



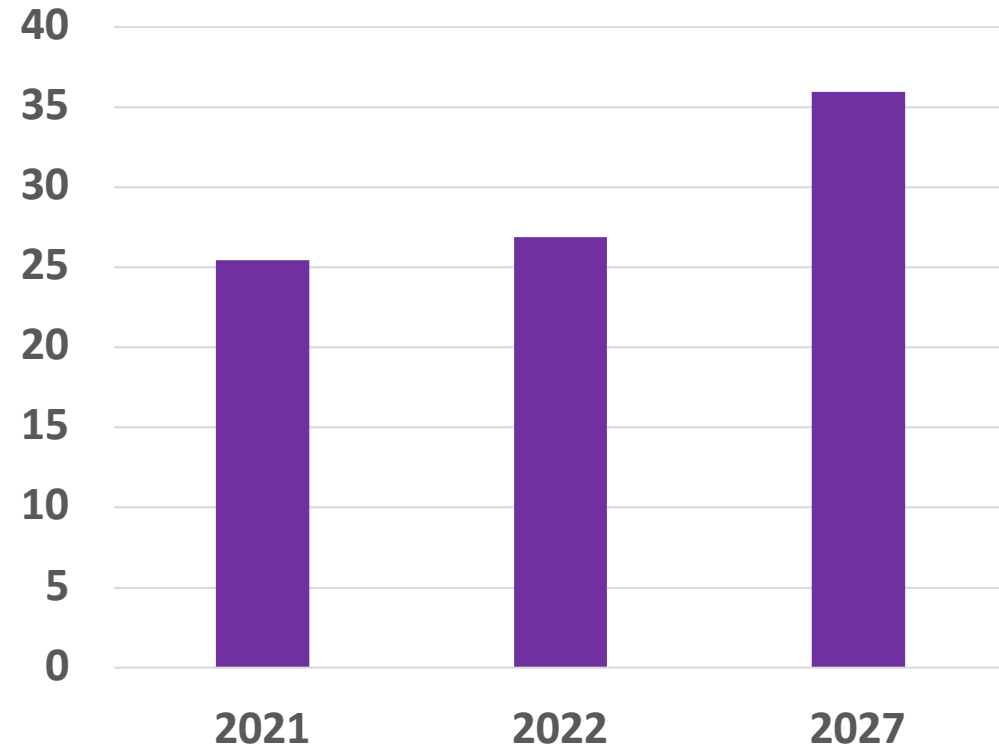
MobiCom 2023

# XPorter: A Study of the Multi-Port Charger Security on Privacy Leakage and Voice Injection

Tao Ni<sup>\*</sup>, Yongliang Chen<sup>\*</sup>, Weitao Xu<sup>\*</sup>, Lei Xue<sup>†</sup>, Qingchuan Zhao<sup>\*</sup> 

<sup>\*</sup>*City University of Hong Kong*   <sup>†</sup>*Sun Yat-Sen University*

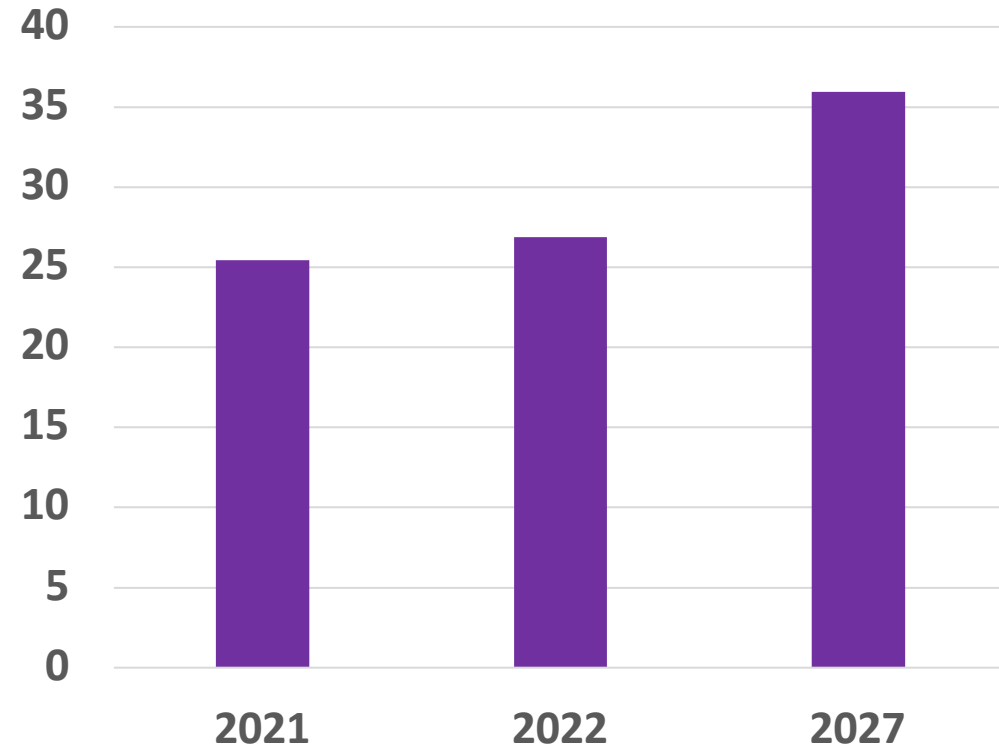
## Global USB Charger Market (Billion Dollars)



Source from: [BusinessWire](#)

# Introduction

Global USB Charger Market (Billion Dollars)



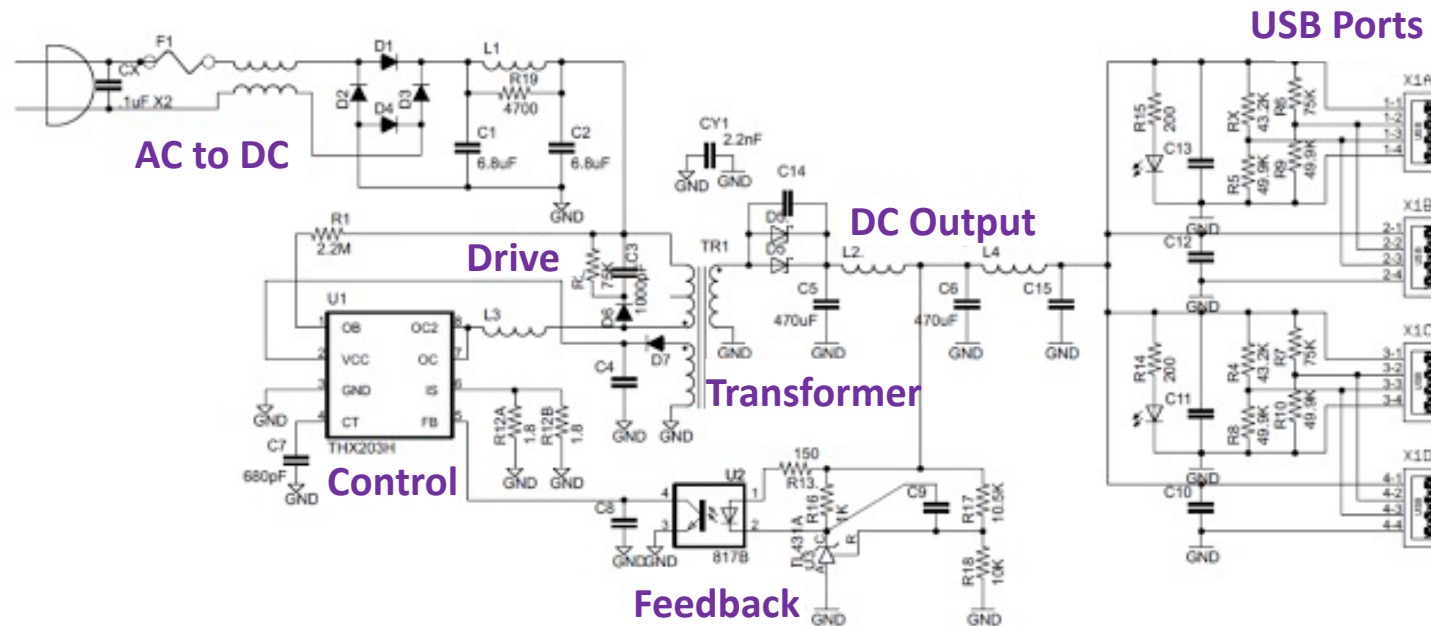
Source from: [BusinessWire](#)

