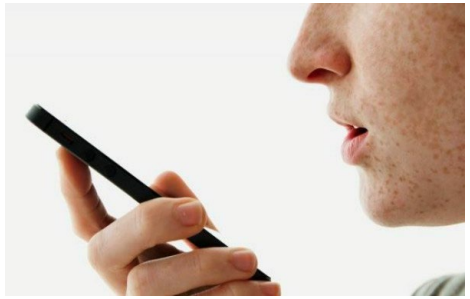
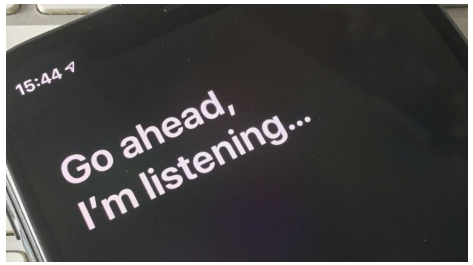
GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line

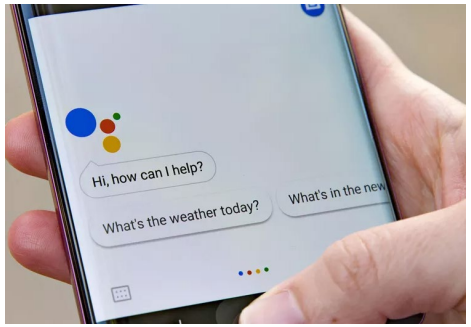
Yuanda Wang, Hanqing Guo, Guangjing Wang, Bocheng Chen, Qiben Yan

Michigan State University

Smartphone Voice Assistants







Read my message

Calling Alice

Send a message to Bob

Open the door

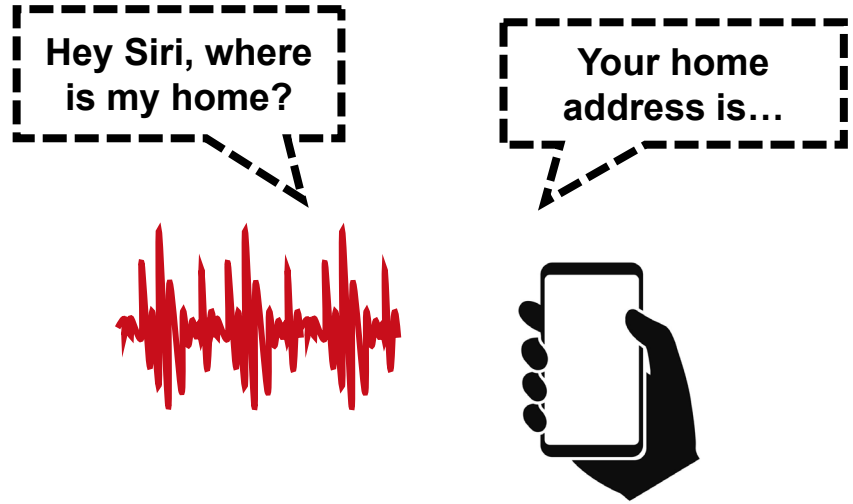
What's my schedule today?

Where am I?

What is my address?

What is my car plate number?

