black hat USA 2022

Nelms Institute for the Connected World
UNIVERSITY of FLORIDA

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

Haoqi Shan[1], Boyi Zhang[1], Zihao Zhan[1],
Dean Sullivan[2], Shuo Wang[1], Yier Jin[1]

1: University of Florida

2. University of New Hampshire

Agenda

- Who we are?
- TL;DR
- How does touchscreen work?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

Agenda

- Who we are?
- TL;DR
- How touchscreen works?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

Who We Are?

- Security in Silicon Lab (SSL), University of Florida
  - Architectural Security
  - Side Channel Security
  - IP Core Security
  - AI Security
  - IoT/CPS Security
- Published work on S&P, NDSS, AAAI....
- Actively hiring Ph.D students!

Invisible Finger

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

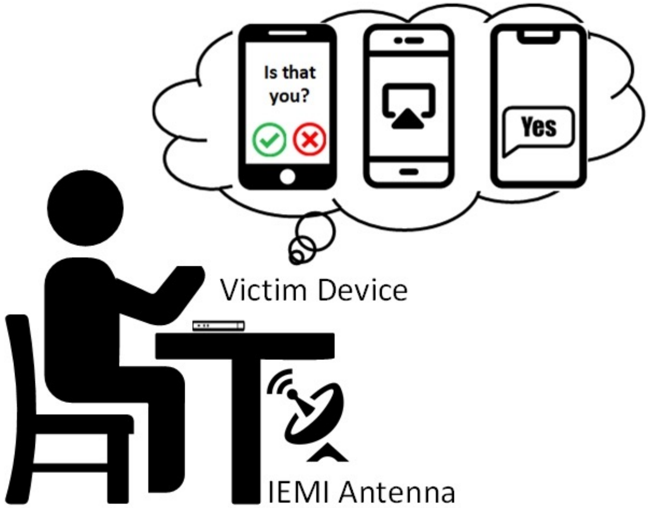
Agenda

- Who we are?
- TL;DR
- How touchscreen works?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

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
  - First practical attack with out-of-sight screen locator and touch event detectors

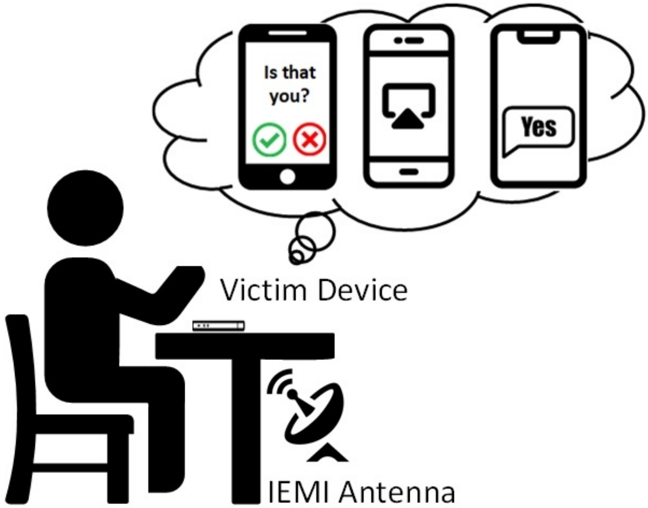
https://invisiblefinger.click



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
  - First practical attack with out-of-sight screen locator and touch event detectors

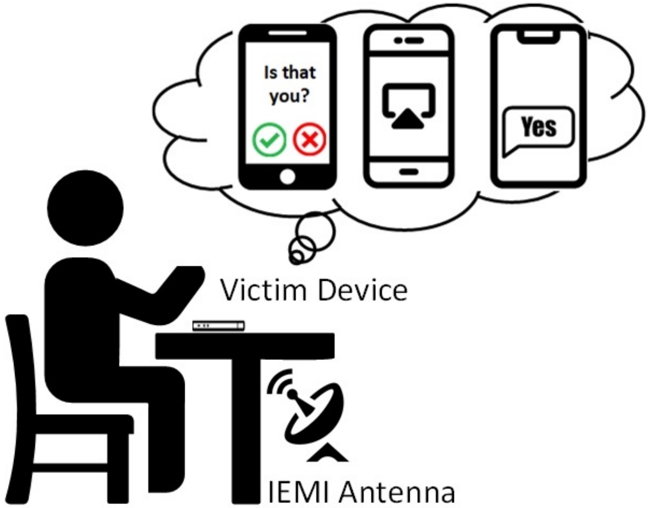
https://invisiblefinger.click



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
  - First practical attack with out-of-sight screen locator and touch event detectors

