MagDefender: Detecting Eavesdropping on Mobile Devices Using the Built-in Magnetometer

Hao Pan[1], Feitong Tan[2], Wenhao Li[1], Yi-Chao Chen[1], Lanqing Yang[1], Guangtao Xue[1], Xiaoyu Ji[3]

[1] Shanghai Jiao Tong University
[2] Simon Fraser University
[3] Zhejiang University

Outline

- **Background and Motivation**
- Related Works and Limitations
- Our idea —— EMI side channel
- Preliminary Analysis
- System Design
- Evaluation
- Limitation and Discussion
- Conclusion

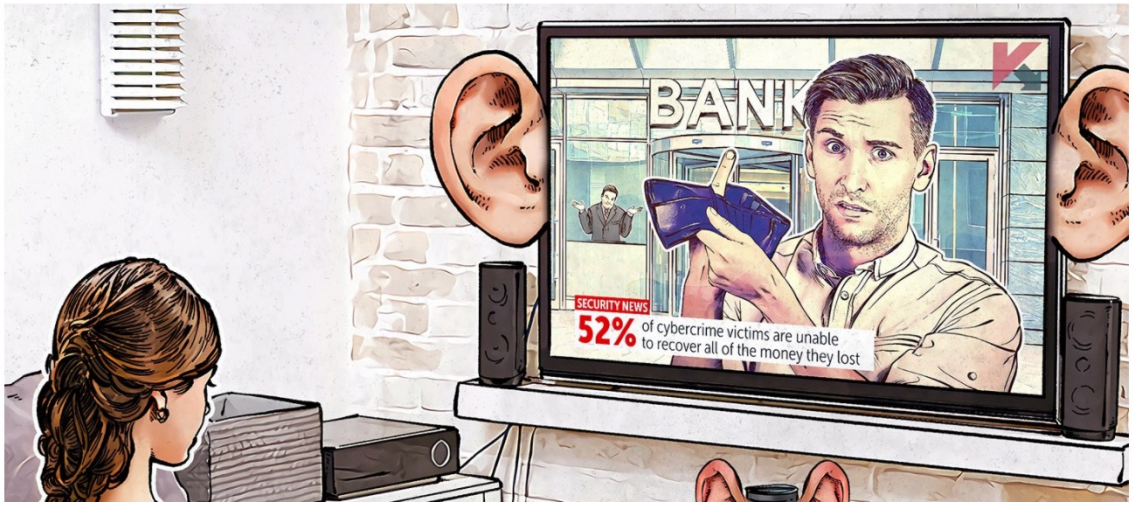
Your smartphone is secretly listening to you?

Ad personalized recommendations

Eavesdropping smartphones: Fact or fiction?

Many swear phones secretly listen in through their built-in microphones. We investigate the claims — and offer other explanations for spookily precise mobile ads.

Alexey Malanov August 2, 2019



News & Cases —— Eavesdropping on Mobile Devices

FBI taps cell phone mic as eavesdropping tool

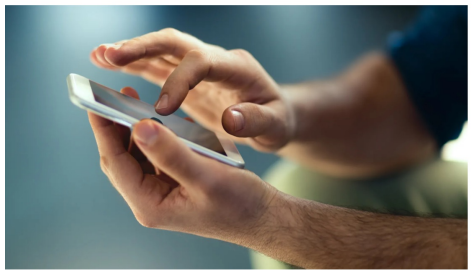
Agency used novel surveillance technique on alleged Mafioso: activating his cell phone's microphone and then just listening.

Written by **Declan McCullagh,** Contributor on Dec. 1, 2006

The FBI appears to have begun using a novel form of electronic surveillance in criminal investigations: remotely activating a mobile phone's microphone and using it to eavesdrop on nearby conversations.

The technique is called a "roving bug," and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance

You're not paranoid. Your phone really is listening in.



your phone listening in on you? (iStock)

Fox News SciTech

Get a daily look at what's developing in science and technology throughout the world.

Arrives Weekly

Subscribe

Can Your Phone Hear Your Conversations? (Yes, But Here's How)

FATIMA AL-HUSSAINI
August 20, 2020

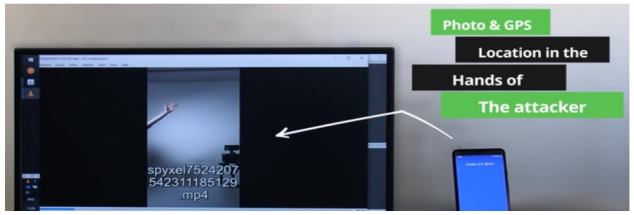
SHARE THIS BLOG POST

Zeljka Zorz, Managing Editor, Help Net Security
November 19, 2019

Share

Android camera apps could be hijacked to spy on users

A vulnerability in the Google Camera app may have allowed attackers to surreptitiously take pictures and record videos even if the phone is locked or the screen is off, Checkmarx researchers have discovered.

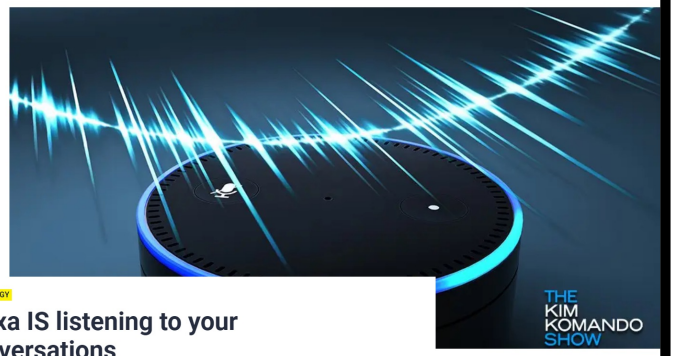


Apple iOS FaceTime

By Casey Ellis | Jan 29, 2019

THE IOS FACETIME VULNERABILITY: WHAT IT MEANS AND WHAT YOU CAN DO TO PROTECT YOURSELF

Amazon Alexa



Feasibility analysis of low power eavesdropping with microphones

Technical leader of a news app said:

"Doing so (**microphone eavesdropping**) consumes too much on the phone's resources, the network's traffic consumption ..... **Continuous voice recording generates large amounts of data, and advanced compression techniques cannot compress large amounts of voice data without compromising quality**."

Index	Audio file (format/size)	Sampling rate	Type	Time	Power consumption
1	**m4a/ 112.39MB**	**48KHz**	**stereo**	**1 hour**	**6%**
2	m4a/ 20.79MB	8KHz	stereo	1 hour	**5%**
3	3gp	8KHz	mono	1 hour	**3-4%**
4	none	none	none	1 hour	**1%**

https://blog.csdn.net/EGEFCXzo3Ha1x4/article/details/80997468

http://cn-sec.com/archives/218533.html

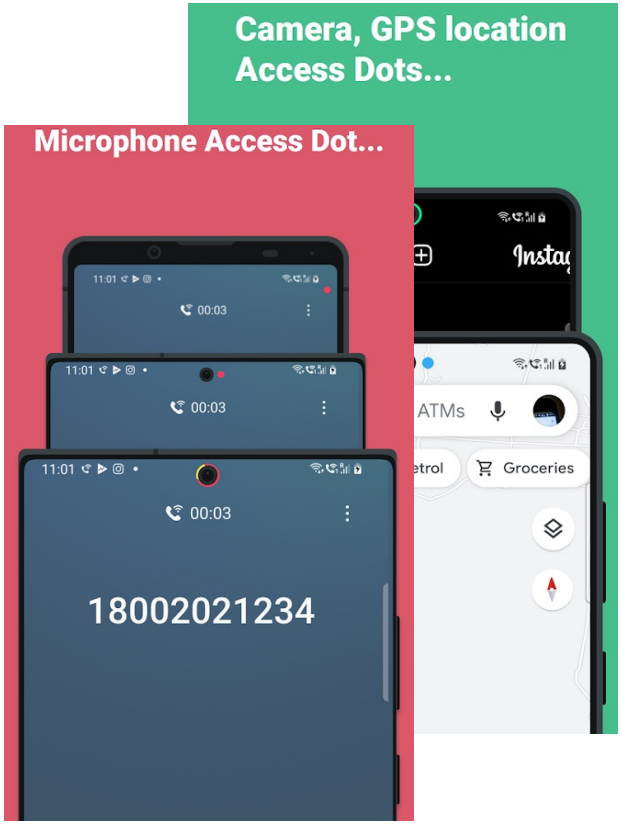
Outline

- Background and Motivation
- **Existing Monitoring Methods and Attack Cases**
- Preliminary Analysis
- Our idea —— EMI side channel
- System Design
- Evaluation
- Limitation and Discussion
- Conclusion