Challenges of Traditional Voice Command Attacks



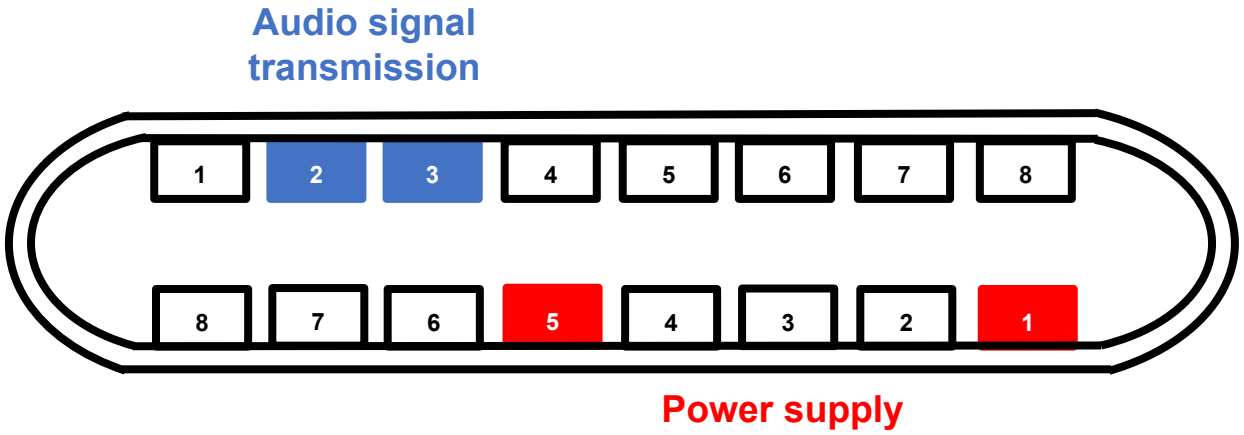
Noisy environments

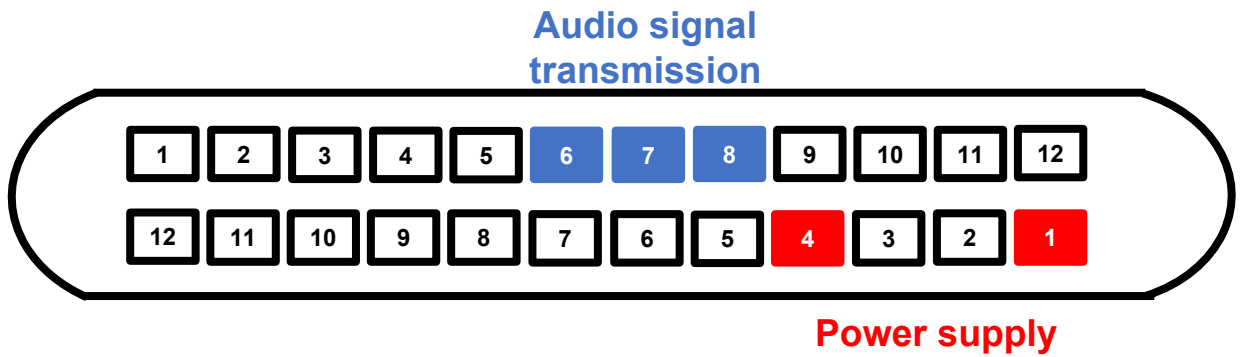
Voice recognition

Interaction

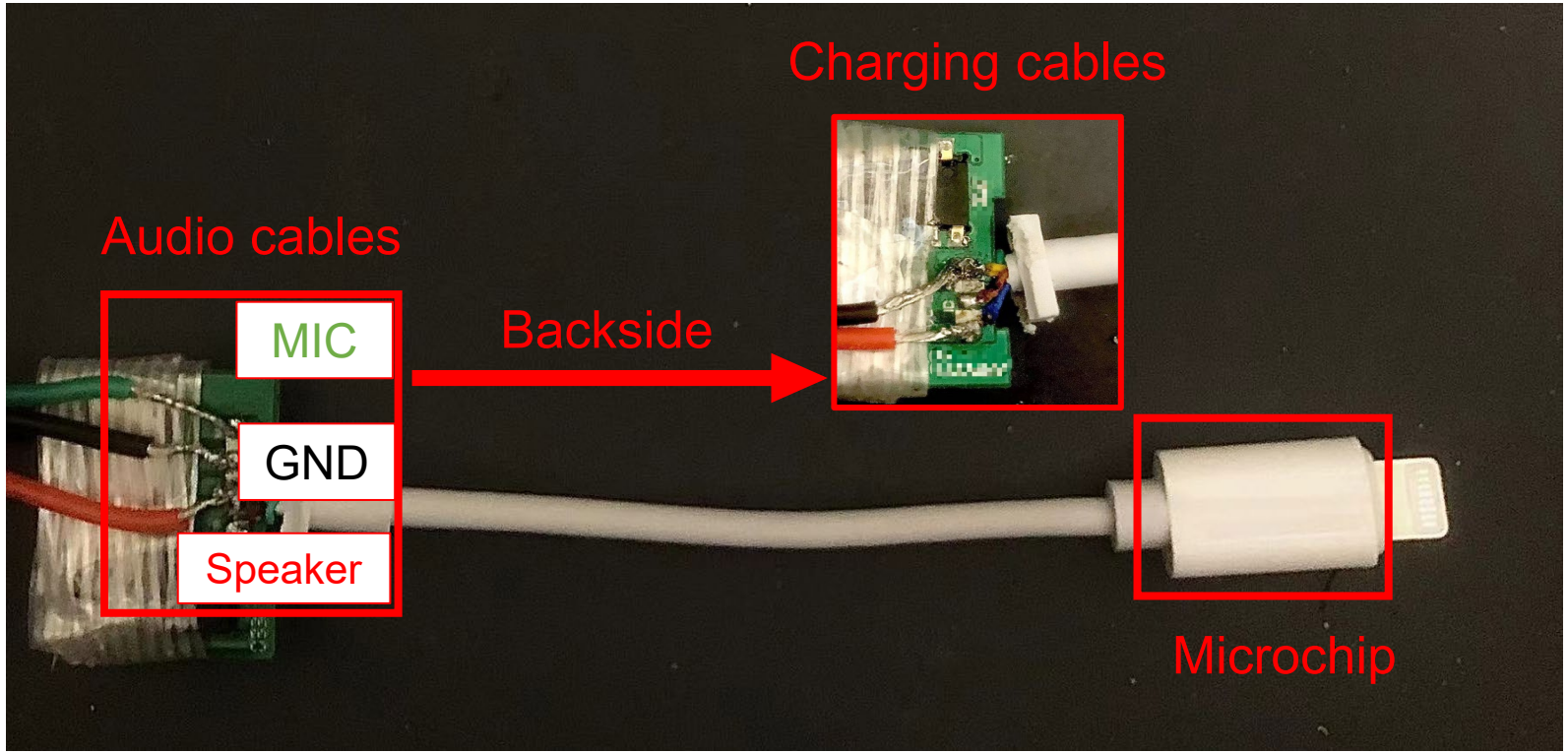
How do we address these challenges?

Design of Charging Ports

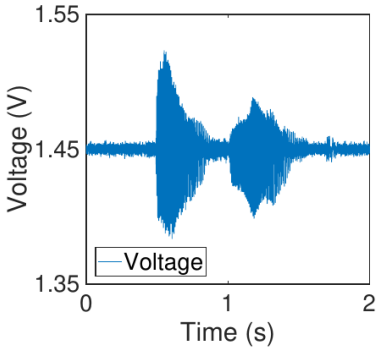




Inaudible Attack through Charging Ports via Malicious Cable

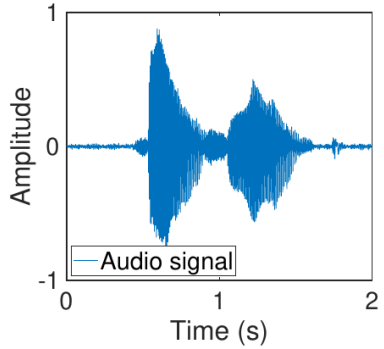


Preliminary Observations

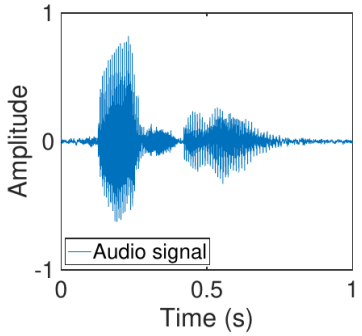


Electric signal

Inject

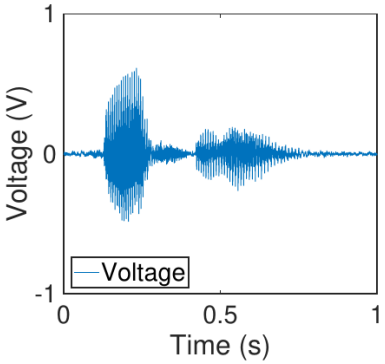


Audio input



Audio output

Eavesdrop

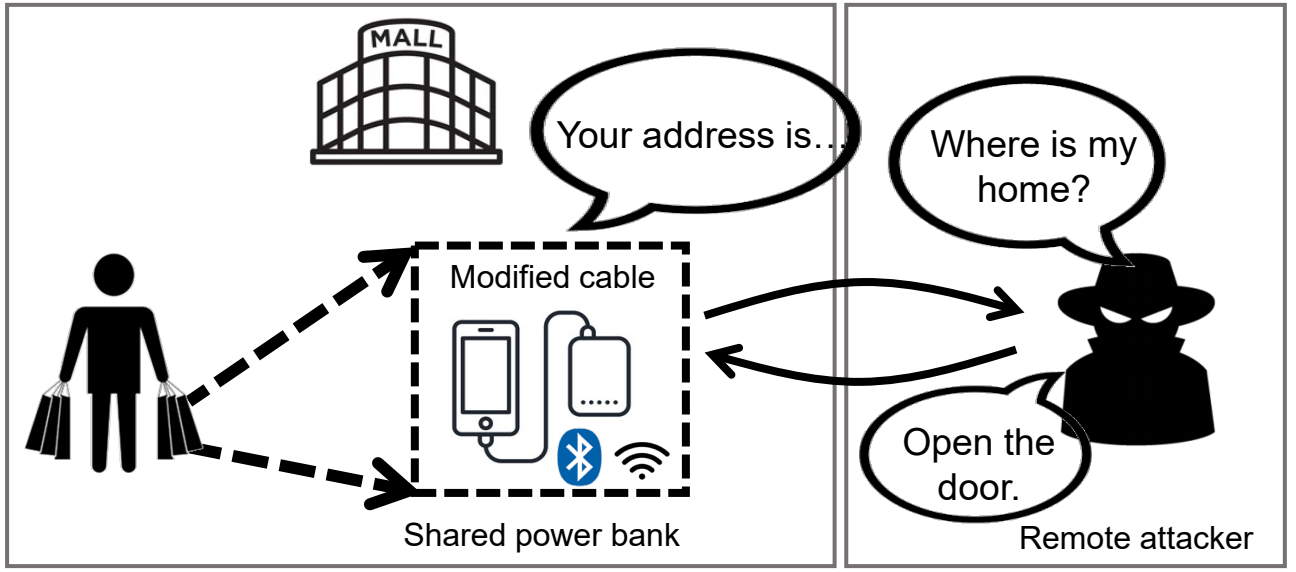


Electric signal

Electric signals can be converted to audio signals, and vice versa.

GhostTalk Attack

- Shared power bank raise the potential risk of such attack!