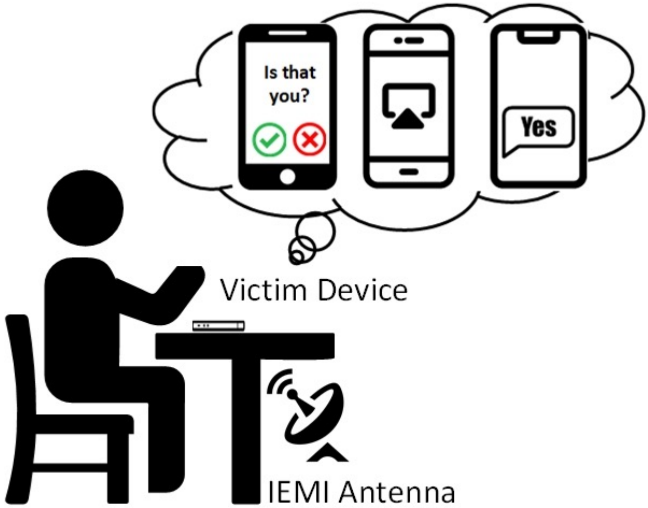
https://invisiblefinger.click



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
  - First practical attack with out-of-sight screen locator and touch event detector

https://invisiblefinger.click

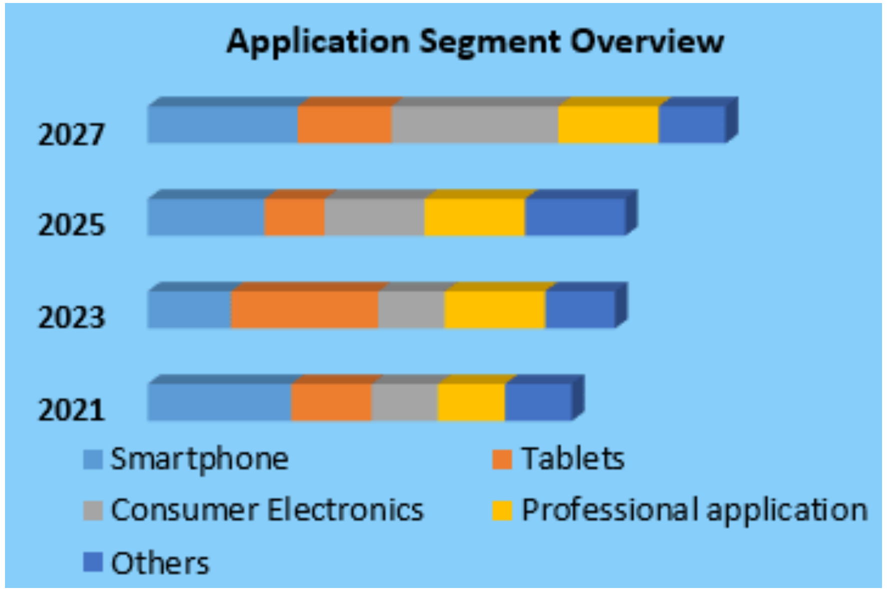


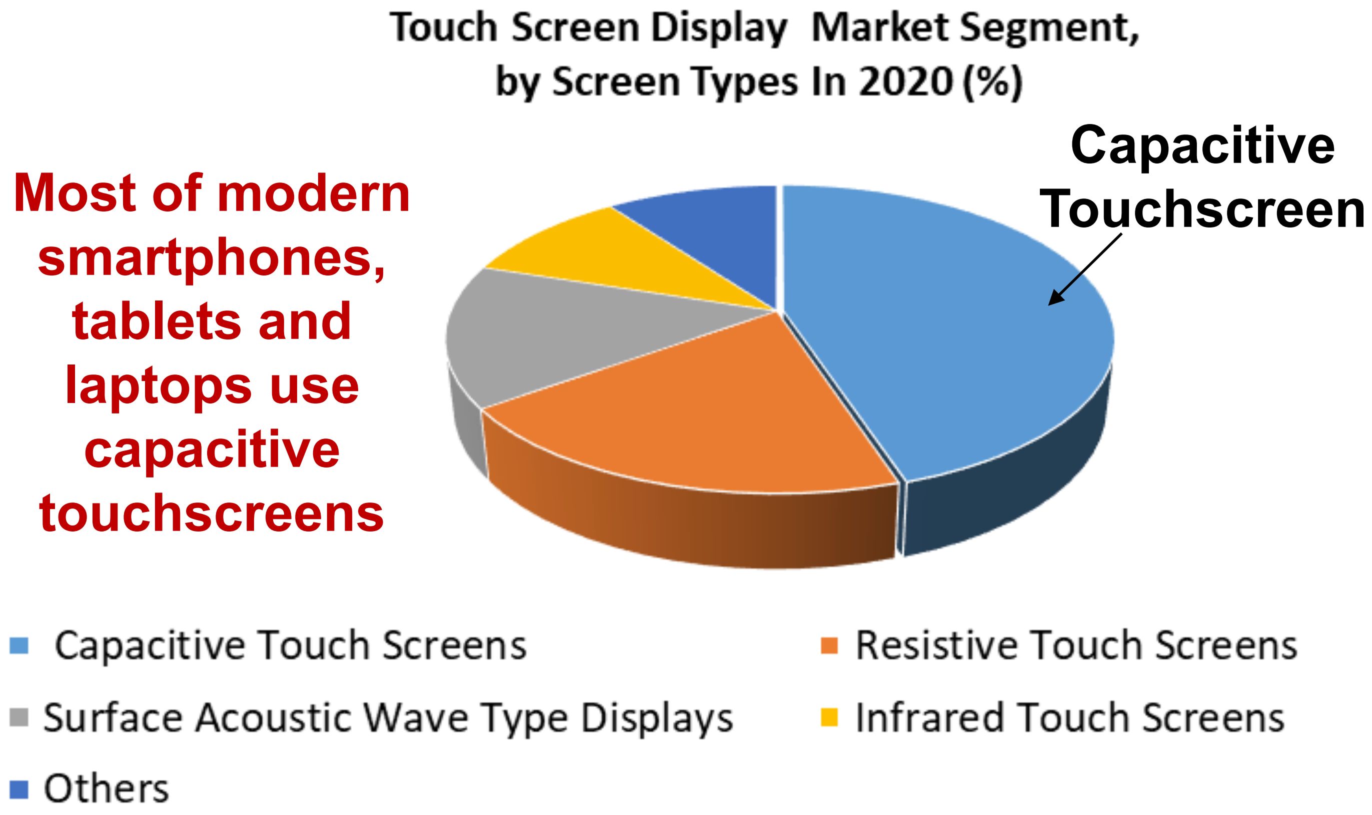
Agenda

- Who we are?
- TL;DR
- How touchscreen works?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