Existing camera/mic working status monitor solutions

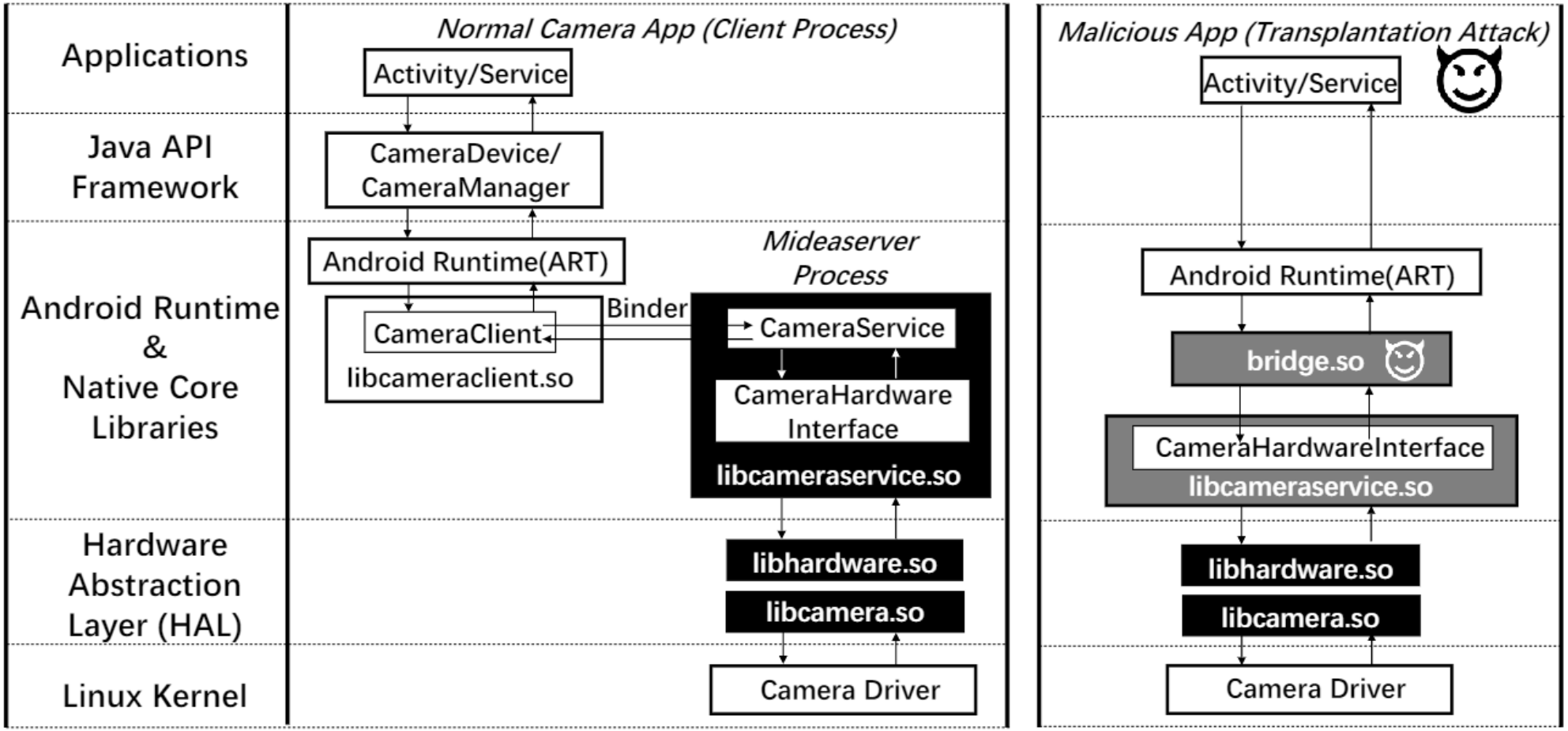
iOS/Android

Smartphone manufacturers



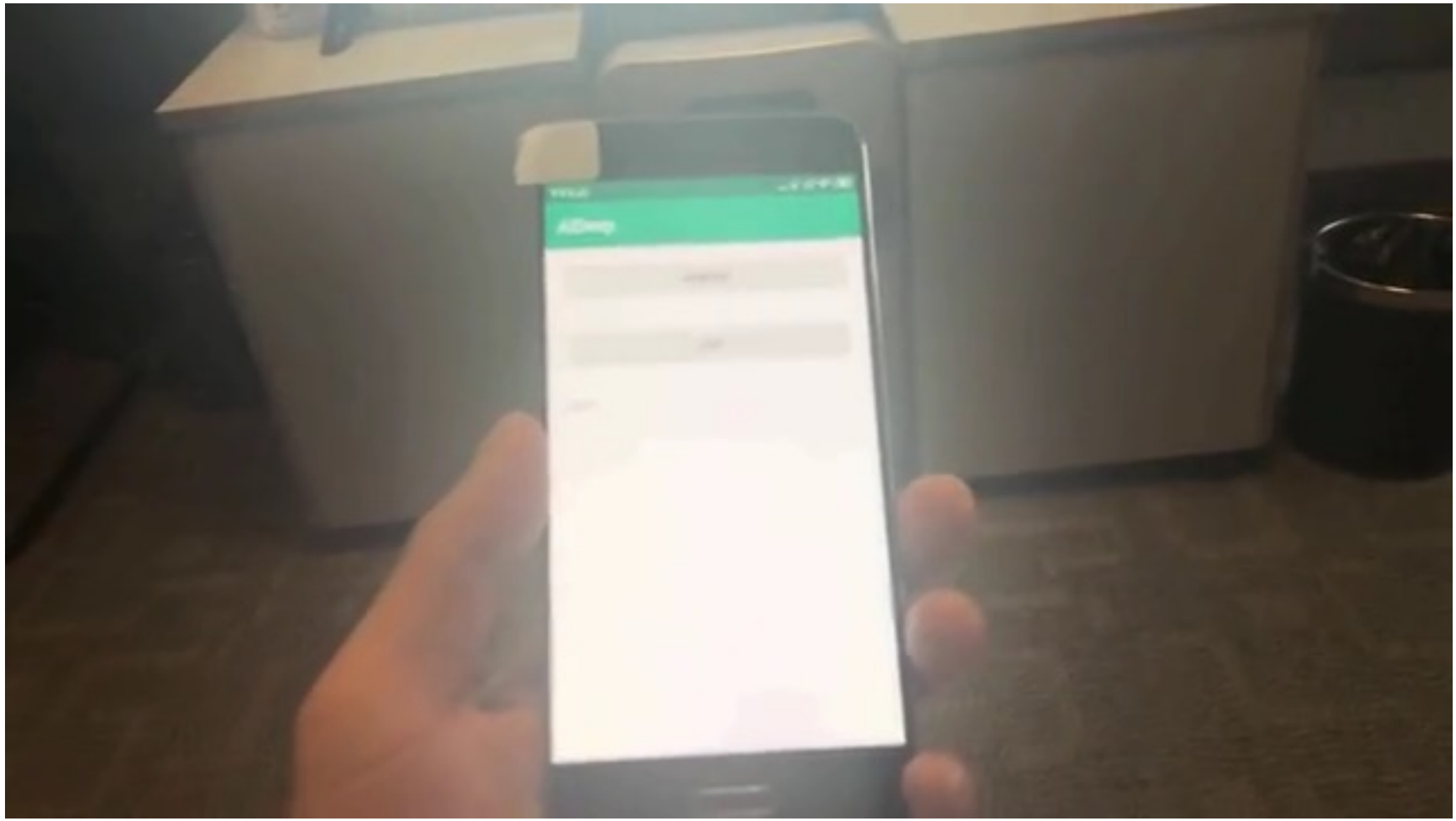
Third-party app developers

Vulnerability of existing monitor methods - Transplantation Attack



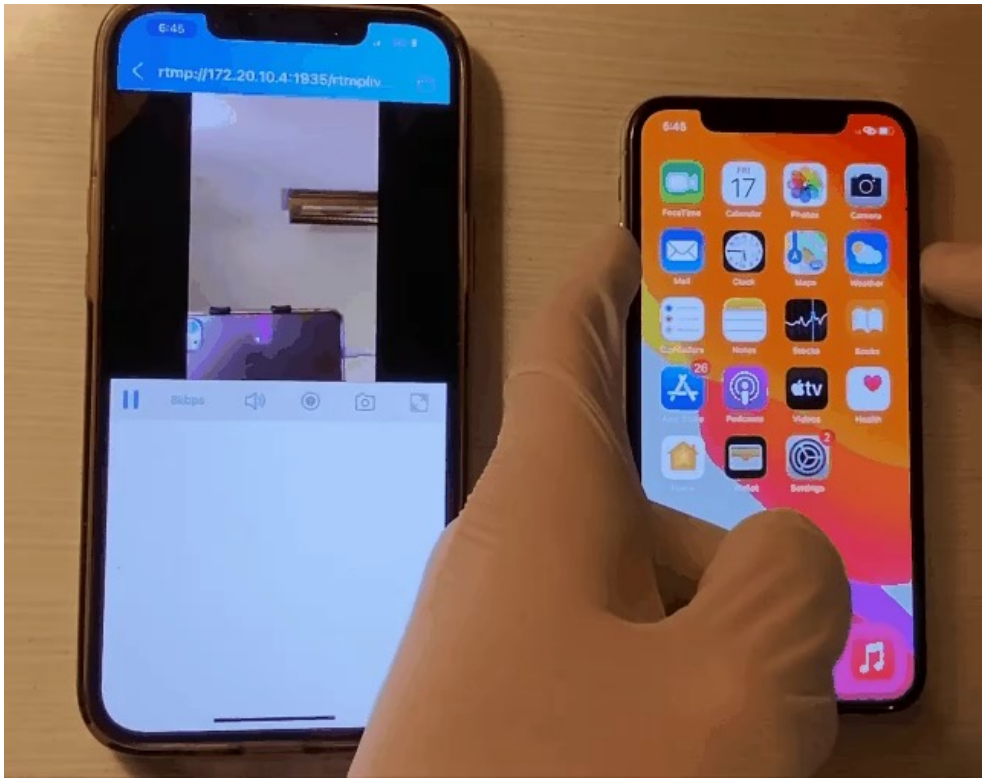
[1] How your phone camera can be used to stealthily spy on you: **Transplantation attack**s against android camera service

Real-time voice recognition after turning off the screen



https://m.thepaper.cn/rss_newsDetail_3169622?from=sohu

Record video after turning off the screen in iPhone



https://zhuanlan.zhihu.com/p/455077659

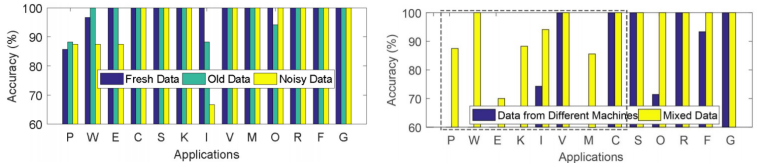
Outline

- Background and Motivation
- Existing Monitoring Methods and Attack Cases
- **Our idea —— EMI side channel**
- Preliminary Analysis
- System Design
- Evaluation
- Limitation and Discussion
- Conclusion

Related Work: Application behavior identification with EMI side-channel signals

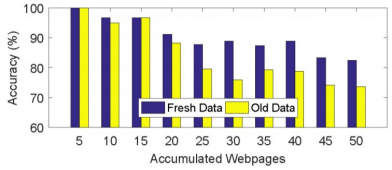
Use smartphone to sense victim's app usage on surrounding laptops

Applications classification:



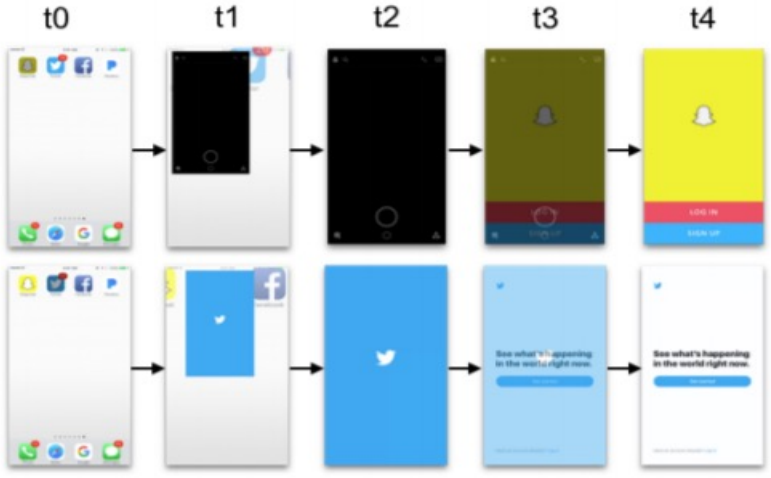
Sniff app usage on the smartphone with built-in magnetometer

Websites classification:



MagAttack (ACM/IEEE TMC 2021)
MagTheif (IEEE SECON 2021)
Magneticspy (ACM WPES 2019)

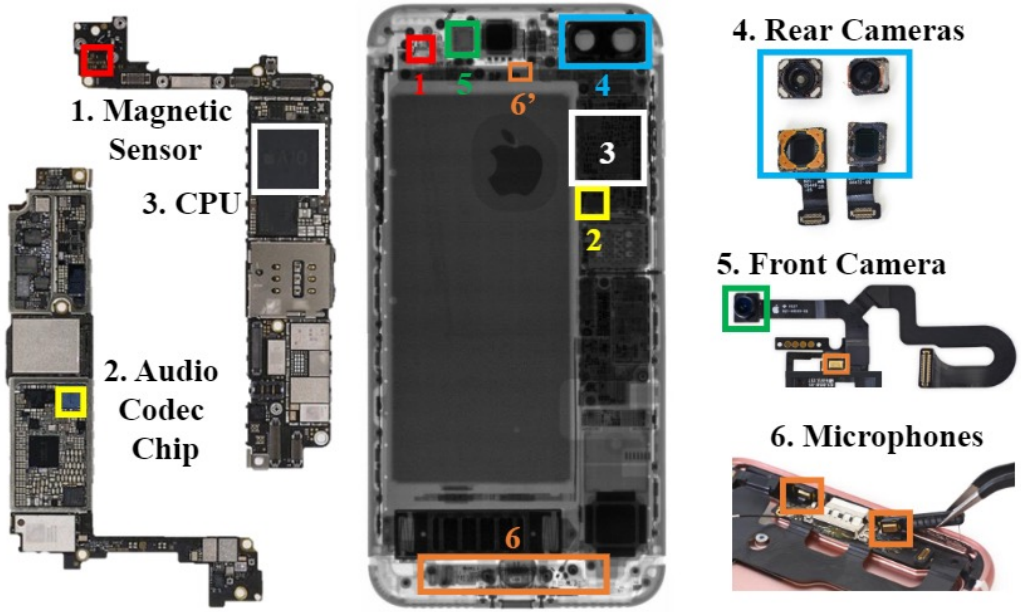
Infer app usage with magnetometer readings by training CNN model



Distance to Refrigerator (cm)	25	50	100
Magnetic Model (Cross Model Mix) + Motion	0.9721	0.9817	0.9769
Orientation Model (Cross Model Mix) + Motion	0.9768	0.9761	0.9782

Deepmag (IEEE PerCom 2018)

Eavesdrop behaviors are different, but hardware is always working!



Can we treat the eavesdrop behaviors as an app, and use the classification methods to detect eavesdropping behaviors?

1. Too many eavesdropping behaviors ☹

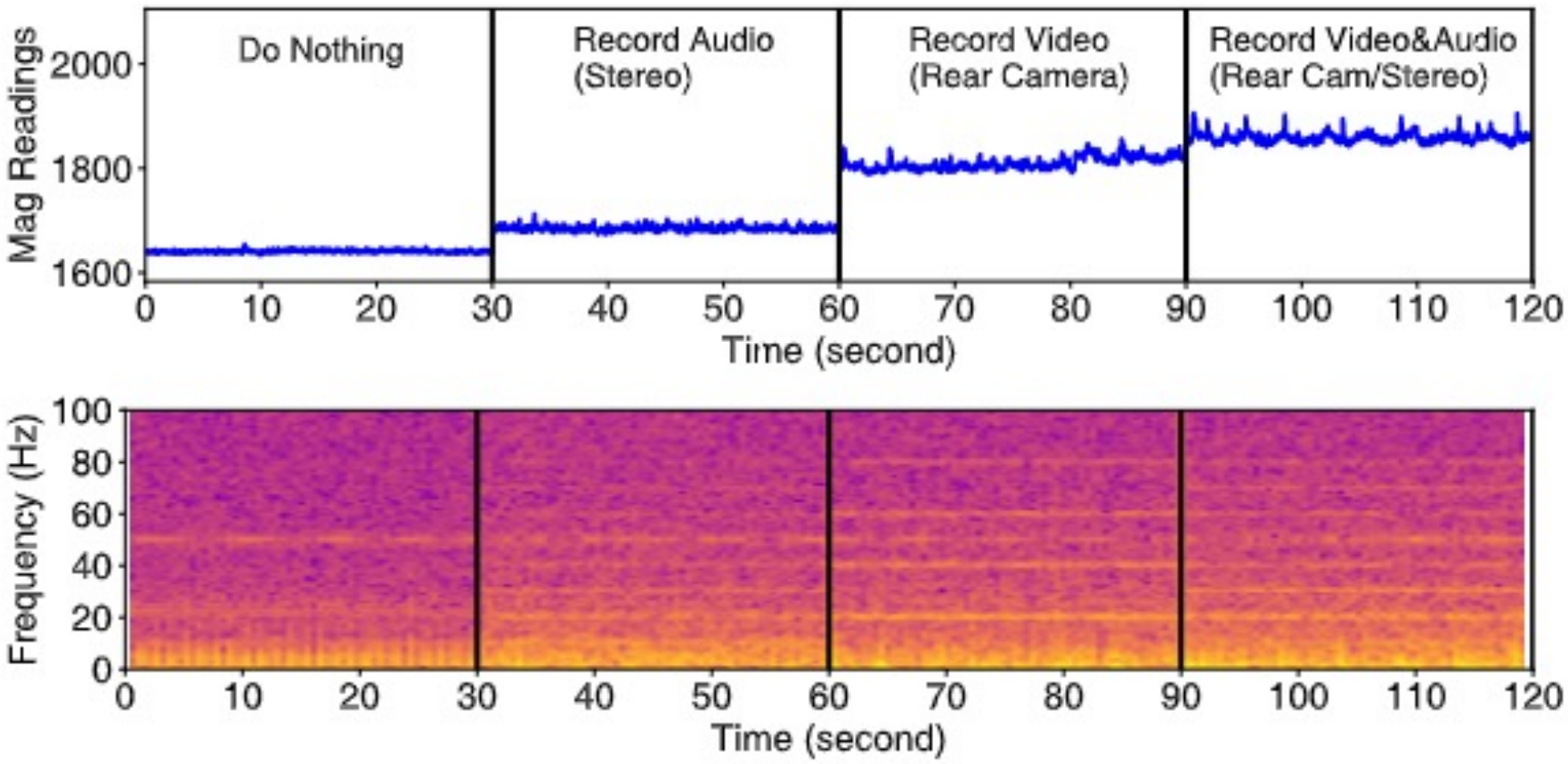
2. Supervised learning needs to know the eavesdropping app labels ☹

3. Eavesdropping apps are always in the background☹

Outline

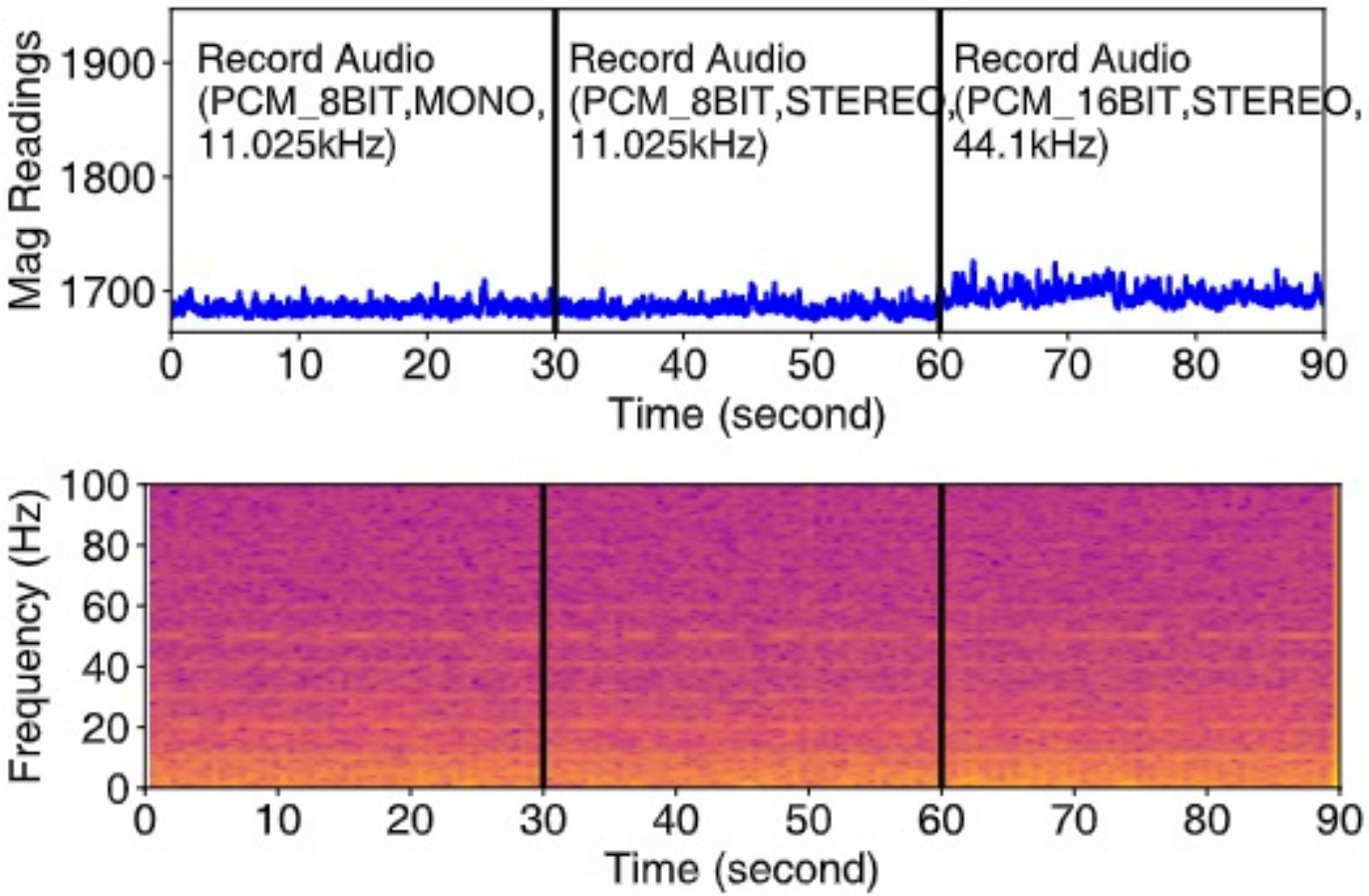
- Background and Motivation
- Existing Monitoring Methods and Attack Cases
- Our idea —— EMI side channel
- **Preliminary Analysis**
- System Design
- Evaluation
- Limitation and Discussion
- Conclusion

