



Invisible Finger: Practical Electromagnetic Interference Attack on Touchscreen-based Electronic Devices

Haoqi Shan¹, Boyi Zhang¹, Zihao Zhan¹,

Dean Sullivan², Shuo Wang¹, Yier Jin¹

1: University of Florida

2. University of New Hampshire

Invisible Finger

Remote precise touch events injection
attack against capacitive touchscreens
using IEMI signal

TL;DR

- **Invisible Finger**
 - Remote precise touch events injection attack against capacitive touchscreens using IEMI signals.
 - **Effective attack distance** ~3cm
 - Can induce short-tap, long-press, omnidirectional swipe gesture
 - Works on different touchscreen devices, different scanning methods
 - A practical attack with out-of-sight screen locator and touch event detectors

<https://invisiblfinger.click>

TL;DR

- **Invisible Finger**
 - Remote precise touch events injection attack against capacitive touchscreens using IEMI signals.
 - Effective attack distance \sim 3cm
 - Can induce short-tap, long-press, omnidirectional swipe gesture
 - Works on different touchscreen devices, different scanning methods
 - A practical attack with out-of-sight screen locator and touch event detectors

<https://invisiblfinger.click>

TL;DR

- **Invisible Finger**
 - Remote precise touch events injection attack against capacitive touchscreens using IEMI signals.
 - Effective attack distance ~3cm
 - Can induce short-tap, long-press, omnidirectional swipe gesture
 - Works on different touchscreen devices, different scanning/driving methods
 - A practical attack with out-of-sight screen locator and touch event detectors

<https://invisiblfinger.click>

TL;DR

- **Invisible Finger**
 - Remote precise touch events injection attack against capacitive touchscreens using IEMI signals.
 - Effective attack distance ~3cm
 - Can induce short-tap, long-press, omnidirectional swipe gesture
 - Works on different touchscreen devices, different scanning methods
 - A practical attack with out-of-sight screen locator and touch event detector

<https://invisiblfinger.click>

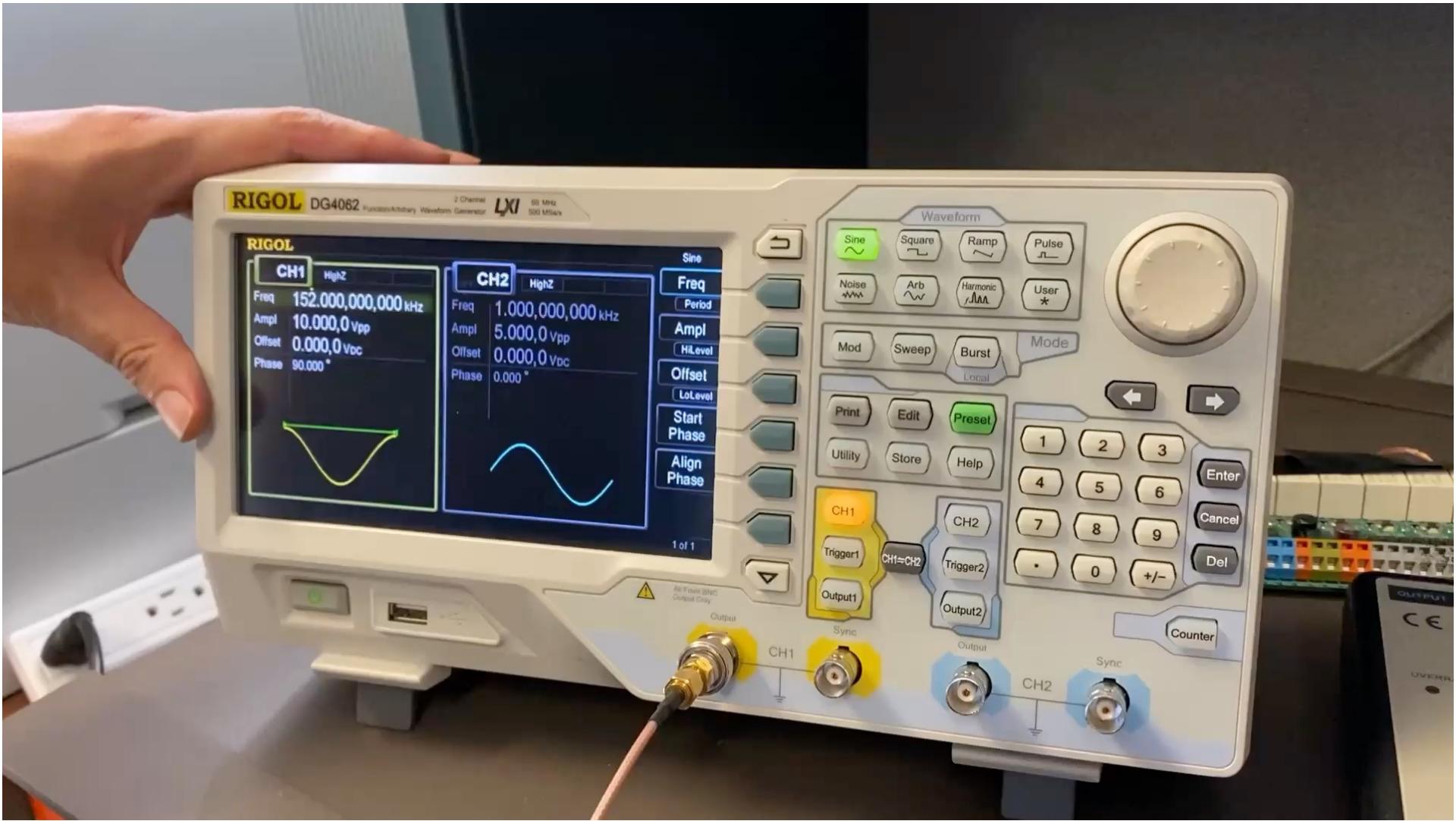


Table of Contents

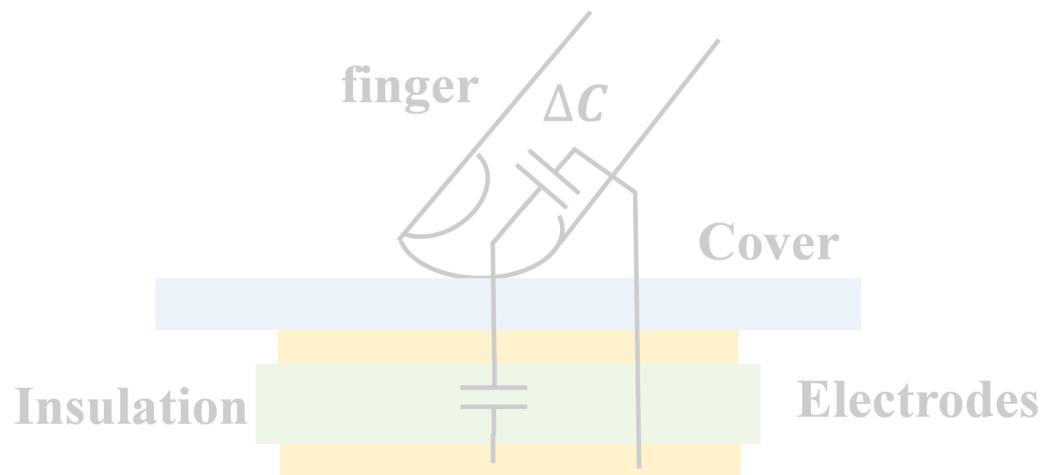
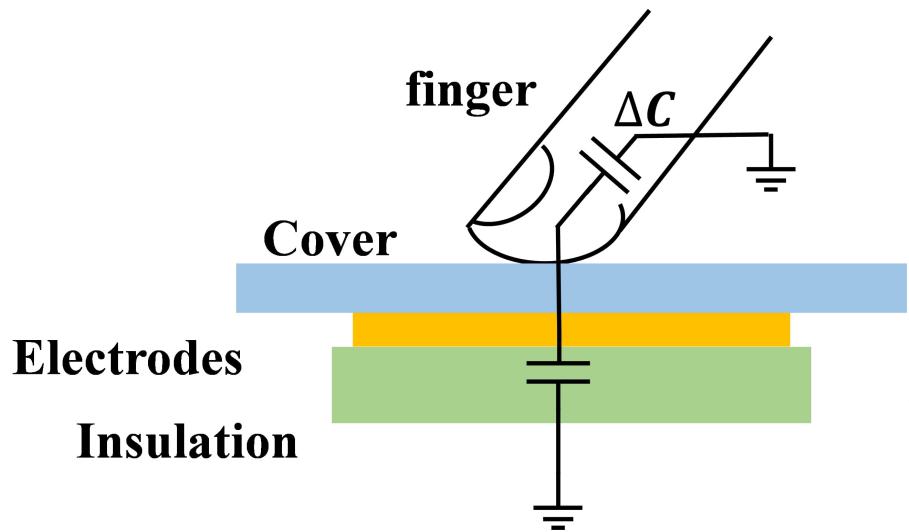
- Background
- Theoretical Analysis
- Precise Touch Events Generation
- Road to Practical Attacks
- Q&A

Table of Contents

- Background
- Theoretical Analysis
- Precise Touch Events Generation
- Road to Practical Attacks
- Q&A

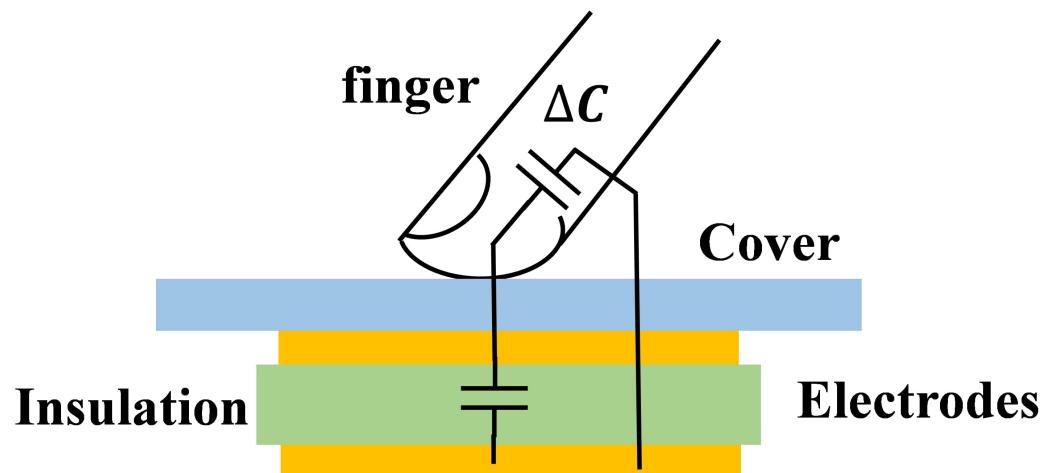
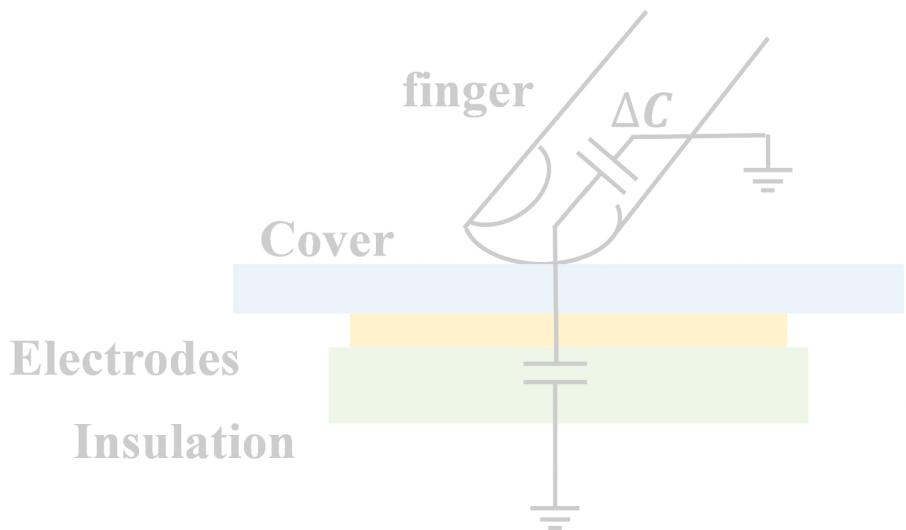
Touchscreen