Multi-Port Chargers



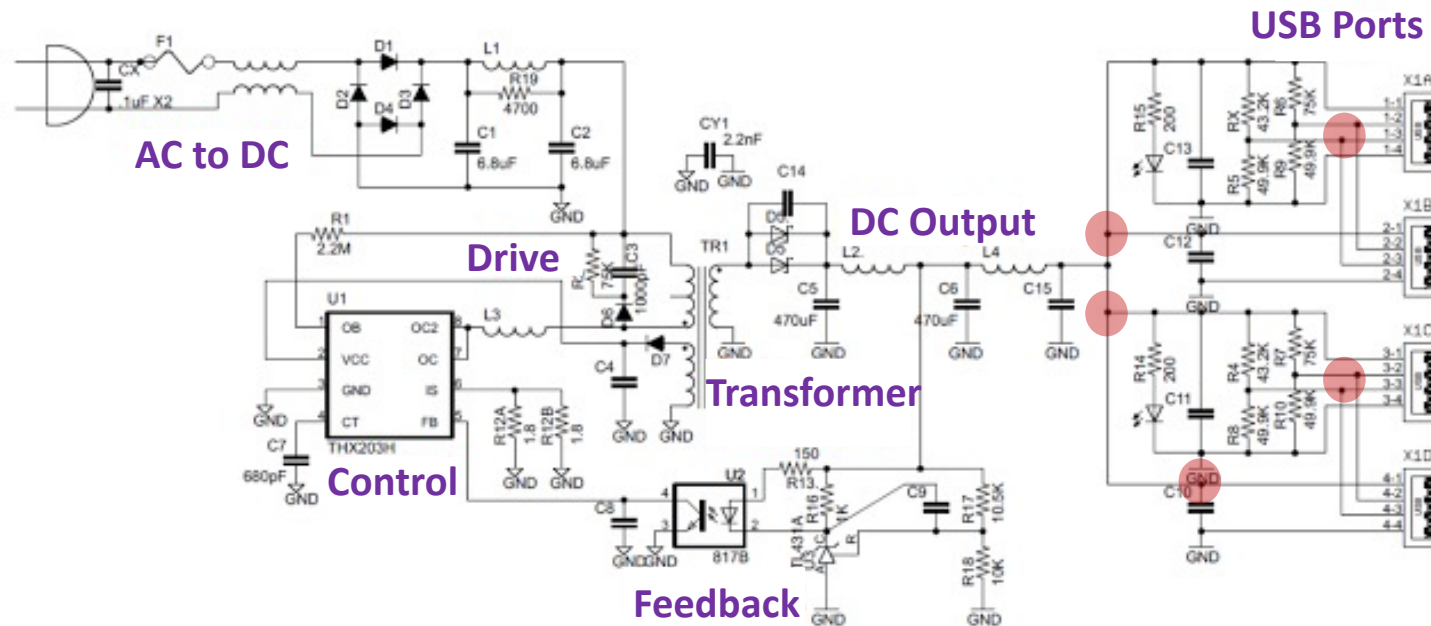
# Design Flaw in Multi-Port Chargers

## Circuit of a Four-Port Charger



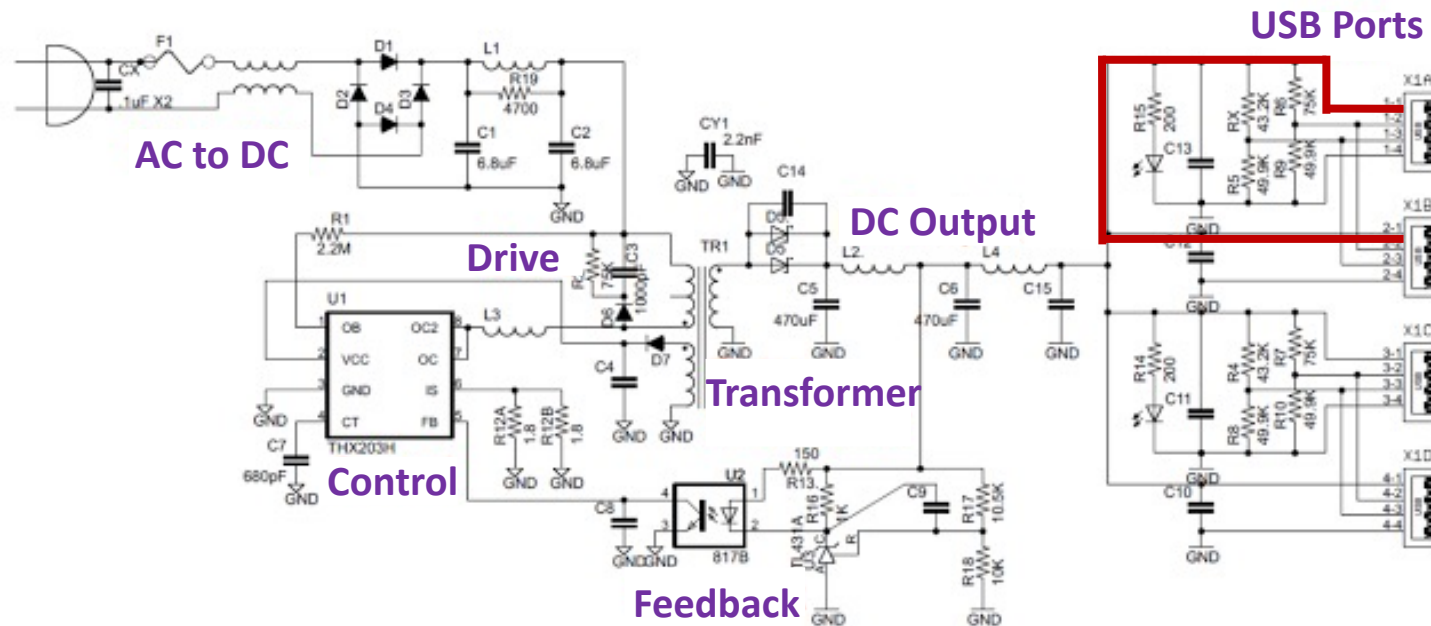
# Design Flaw in Multi-Port Chargers

## Circuit of a Four-Port Charger



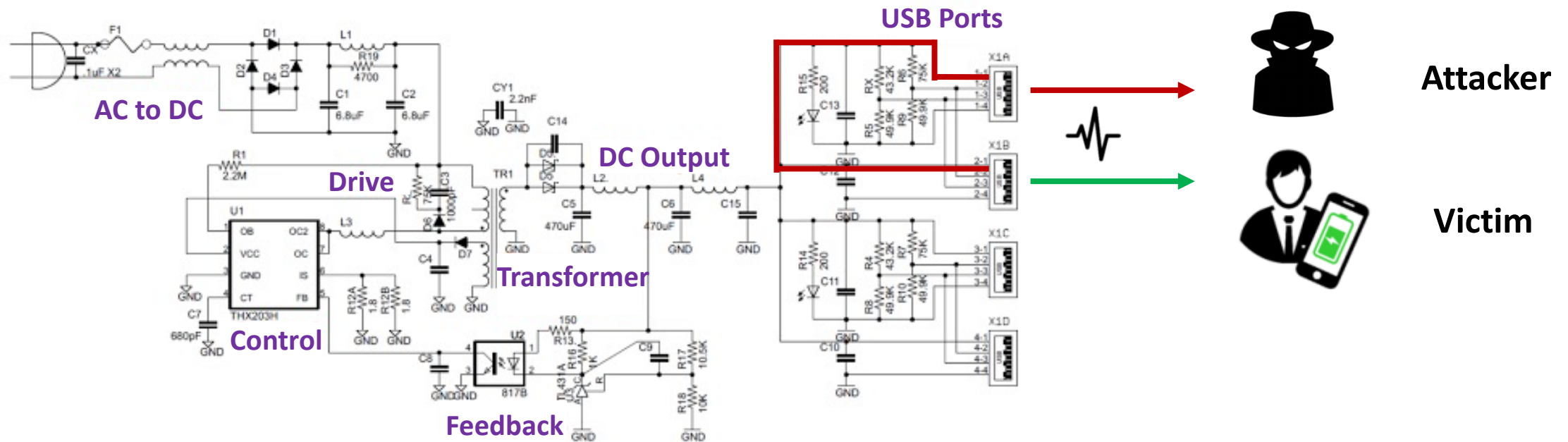
# Design Flaw in Multi-Port Chargers

## Circuit of a Four-Port Charger

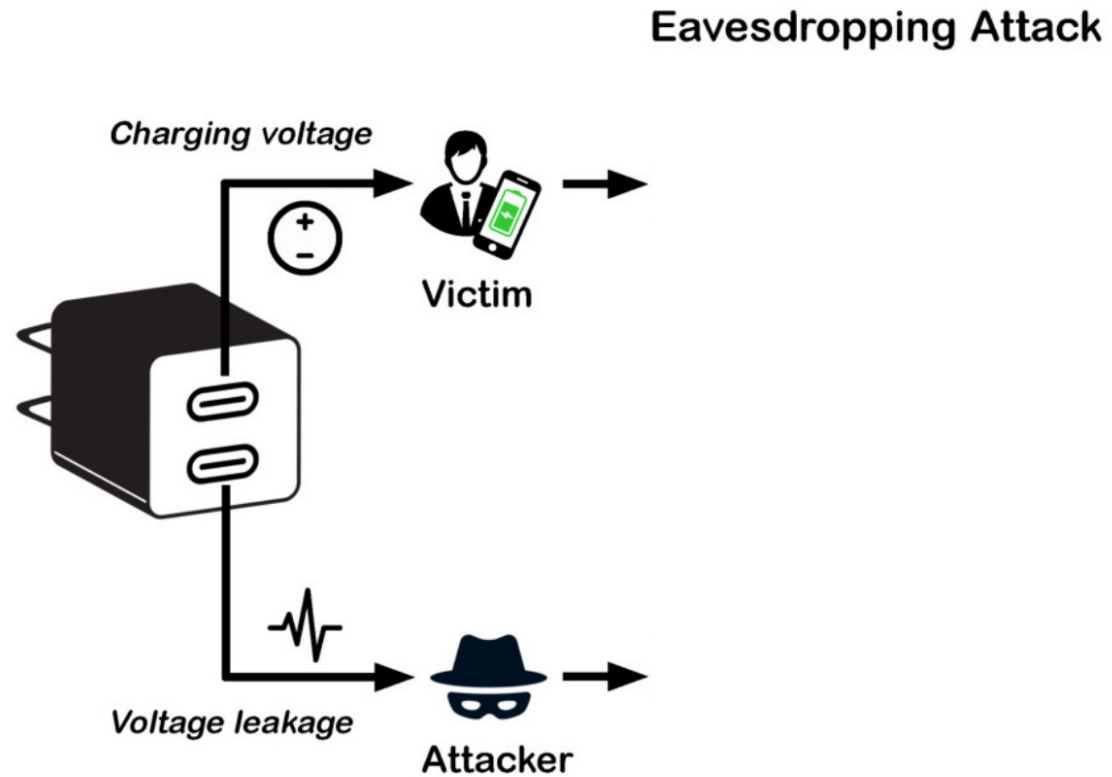


# Design Flaw in Multi-Port Chargers

## Circuit of a Four-Port Charger

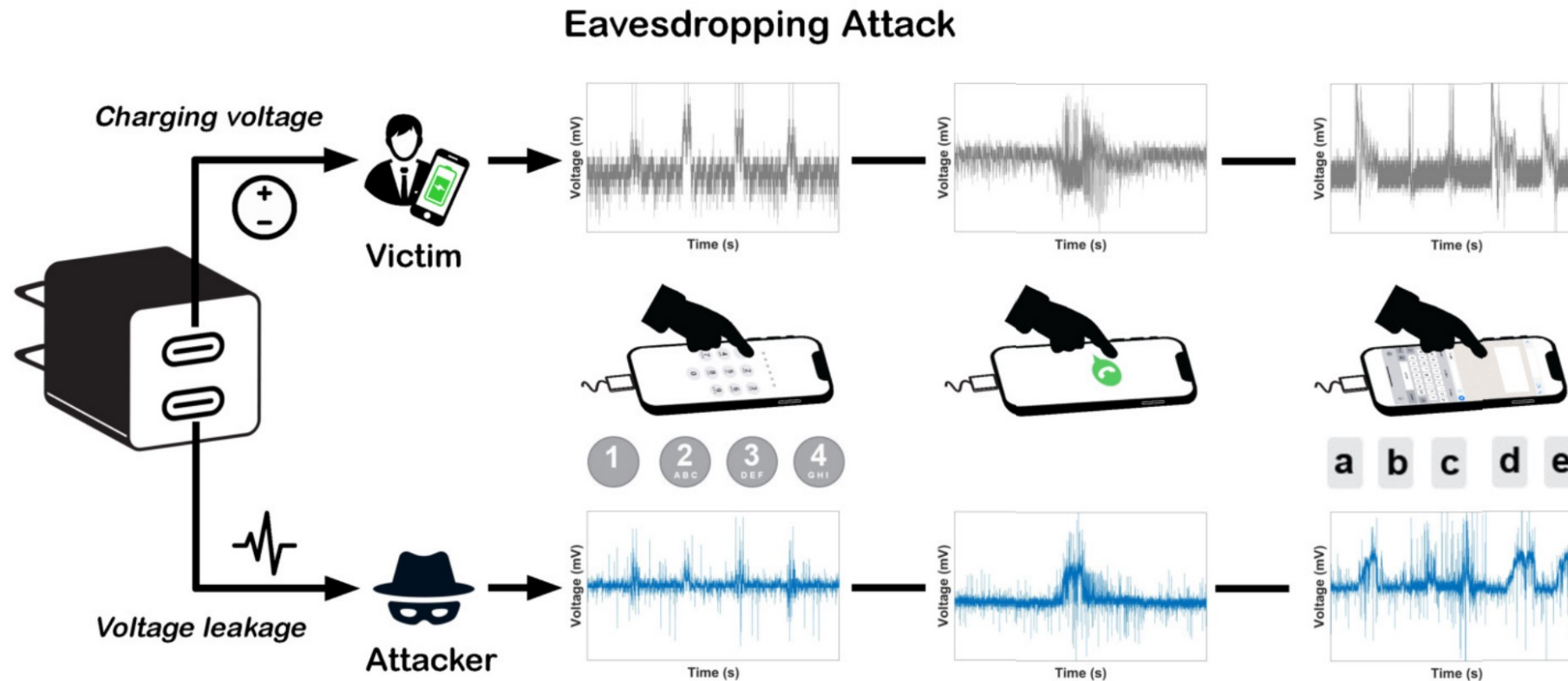


# Eavesdropping Attacks in Multi-Port Charger





# Eavesdropping Attacks in Multi-Port Charger



# Is USB-C Safe ?



LOKi