Preliminary Study 1—— Cameras and Mics indeed emit EM signals

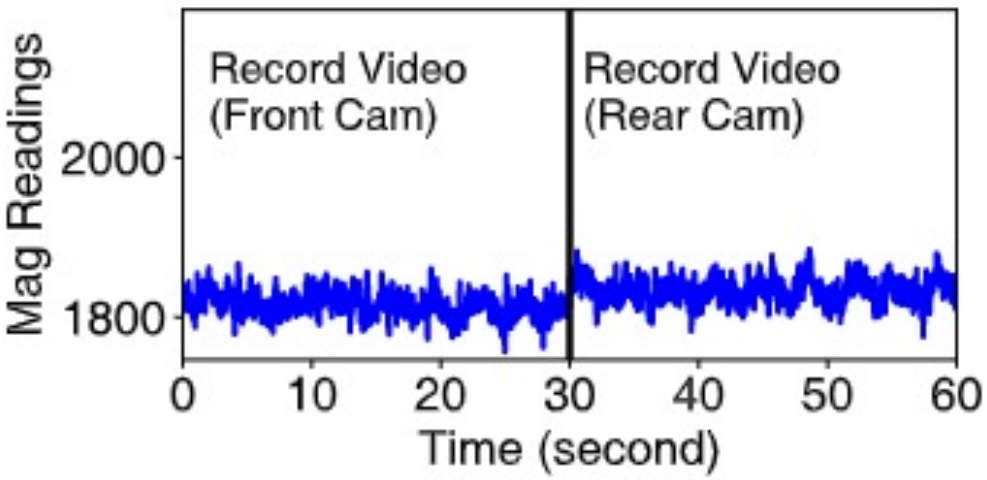


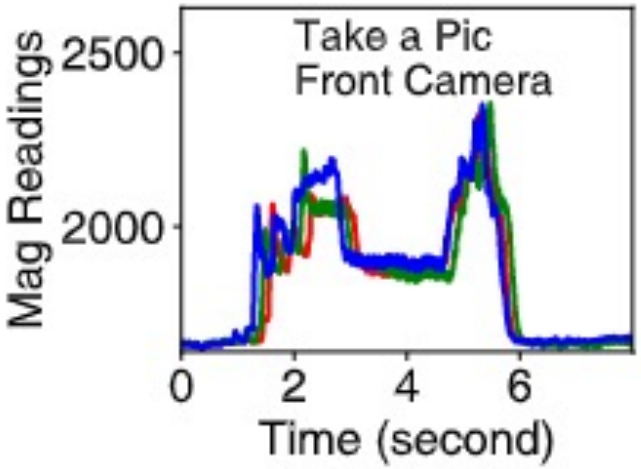
Test smartphone: Huawei P20Pro

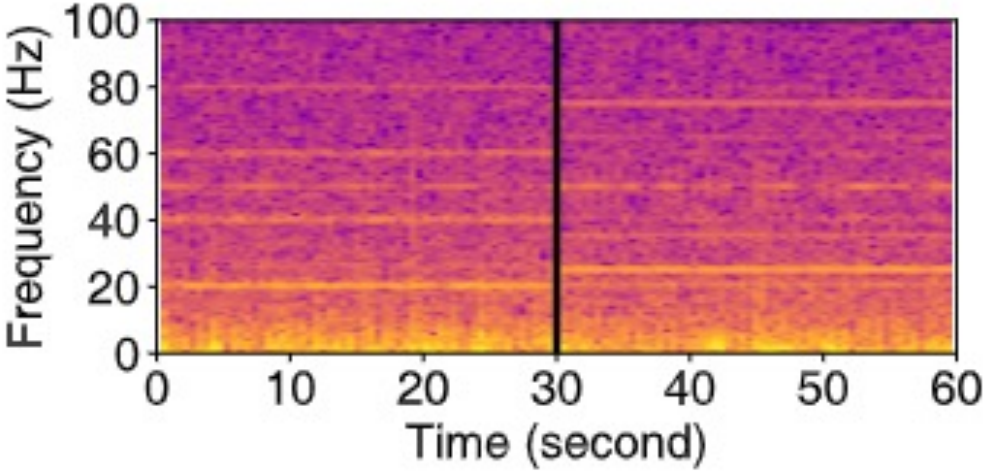
Preliminary Study 2—— Different Mics generate similar EM signals