- Capacitive Touchscreen
 - Self capacitance touchscreen
 - Mutual capacitance touchscreen



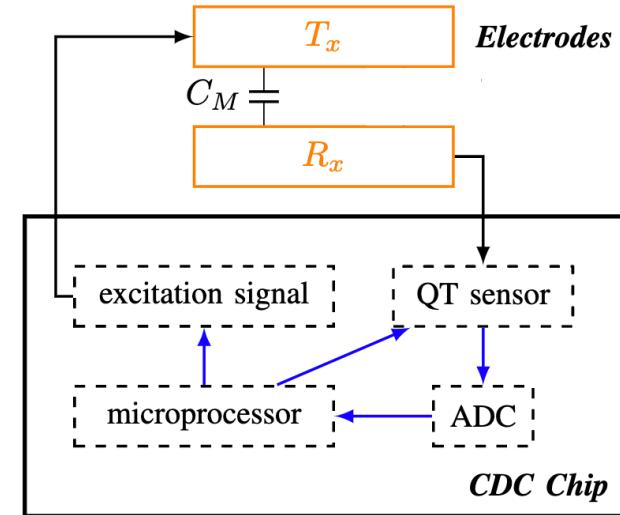
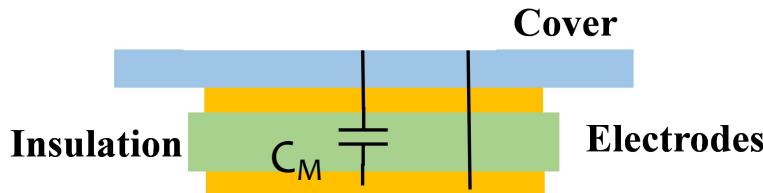
Touchscreen

- Capacitive Touchscreen
 - Self capacitance touchscreen
 - Mutual capacitance touchscreen



Touchscreen

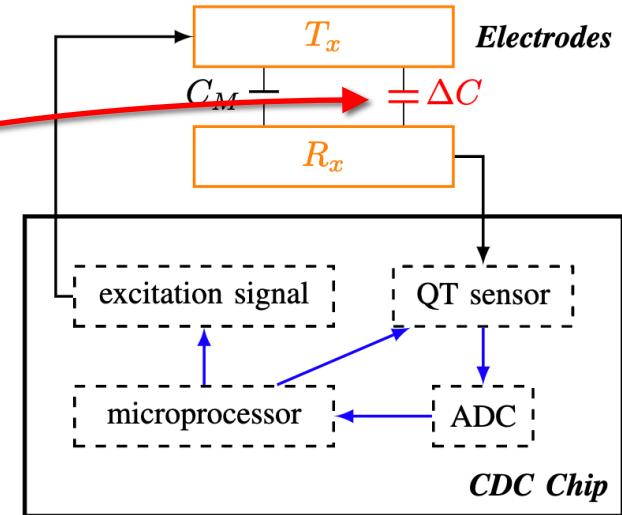
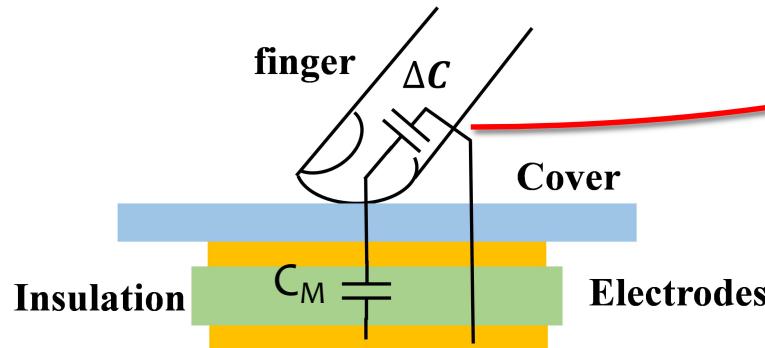
- Capacitive Touchscreen
 - Self capacitance touchscreen
 - Mutual capacitance touchscreen



Mutual capacitance touchscreen (no finger)

Touchscreen

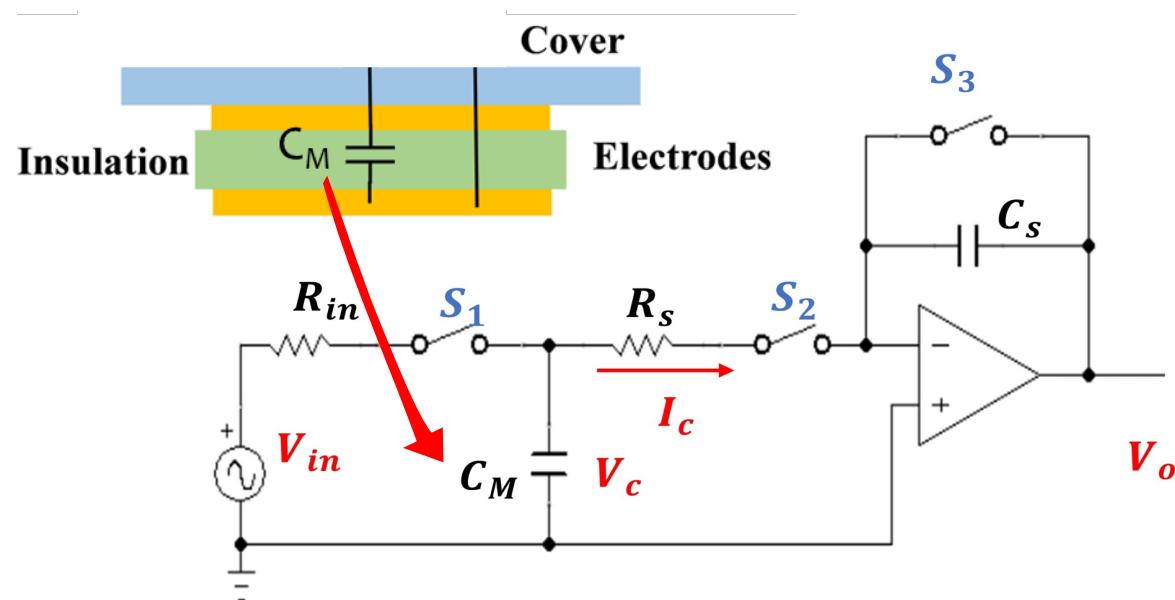
- Capacitive Touchscreen
 - Self capacitance touchscreen
 - Mutual capacitance touchscreen



Mutual capacitance touchscreen (with finger)