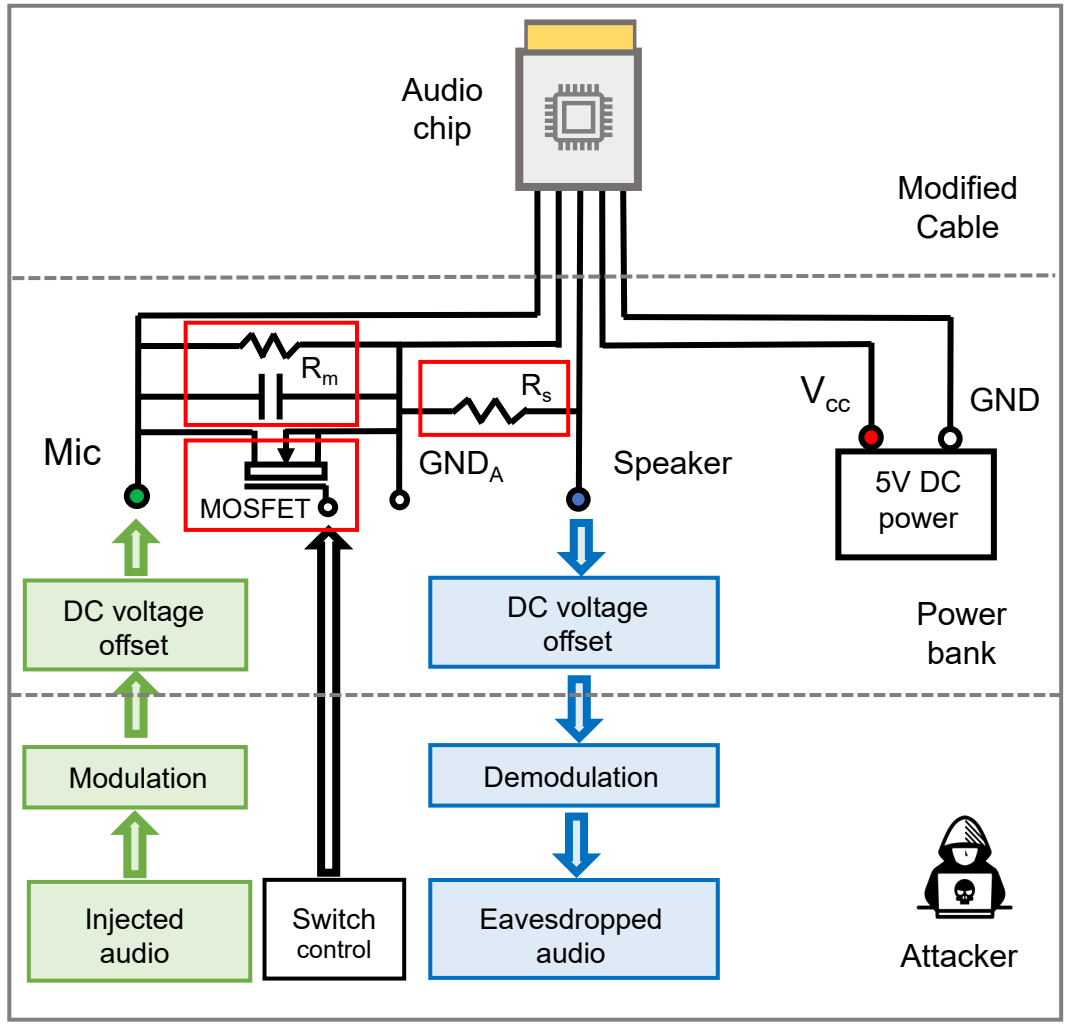


GhostTalk System Design

Noisy environments

Interaction

Voice recognition

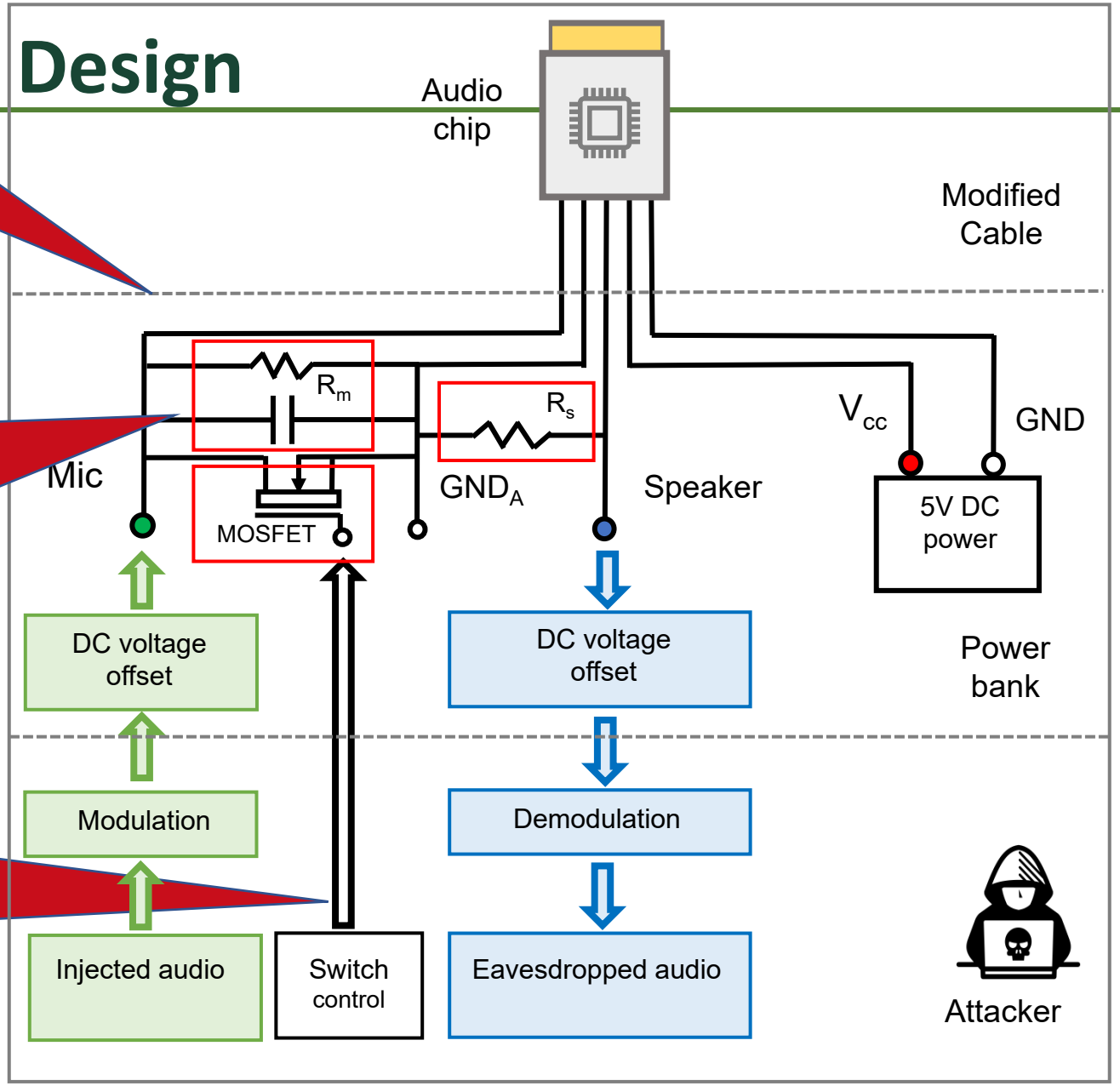


G m Design

Noise Robustness:
GhostTalk injects voice command through electric signals, so that environmental noise has no impact on the

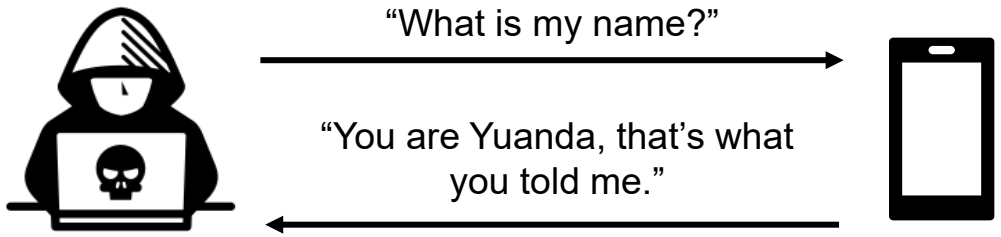
Interactivity:
GhostTalk uses resistances to emulate a fake “headphone” and make the smartphone play audio through it. And it can hack the output audio signals by measuring the voltage on the speaker cable.

Bypass speaker recognition:
GhostTalk adds a MOSFET between the microphone and ground, to emulate a fake “press button” on the headphone and activate the voice assistant.

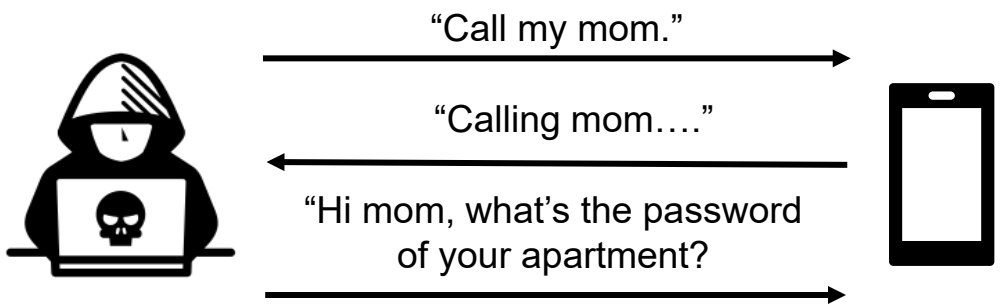


GhostTalk Attack Scenarios

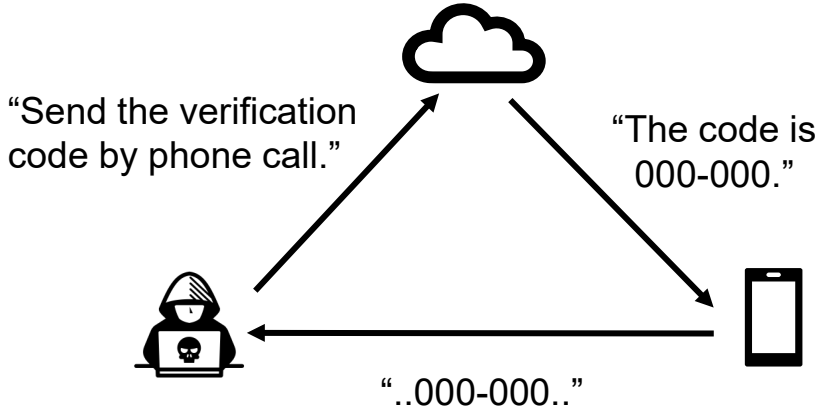
Scenario 1: Privacy information query



Scenario 2: Ghost phone call



Scenario 3: Hacking verification code



What if attackers CANNOT modify the charging cable?