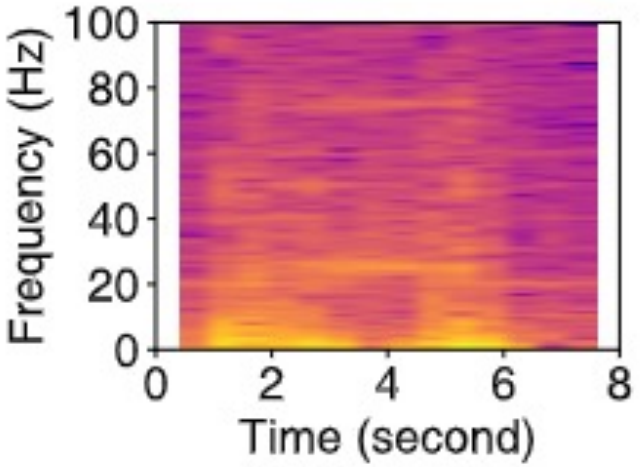


Preliminary Study 2 —— Different cameras generate different EM signals

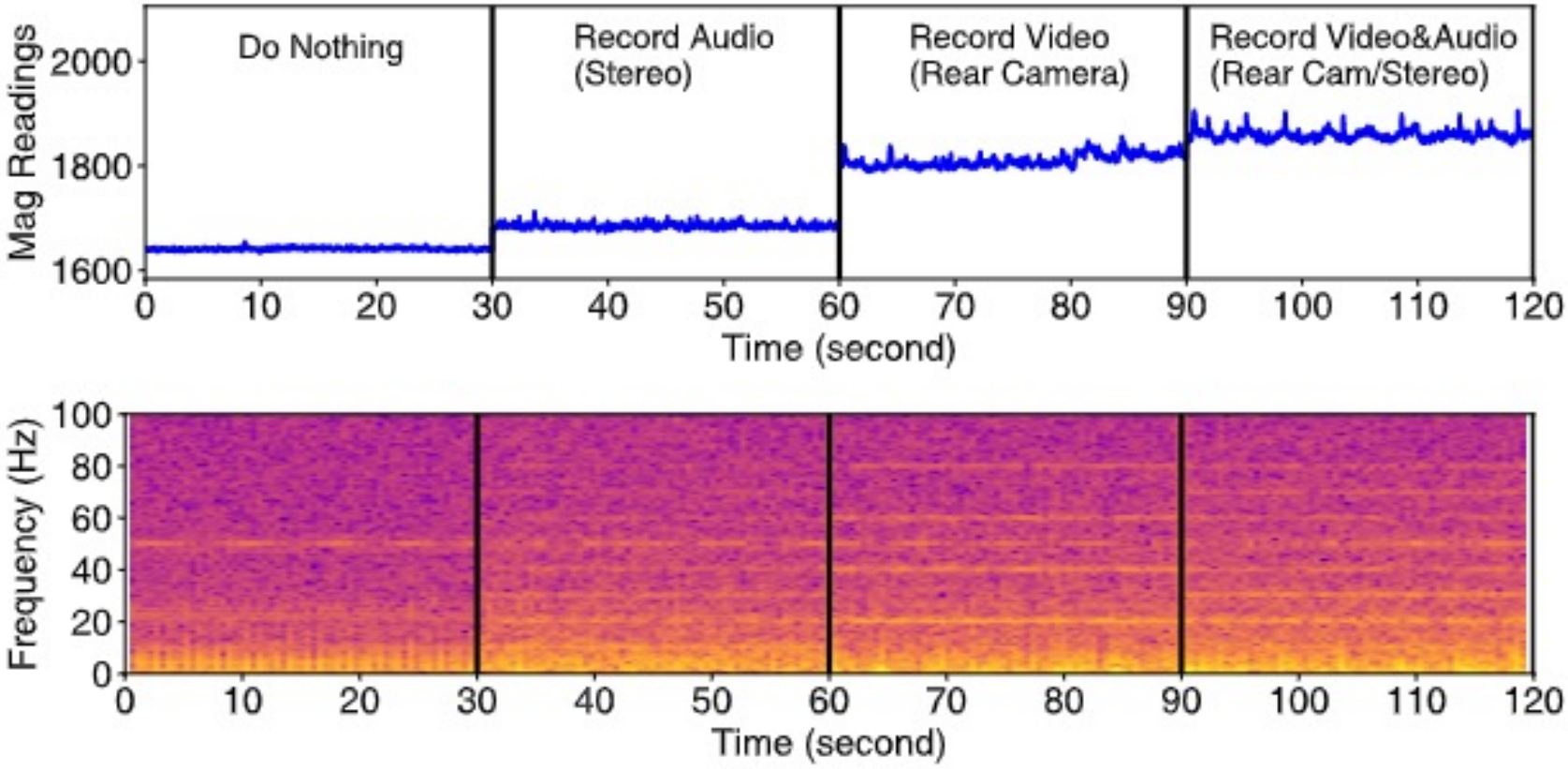






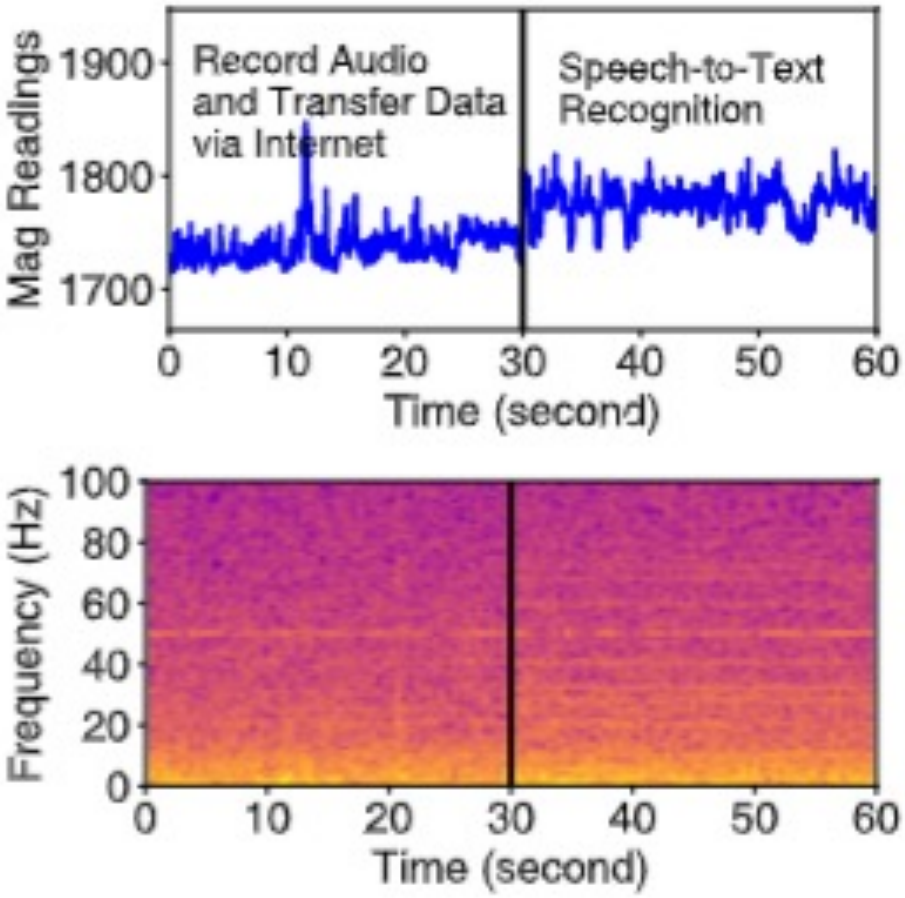


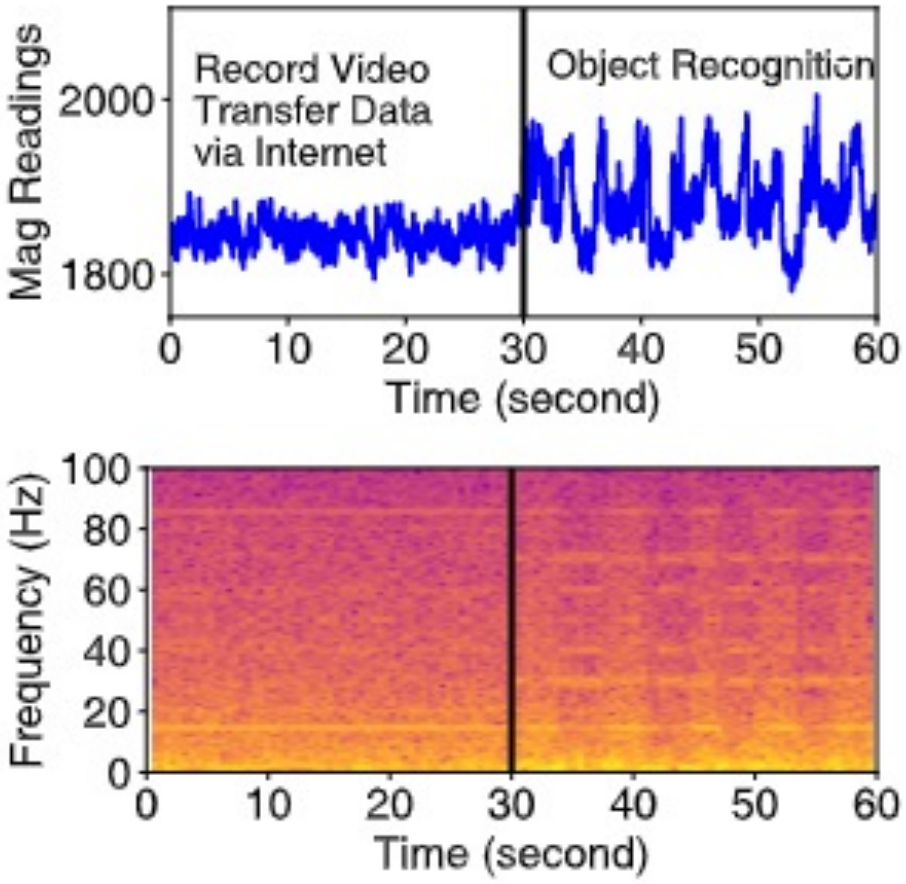
Preliminary Study 3 —— Different smartphone will generate different EM signals when executing the same tasks



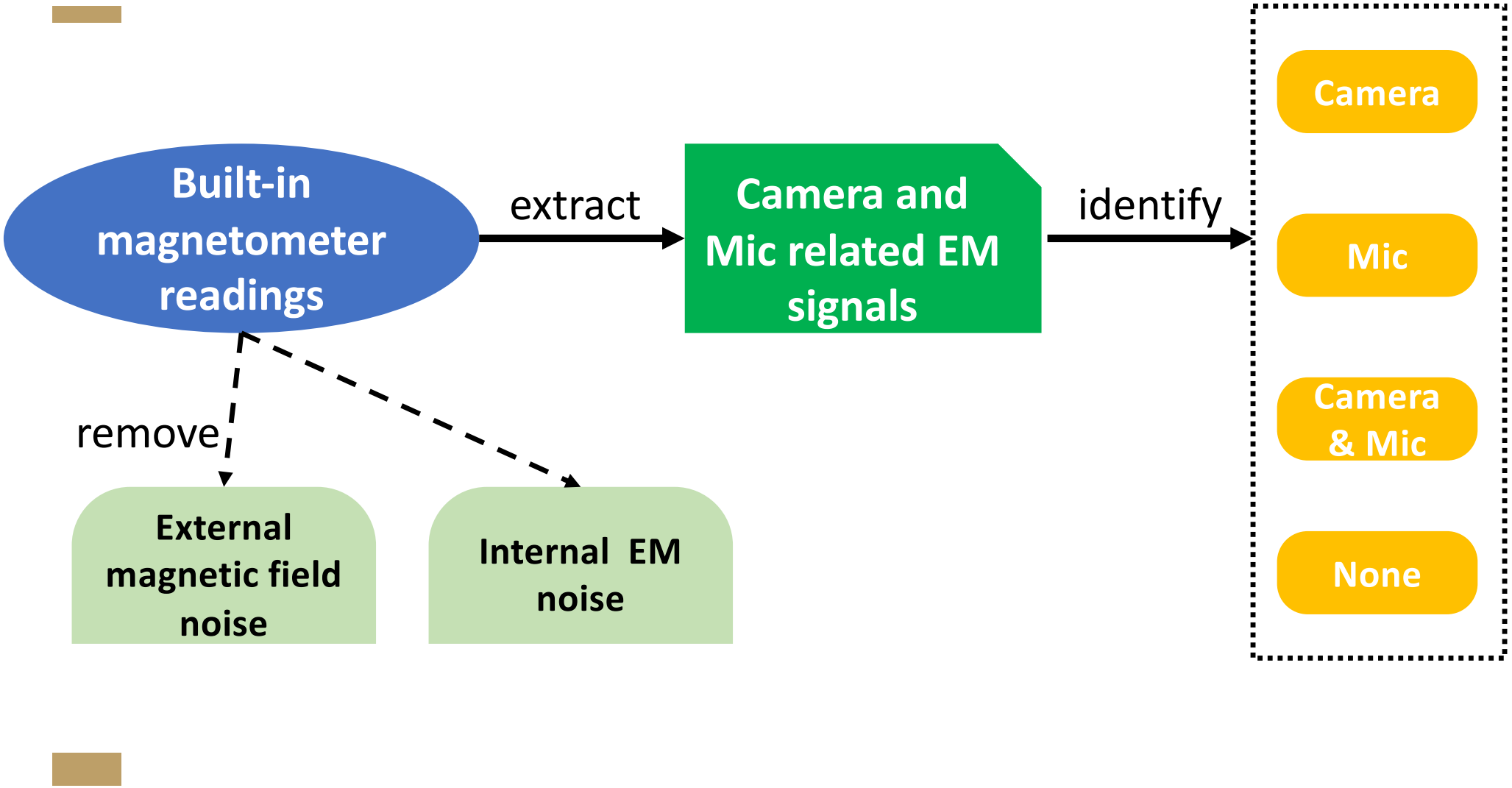
(b) Huawei P20Pro.