Simplified Touchscreen Design

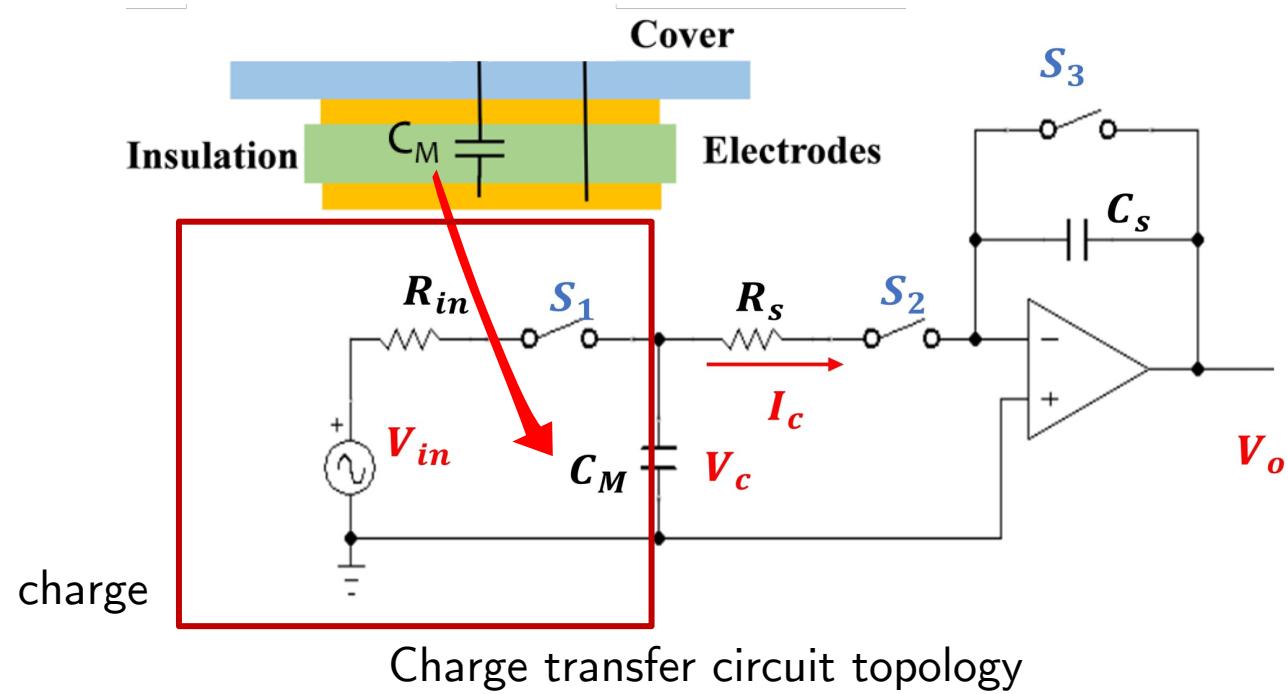
- Charge transfer



Charge transfer circuit topology

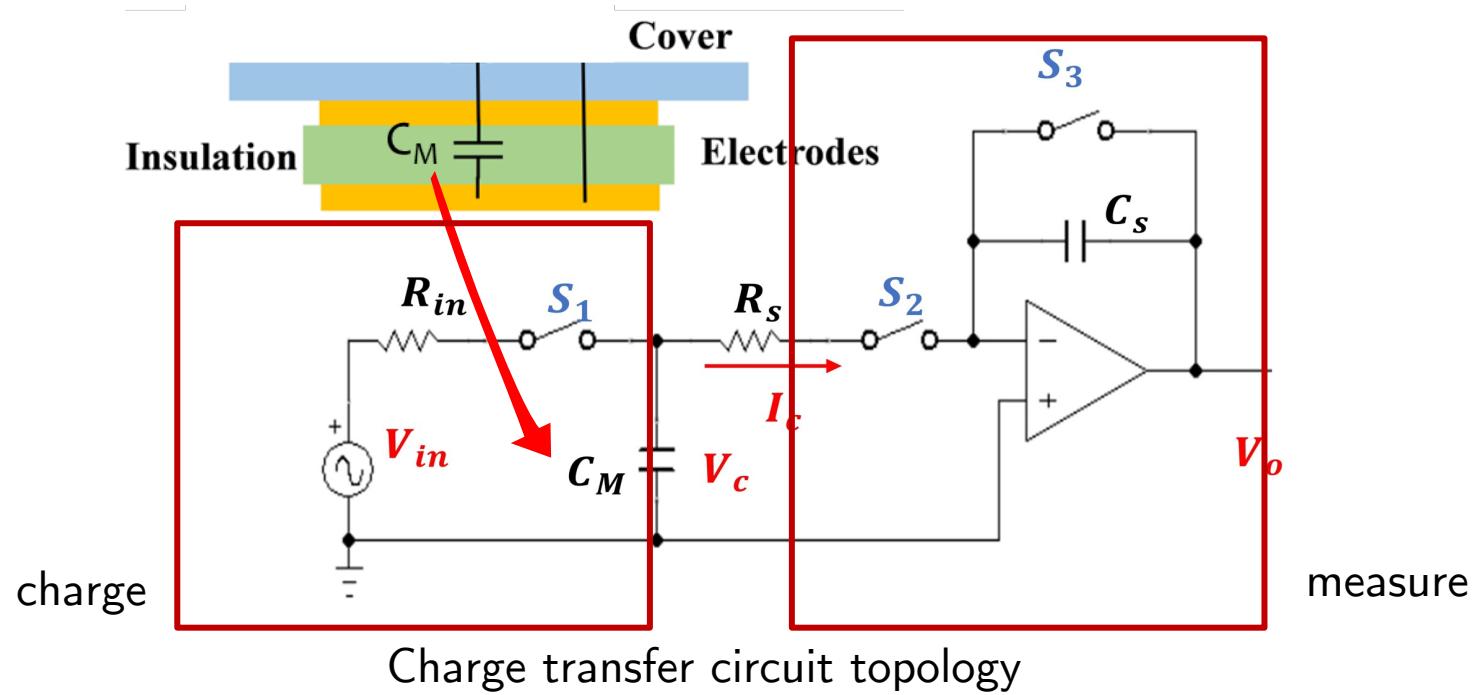
Simplified Touchscreen Design

- Charge transfer



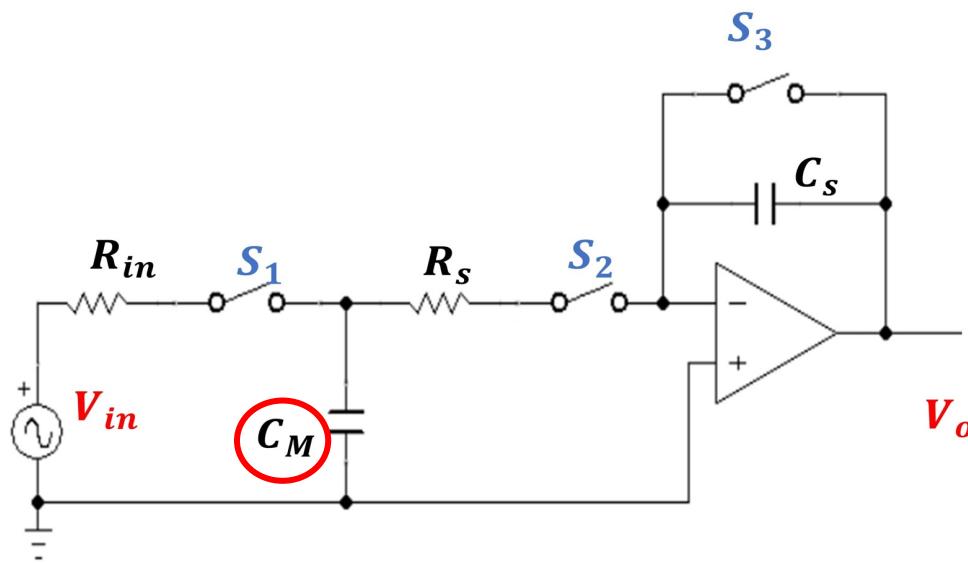
Simplified Touchscreen Design

- Charge transfer

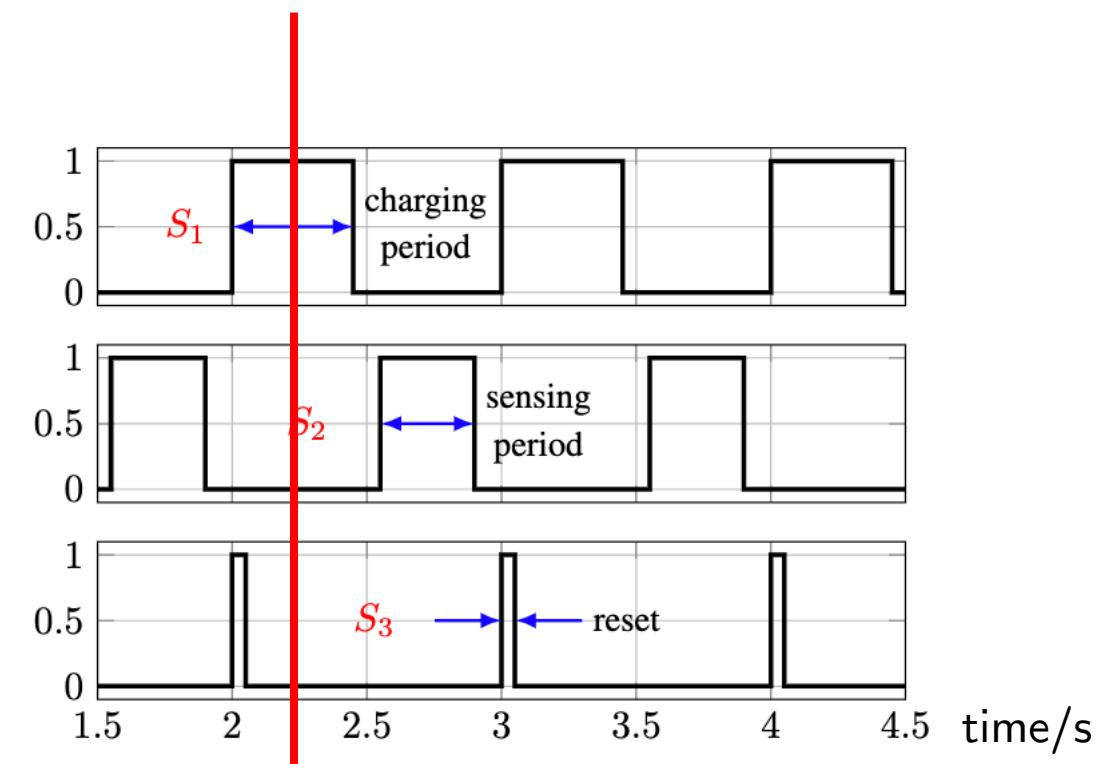


Simplified Touchscreen Design

- Charge transfer

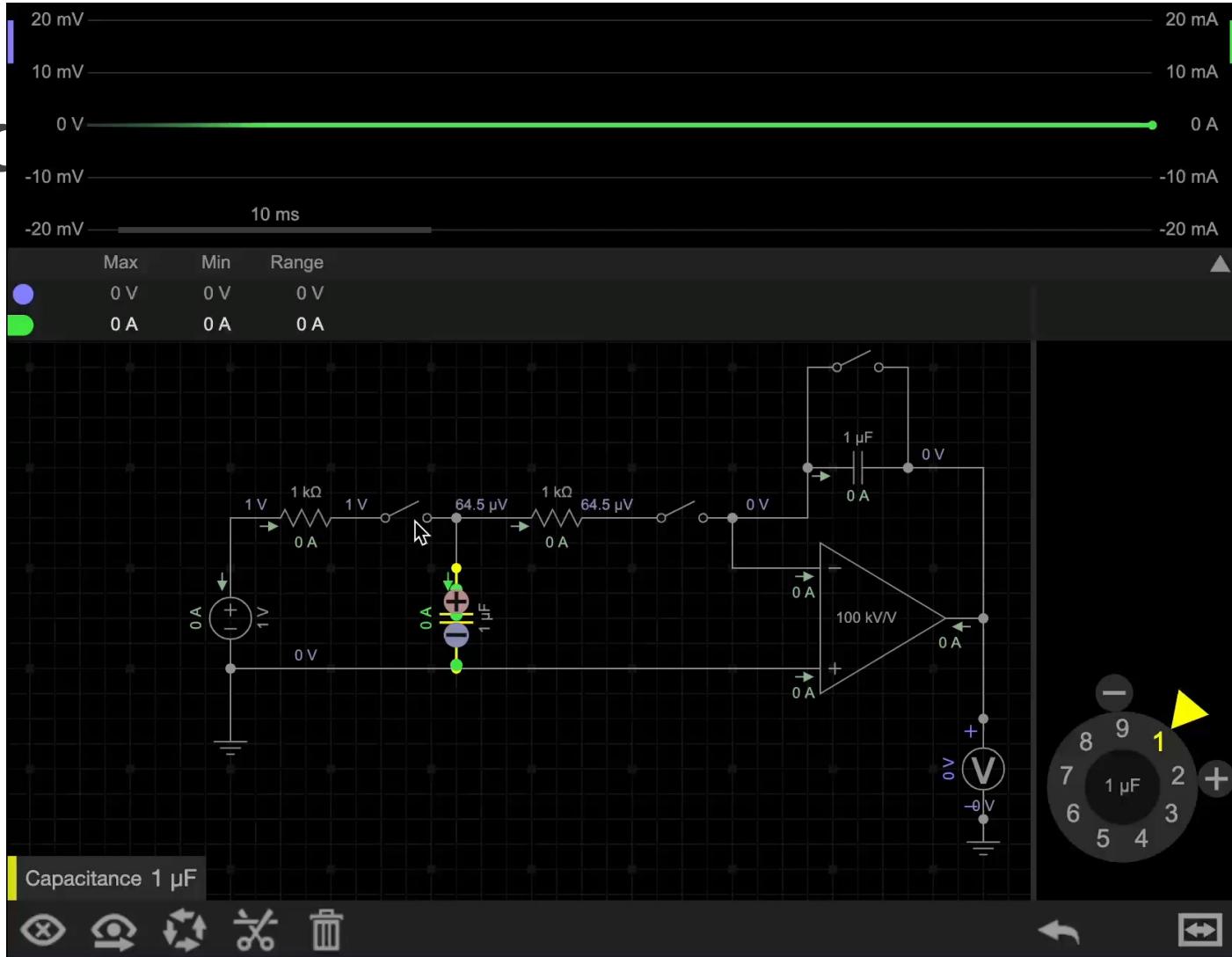


Charge transfer circuit topology

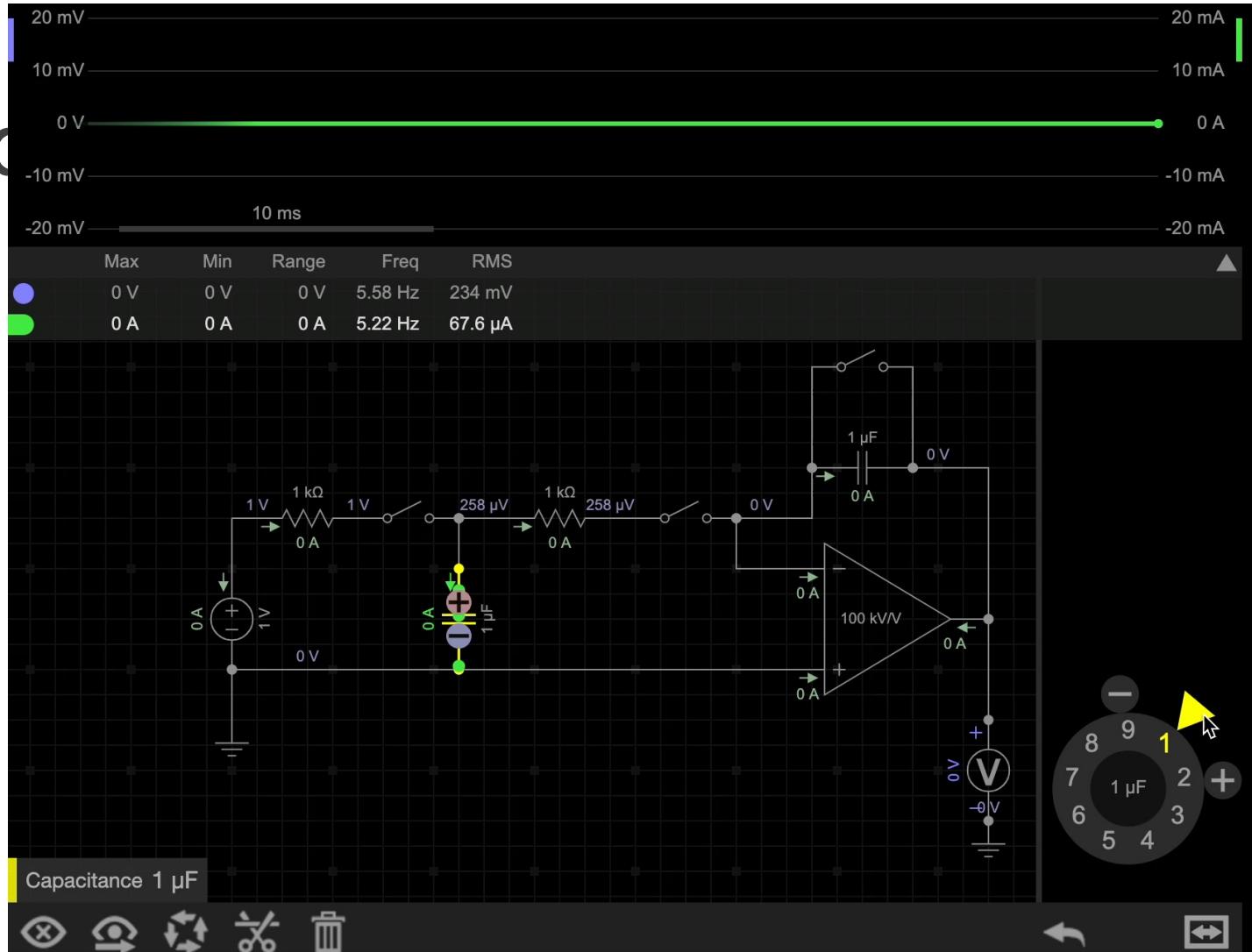


Control signal of charge transfer

Simplified



Simplified



Touchscreen under Interference

- EMI Noise caused equivalent capacitance change

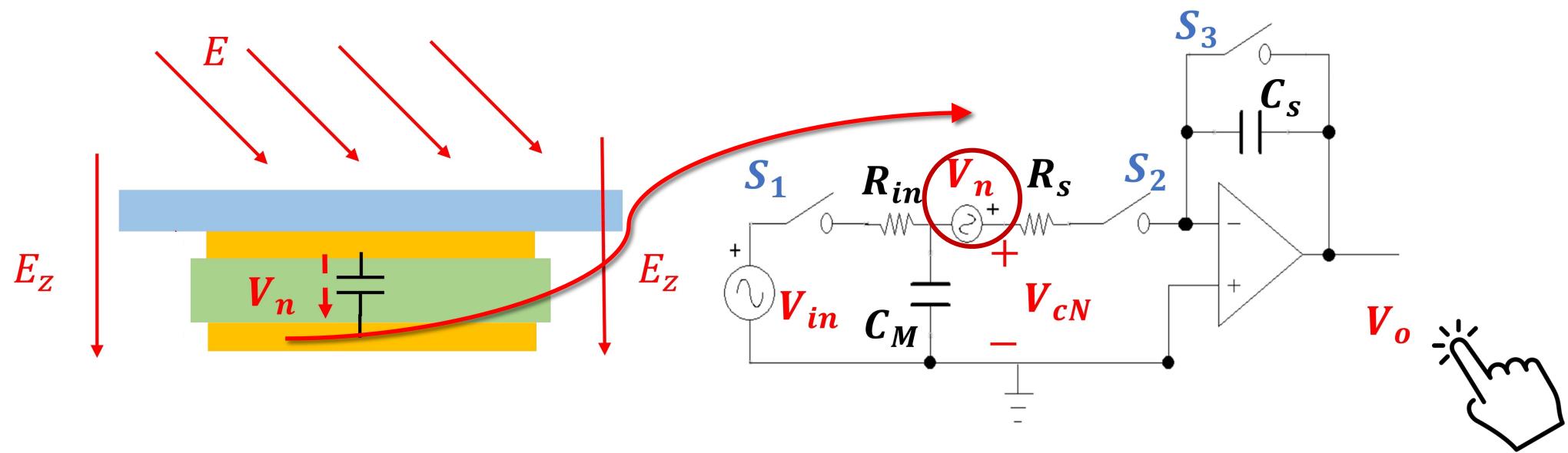


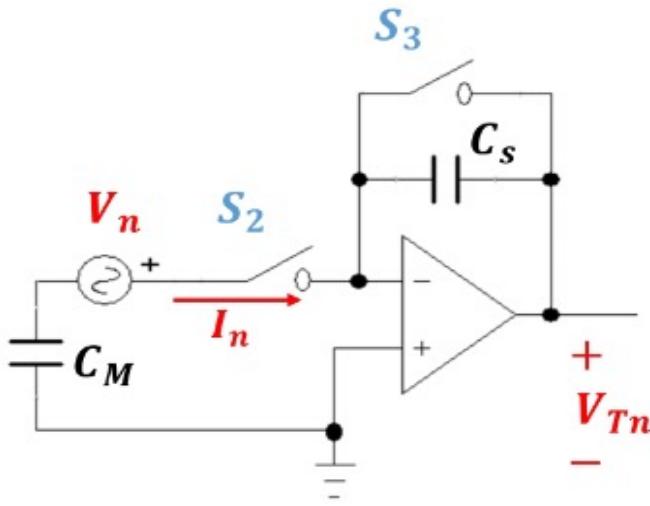
Table of Contents

- Background
- Theoretical Analysis
- Precise Touch Events Generation
- Road to Practical Attacks
- Q&A

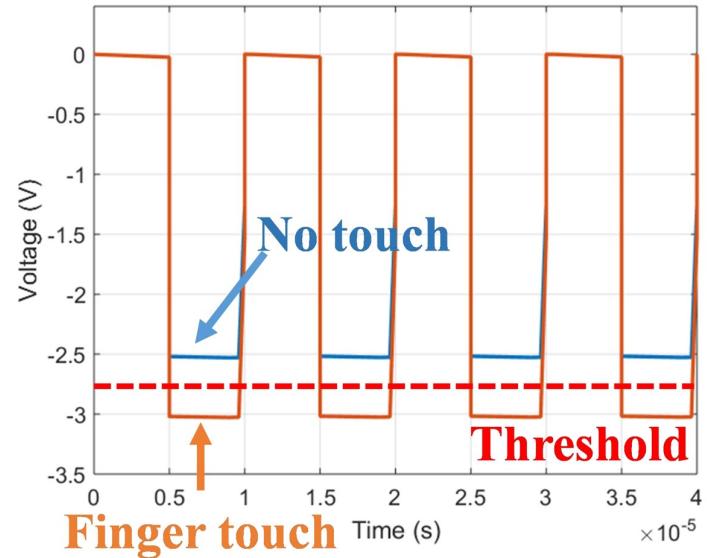
Coupling theoretical analysis with actual attack vectors