@Loki\_Naidu\_



Apple announcing USB C in iPhone 15

#AppleEvent 🍏 #iPhone15



11:34 PM · Sep 12, 2023 · 1,102 Views

# Is USB-C Safe ?



LOKi

@Loki\_Naidu\_

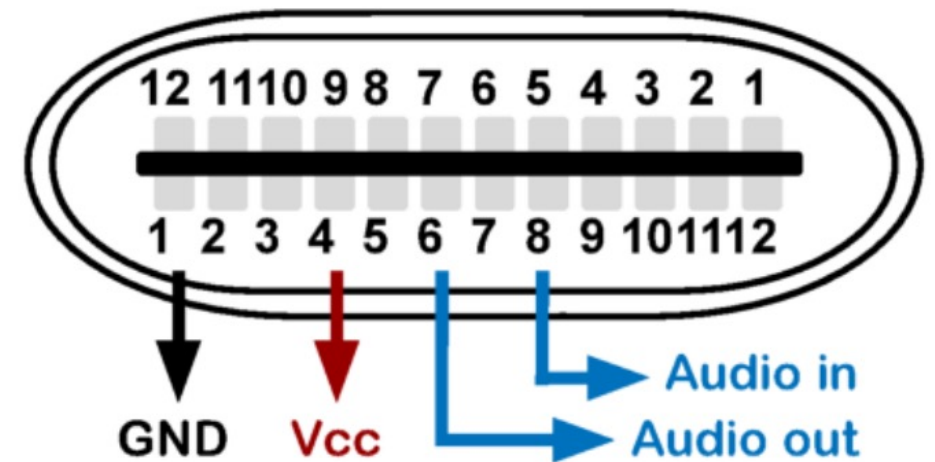
Apple announcing USB C in iPhone 15

#AppleEvent 🍏 #iPhone15



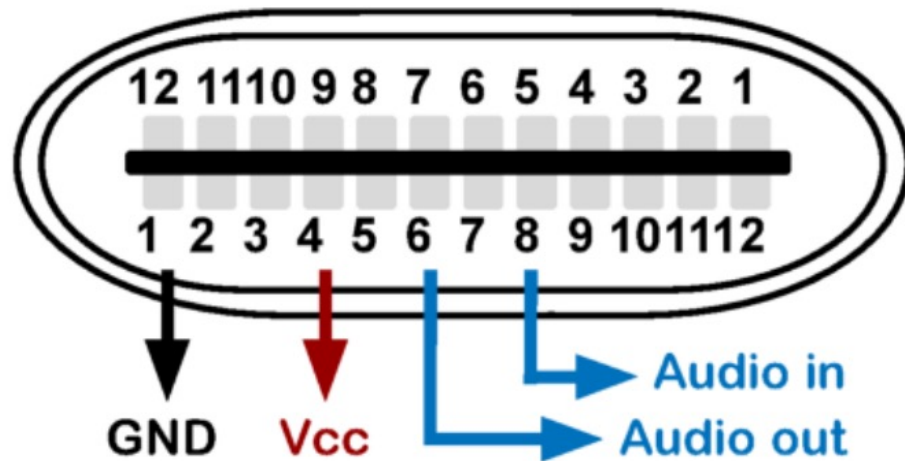
11:34 PM · Sep 12, 2023 · 1,102 Views

## USB-C Port Structure

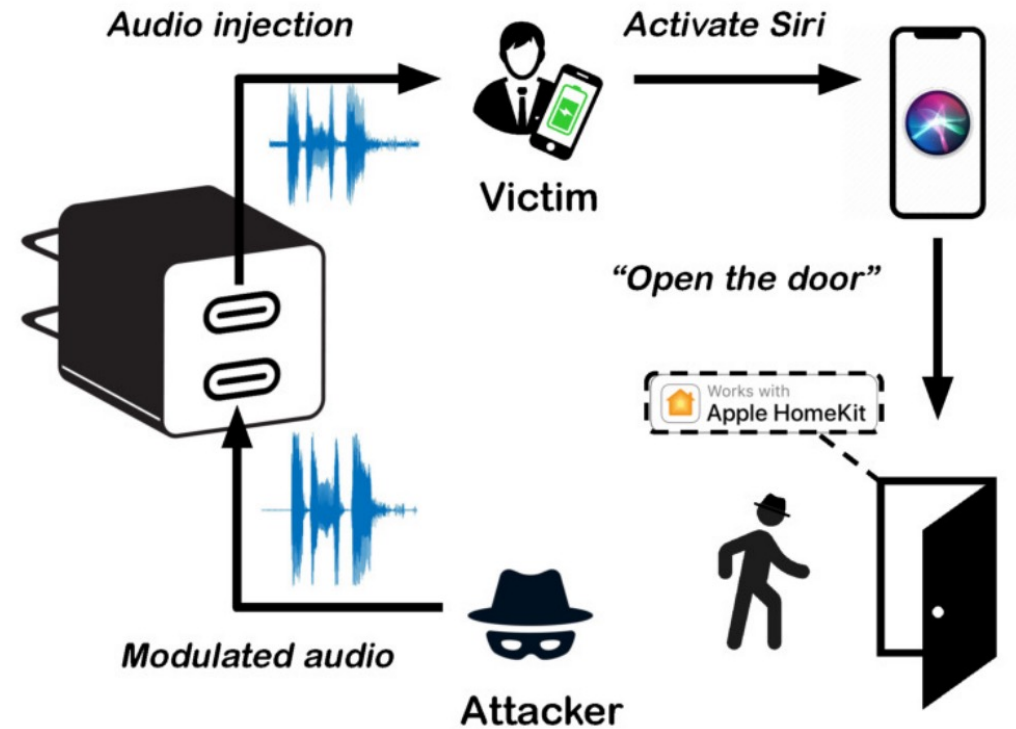


# Inaudible Audio Injection Attack vis USB-C

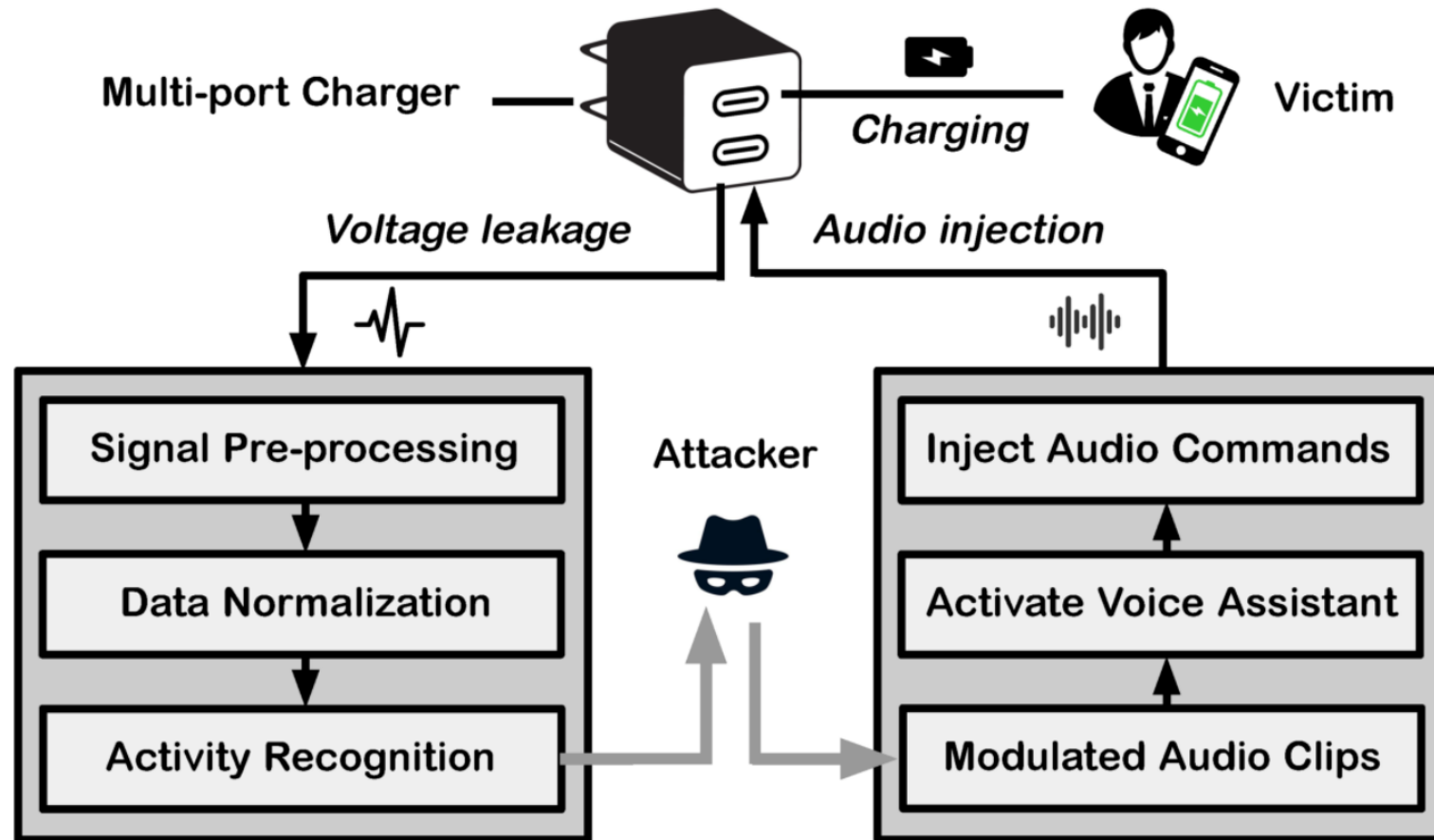
USB-C Port Structure