Touchscreen

- Touchscreens Prevail in Modern Portable / Consumer Electronics

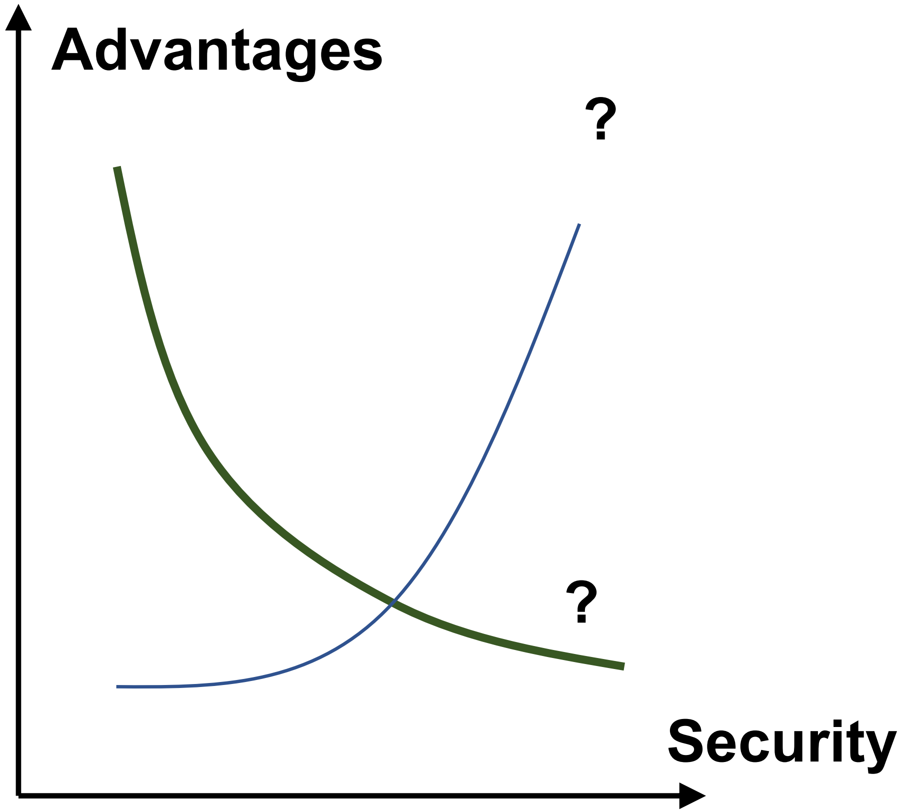




Most of modern smartphones, tablets and laptops use capacitive touchscreens

Capacitive Touchscreen

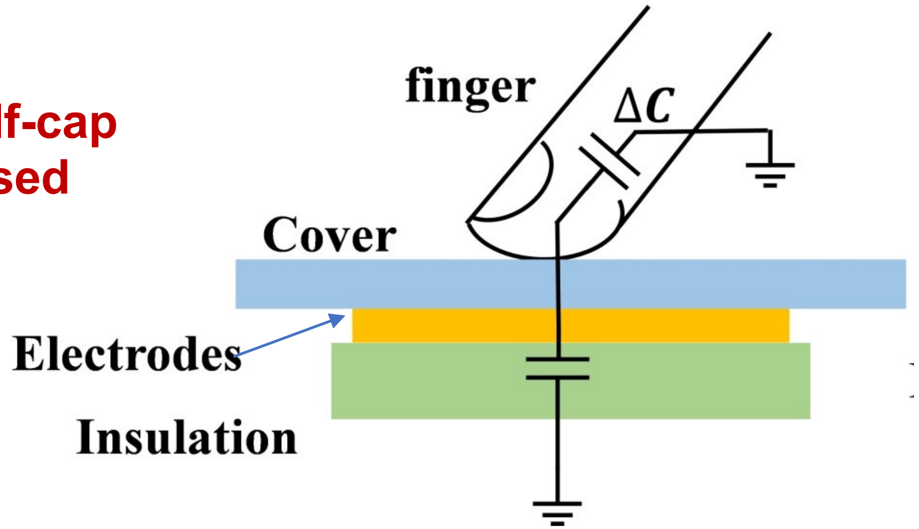
- Advantages
  - Touch operation can be done with fingers, no need for touch pen to cooperate with;
  - Longer life, easy to operate, easy to maintain, wear-resistant, and low-cost;
  - It can support gesture recognition, real-time feedback can be realized when the current of the finger is sensed, without generating a signal through pressure;
  - After the production is completed, you only need to calibrate once.
- Security