QT Sensor under Attack

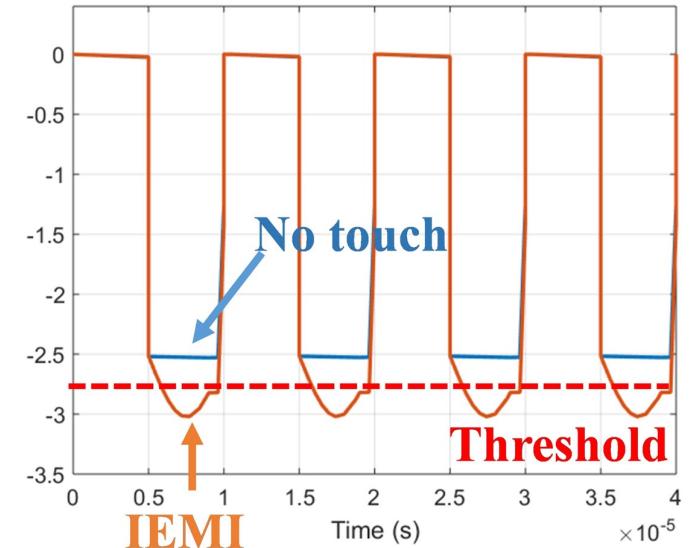
- What makes QT (charge transfer) sensor recognize a touch?
- Threshold detection voltage value



QT Sensor Simplified Circuit



QT Sensor Output Voltage (Touched vs IEMI caused)



IEMI Signal

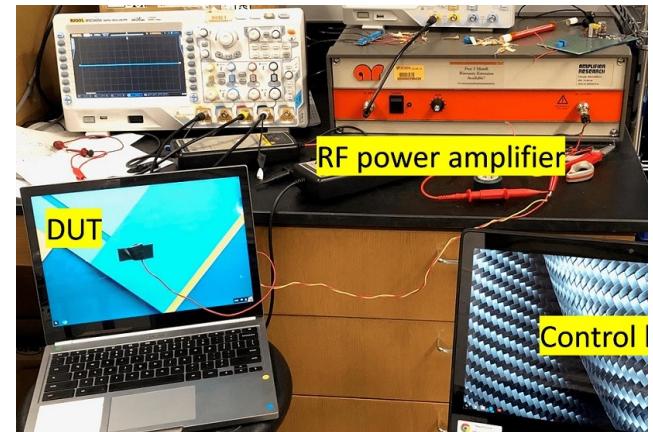
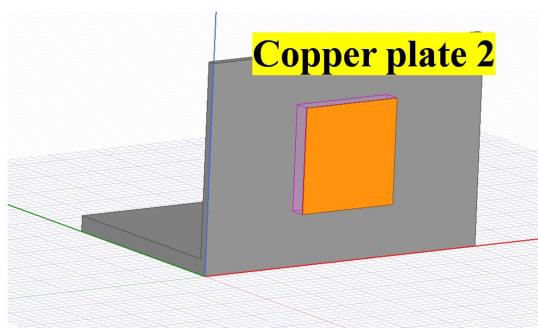
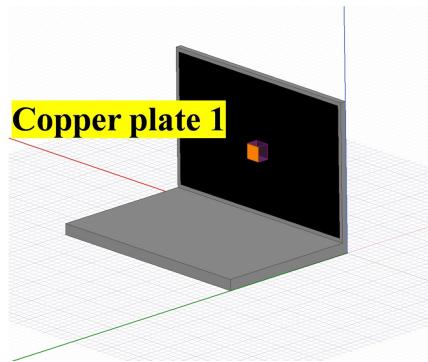
- What is the most effective interference signal?
 - Amplitude and Frequency

$$V_{TnM} = -\frac{C_M V_n}{C_s} \sum_0^M (\sin(2\pi f_E \cdot T_s + \varphi_M) - \sin(\varphi_M))$$

$$f_E = \frac{3f_{sw}}{4D_s} + \frac{k f_{sw}}{D_s} \quad k = 0, 1, 2, 3, \dots$$

IEMI Signal

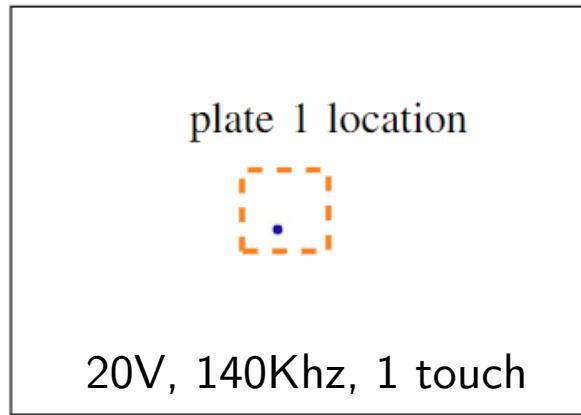
- Validation (Chromebook)



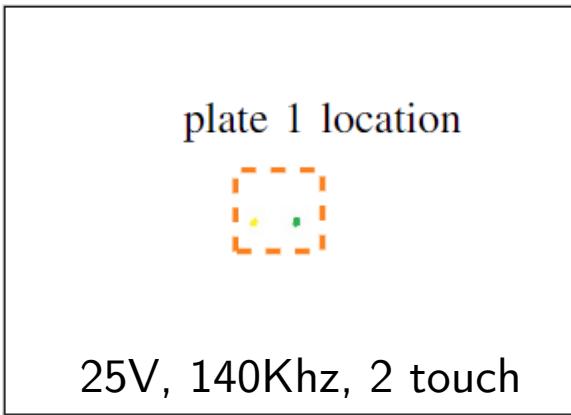
Preliminary experiment setup using copper plates (simulation and actual hardware)

When, Where, How

- Result collection
 - Induced touch events or not?
 - Excitation signal amplitude, frequency?