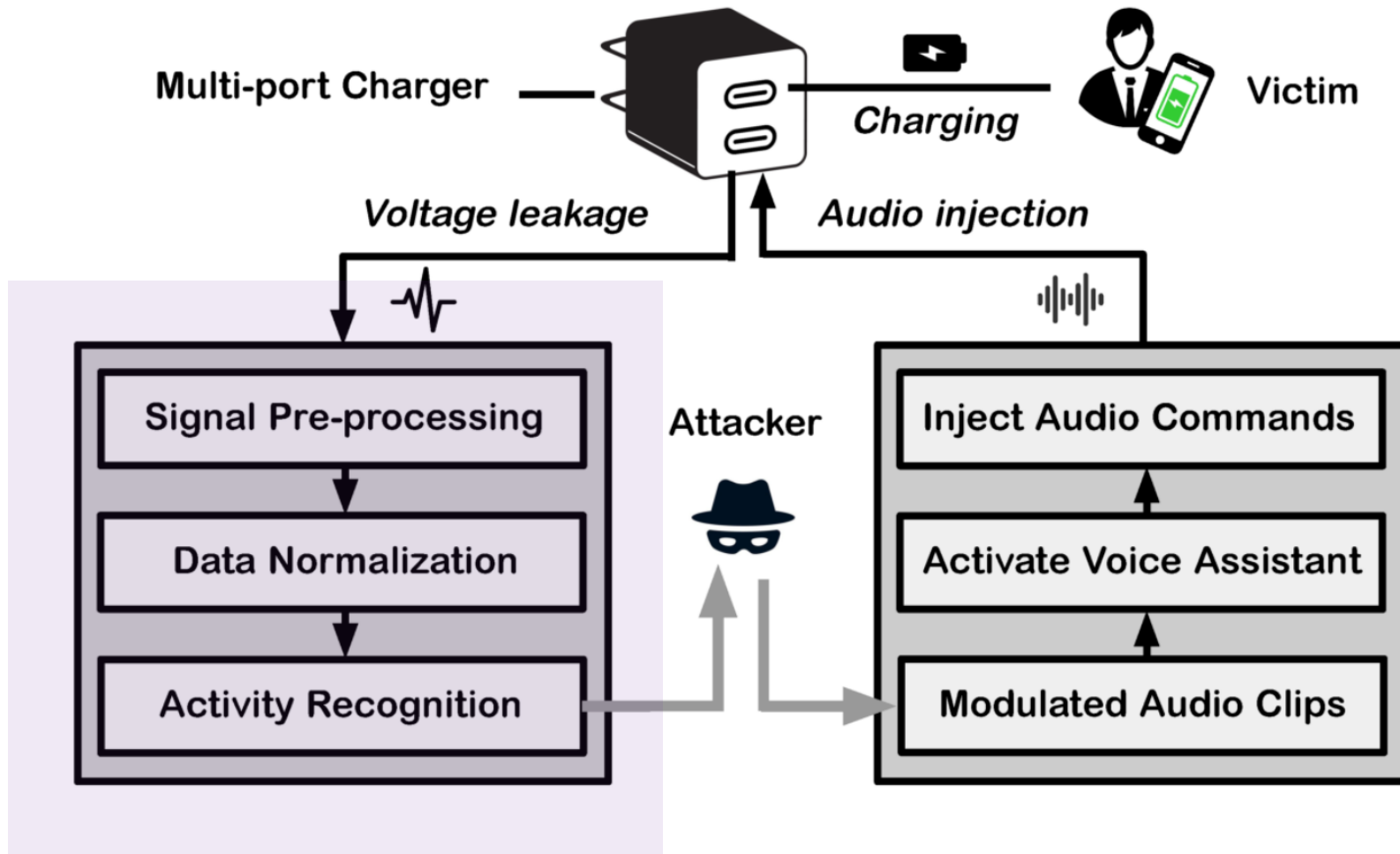
Inaudible Audio Injection Attack



# XPorter – Attacks across (X) Charging Ports of a Multi-Port Charger

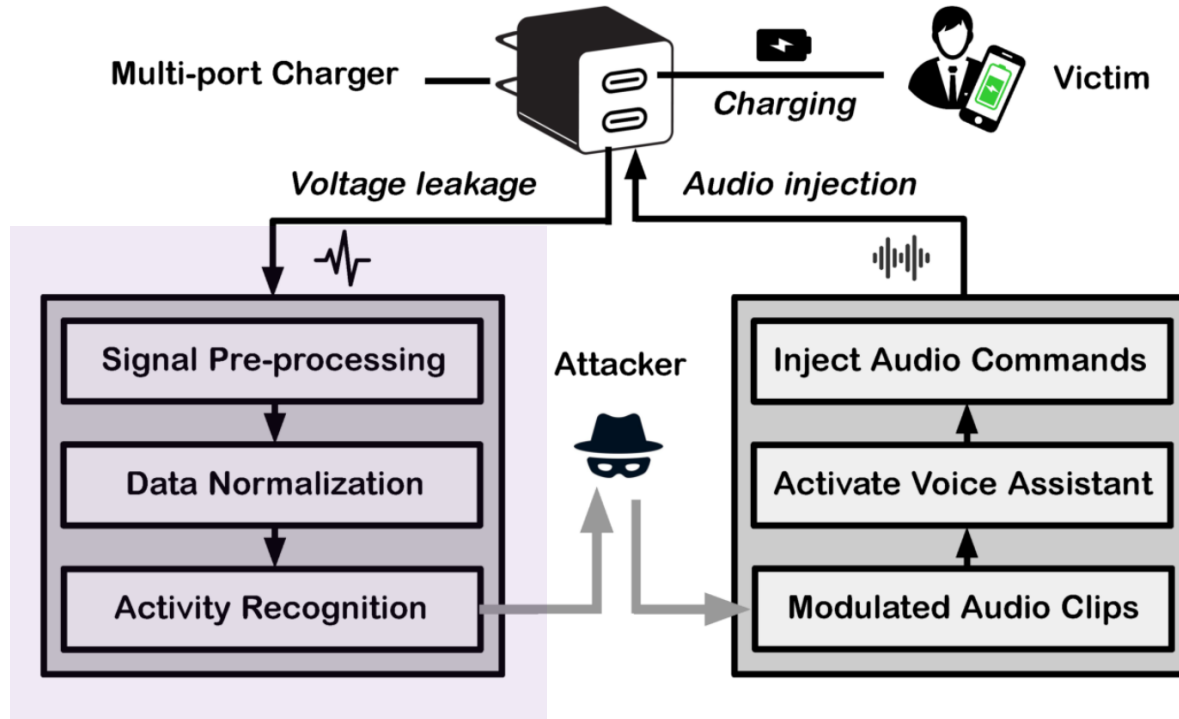


# XPorter – Eavesdropping Attacks





# Eavesdropping Attacks – Signal Processing



## Signal Processing Algorithm

**Algorithm 1:** Signal processing of eavesdropping attack

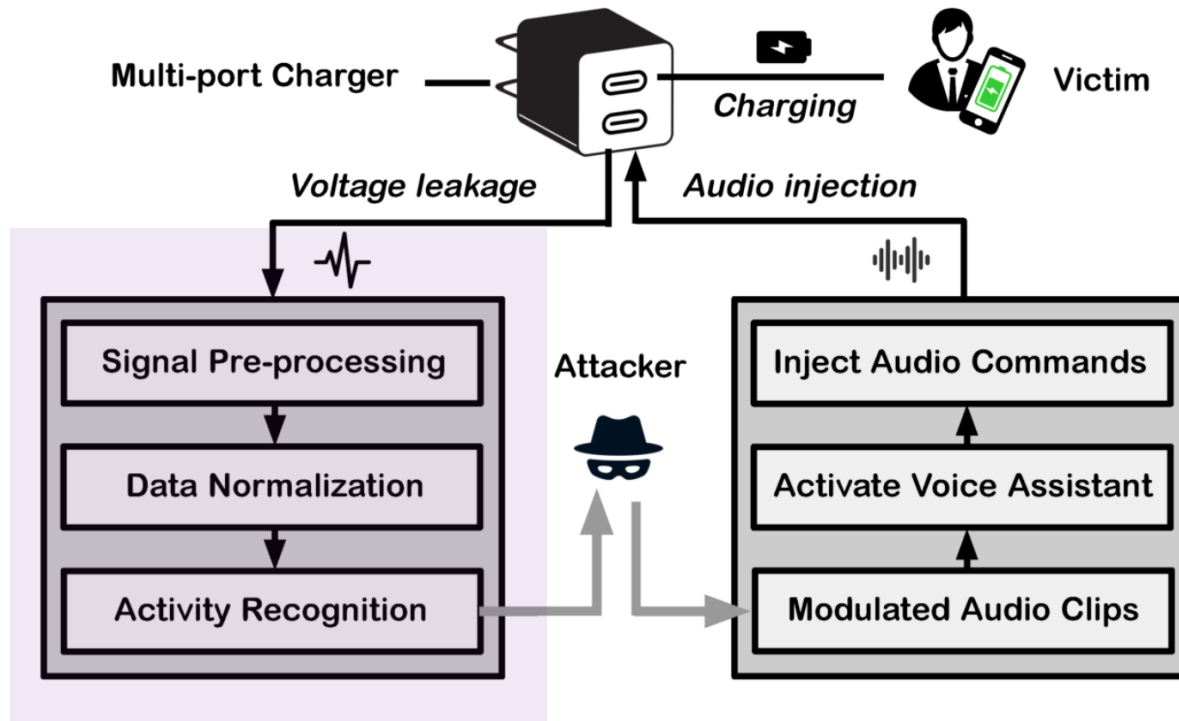
**Input:**  $\mathcal{V} = [v_{c_1}(t_1), v_{c_2}(t_2), \dots, v_{c_m}(t_m)]$ : obtained signals from the voltage leakage.  $o, f$ : order and frequency of the S-G filter.  $\tau$ : threshold of the variance.