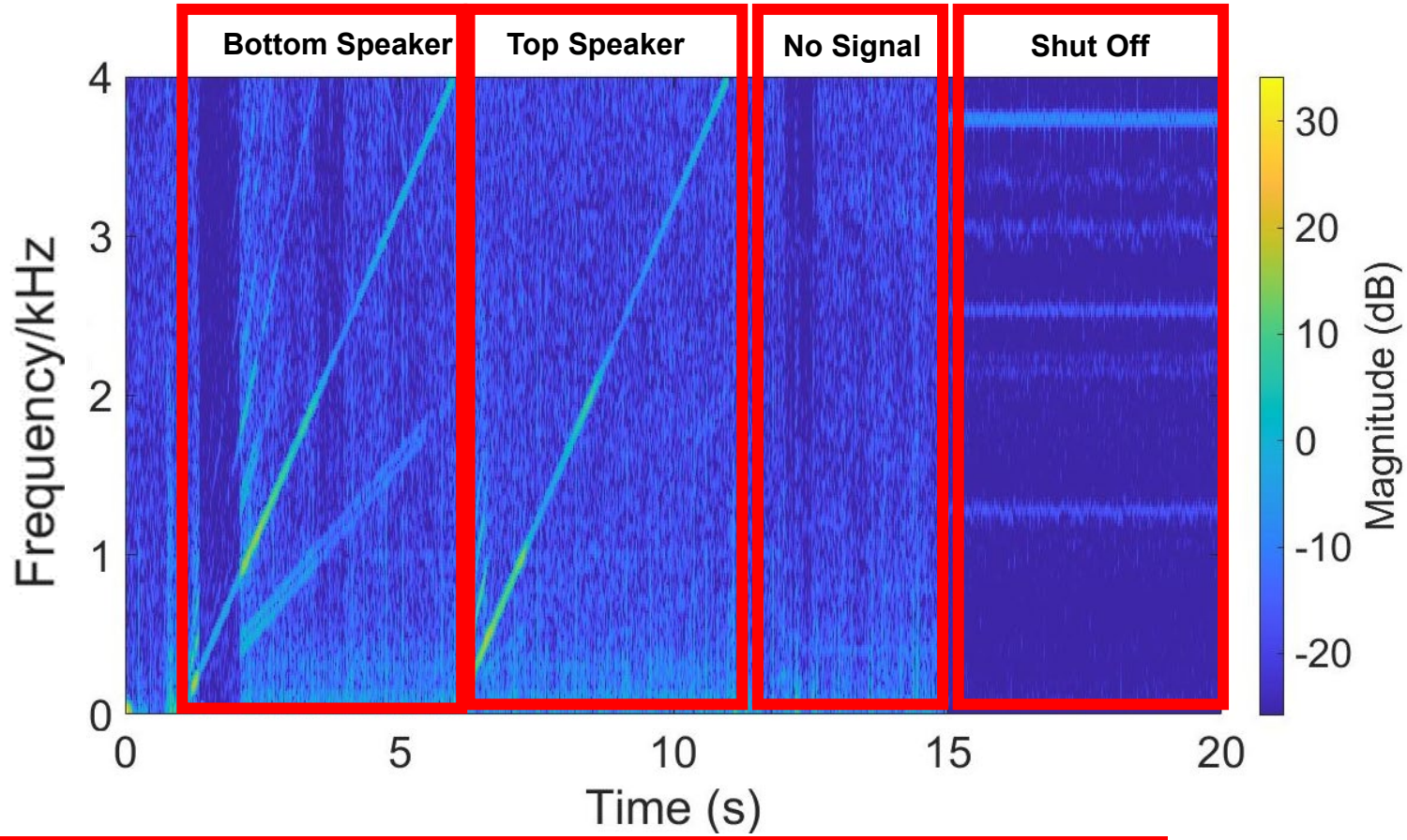
Eavesdrop from Public Charging Ports

Public USB charging ports in hotels and airports.

