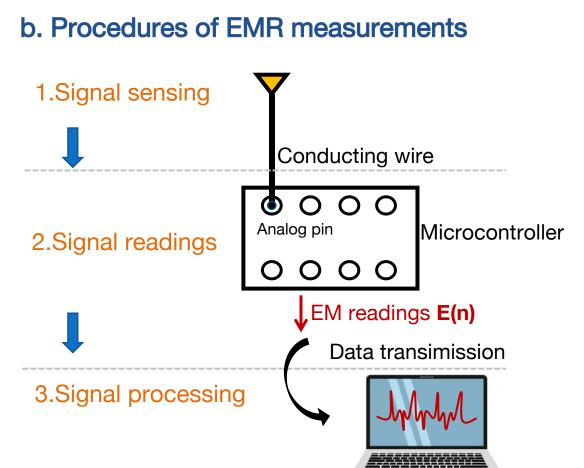
- ☐ Step1: EMR measurements
  - How to sense the EM signal?
  - What sensing device should be used?
- ☐ Step2: Audio recovery
  - How to remove noises?
  - How to convert extracted EMRs to audio?



#### **EMR** measurements

The electromagnetic field can result in an electric potential on a conductor.





# **Attack Design**

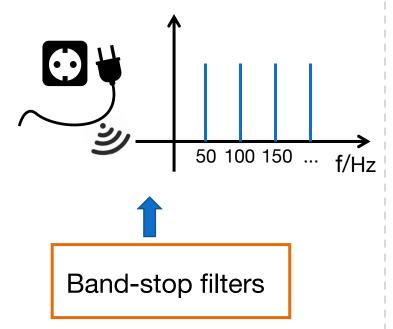
- ☐ Step1: EMR measurements
  - How to sense the EM signal?
  - What sensing device should be used?
- ☐ Step2: Audio recovery
  - How to remove noises?
  - How to convert extracted EMRs to audio contents?



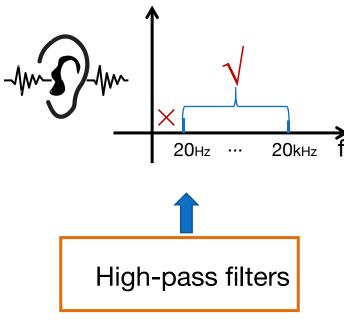
#### **Audio Recovery: Denoising**

#### Preprocessing

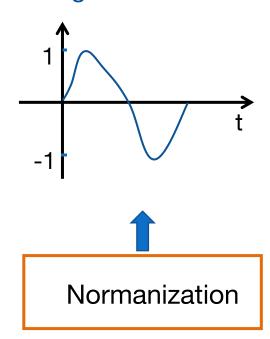
1. Remove noises from power cables



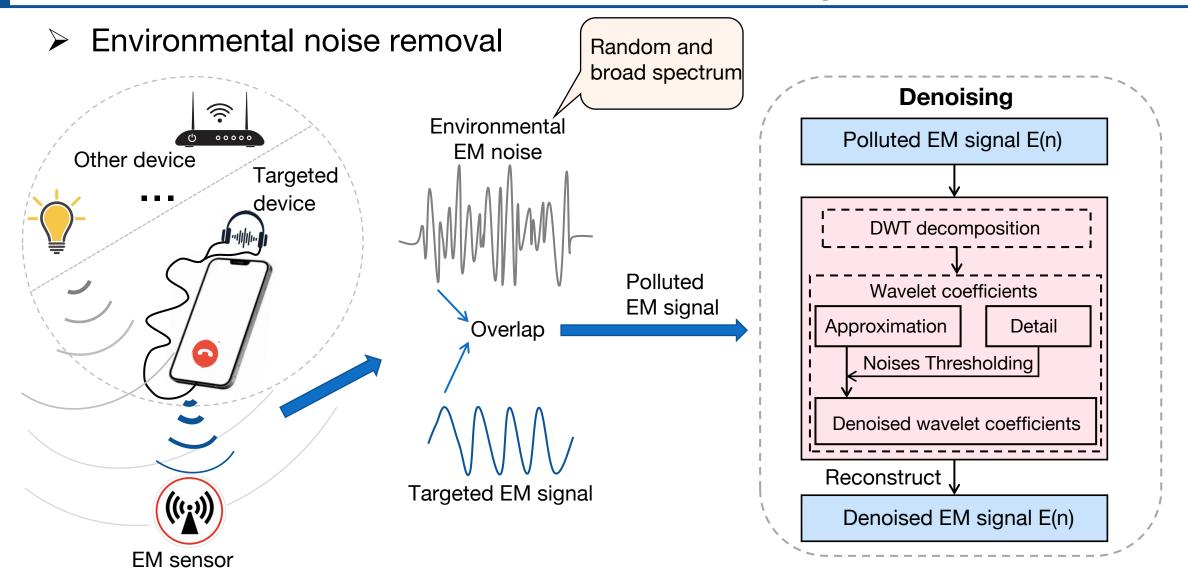
2. Remove noises beyond human hearing range