**Output:**  $\mathcal{S} = [S_1, S_2, \dots, S_n]$ : filtered voltage signal clips containing specific smartphone activities.

```

1  $\tilde{\mathcal{V}} \leftarrow [], \mathcal{S} \leftarrow []$   $\triangleright$  initialize the empty array to record
   filtered signals and segmented voltage signal clips.
2  $filter \leftarrow sgolayfilt(o, f)$   $\triangleright$  initialize an S-G filter with the
   given order  $o$  and the frequency  $f$ .
3 for each signal  $v_{c_i}(t_i) \in \mathcal{V}$  do
4    $\tilde{v}_{c_i}(t_i) \leftarrow filter(v_{c_i}(t_i))$ 
5    $\tilde{\mathcal{V}} \leftarrow [\tilde{v}_{c_1}(t_1), \tilde{v}_{c_2}(t_2), \dots, \tilde{v}_{c_i}(t_i)]$ 
6  $\tilde{\mathcal{V}} \leftarrow [\tilde{v}_{c_1}(t_1), \tilde{v}_{c_2}(t_2), \dots, \tilde{v}_{c_m}(t_m)]$   $\triangleright$  the filtered signals.
7  $\tilde{\mathcal{V}} \leftarrow \tilde{\mathcal{V}} - average([\tilde{v}_{c_1}(t_1), \dots, \tilde{v}_{c_f}(t_f)])$   $\triangleright$  deduct offset.
8  $window \leftarrow movvar(\tau, f/10)$   $\triangleright$  initialize an moving-variance
   window with the given threshold  $\tau$  and size of  $f/10$ .
9 for each filtered signal  $\tilde{v}_{c_i}(t_i) \in \tilde{\mathcal{V}}$  do
10   $\mathcal{R}_{c_i}(t_i) \leftarrow window(\tilde{v}_{c_i}(t_i))$   $\triangleright$  obtain the time-variance
    signal from the moving-variance window.
11  for each  $r_i \in \mathcal{R}_{c_i}(t_i)$  do
12    if  $\forall r_j \in [r_i, r_{i+f/10}], r_j < r_{j+1}$  and  $r_j > \tau$  then
13       $k_{start} \leftarrow r_i$   $\triangleright$  obtain start index of the activity.
14    else if  $\forall r_j \in [r_i, r_{i+f/10}], r_j > r_{j+1}$  and  $r_j > \tau$ 
15      then
16         $k_{end} \leftarrow r_{i+f/10}$   $\triangleright$  obtain end index.
17     $S_i \leftarrow [\tilde{v}_{c_i}(k_{start}), \tilde{v}_{c_i}(k_{end})]$   $\triangleright$  voltage signal clip that
    contains the specific activity.
18   $\mathcal{S} \leftarrow [S_1, S_2, \dots, S_i]$ 
19  $\mathcal{S} = [S_1, S_2, \dots, S_n]$ 
20 Output voltage signal clips  $\mathcal{S}$  that contain user activities.
  
```

# Eavesdropping Attacks – Normalization and Activity Recognition



## DTW-based Data Normalization

$$DTW_q(S_i, S'_i) = \min_{\pi \in \mathcal{P}(S_i, S'_i)} \left( \sum_{(i,j) \in \pi} d(S_i, S'_j)^q \right)^{\frac{1}{q}},$$

$$R_{i,j} = DTW_q(S_{\rightarrow i}, S'_{\rightarrow j})^q,$$

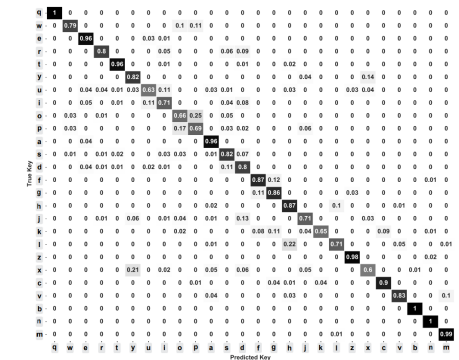
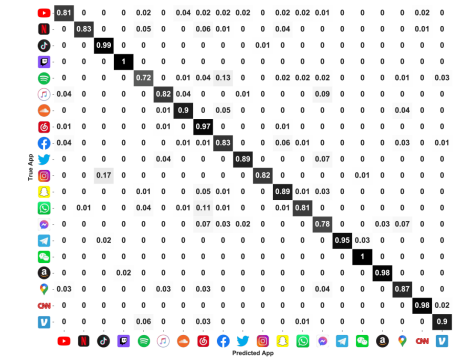
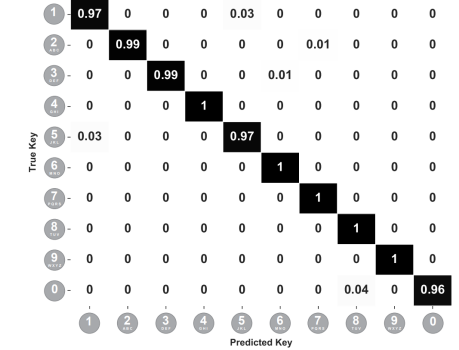
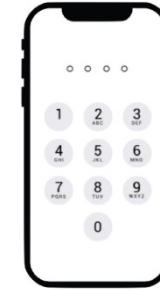
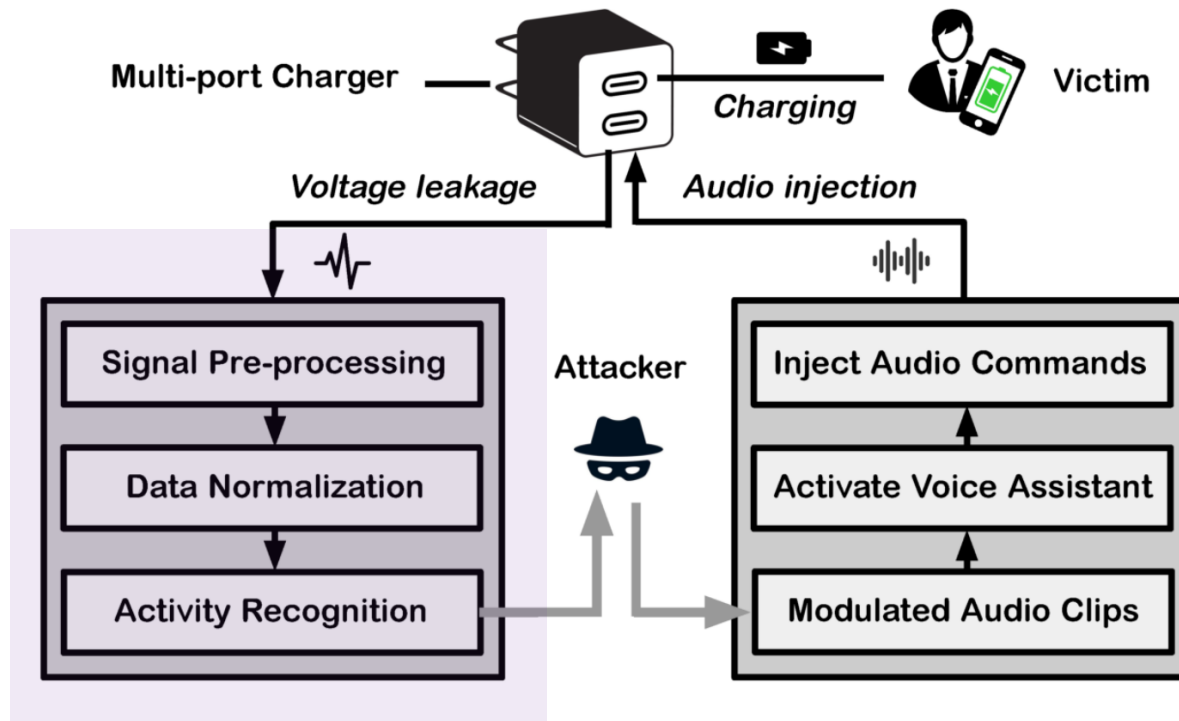
$$\begin{aligned} R_{i,j} &= \min_{\pi \in \mathcal{P}(S_{\rightarrow i}, S'_{\rightarrow j})} \sum_{(k,l) \in \pi} d(S_k, S'_l)^q \\ &= d(S_i, S'_j)^q + \min_{\pi \in \mathcal{P}(S_{\rightarrow i}, S'_{\rightarrow j})} \sum_{(k,l) \in \pi[: -1]} d(S_k, S'_l)^q \\ &= d(S_i, S'_j)^q + \min(R_{i-1,j}, R_{i,j-1}, R_{i-1,j-1}), \end{aligned}$$