Audio Signal in Power Side-channel

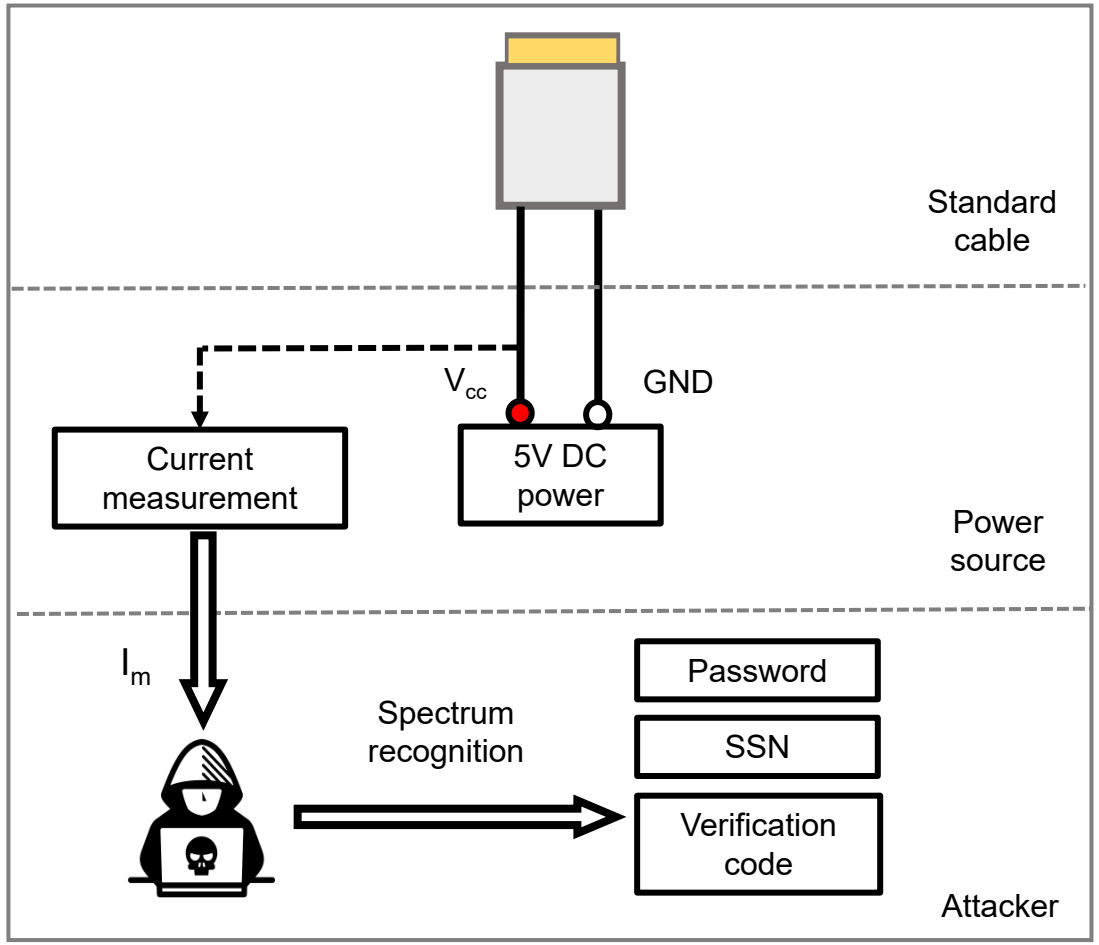
Top loudspeaker

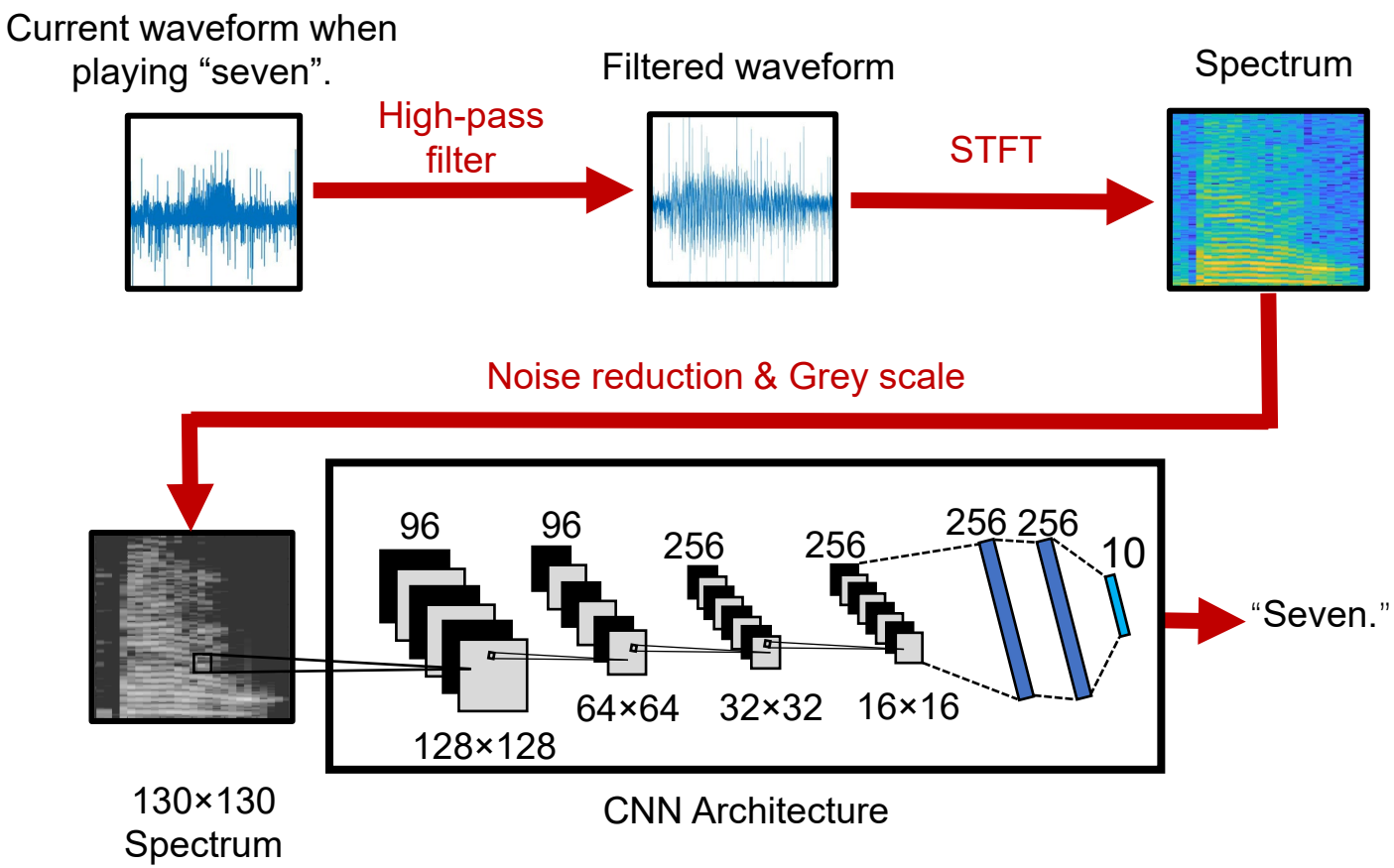
Bottom loudspeaker



The audio signal patterns in the charging current is leaked due to the high-power profile of the loudspeaker