  - Content stealing (microphones/EM/mmWave/..)
  - Fault injection? Hmmmm…
    - Tap'n Ghost (S&P), GhostTouch (Usenix)



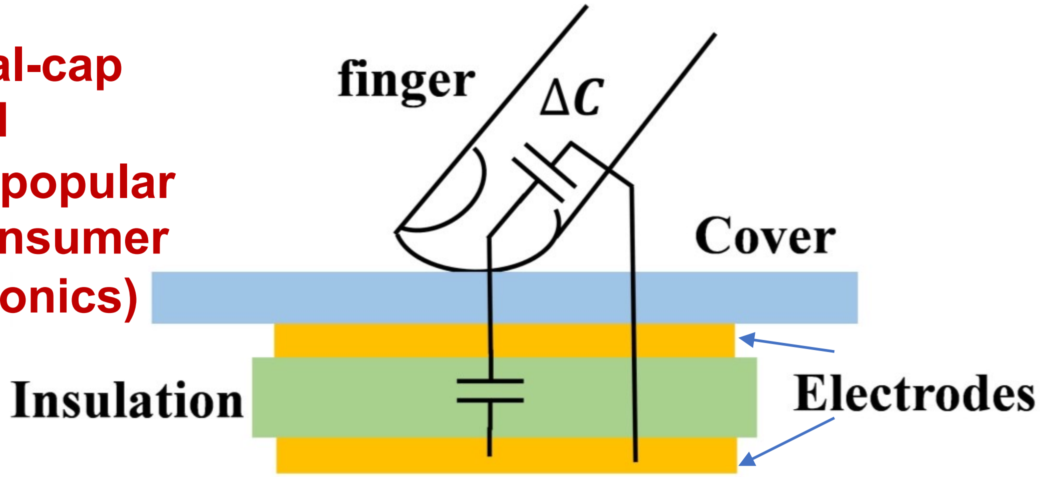
Capacitive Touchscreen

- Self-capacitance based
  - Sense the changes of the capacitance between the electrodes and the ground to register
- Mutual-capacitance based
  - Sense the change of mutual-capacitance between two electrodes to register

Self-cap based

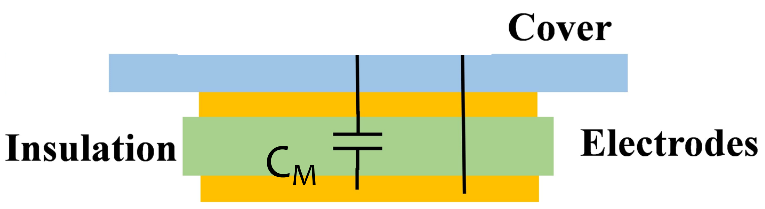


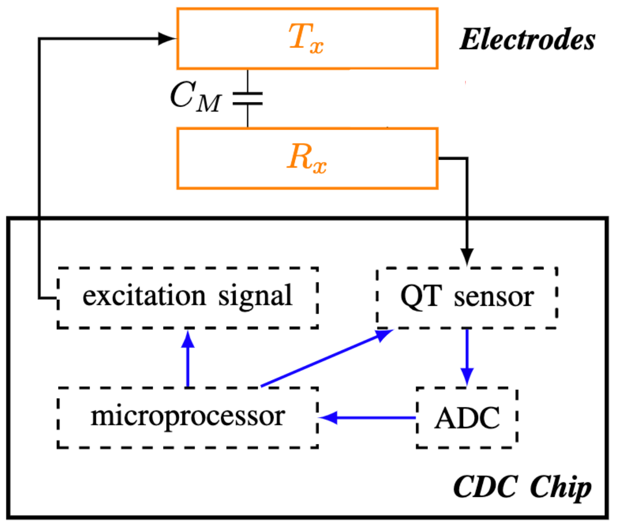
Mutual-cap based (Very popular in consumer electronics)



Capacitive Touchscreen

- Capacitive Touchscreen
  - Self capacitance touchscreen
  - Mutual capacitance touchscreen