Preliminary Study 4 —— Different post-processing will generate different EM signals



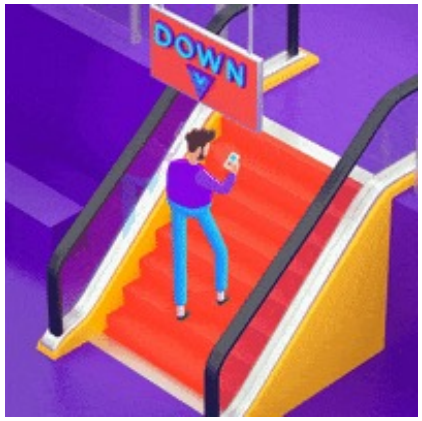


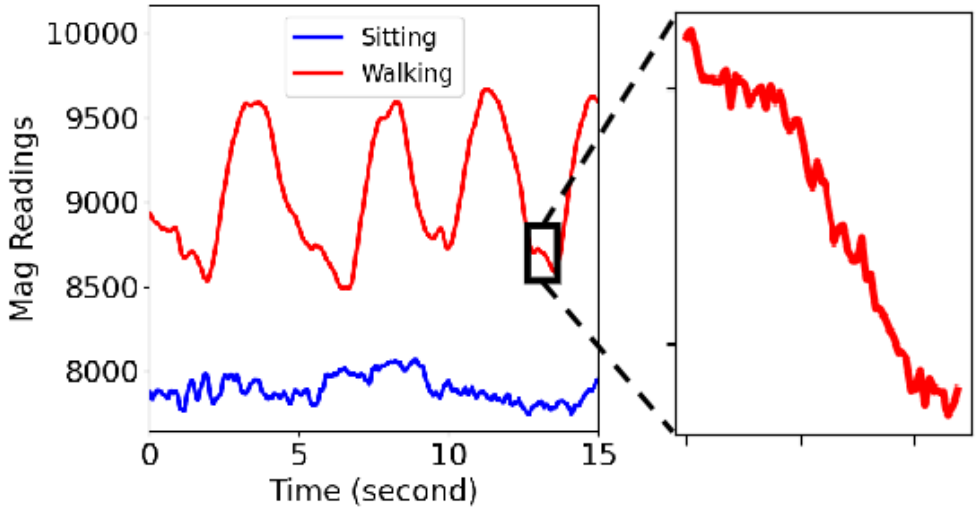
Our target —— EM signals associated with the acquisition of camera/mic data

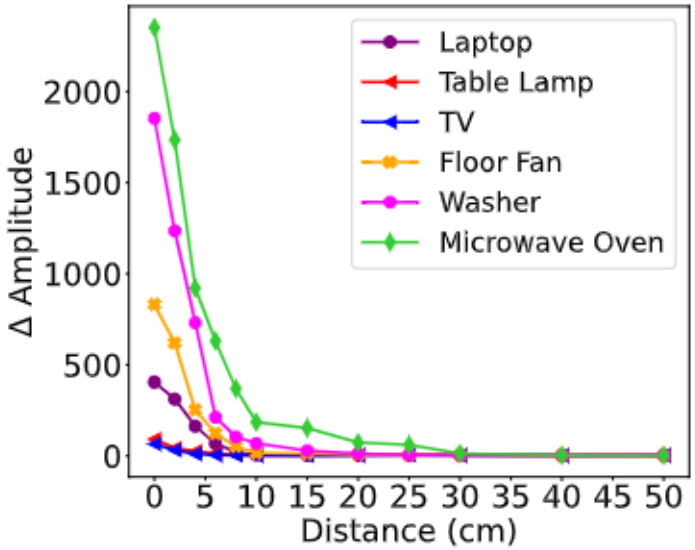


Challenge: Remove the external magnetic field noises

Using phones when walking

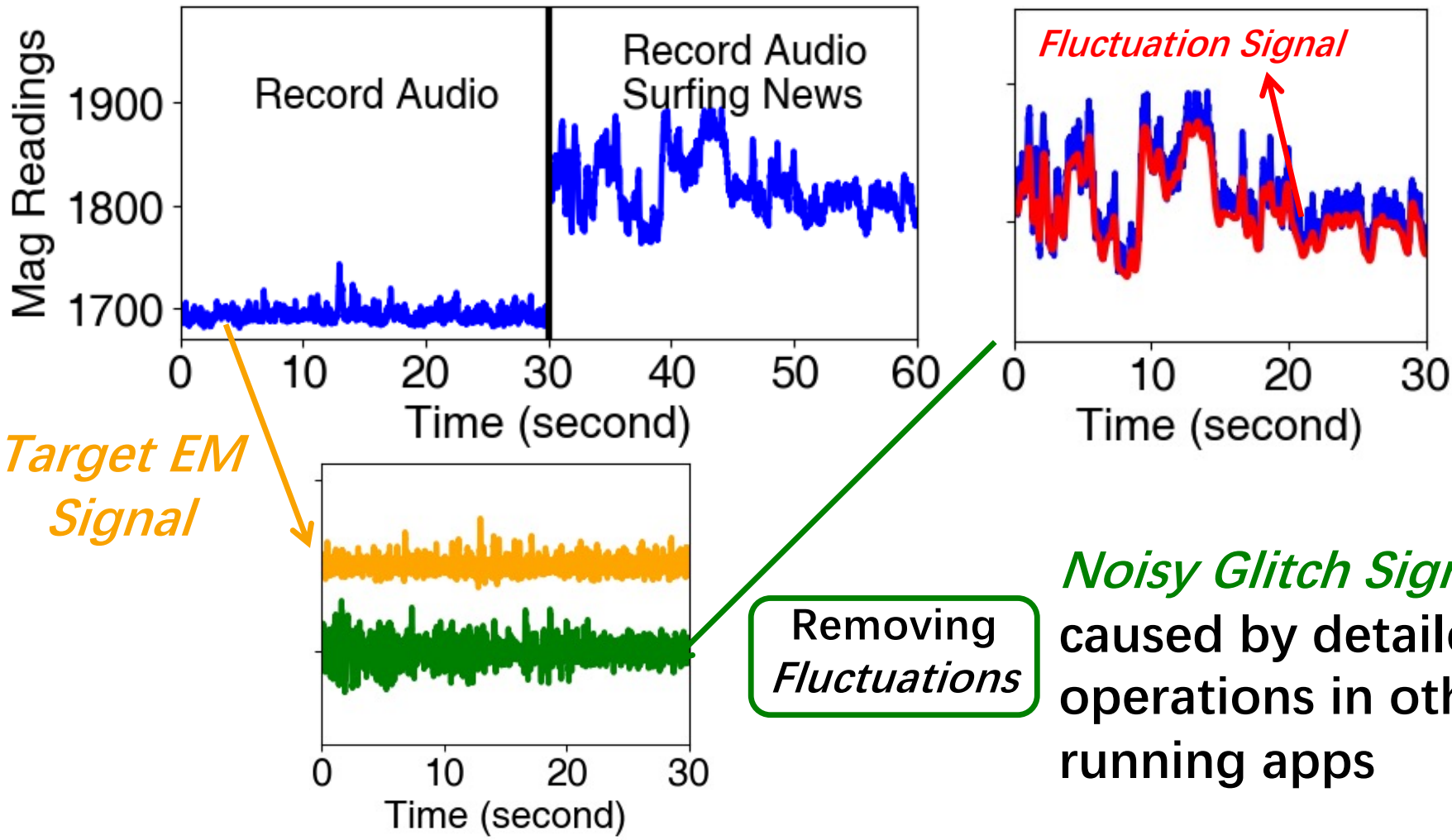




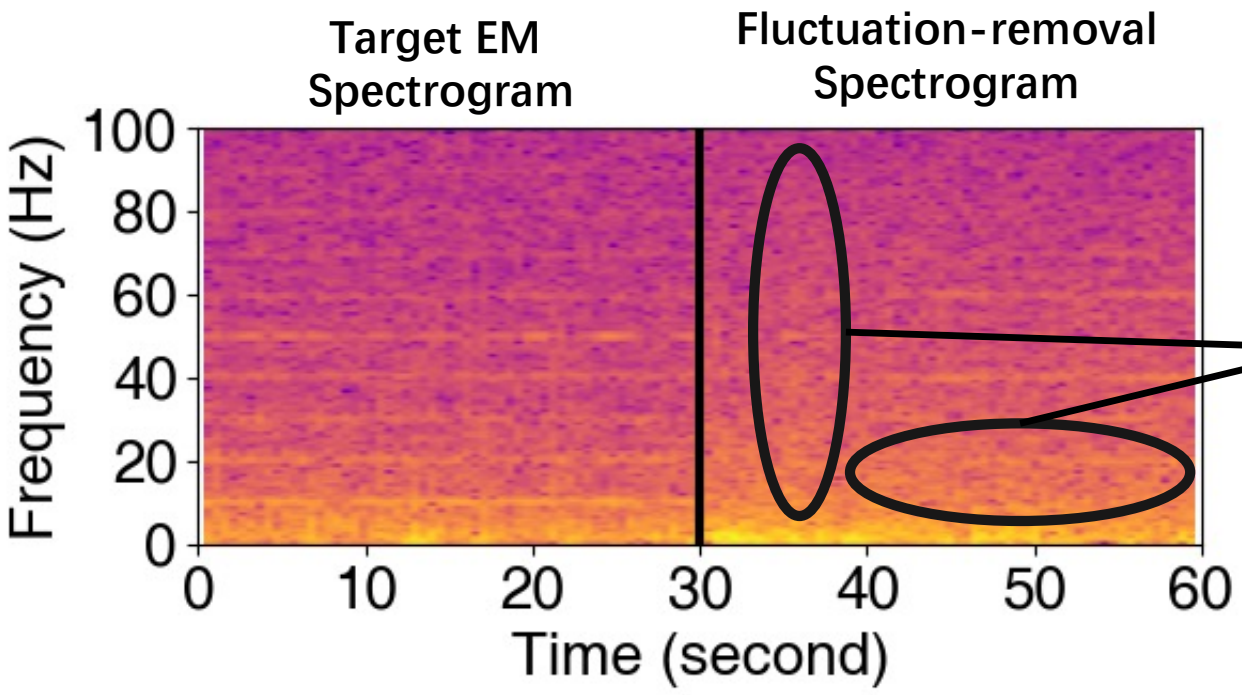


Median-mean filter (MMF)