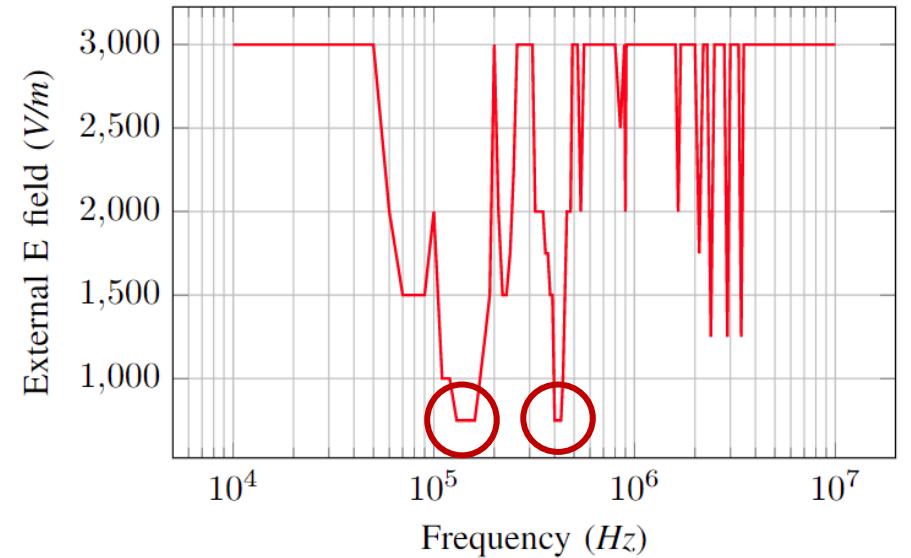


(a)



(b)

$$f_E = \frac{3f_{sw}}{4D_s} + \frac{k f_{sw}}{D_s} \quad k = 0, 1, 2, 3, \dots$$



Minimum E field to generate touch events

#BHUSA @BlackHatEvents

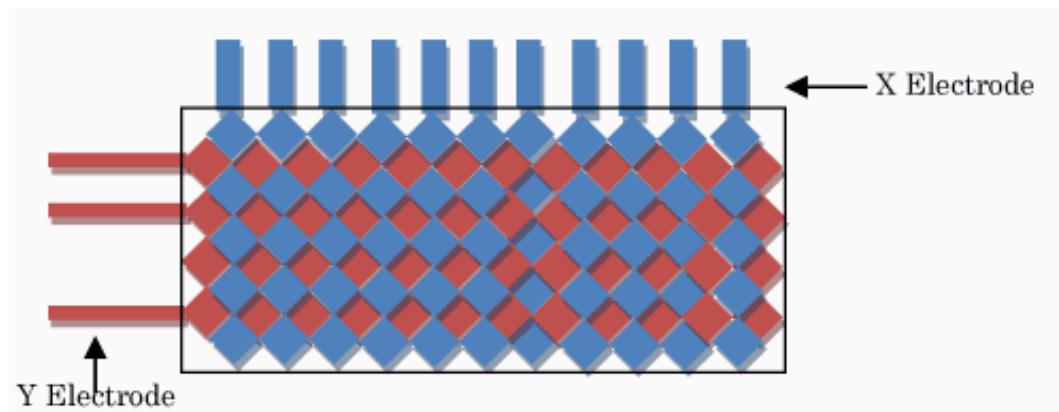
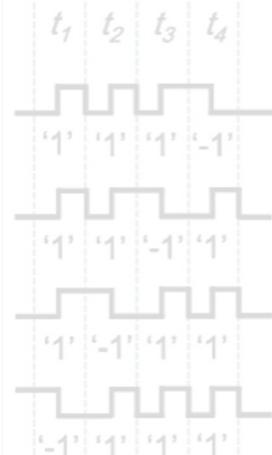
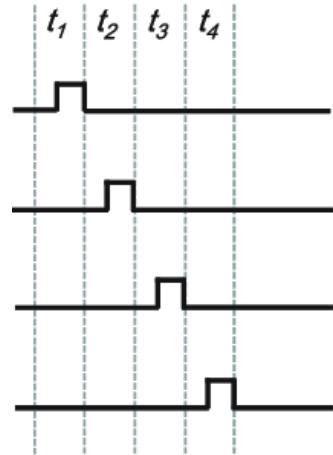
Table of Contents

- Background
- Theoretical Analysis
- Precise Touch Events Generation
- Road to Practical Attacks
- Q&A

Precise touch events generation and thorough experiments

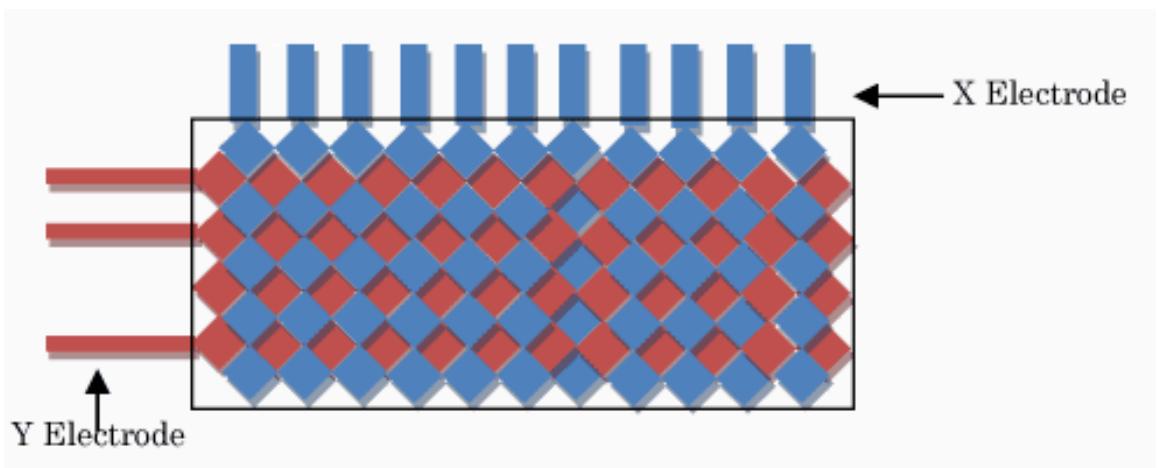
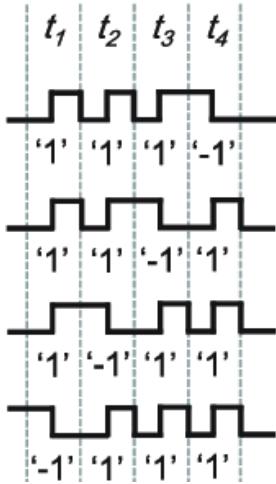
Precise Touch Events

- Challenges?
- Scanning/Driving Methods
 - Sequential scanning
 - Parallel scanning
- Previous approaches



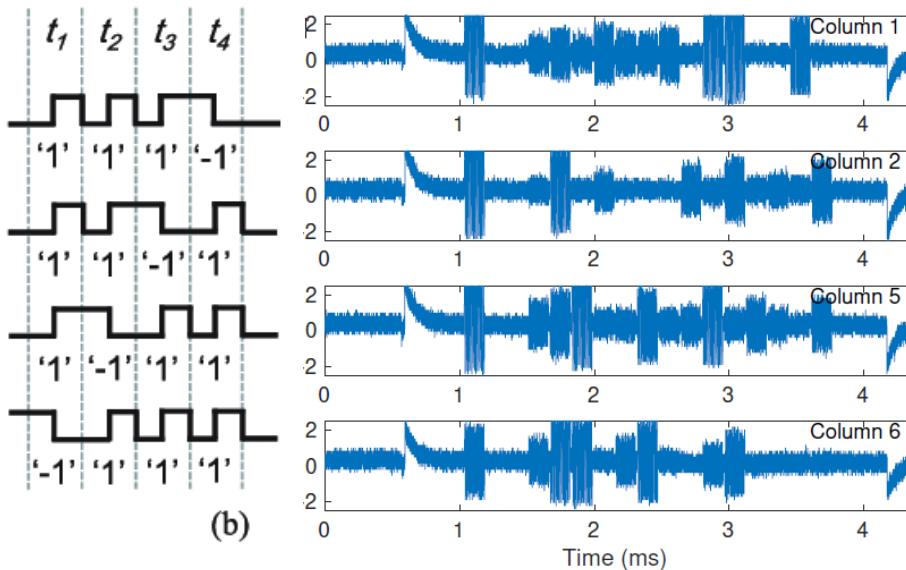
Precise Touch Events

- Challenges?
- Scanning/Driving Methods
 - Sequential scanning
 - Parallel scanning
- Previous approaches

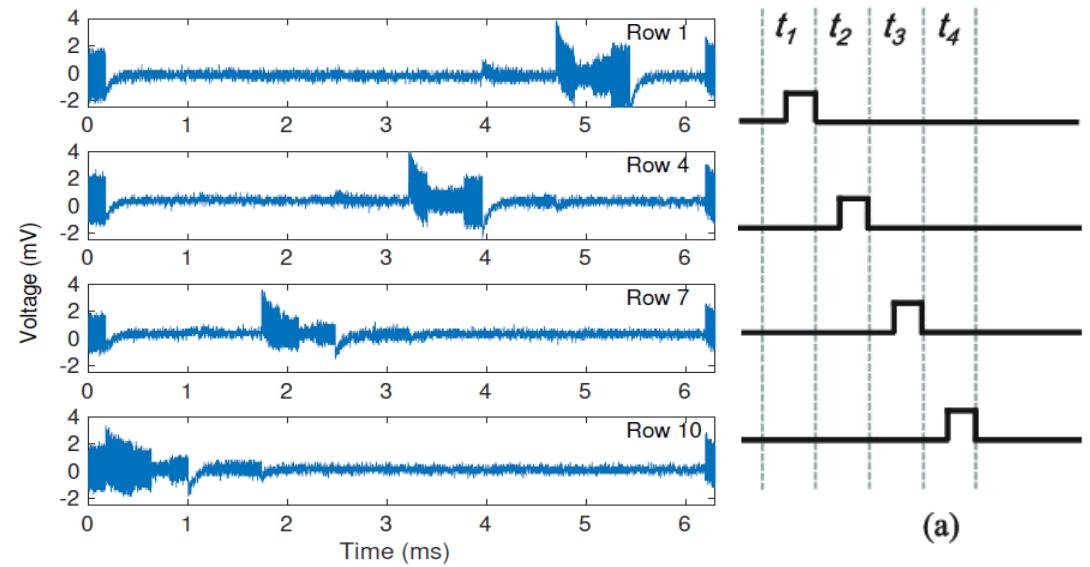


Precise Touch Events

- Challenges from different driving mechanism (measured on different row/column)