3. Strengthen the audiorelated signal

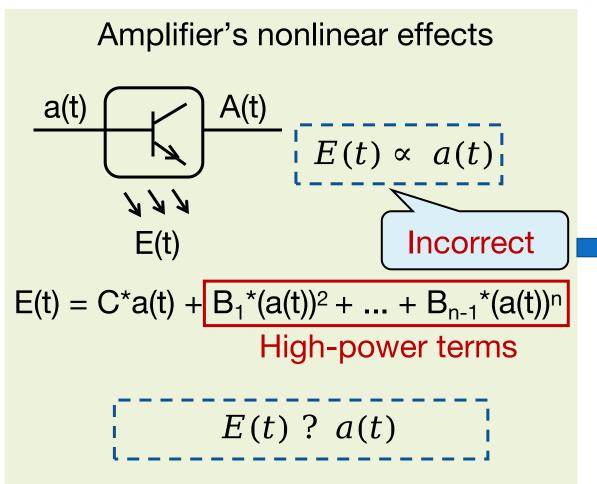


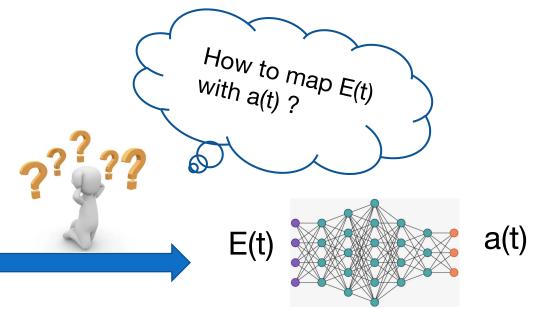
# **Audio Recovery: Denoising**



#### **Audio Recovery: Audio Extraction**

In practice, amplifier's nonlinear characteristics can affect the direct proportion between E(t) and a(t), making it difficult to extract audio a(t).

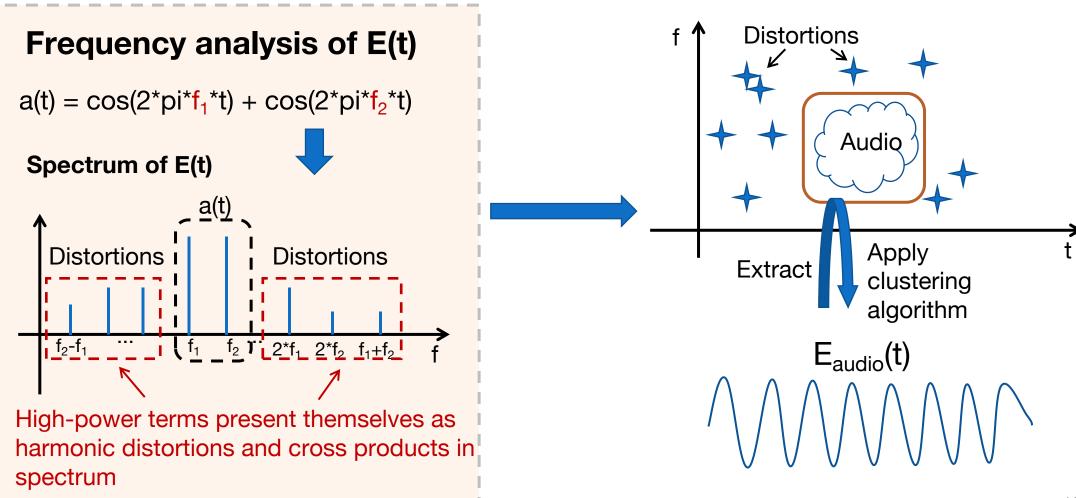




To build training-based model requires a large amount of collected data in advance of the attack