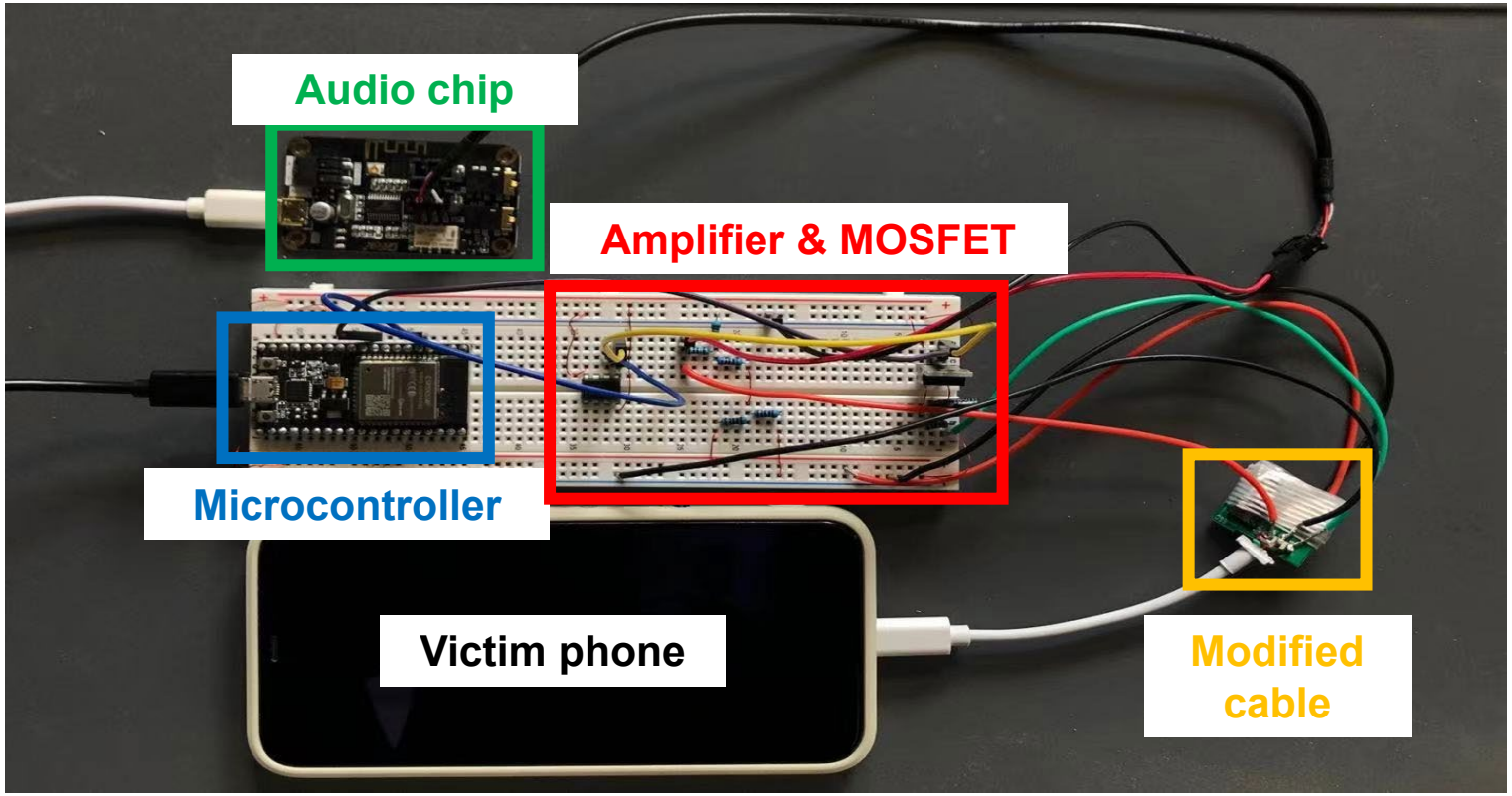
GhostTalk-SC System Design





Evaluation

- Attack hardware



- Low-cost
- Portable
- Small enough to be hidden in a power bank

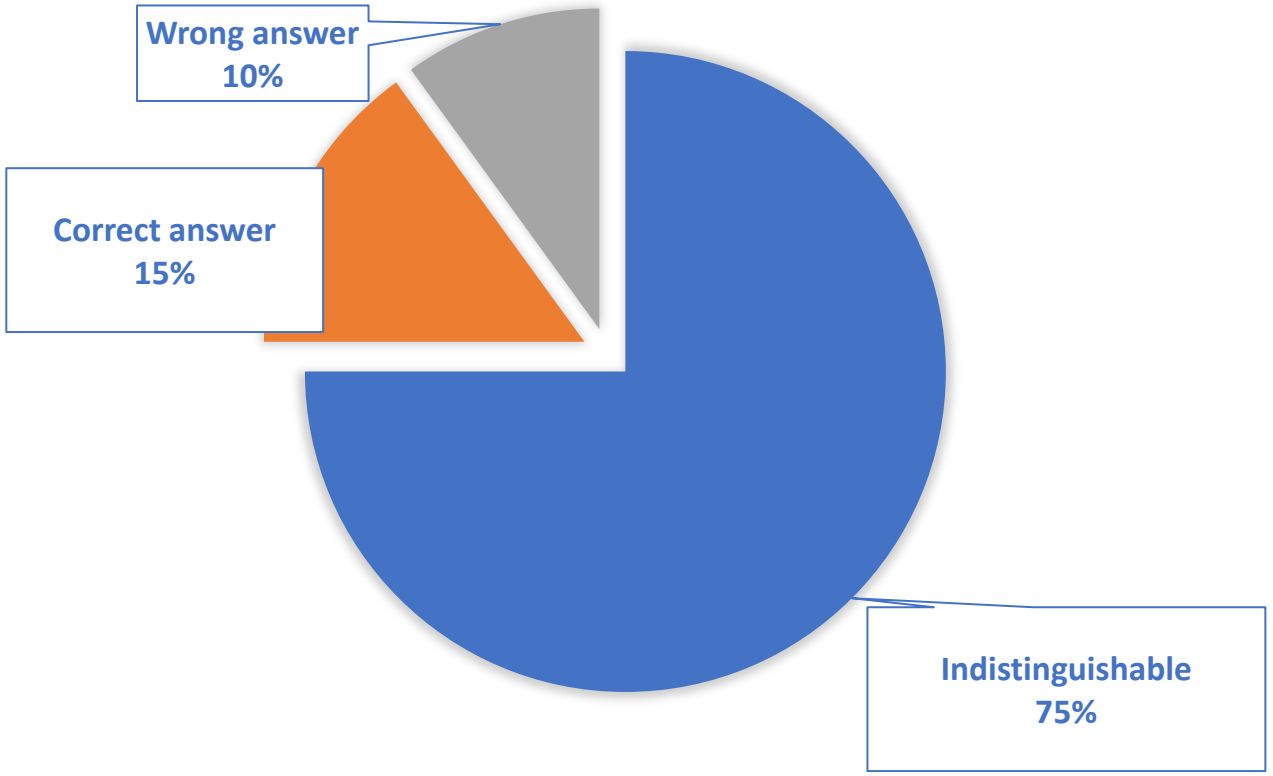
GhostTalk Evaluation

Manufacturer	Model	OS	Assistants	fs (kHz)	GhostTalk			SNR (dB)	ASR
					Act.	Inj.	Eav.		
Apple	iPhone 5s	iOS 12.5	Siri	44.1	√	√	√	19.7	100%
Apple	iPhone X	iOS 14.5	Siri	48.0	√	√	√	21.3	100%
Huawei	Honor 10	Android 9.0	Google	48.0	√	√	√	20.4	100%
Xiaomi	MI 8 Lite	Android 9.0	Google	44.1	√	√	√	18.9	100%
Xiaomi	Pocophone	Android 9.0	Google	48.0	√	√	√	21.8	100%
Samsung	Note 10	Android 10.0	Google	44.1	√	√	√	21.2	100%
Samsung	S9	Android 10.0	Google	44.1	√	√	√	20.1	100%
Google	Pixel 1	Android 10.0	Google	44.1	√	√	√	19.3	100%
Google	Pixel 4XL	Android 11.0	Google	32.0	√	√	√	15.4	100%

We evaluate GhostTalk on 9 different smartphones, and the results show that our attack can successfully compromise all smartphones with 100% success rate.

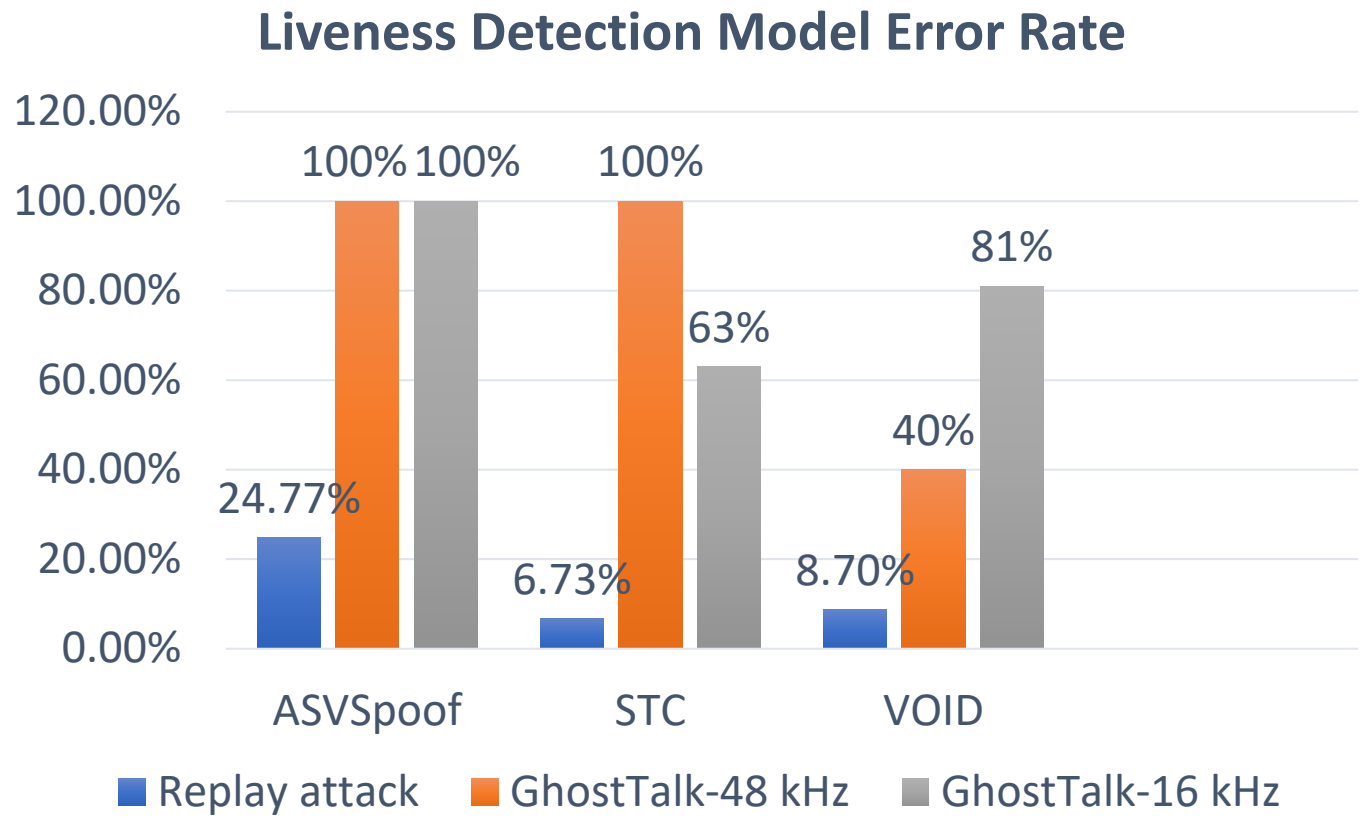
GhostTalk User Study

20 listeners, 10 question for each listener. And 150 answers are indistinguishable.