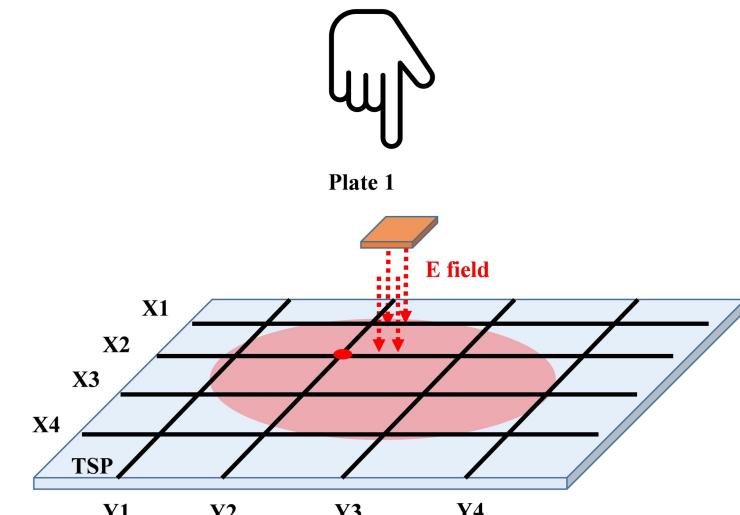
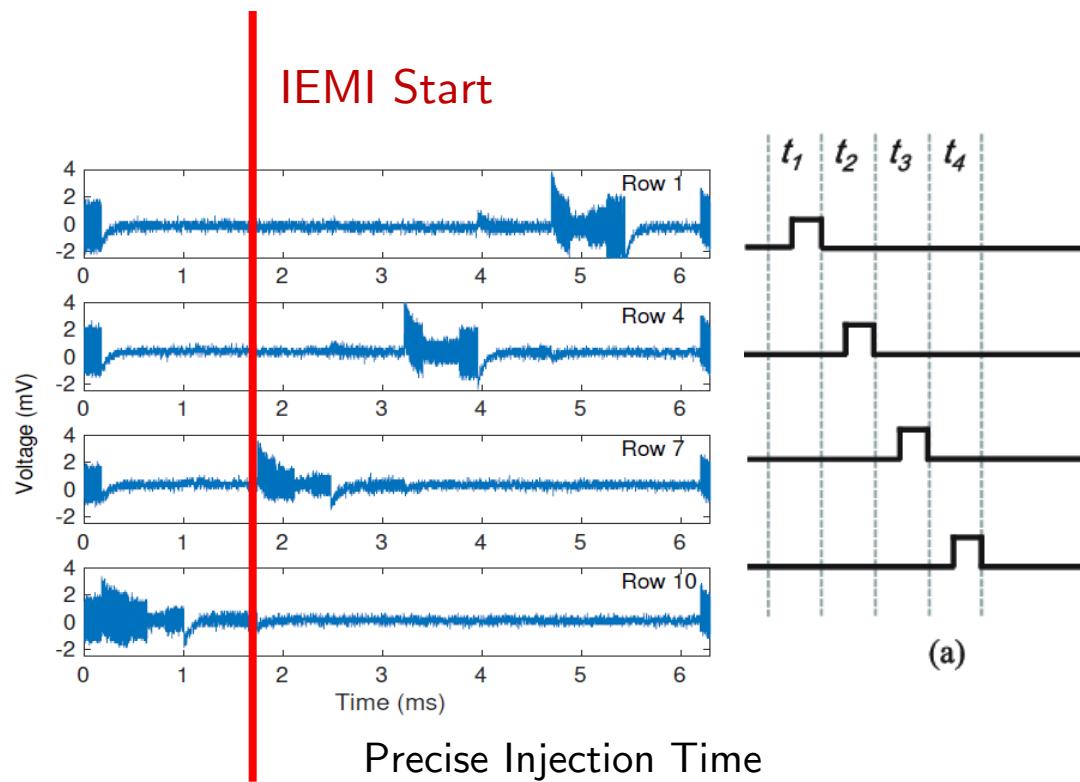
Parallel Driving iPhone 11 Pro



Sequential Driving Pixel 2

Precise Touch Events

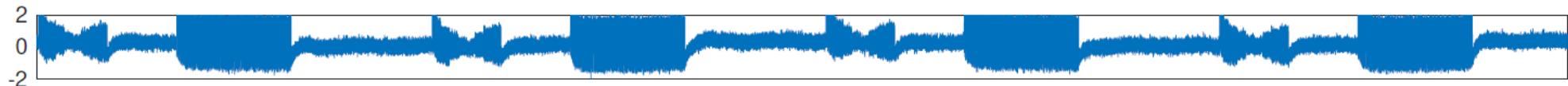
- Precise injection time or precise injected location?



Precise Injection Location

Precise Touch Events

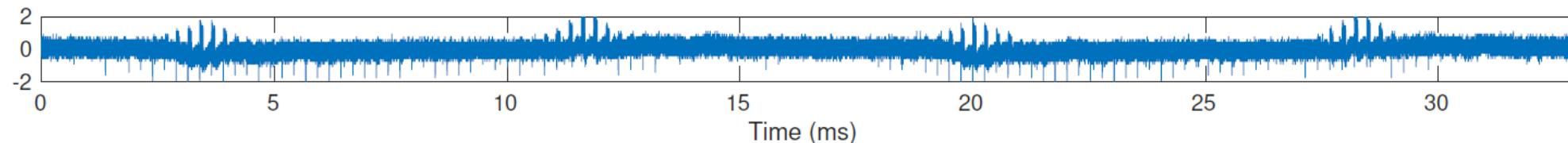
- Challenges from different scanning mechanism (measured on different target devices)



Pixel 2 Touchscreen Driving Signal



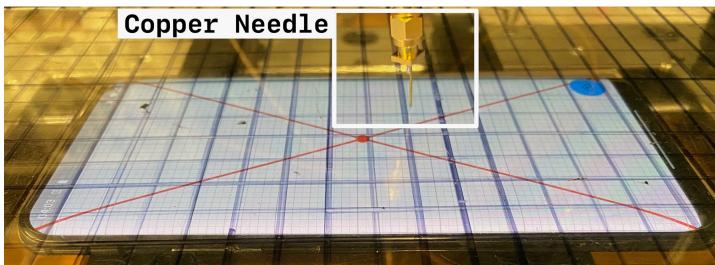
iPhone 11 Pro Touchscreen Driving Signal



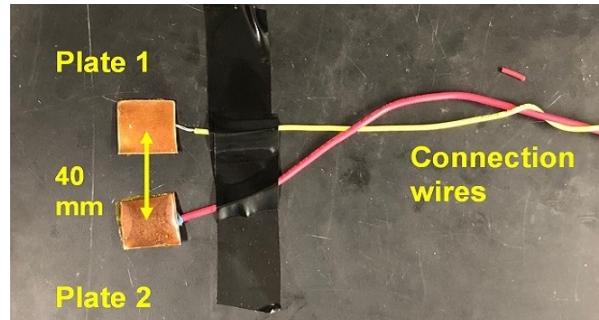
Nexus 5X Touchscreen Driving Signal

Precise Touch Events

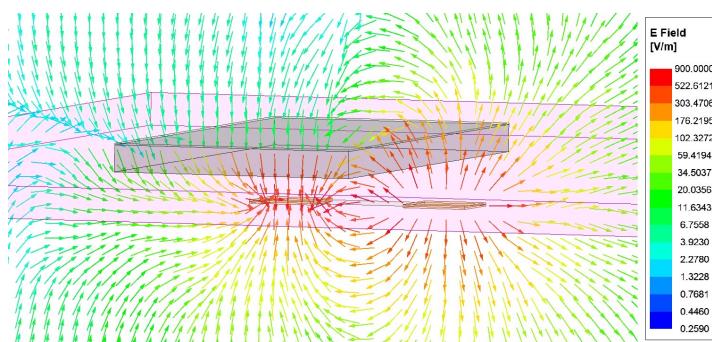
- Antenna design



Copper Needle



Copper Plates



Copper Plates Antenna E-Field Simulation

Precise Touch Events

DEVICE	DRIVING	SUCCESS RATE	Quartile Deviation (pixels)		Gestures		
			QD(X)	QD(Y)	SHORT	LONG	SWIPE
🍎 iPad Pro	P	>99%	1.0	0.5	✓	✓	✓
_ANDROID OnePlus 7 Pro	P	>99%	196.5	3.0	✓	✗	?
_ANDROID Google Pixel 2	S	>99%	10.0	149.5	✓	✓	?
_ANDROID Nexus 5X	S	>99%	3.5	182.5	✓	✗	?
WINDOWS Surface Pro 7	P	88%	12.5	7.5	✓	✓	✓
🍎 iPhone 6	P	86%	14.0	10.0	✓	✓	✗
🍎 iPhone 11 Pro	P	77%	4.5	8.5	✓	✓	✗
🍎 iPhone SE	P	57%	10.5	6.0	✓	✗	✗

Precise Touch Events

DEVICE	DRIVING	SUCCESS RATE	Quartile Deviation (pixels)		Gestures		
			QD(X)	QD(Y)	SHORT	LONG	SWIPE
🍎 iPad Pro	P	>99%	1.0	0.5	✓	✓	✓
_ANDROID OnePlus 7 Pro	P	>99%	196.5	3.0	✓	✗	?
_ANDROID Google Pixel 2	S	>99%	10.0	149.5	✓	✓	?
_ANDROID Nexus 5X	S	>99%	3.5	182.5	✓	✗	?
WINDOWS Surface Pro 7	P	88%	12.5	7.5	✓	✓	✓
🍎 iPhone 6	P	86%	14.0	10.0	✓	✓	✗
🍎 iPhone 11 Pro	P	77%	4.5	8.5	✓	✓	✗
🍎 iPhone SE	P	57%	10.5	6.0	✓	✗	✗

Driving method: P (Parallel), S (Sequential)

Precise Touch Events

DEVICE	DRIVING	SUCCESS RATE	Quartile Deviation (pixels)		Gestures		
			QD(X)	QD(Y)	SHORT	LONG	SWIPE
iPad Pro	P	>99%	1.0	0.5	✓	✓	✓
OnePlus 7 Pro	P	>99%	196.5	3.0	✓	✗	?
Google Pixel 2	S	>99%	10.0	149.5	✓	✓	?
Nexus 5X	S	>99%	3.5	182.5	✓	✗	?
Surface Pro 7	P	88%	12.5	7.5	✓	✓	✓
iPhone 6	P	86%	14.0	10.0	✓	✓	✗
iPhone 11 Pro	P	77%	4.5	8.5	✓	✓	✗
iPhone SE	P	57%	10.5	6.0	✓	✗	✗

Driving method: P (Parallel), S (Sequential)