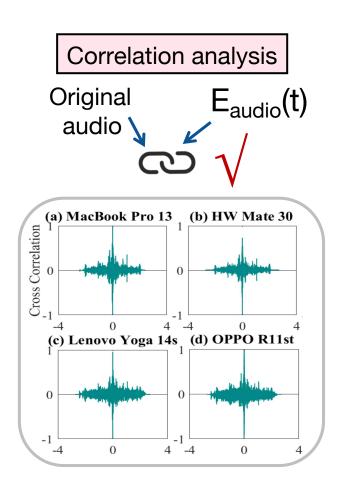
# **Audio Recovery: Audio Extraction**

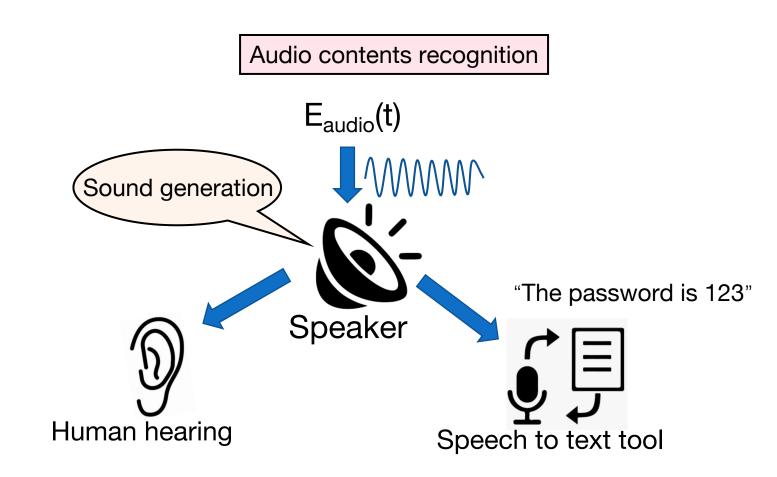
By leveraging a advanced signal processing technique to eliminate the impact of amplifier's nonlinear characteristics.



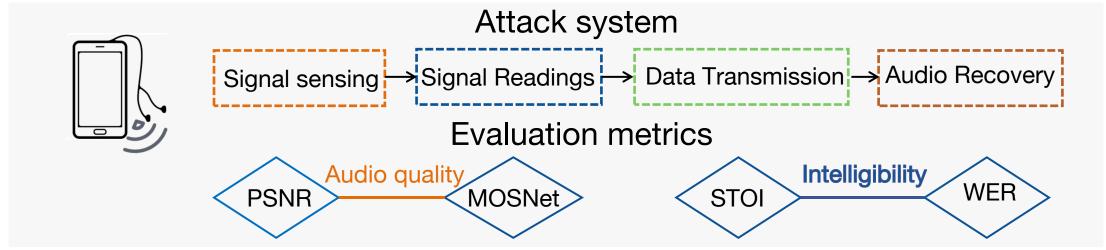
# **Audio Recovery: Sound Generation**

The extracted audio is highly similar to the original audio, moreover, it can be recognized by human hearing and commercial speech recognition tools.