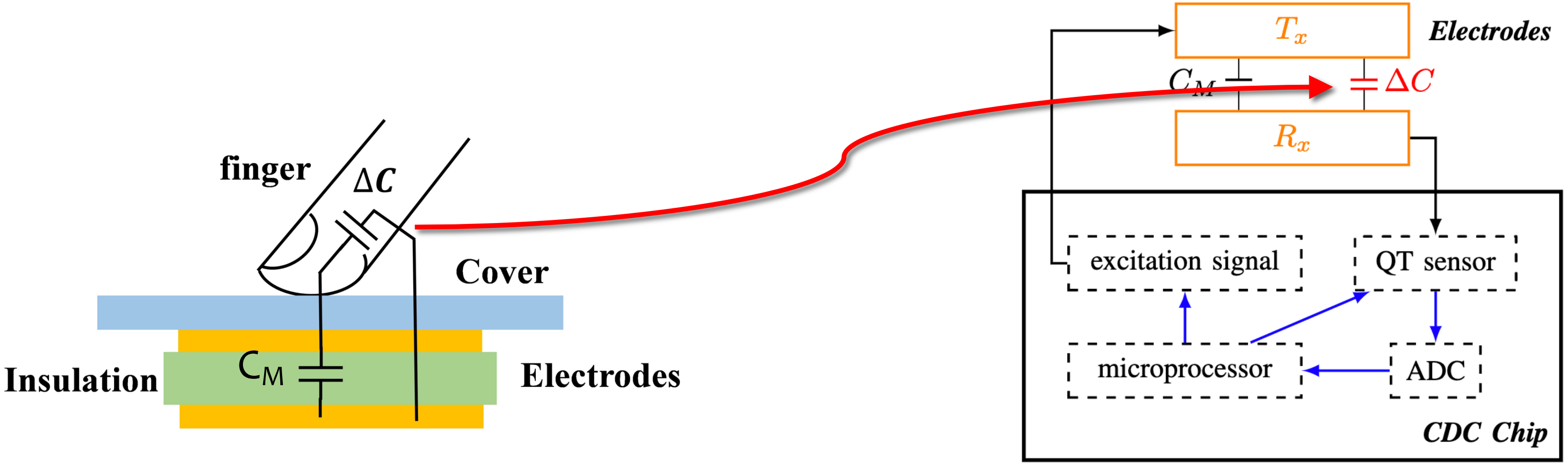




Mutual capacitance touchscreen (no finger)