## CNN-LSTM Classification

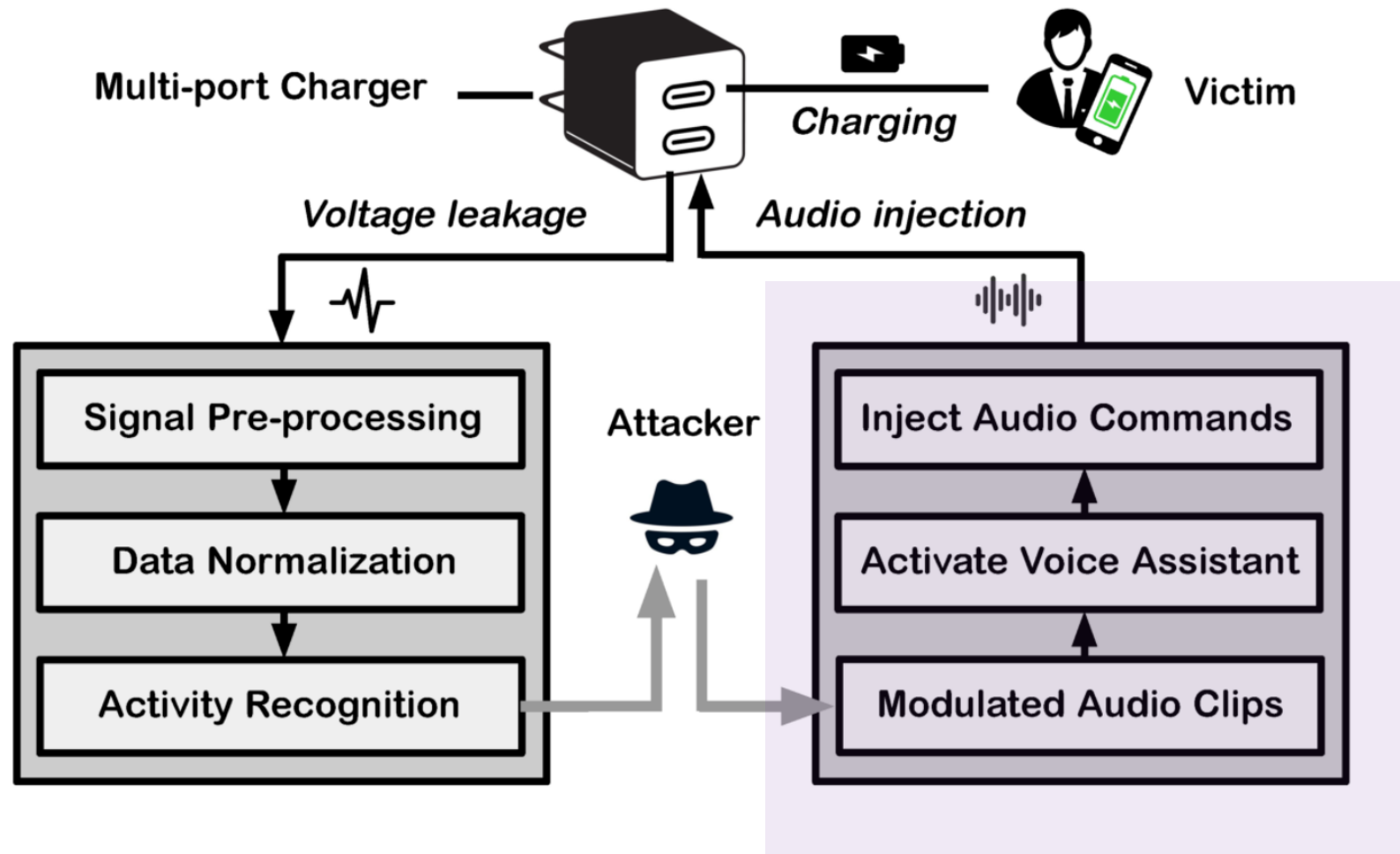




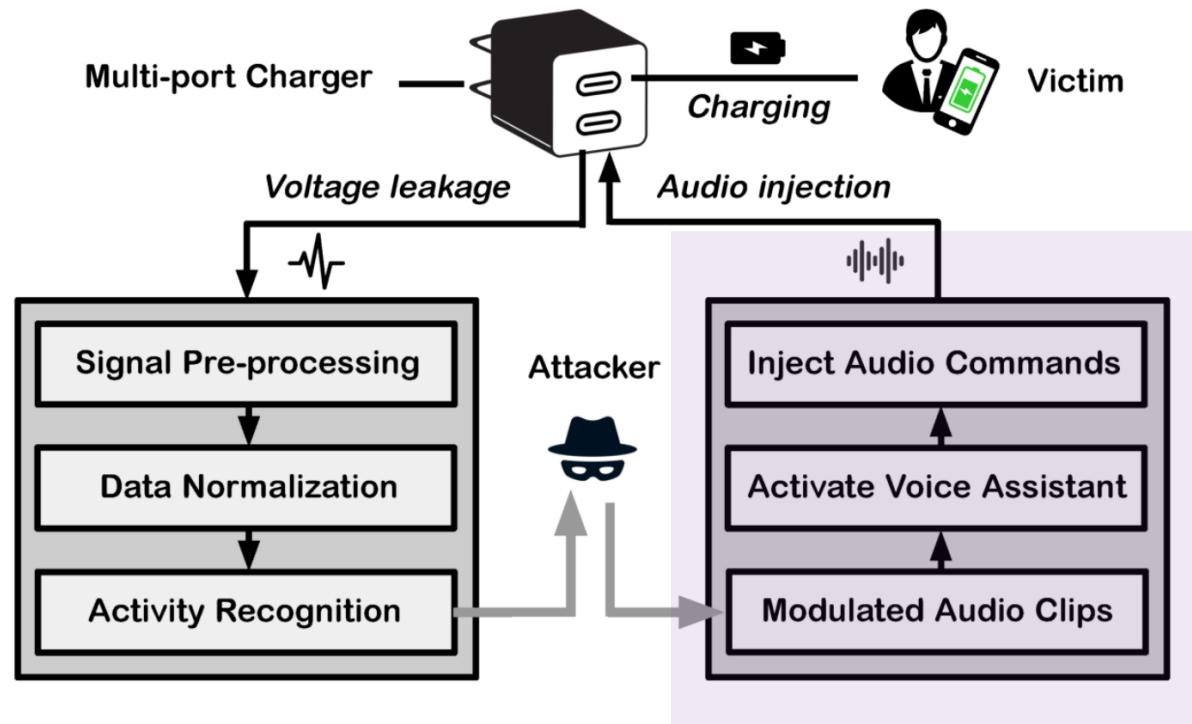
## Eavesdropping Attacks – Results



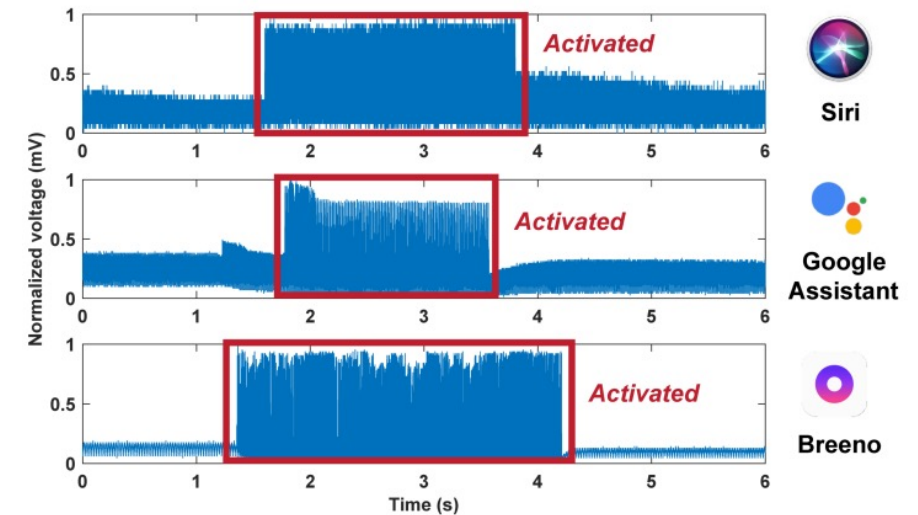
# XPorter – Inaudible Audio Injection Attacks



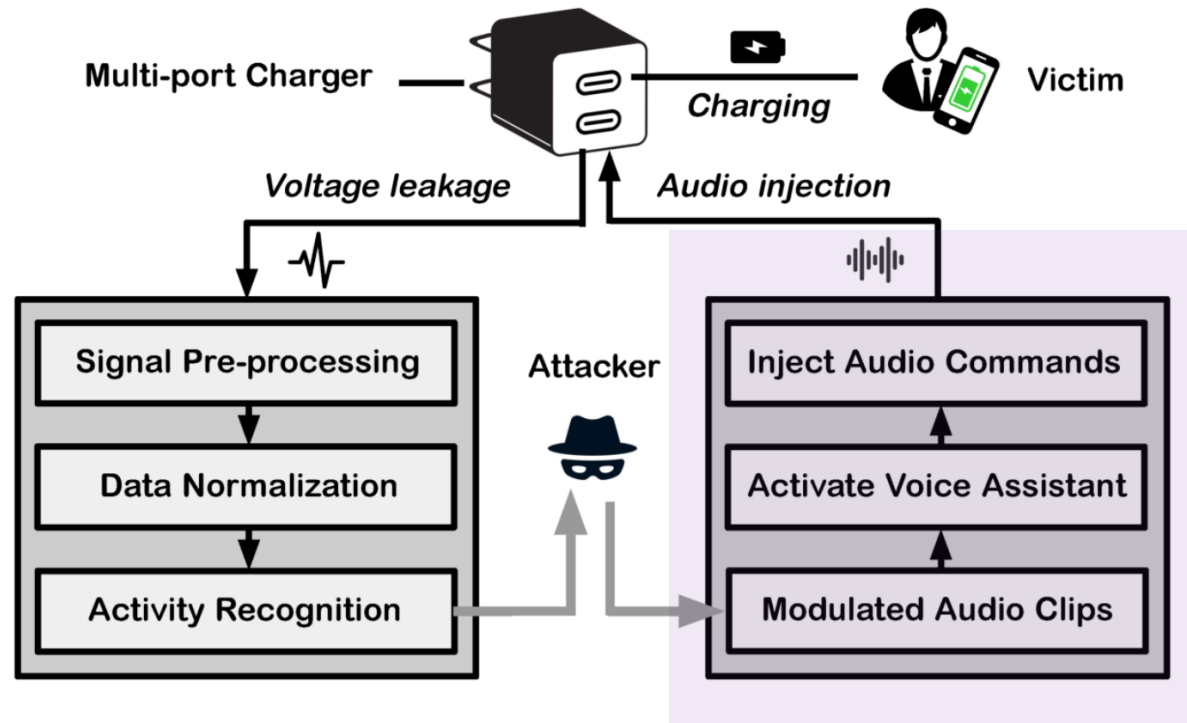
# Audio Injection Attacks – How to trigger the Voice Assistant?



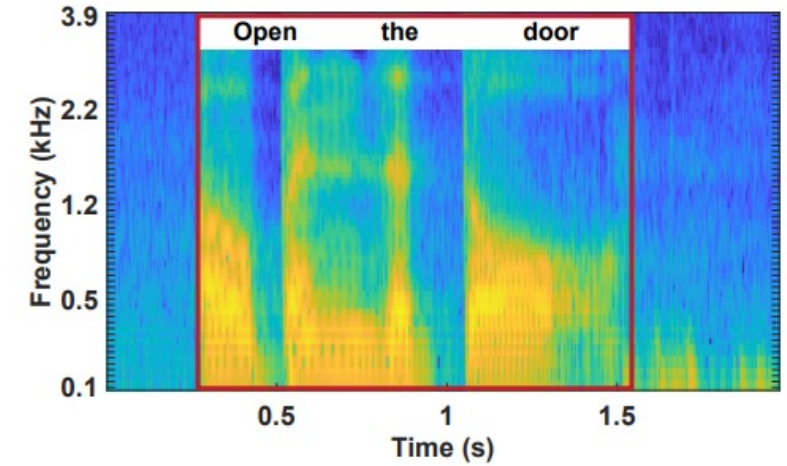
Voltage from the Audio Pin



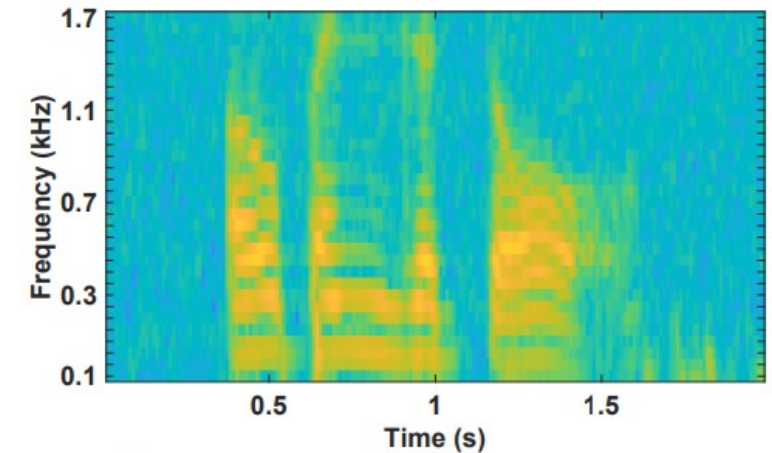
# Audio Injection Attacks – Inject Audio via USB-C