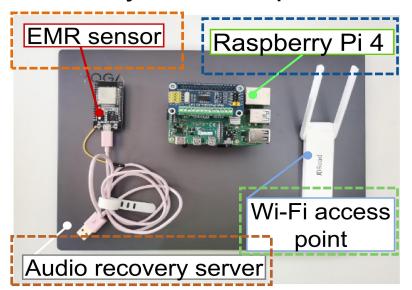




# **Experimental Setup**



#### Physical setup



#### Target device



# **Overall performance**

|                  | Туре       | Manufacturer  | Sensory Range(cm) | Attack<br>Range(m) | Evaluation metrics |      |            |              |
|------------------|------------|---------------|-------------------|--------------------|--------------------|------|------------|--------------|
| Mobile Device    |            |               |                   |                    | MOSNet             | STOI | WER<br>(%) | PSNR<br>(dB) |
| MacBook Pro 13   | Laptop     | Apple, USA    | 82                | 15.82              | 2.80               | 0.74 | 19.50      | 20.48        |
| MacBook Air 13   | Laptop     | Apple, USA    | 81                | 15.81              | 2.89               | 0.75 | 18.43      | 21.28        |
| RMN TPN-Q173     | Laptop     | HP, USA       | 94                | 15.94              | 2.95               | 0.78 | 14.66      | 22.23        |
| Yoga 14s         | Laptop     | Lenovo, China | 103               | 16.03              | 3.05               | 0.84 | 12.60      | 25.26        |
| Inspiron 14 5410 | Laptop     | Dell, USA     | 97                | 15.97              | 3.04               | 0.79 | 12.33      | 23.15        |
| MateBook D14     | Laptop     | HW, China     | 105               | 16.05              | 3.06               | 0.82 | 7.44       | 26.00        |
| iPhone SE2       | Smartphone | Apple, USA    | 55                | 15.55              | 2.70               | 0.76 | 20.43      | 19.24        |
| iPhone 14 Pro    | Smartphone | Apple, USA    | 45                | 15.45              | 2.62               | 0.71 | 23.77      | 17.44        |
| iPhone 14        | Smartphone | Apple, USA    | 49                | 15.49              | 2.68               | 0.73 | 20.85      | 18.45        |
| Mate 30          | Smartphone | HW, China     | 44                | 15.44              | 2.60               | 0.71 | 26.85      | 16.88        |
| R11st            | Smartphone | OPPO, China   | 48                | 15.48              | 2.66               | 0.72 | 21.75      | 18.25        |

This attack can achieve the lowest WER at 7.44%, and average MOSNet, STOI, WER, and PSNR at 2.83, 0.75,17.83%, and 20.85, respectively.

#### **Impact Factors**

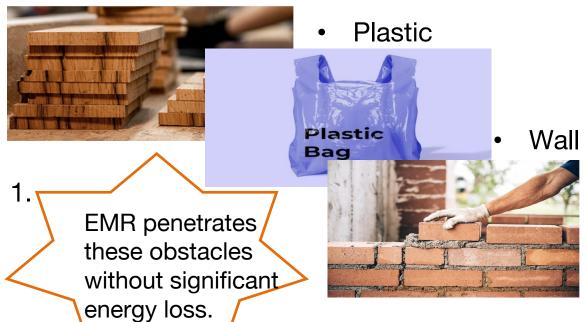
#### 1. Physical obstacle

| Mobile         | MOSNet/STOI    |           |           |           |  |  |  |
|----------------|----------------|-----------|-----------|-----------|--|--|--|
| Device         | No<br>obstacle | Wood      | Plastic   | Wall      |  |  |  |
| MateBook D14   | 2.80/0.80      | 2.75/0.78 | 2.72/0.75 | 2.62/0.74 |  |  |  |
| Yoga 14s       | 2.76/0.78      | 2.70/0.74 | 2.72/0.73 | 2.55/0.70 |  |  |  |
| MacBook Pro 13 | 2.69/0.76      | 2.55/0.72 | 2.50/0.73 | 2.43/0.69 |  |  |  |
| iPhone 14      | 2.45/0.69      | 2.32/0.67 | 2.35/0.68 | 2.27/0.65 |  |  |  |
| Mate 30        | 2.51/0.72      | 2.50/0.71 | 2.49/0.70 | 2.34/0.63 |  |  |  |

#### 2. Volume

| Volume (%) | 20    | 40    | 60    | 80    | 100   |
|------------|-------|-------|-------|-------|-------|
| Level (dB) | 30.4  | 47.4  | 53.1  | 81.7  | 90.6  |
| PSNR (dB)  | 3.75  | 9.50  | 16.42 | 25.75 | 36.00 |
| WER (%)    | 94.10 | 53.44 | 28.45 | 8.45  | 5.01  |
| MOSNet     | 2.10  | 2.56  | 2.85  | 2.90  | 3.10  |
| STOI       | 0.56  | 0.72  | 0.78  | 0.80  | 0.86  |