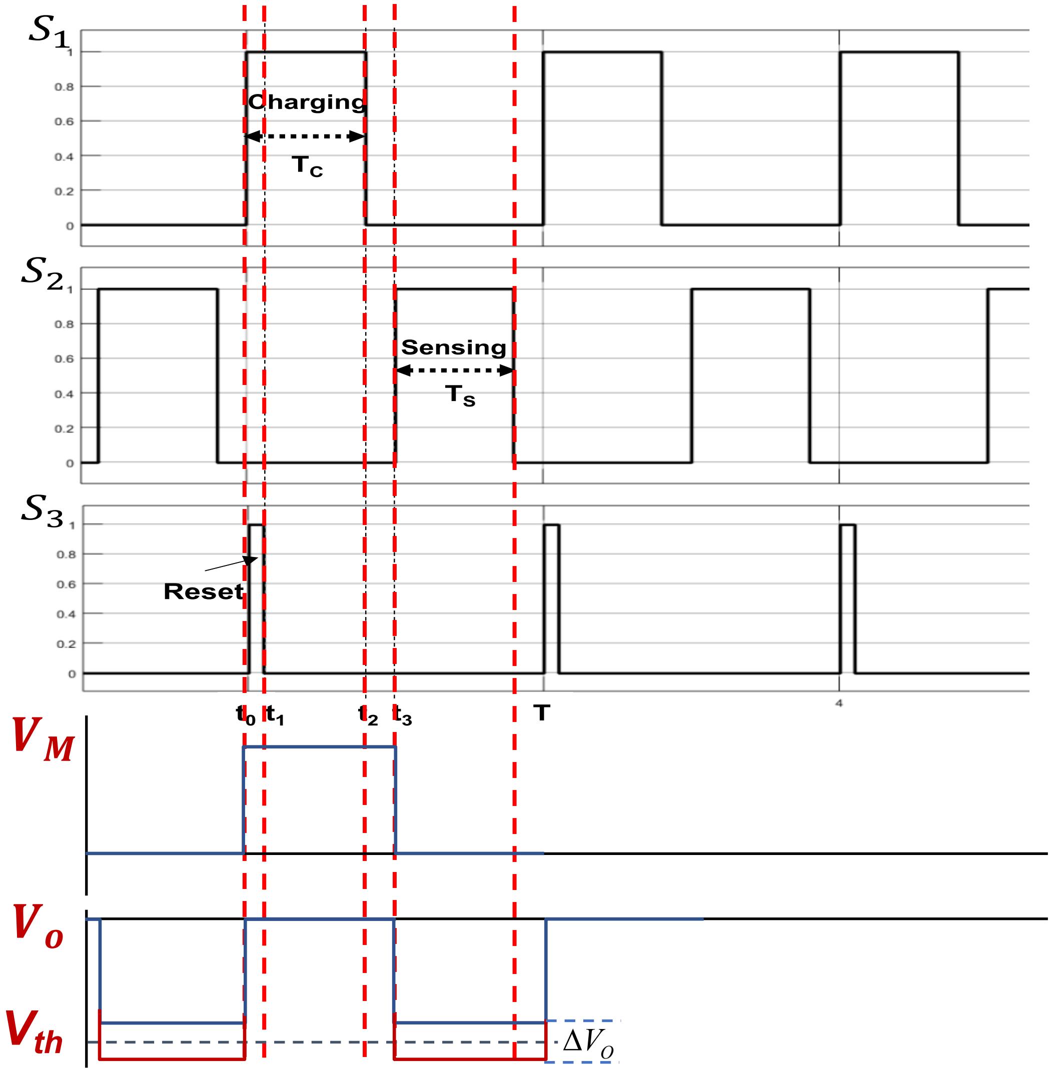
Capacitive Touchscreen

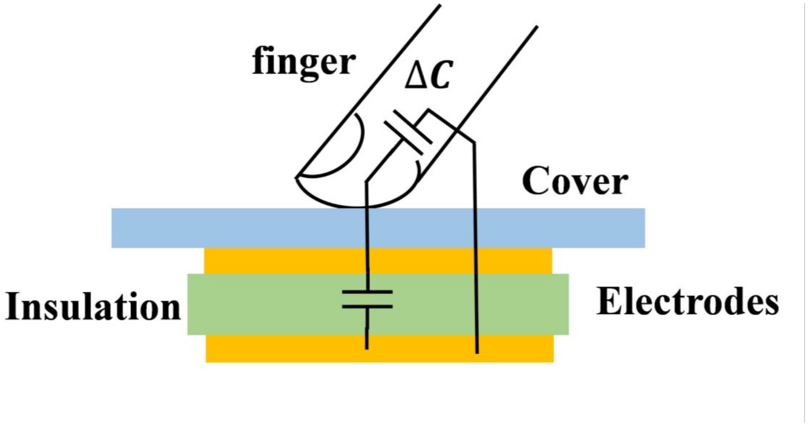
- Capacitive Touchscreen
  - Self capacitance touchscreen
  - Mutual capacitance touchscreen



Mutual capacitance touchscreen (with finger)