Challenge: Remove the internal EM noises caused by executing app tasks



Challenge: Remove the internal EM noises caused by executing app tasks

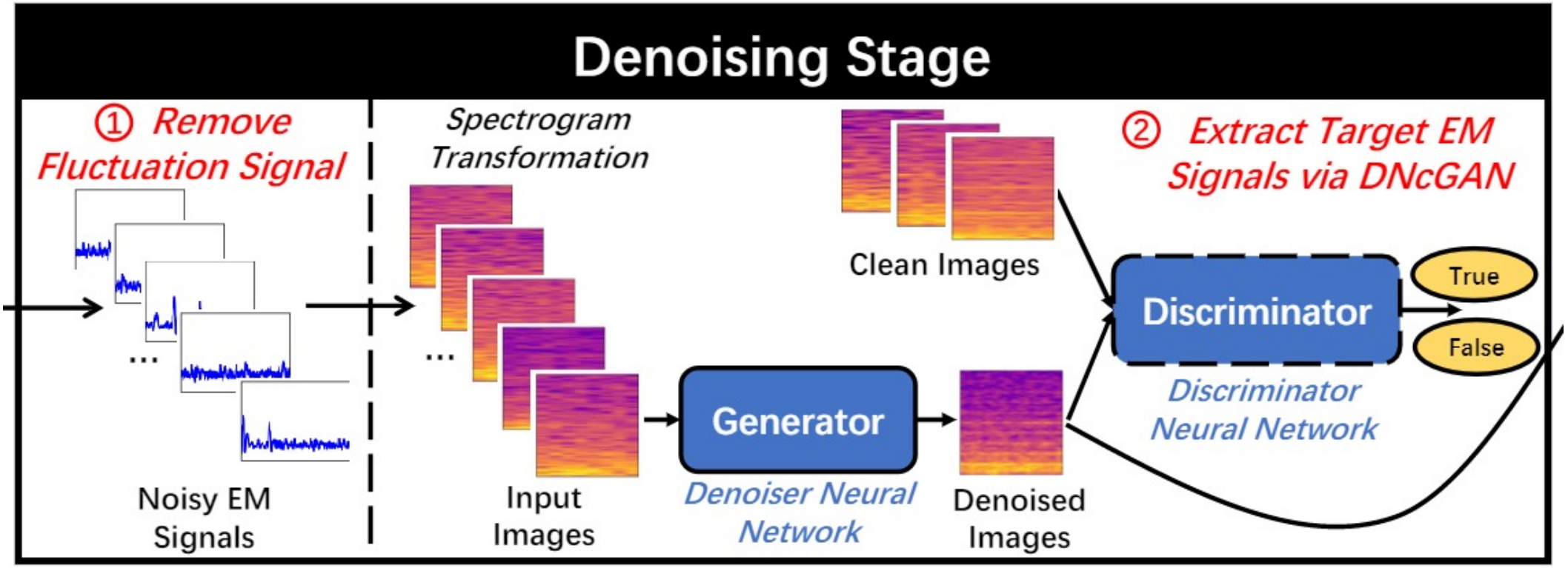


Characteristics of Target EM are submerged by noise

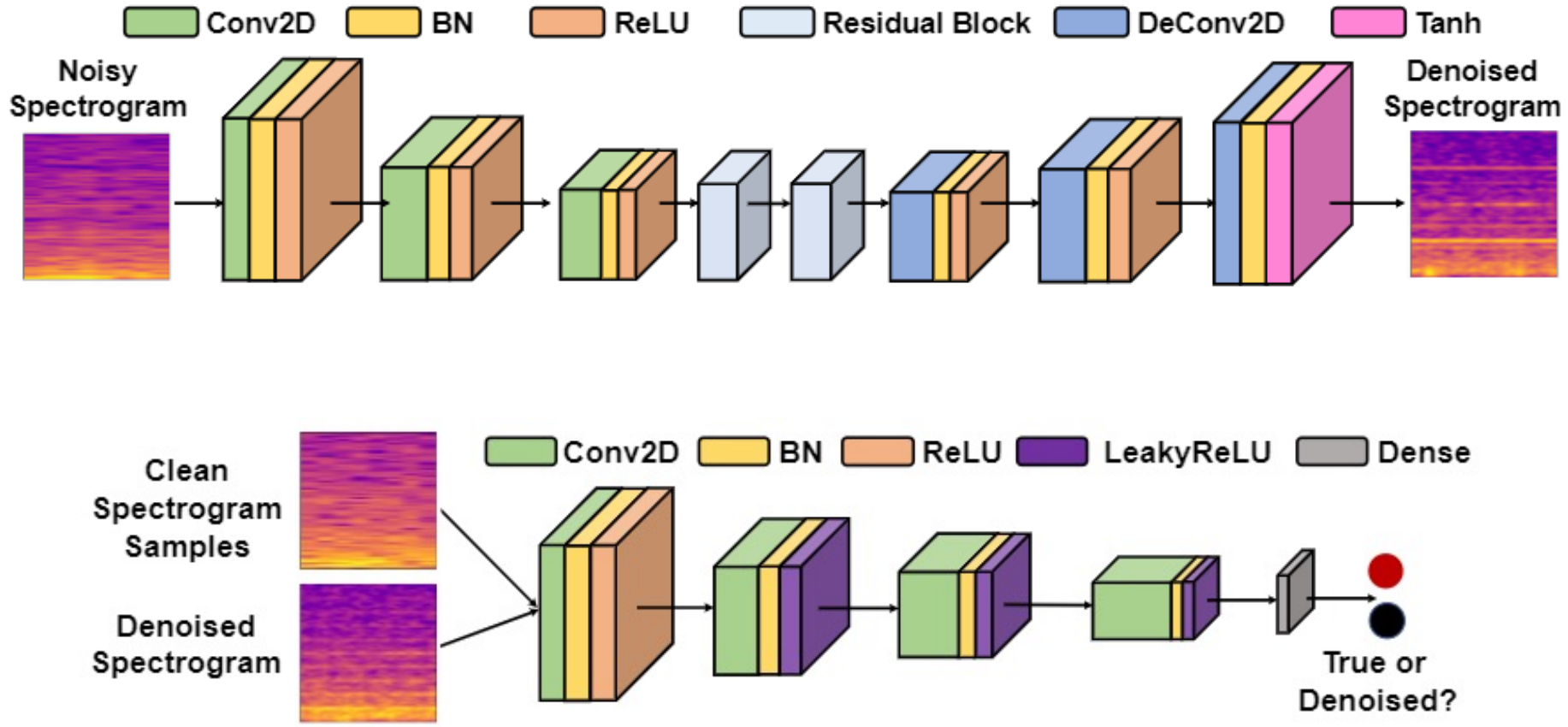
Outline

- Background and Motivation
- Existing Monitoring Methods and Attack Cases
- Our idea —— EMI side channel
- Preliminary Analysis
- **System Design**
- Evaluation
- Limitation and Discussion
- Conclusion