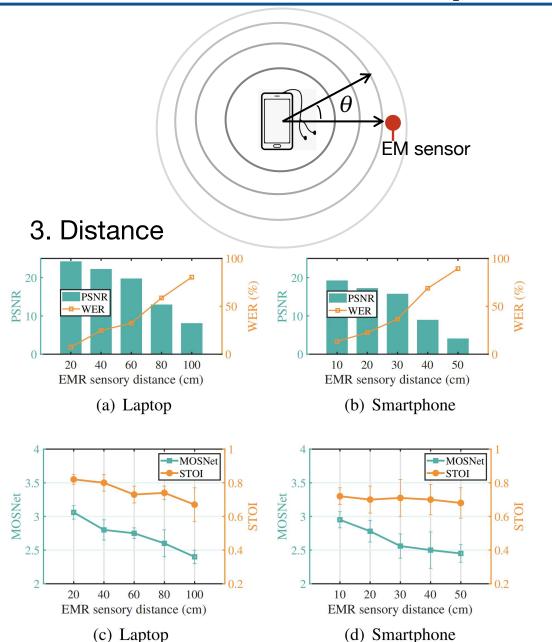
Wood

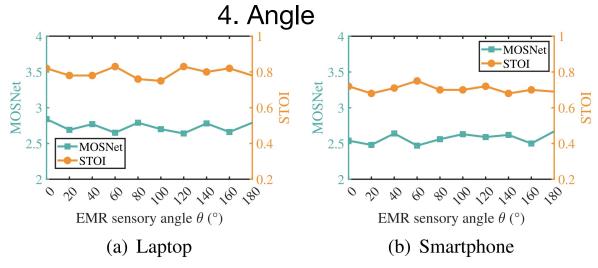


2.

A higher volume setting inceases the the risk of audio leakage!

#### **Impact Factors**



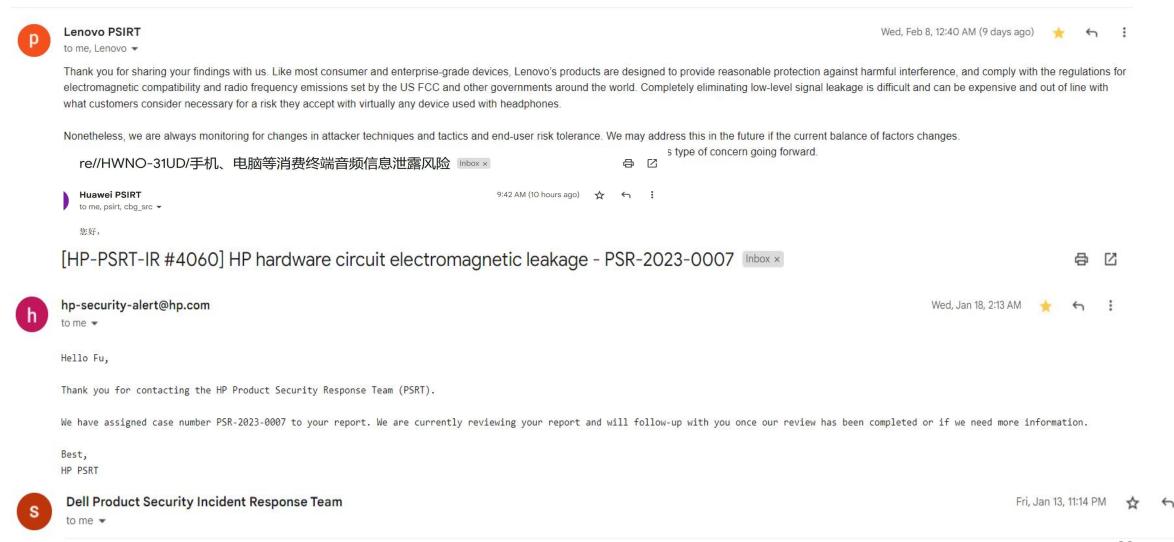


The effectiveness of the attack decreases as the sensory distance increases.

For attaker, all angles can be lauched to conduct a effective audio eavesdropping.

#### Responsible disclosure

We have contacted the product security team, and received their feedback.



#### Conclusion

✓ Proposed a new audio eavesdropping attack that exploits electromagnetic radiation of mobile device's amplifier to recover victim's private audio.

✓ Designed an audio recovery algorithm that requires no prior knowledge about the target device to extract audio contents from EMRs.

✓ Evaluated the effectiveness of this attack on 11 mobile devices and 6 headphones, and reported this security threat to leading manufacturers.

# Thanks for listening!

Q&A