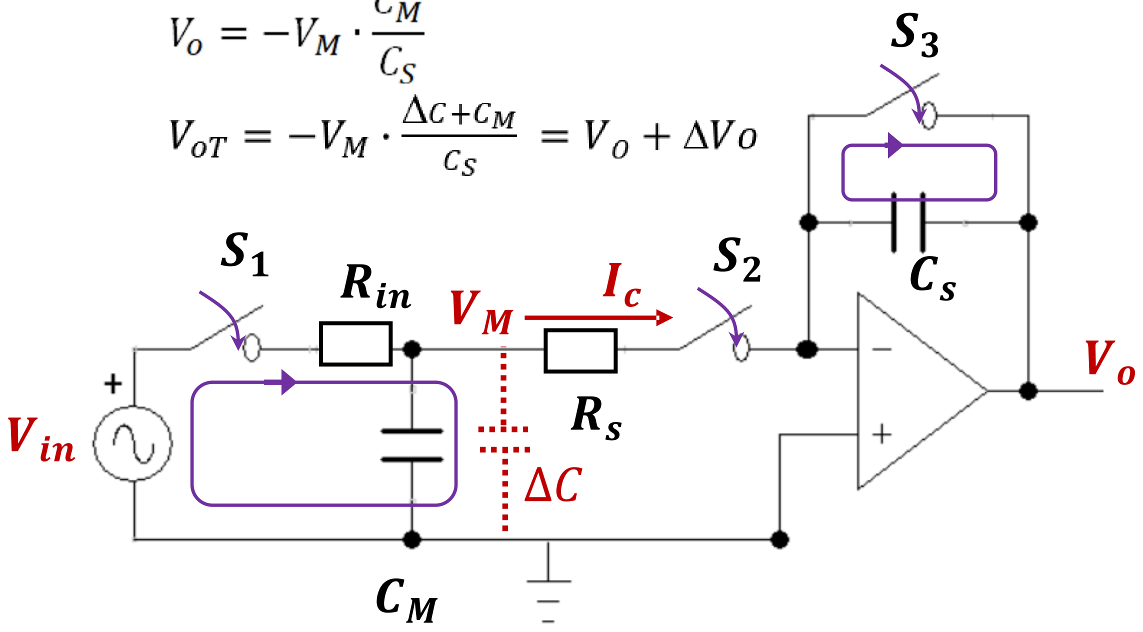
Capacitive Sensing





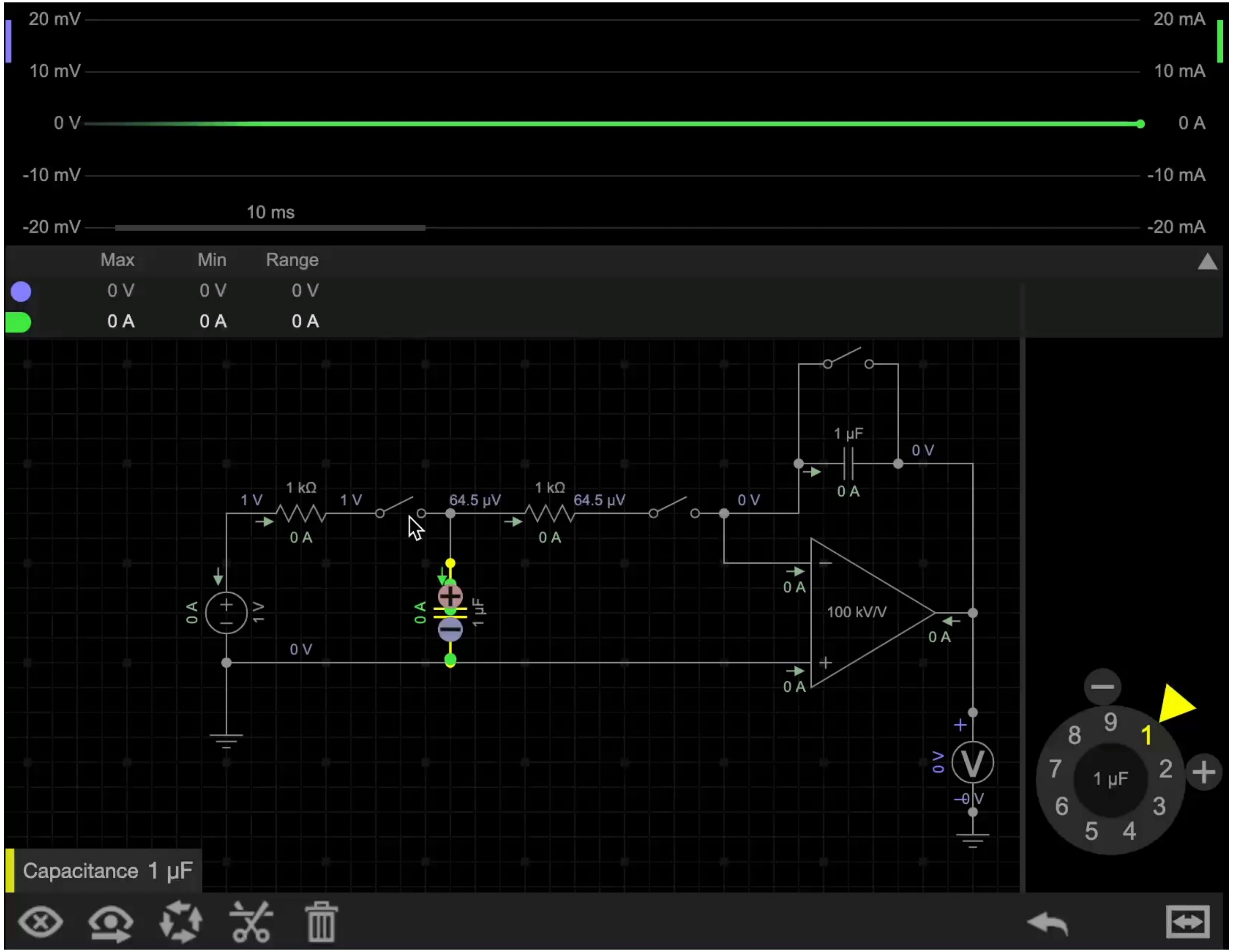
$$V_o = -V_M \cdot \frac{C_M}{C_S}$$

$$V_{oT} = -V_M \cdot \frac{\Delta C + C_M}{C_S} = V_o + \Delta V o$$



Charge transfer topology

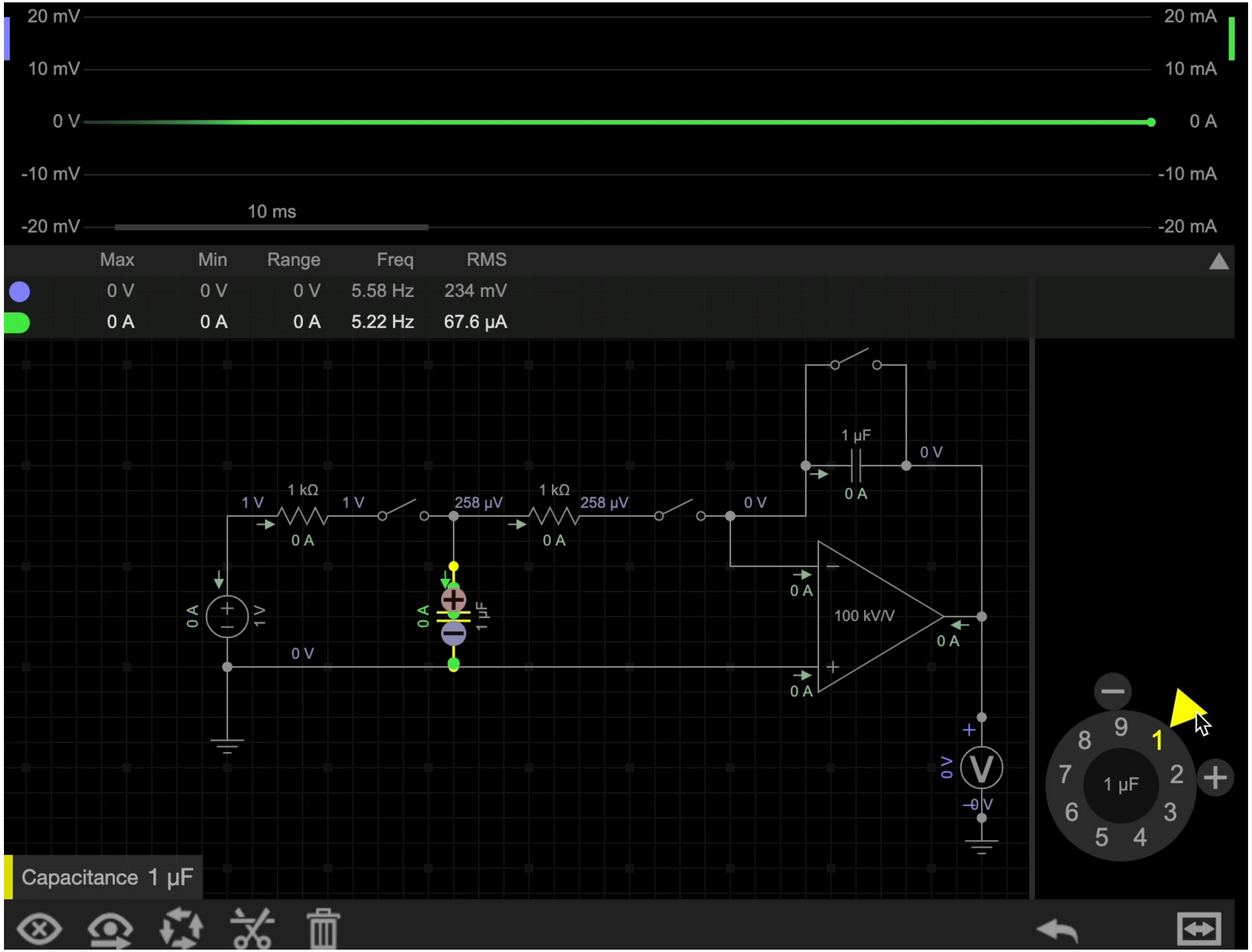