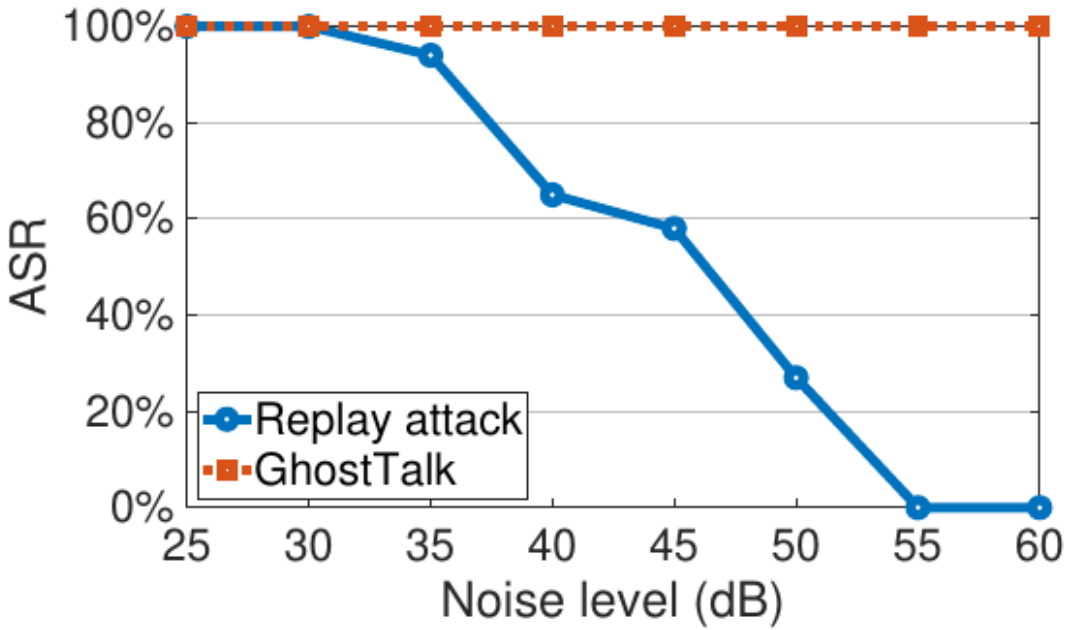
Our injected audio signal can fool human ears!

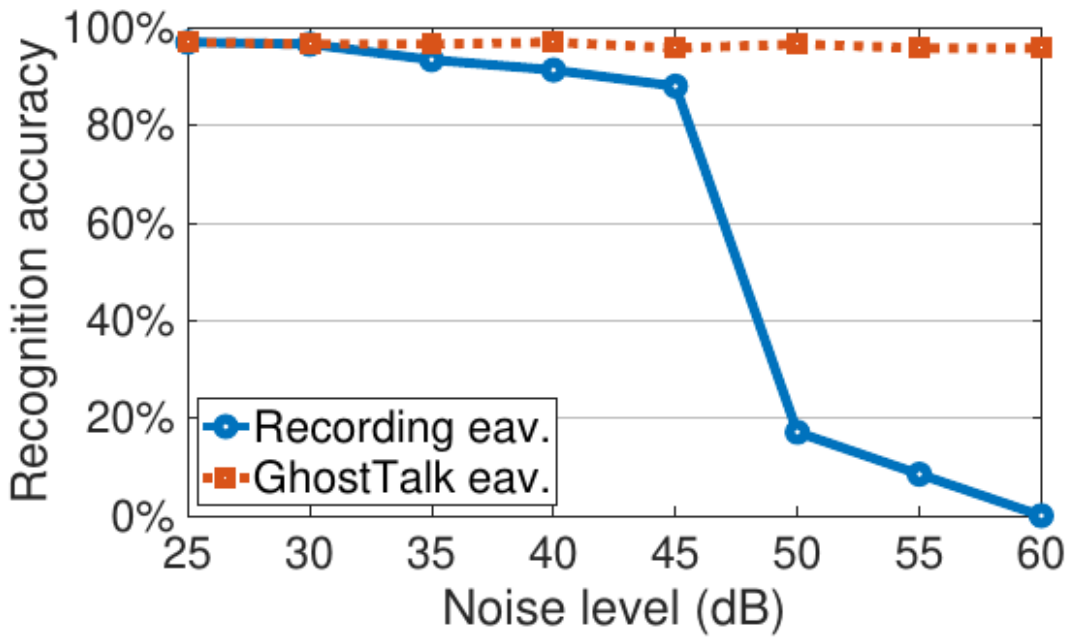
GhostTalk's Robustness against Liveness Detection



GhostTalk attack can bypass existing liveness detection models with high success rate.

GhostTalk's Robustness in Noisy Environment





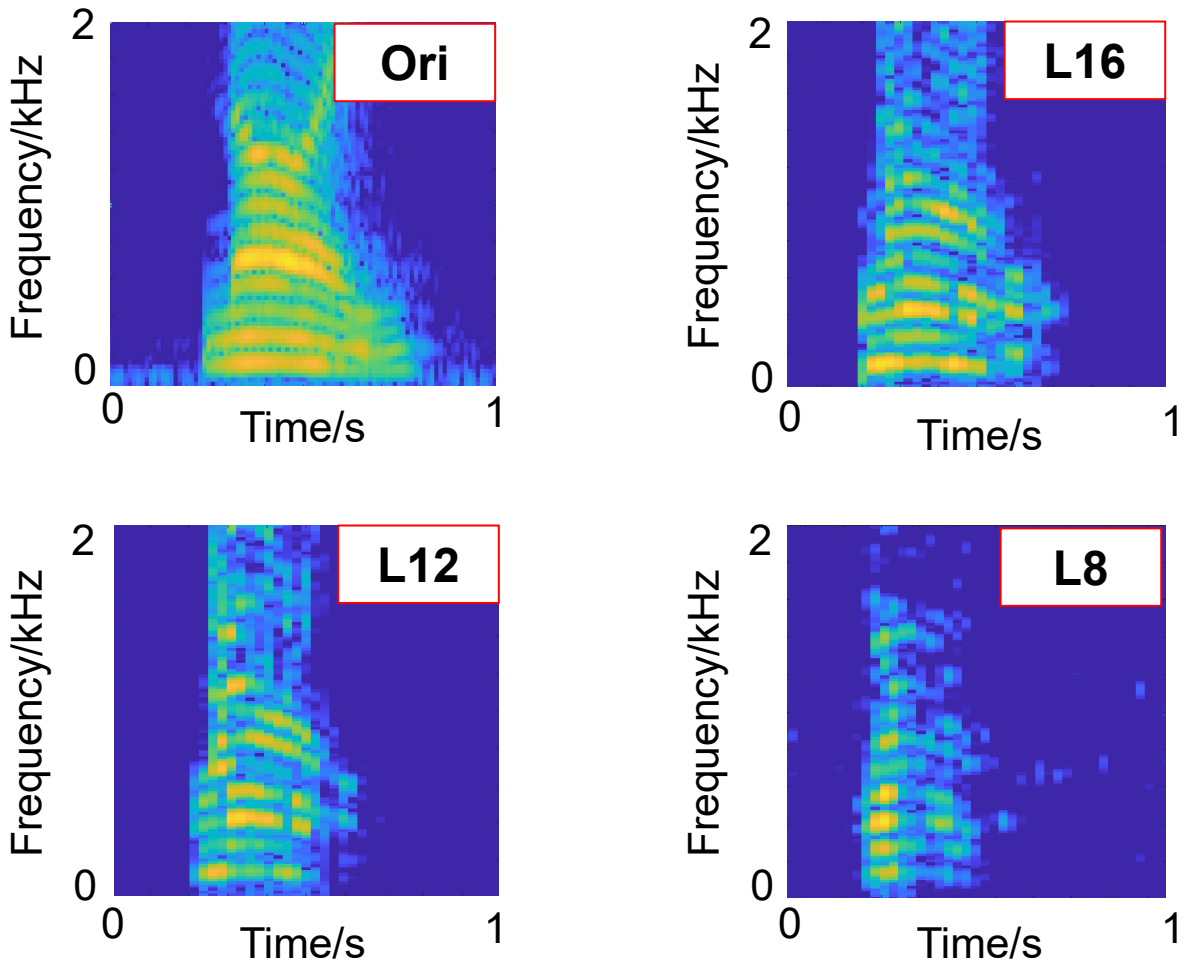
GhostTalk injection and eavesdropping attacks are robust in noisy environments.