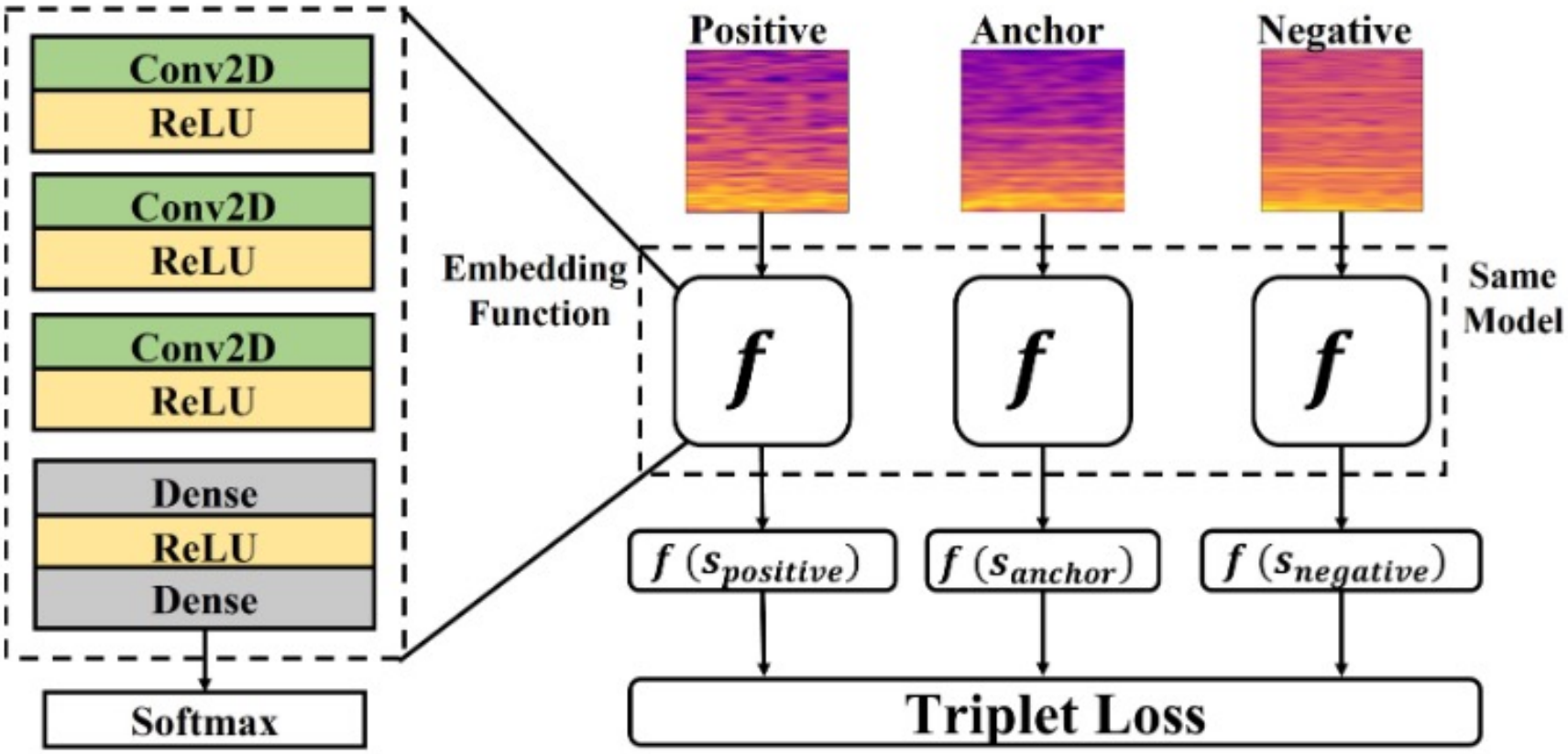
Solution: Denoising conditional GAN



DeNoising conditional GAN : Generator and Discriminator



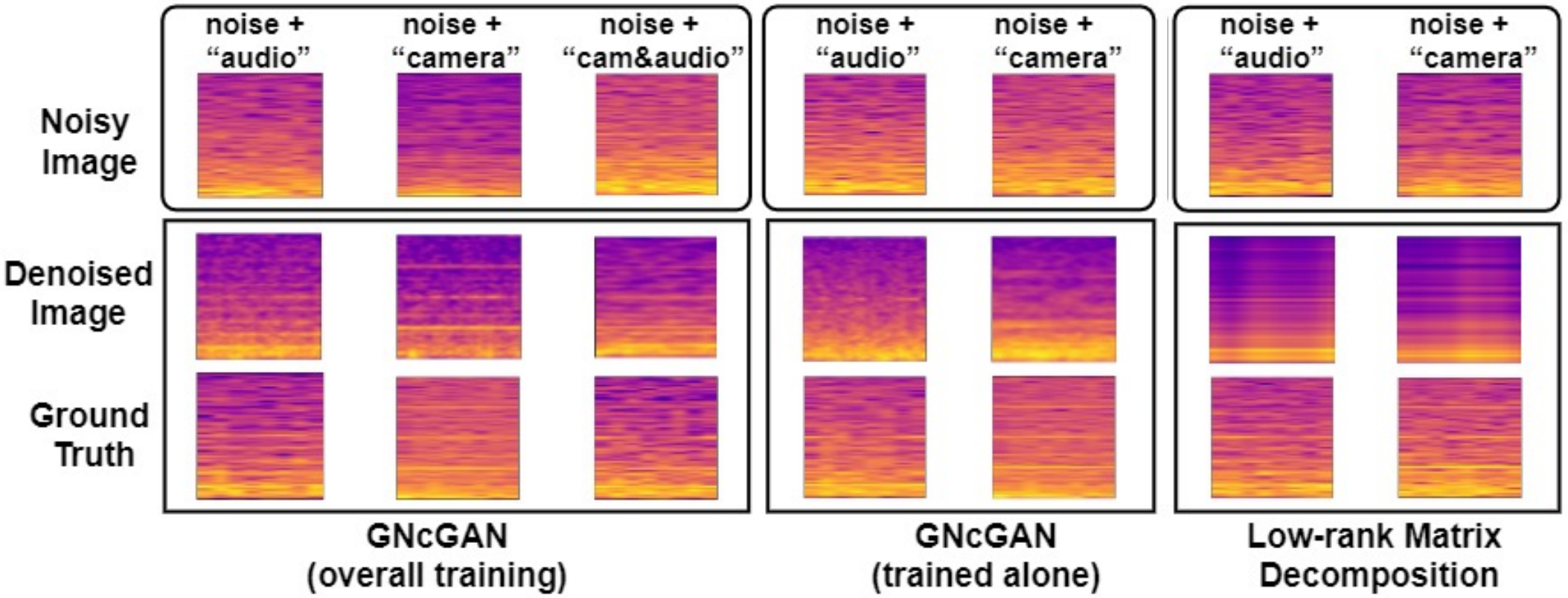
Solution : Triple loss function



Outline

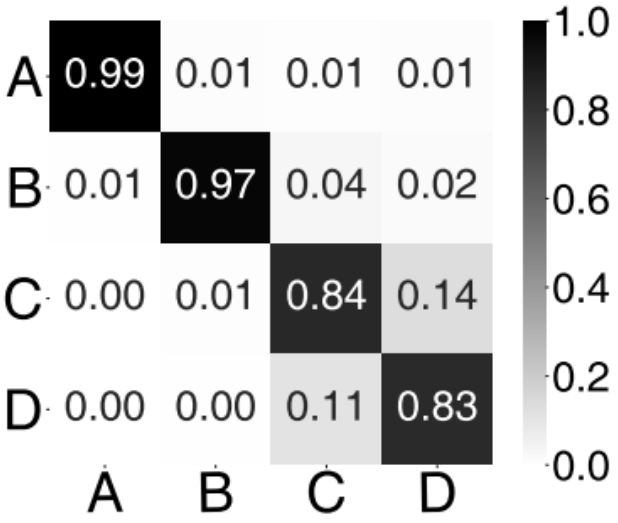
- Background and Motivation
- Existing Monitoring Methods and Attack Cases
- Our idea —— EMI side channel
- Preliminary Analysis
- System Design
- **Evaluation**
- Limitation and Discussion
- Conclusion

Evaluation —— Performance of Denoisng cGAN

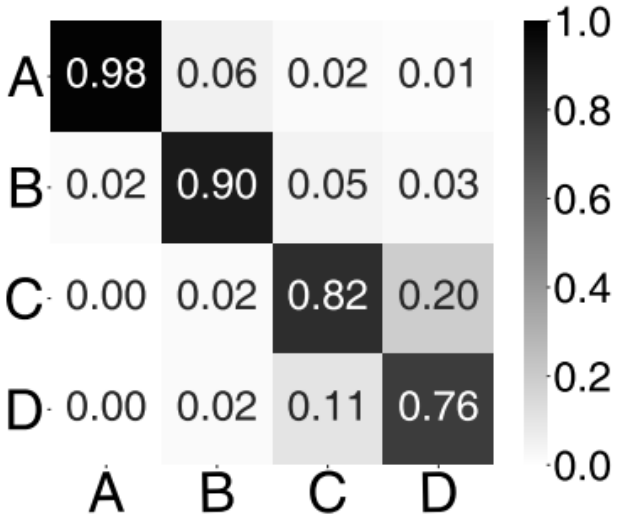


Evaluation —— Performance of camera/mic working detection

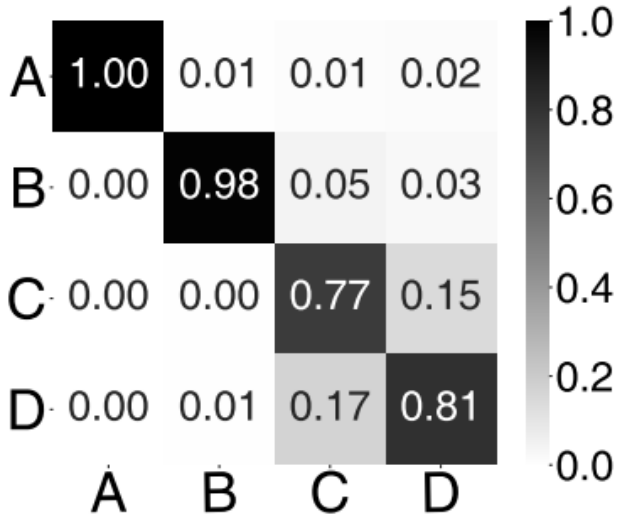
A-D denote "none", "audio", "camera", and "camera-audio"



a) Huawei Mate9



b) LG Nexus5



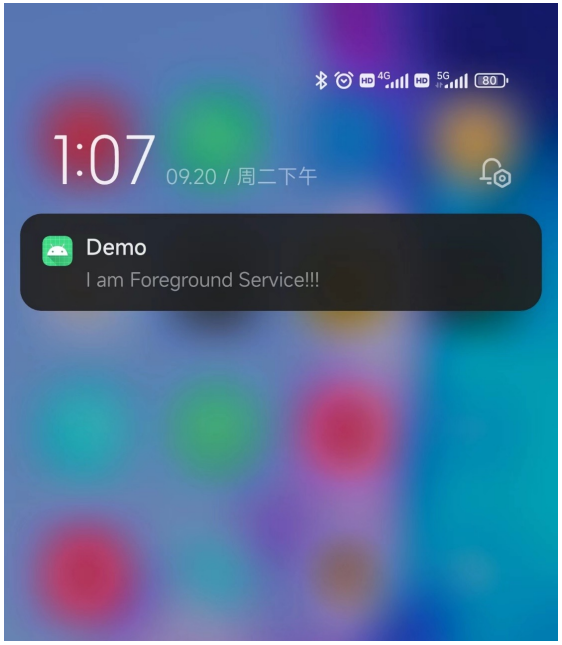
c) iPhoneX

Outline

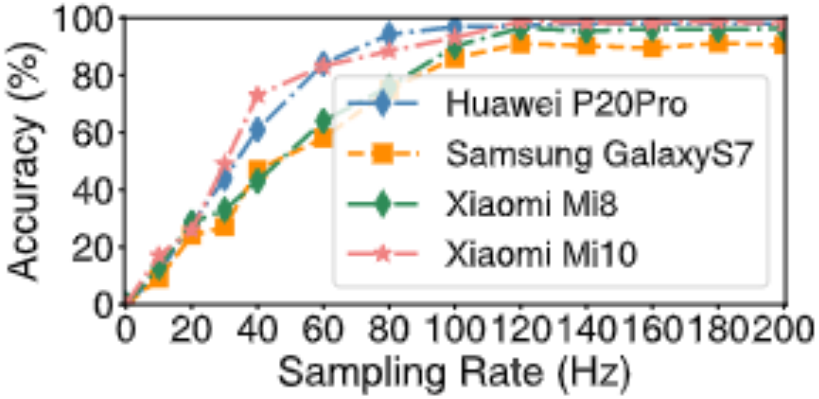
- Background and Motivation
- Existing Monitoring Methods and Attack Cases
- Our idea —— EMI side channel
- Preliminary Analysis
- System Design
- Evaluation
- **Limitation and Discussion**
- Conclusion

Limitations in practical scenarios

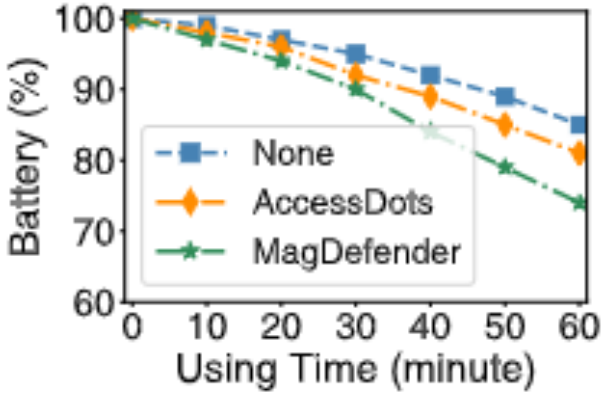
Continuously running in the background



Magnetometer sampling rate



Power Consumption



Cannot identify the eavesdropping app types

Cannot prevent the eavesdropping happening

Outline

- Background and Motivation
- Existing Monitoring Methods and Attack Cases
- Our idea —— EMI side channel
- Preliminary Analysis
- System Design
- Evaluation
- Limitation and Discussion
- **Conclusion**

Conclusion

- **MagDefender** can identify the cameras and microphones working states with the built-in magnetometer readings:
  - ✓ We proposed an *EM-side-channel based method* to monitor the cameras and microphones working states without using OS-related APIs.
  - ✓ We conducted a pilot study to verify that the media-related hardware modules in smartphones generate unique and consistent EM signals detectable using the built-in magnetometer.
  - ✓ We utilized a denoising cGAN to extract the target EM signals associated with camera/mics. Final experiment results show the performance (97.3%) in identifying instances of eavesdropping.


上海交通大學
SHANGHAI JIAO TONG UNIVERSITY
Thanks!