Modulated Audio Clip

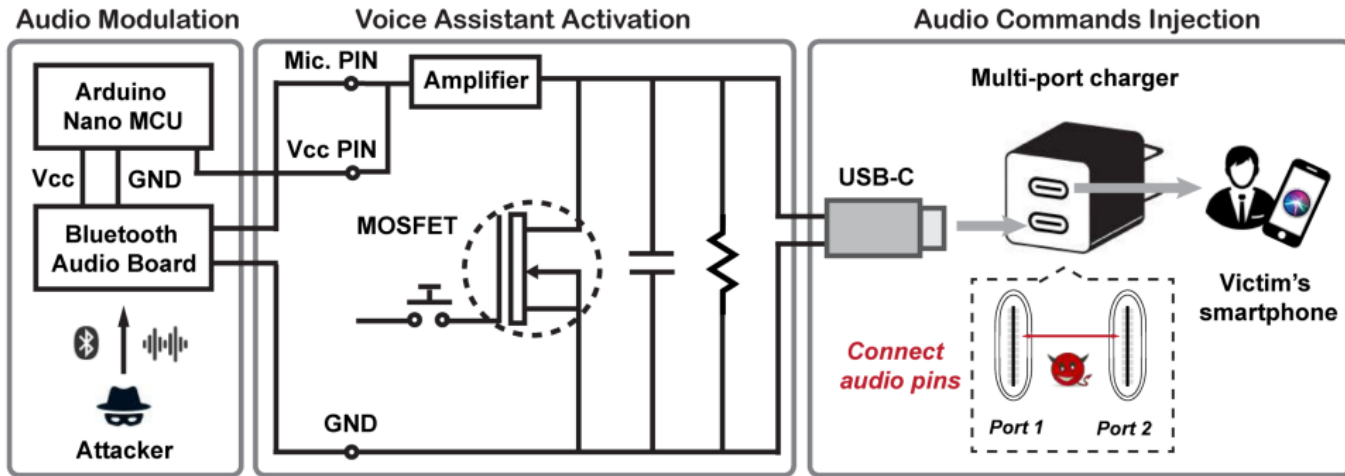


Injected Signal of USB-C



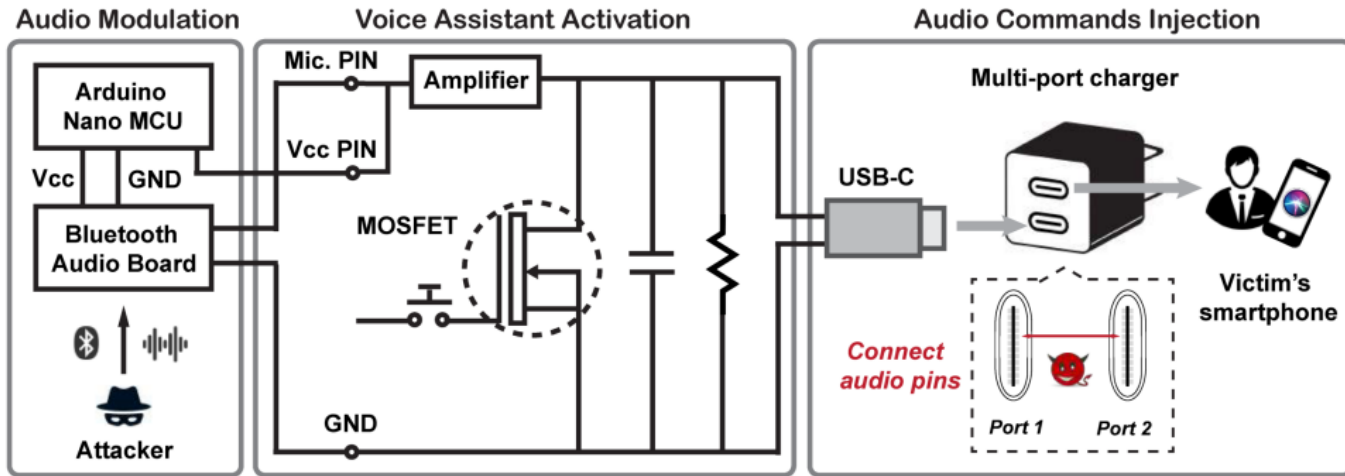
# Audio Injection Attacks – Portable Attacking Device

## Circuit Design

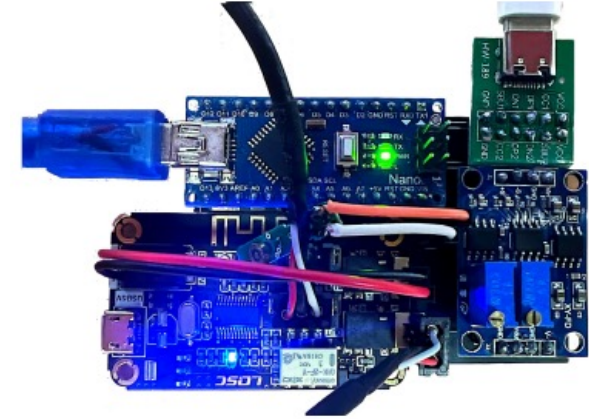


# Audio Injection Attacks – Portable Attacking Device

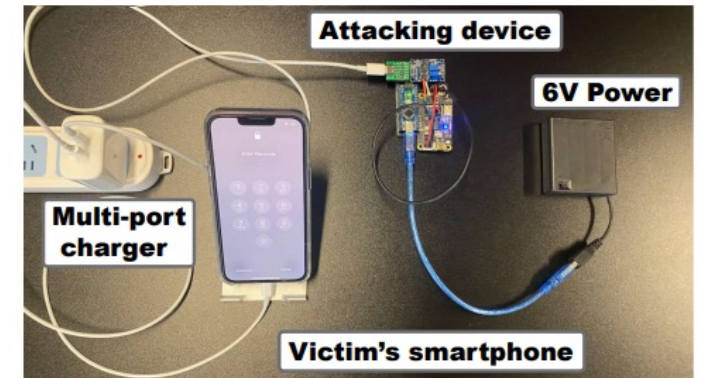
## Circuit Design



## Prototype

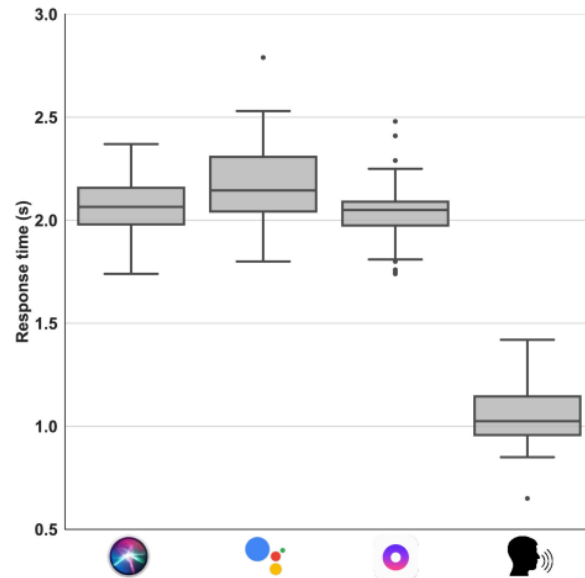


## Attack Scenario









# Audio Injection Attacks – Results

## Response time

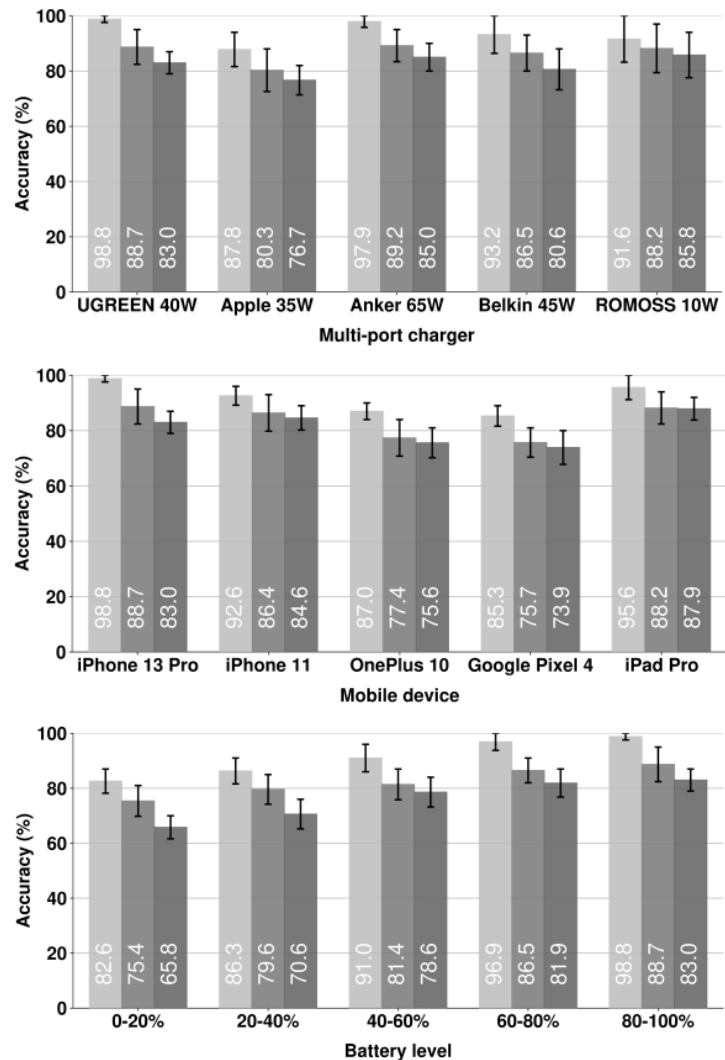


## Inaudible Audio Injection Attack Results













#	Voice Command	SNR (dB)				#	Voice Command	SNR (dB)					
			Act.	Inj.	Act.				Inj.	Act.	Inj.	Act.	Inj.
1	Call mom.	20.7	✓	✓	✓	✓	11	Where is my home?	19.0	✓	✓	✓	✓
2	Call my wife.	21.2	✓	✓	✓	✓	12	What's my ETA?	20.7	✓	✓	✓	✓
3	Call Bob.	20.3	✓	✓	✓	✓	13	Open the garage door.	21.5	✓	✓	✓	✓
4	Open Gmail.	19.8	✓	✓	✓	✓	14	Turn on the lights.	19.8	✓	✓	✓	✓
5	Open WhatsApp.	20.3	✓	✓	✓	✓	15	Turn off all alarms.	20.7	✓	✓	✓	✓
6	Open Paypal.	22.3	✓	✓	✓	✓	16	Send a message to...	19.2	✓	✓	✓	✓
7	Check my voicemail.	19.8	✓	✓	✓	✓	17	Send a reply email to...	18.8	✓	✓	✓	✓
8	Check my emails.	20.7	✓	✓	✓	✓	18	Tell Bob where I am.	20.3	✓	✓	✓	✓
9	Check my wallet.	18.5	✓	✓	✓	✓	19	Did I lock the front door?	21.3	✓	✓	✓	✓
10	What's my name?	21.2	✓	✓	✓	✓	20	What's my next schedule?	19.5	✓	✓	✓	✓