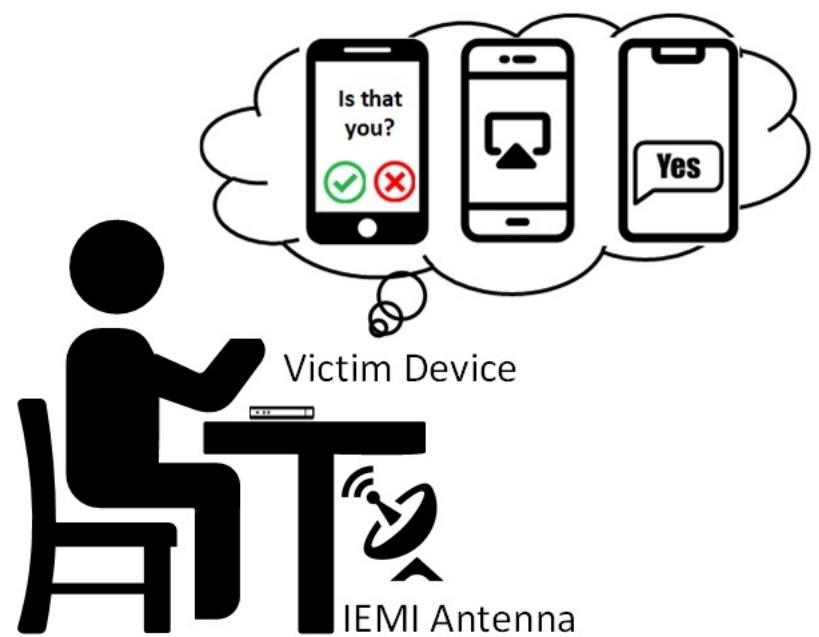
Table of Contents

- Background
- Theoretical Analysis
- Precise Touch Events Generation
- Road to Practical Attacks
- Q&A

Complete practical attack vectors

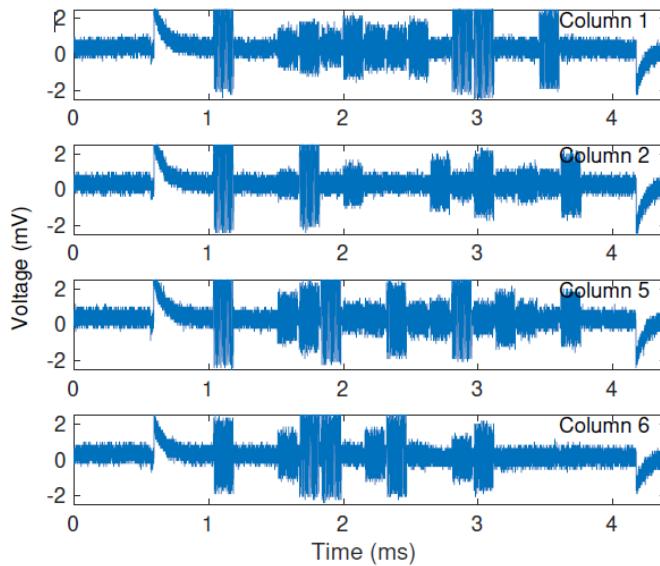
Now what?

- Established the theoretical background knowledge and actual setup needed for inducing precious touch events.
- Missing?
 - Attacking device is under the table
 - Phone is randomly located
- Phone locator
- Attack scenarios
 - Multiple touches at multiple locations
 - Even swipe (gesture unlocking)
- Touch event detector

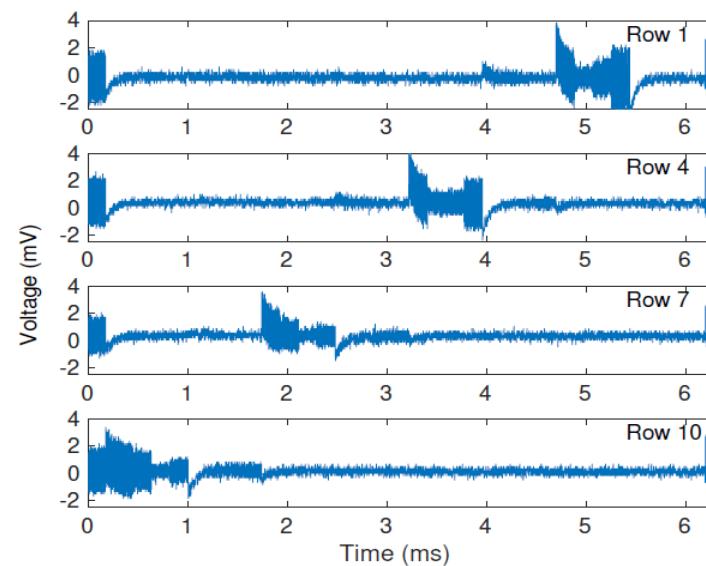


Phone Locator

- Locate the phone and know the orientation by placing multiple antennas under the table
 - The excitation signal from touchscreen leaks info (which row/column pointed at)



Parallel Scanning iPhone 11 Pro



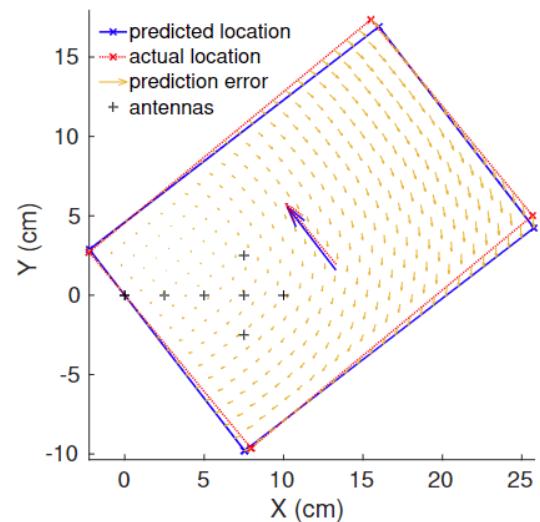
Sequential Scanning Pixel 2

Phone Locator

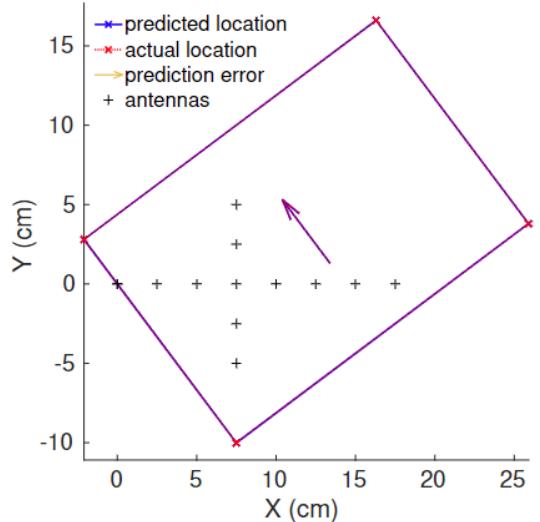
- A quick but reliable KNN classifier

$$\begin{bmatrix} x_{\text{screen}} \\ y_{\text{screen}} \\ 1 \end{bmatrix} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) & x_t \\ \sin(\theta) & \cos(\theta) & y_t \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{\text{antenna}} \\ y_{\text{antenna}} \\ 1 \end{bmatrix}$$

Antenna location/screen location transformation matrix



(a) Screen location detected using 7
antennas



(b) Screen location detected using 12
antennas

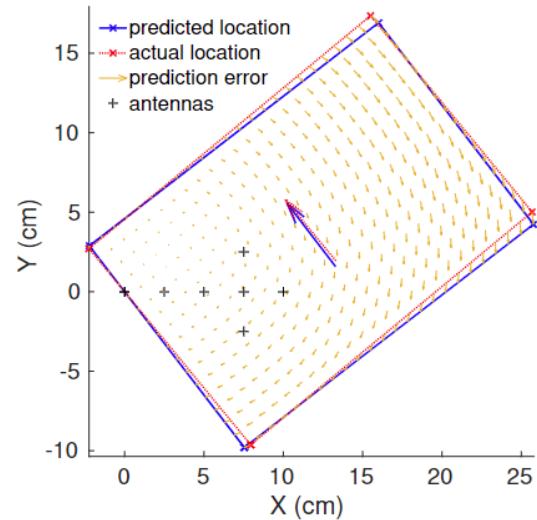
Evaluation using iPad Pro 2020

Phone Locator

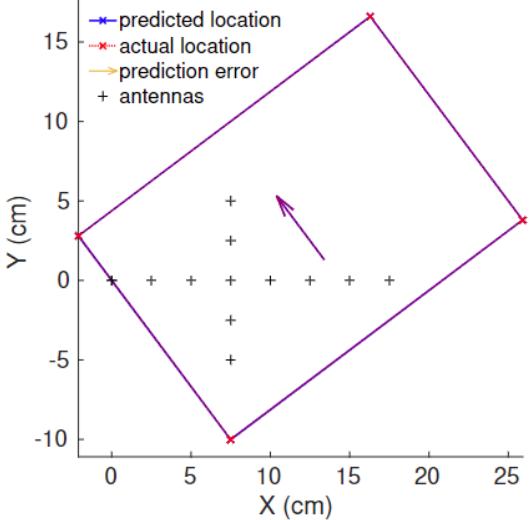
- A quick but reliable KNN classifier

$$\begin{bmatrix} x_{\text{screen}} \\ y_{\text{screen}} \\ 1 \end{bmatrix} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) & x_t \\ \sin(\theta) & \cos(\theta) & y_t \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{\text{antenna}} \\ y_{\text{antenna}} \\ 1 \end{bmatrix}$$

Antenna location/screen location transformation matrix



(a) Screen location detected using 7
antennas



(b) Screen location detected using 12
antennas

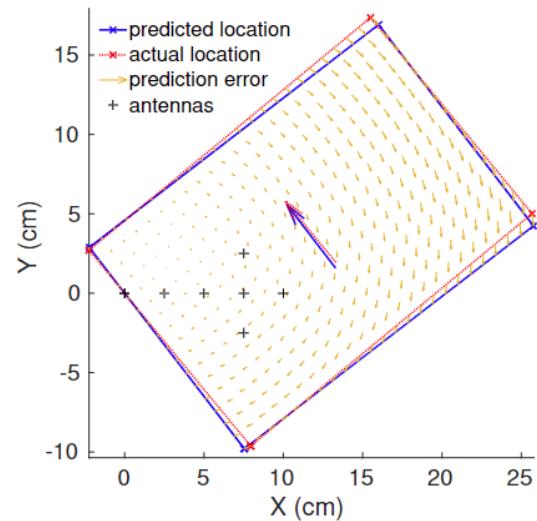
Evaluation using iPad Pro 2020

Phone Locator

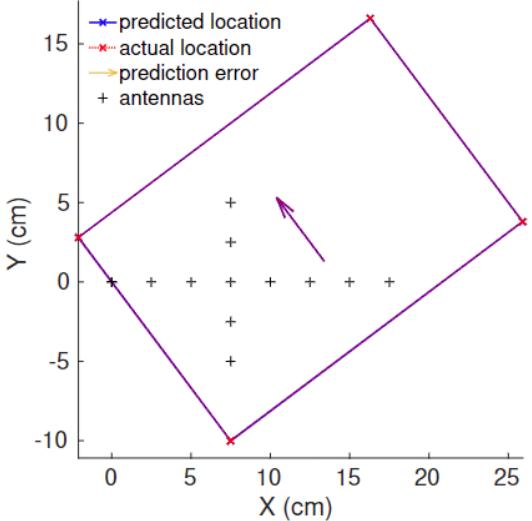
- A quick but reliable KNN classifier

$$\begin{bmatrix} x_{\text{screen}} \\ y_{\text{screen}} \\ 1 \end{bmatrix} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) & x_t \\ \sin(\theta) & \cos(\theta) & y_t \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{\text{antenna}} \\ y_{\text{antenna}} \\ 1 \end{bmatrix}$$