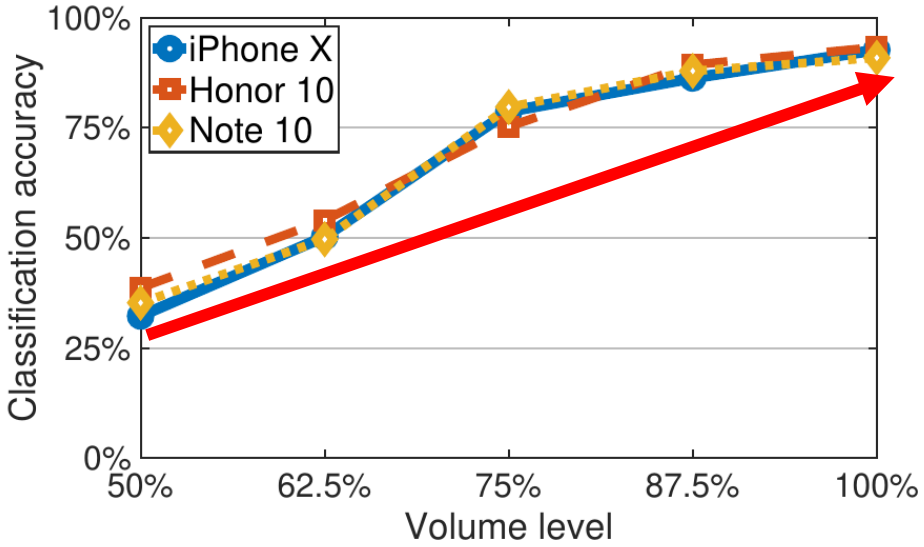
GhostTalk-SC Evaluation

Model	Charging port	Loudspeaker	SNR(dB)	Accuracy
iPhone 5s	Lightning	Single	5.41	93.0%
iPhone X	Lightning	Dual	4.75	92.7%
Honor 10	USB-C	Single	5.75	93.3%
MI 8 Lite	USB-C	Single	4.93	92.7%
Note 10	USB-C	Dual	4.46	91.0%
S9	USB-C	Dual	4.21	90.7%
Pixel 1	USB-C	Single	3.83	89.7%
Pixel 4XL	USB-C	Dual	3.72	90.0%
Pocophone	**USB-C**	**Dual**	**1.51**	**36.0%**

For most of smartphones, GhostTalk-SC can recognize the spoken digits with high accuracy.

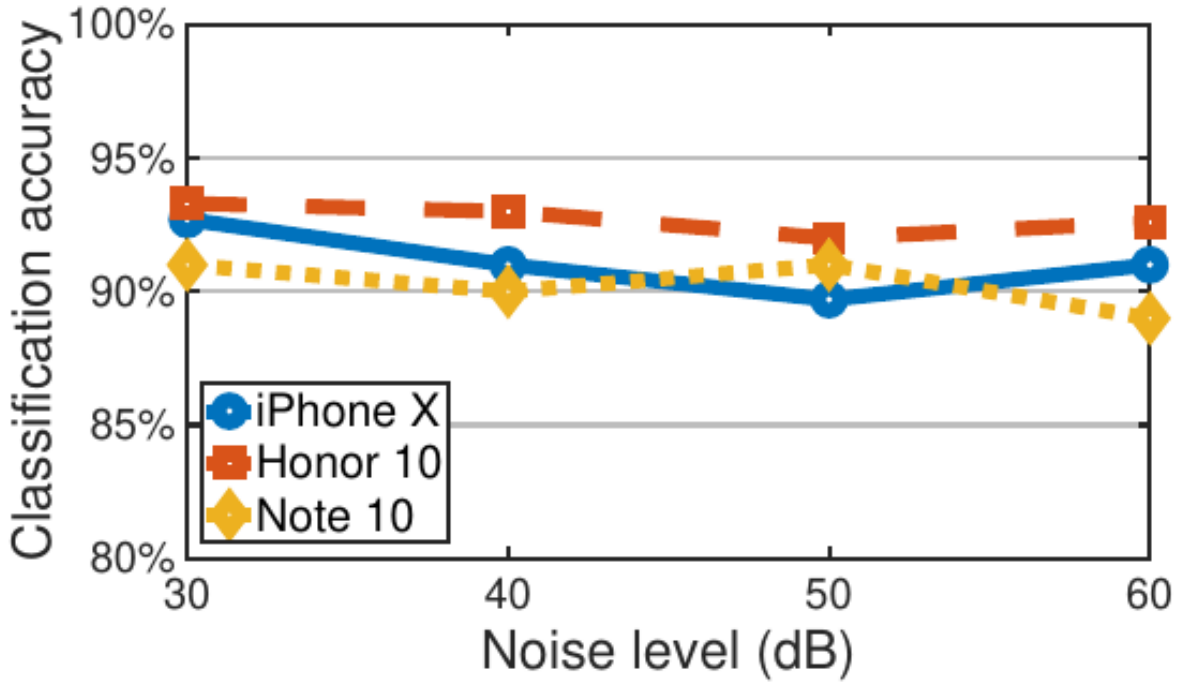
GhostTalk-SC Evaluation - Cont.





Loudspeaker volume and classification accuracy are positively correlated.

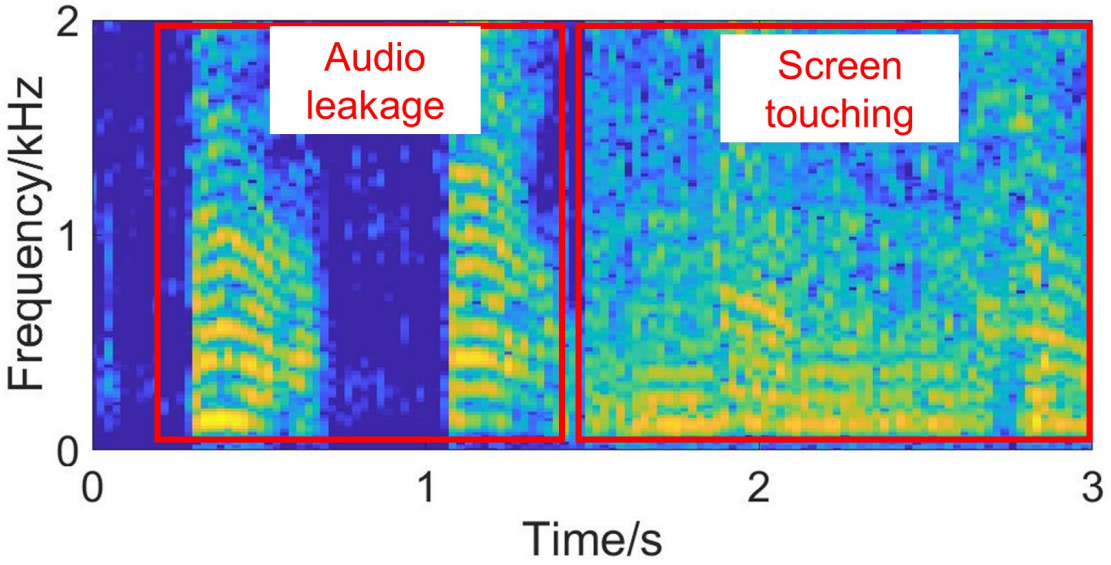
GhostTalk-SC Robustness



GhostTalk-SC attack also maintains high classification accuracy in noisy environments.

Countermeasure and Discussion

- Disable voice assistant activation by headphone.
- Enable headphone notification.
- Stop charging after reaching high battery level.



Conclusion

- GhostTalk is the first **interactive** and **inaudible** voice command attack towards smartphone voice assistants over the **charging cables**.
- We also propose GhostTalk-SC, an eavesdropping attack capturing audio signals from **power side-channel**.
- We test GhostTalk and GhostTalk-SC attacks on **9 different models** of smartphones. And the evaluation results show that both attacks achieve high attack success rate and **resilient to environmental noise**.

SCAN ME

Our website: http://ghosttalkattack.github.io/

We are recruiting graduate students!

SEIT

https://seit.egr.msu.edu/

SCAN ME

MICHIGAN STATE UNIVERSITY

Questions?

We are recruiting graduate students!

SEIT

https://seit.egr.msu.edu/

MICHIGAN STATE UNIVERSITY