## Eavesdropping Attacks



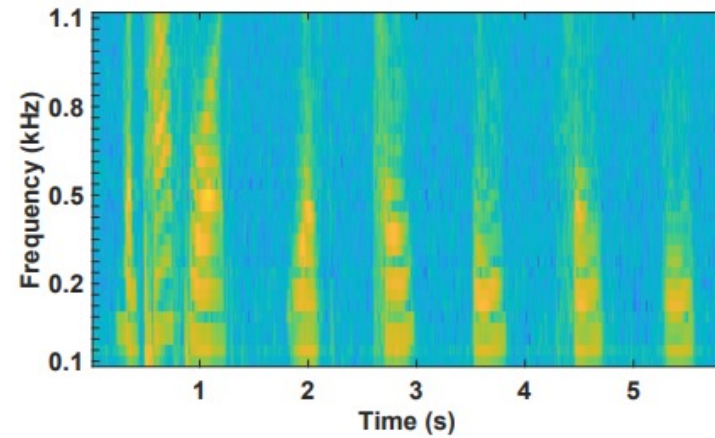
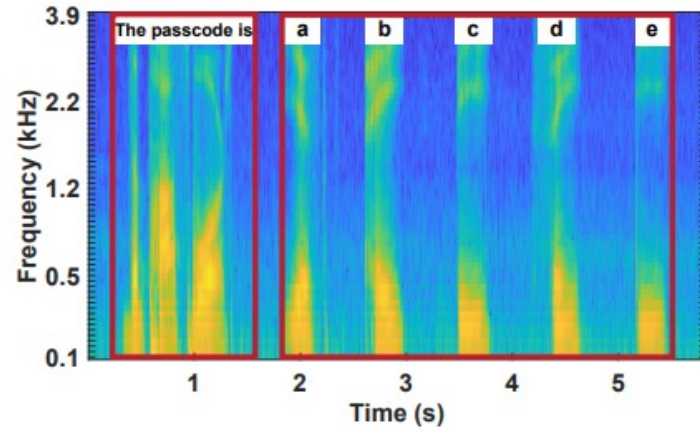
## Inaudible Audio Injection Attacks

Multi-port Charger	# of Ports	Type of Ports	Mobile Device	Voice Assistant	Battery Level	Act. SR.	Inj. SR.
UGREEN 40 W	2	2× USB-C	iPhone 13 Pro		80-100%	100%	100%
Anker 65W	3	1× USB-A 2× USB-C	iPhone 13 Pro		40-60%	100%	100%
Belkin 65W	2	2× USB-C	iPhone 13 Pro		60-80%	100%	100%
UGREEN 40 W	2	2× USB-C	Google Pixel 4		20-40%	100%	100%
Anker 65W	3	1× USB-A 2× USB-C	Google Pixel 4		60-80%	100%	100%
Belkin 65W	2	2× USB-C	Google Pixel 4		0-20%	100%	100%
UGREEN 40 W	2	2× USB-C	OnePlus 10 Pro		80-100%	100%	100%
Anker 65W	3	1× USB-A 2× USB-C	OnePlus 10 Pro		60-80%	100%	100%
Belkin 65W	2	2× USB-C	OnePlus 10 Pro		0-20%	100%	100%
UGREEN 40 W	2	2× USB-C	iPad Pro		60-80%	100%	100%
Anker 65W	3	1× USB-A 2× USB-C	iPad Pro		80-100%	100%	100%
Belkin 65W	2	2× USB-C	iPad Pro		20-40%	100%	100%



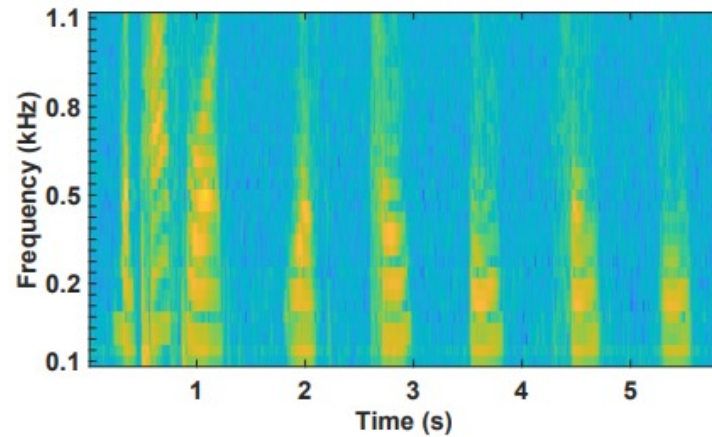
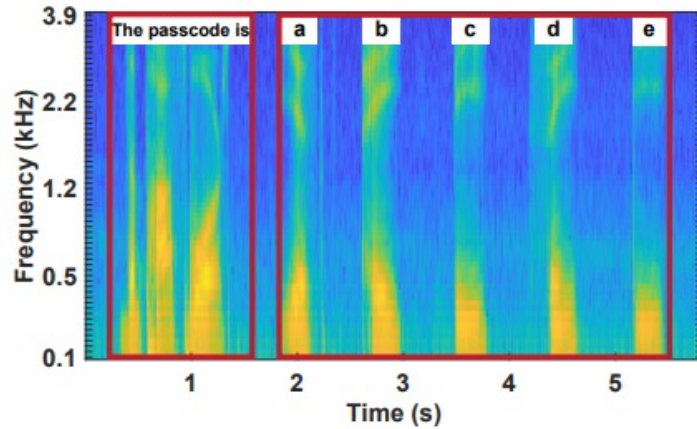
# Extending Attacks

## Audio Eavesdropping

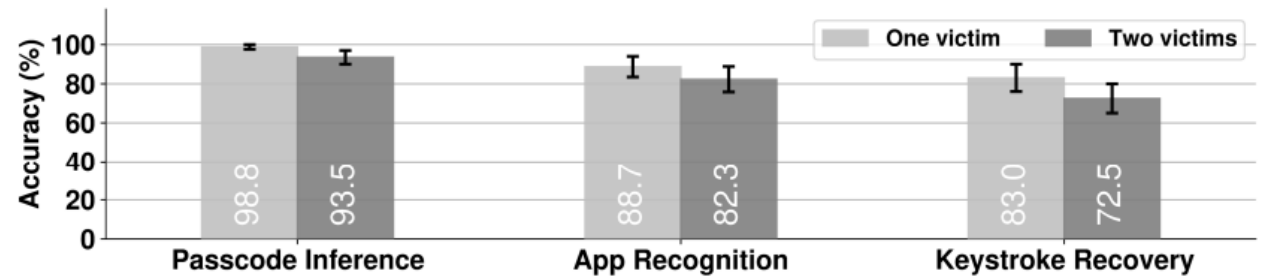
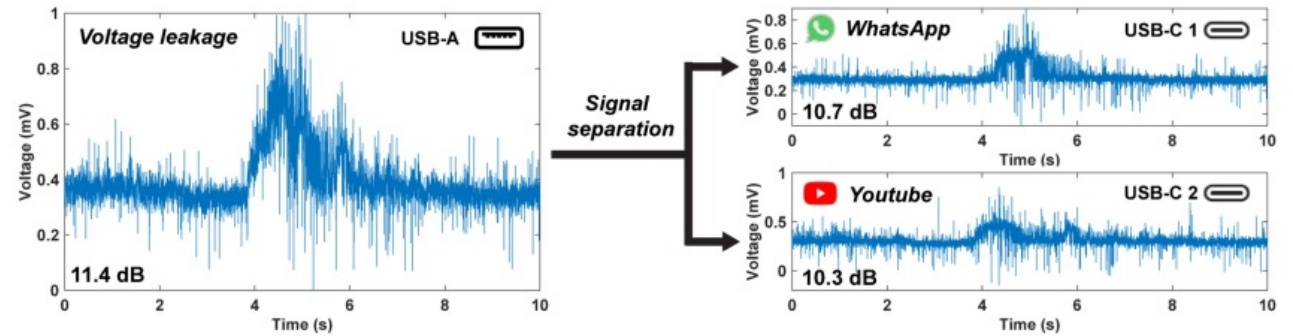


# Extending Attacks

## Audio Eavesdropping

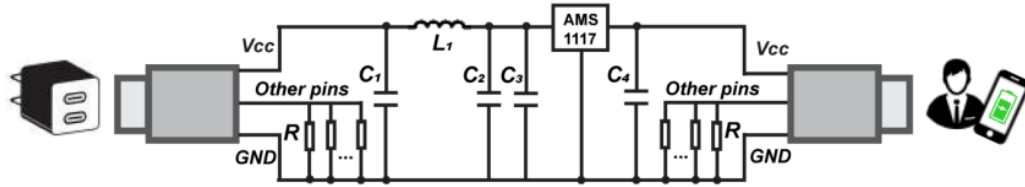


## Attack Multiple Victims

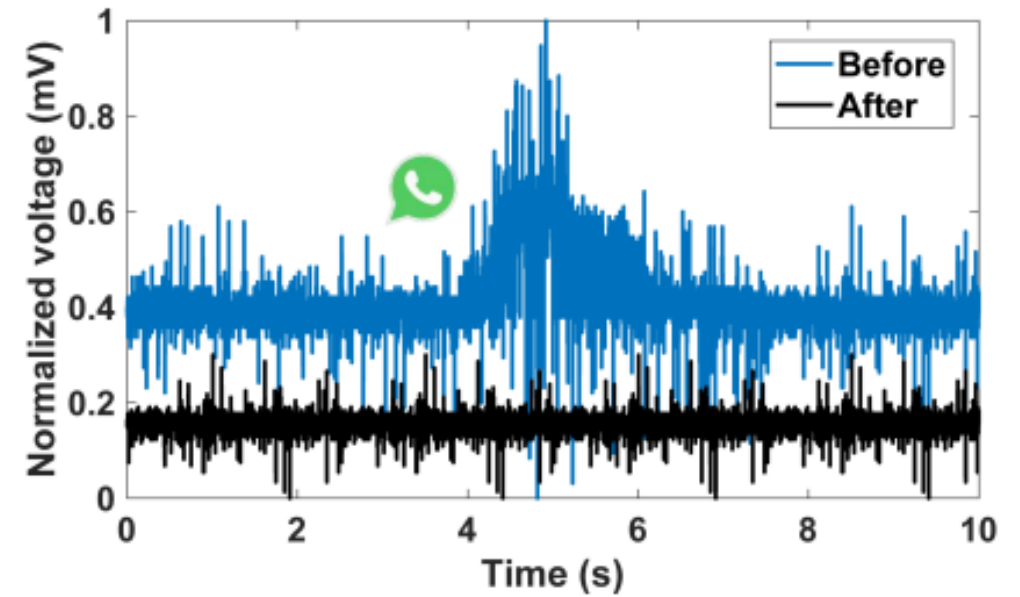


# Countermeasures

## Circuit to smooth out voltage leakages



## Prototype



## **XPorter: A Study of the Multi-Port Charger Security on Privacy Leakage and Voice Injection**

*Demo*



[View in YouTube](#)

- **A novel attack.** We introduce a new attack vector that can be exploited to attack mobile devices charged by a commodity multi-port charger.
- **A new framework.** We propose and implement a new attack framework, XPorter, to demonstrate the feasibility of the proposed attacks.
- **Comprehensive evaluation.** We comprehensively evaluate the effectiveness of XPorter with five commodity multi-port chargers and five mobile devices.

# Thank you!

Speaker: Tao Ni (Tony)

Personal website: [tony520.github.io](https://tony520.github.io)

Email: [taoni2-c@my.cityu.edu.hk](mailto:taoni2-c@my.cityu.edu.hk)

City University of Hong Kong



**I will be on the 2024 job market!**

Read the paper