Antenna location/screen location transformation matrix



(a) Screen location detected using 7
antennas

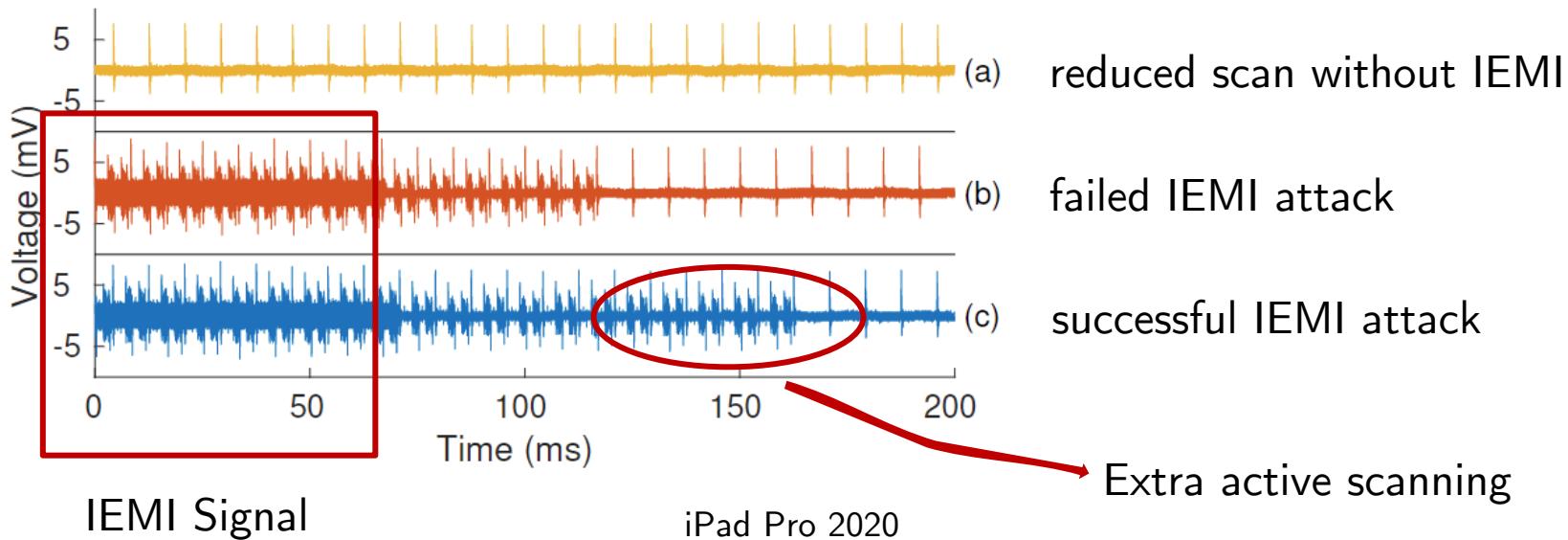


(b) Screen location detected using 12
antennas

Evaluation using iPad Pro 2020

Touch Event Detector

- Scanning signal behaves different if a successful touch event is recognized by touchscreen controller



Attack Scenarios

- Click based attack
 - Malicious application installation (Android)
 - Malicious Bluetooth peripheral connection (iOS)
- Gesture based attack
 - Send messages (bank fraud message)
 - Send money (press-and-hold on PayPal icon)
 - Unlock phone (omnidirectional gesture unlocking)



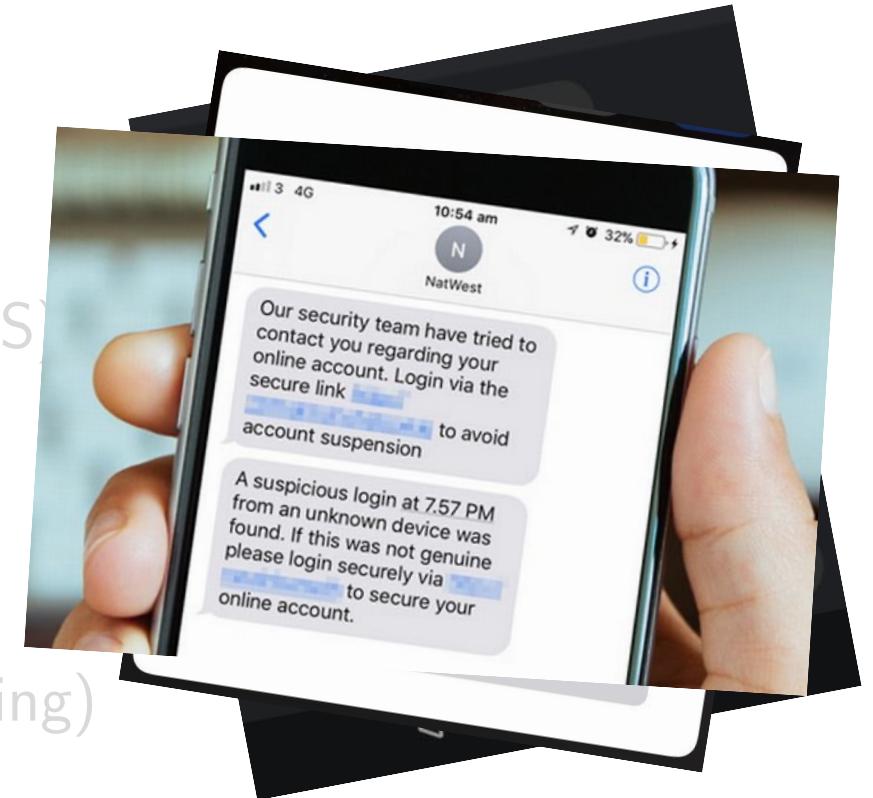
Attack Scenarios

- Click based attack
 - Malicious application installation (Android)
 - Malicious Bluetooth peripheral connection (iOS)
- Gesture based attack
 - Send messages (bank fraud message)
 - Send money (press-and-hold on PayPal icon)
 - Unlock phone (omnidirectional gesture unlocking)



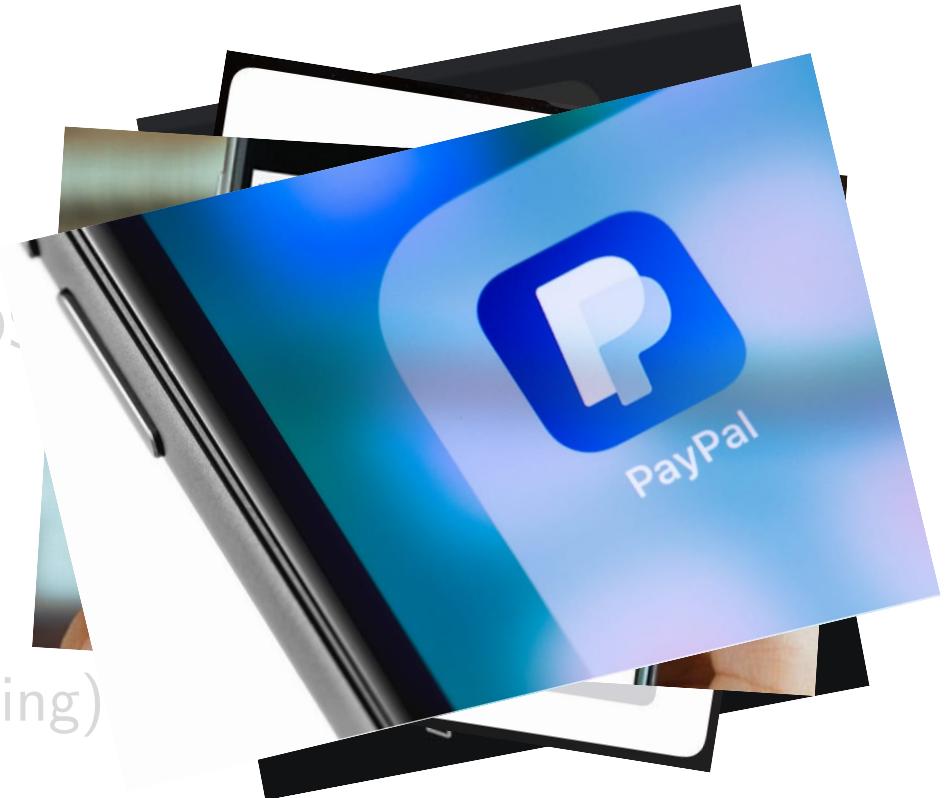
Attack Scenarios

- Click based attack
 - Malicious application installation (Android)
 - Malicious Bluetooth peripheral connection (iOS)
- Gesture based attack
 - Send messages (bank fraud message)
 - Send money (press-and-hold on PayPal icon)
 - Unlock phone (omnidirectional gesture unlocking)



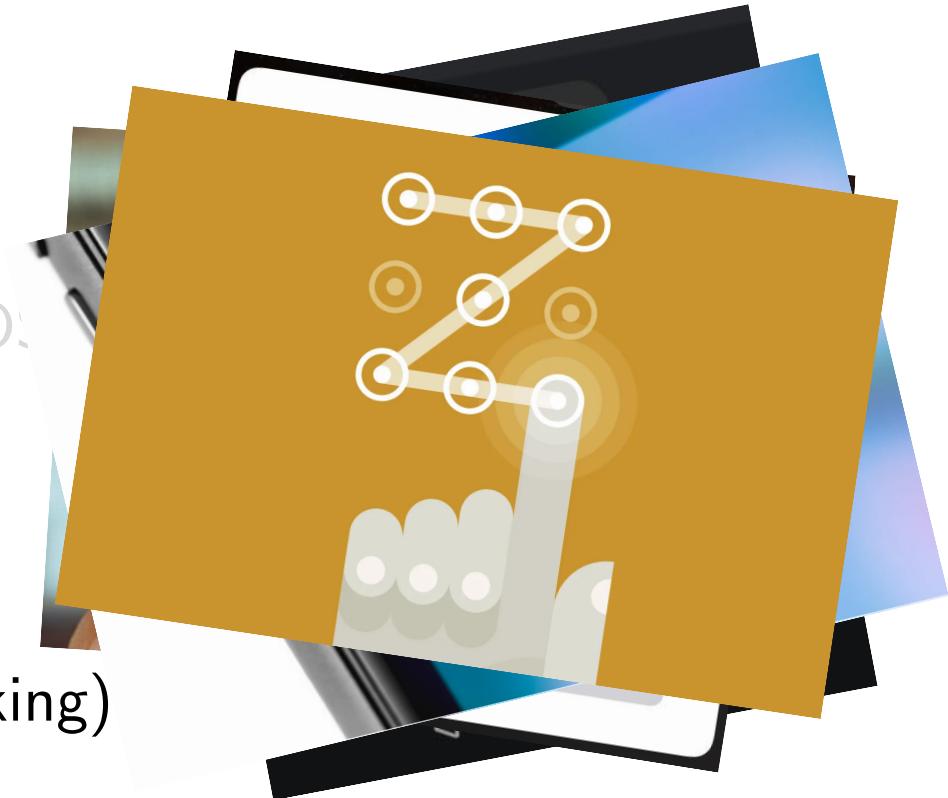
Attack Scenarios

- Click based attack
 - Malicious application installation (Android)
 - Malicious Bluetooth peripheral connection (iOS)
- Gesture based attack
 - Send messages (bank fraud message)
 - Send money (press-and-hold on PayPal icon)
 - Unlock phone (omnidirectional gesture unlocking)



Attack Scenarios

- Click based attack
 - Malicious application installation (Android)
 - Malicious Bluetooth peripheral connection (iOS)
- Gesture based attack
 - Send messages (bank fraud message)
 - Send money (press-and-hold on PayPal icon)
 - Unlock phone (omnidirectional gesture unlocking)



Mitigations

- Pressure detection (Vendors)
- Faraday Fabric (Customers)

Q&A

Questions?

<https://invisiblefinger.click>