Simplified Touchscreen Design



	Max	Min	Range
●	0 V	0 V	0 V
🟩	0 A	0 A	0 A

Capacitance 1 µF

Simplified Touchscreen Design



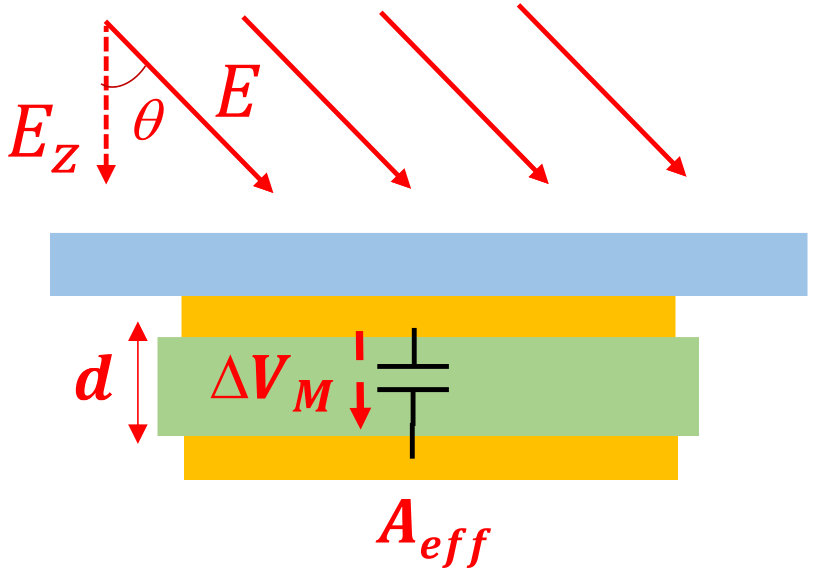
	Max	Min	Range	Freq	RMS
●	0 V	0 V	0 V	5.58 Hz	234 mV
●	0 A	0 A	0 A	5.22 Hz	67.6 μA

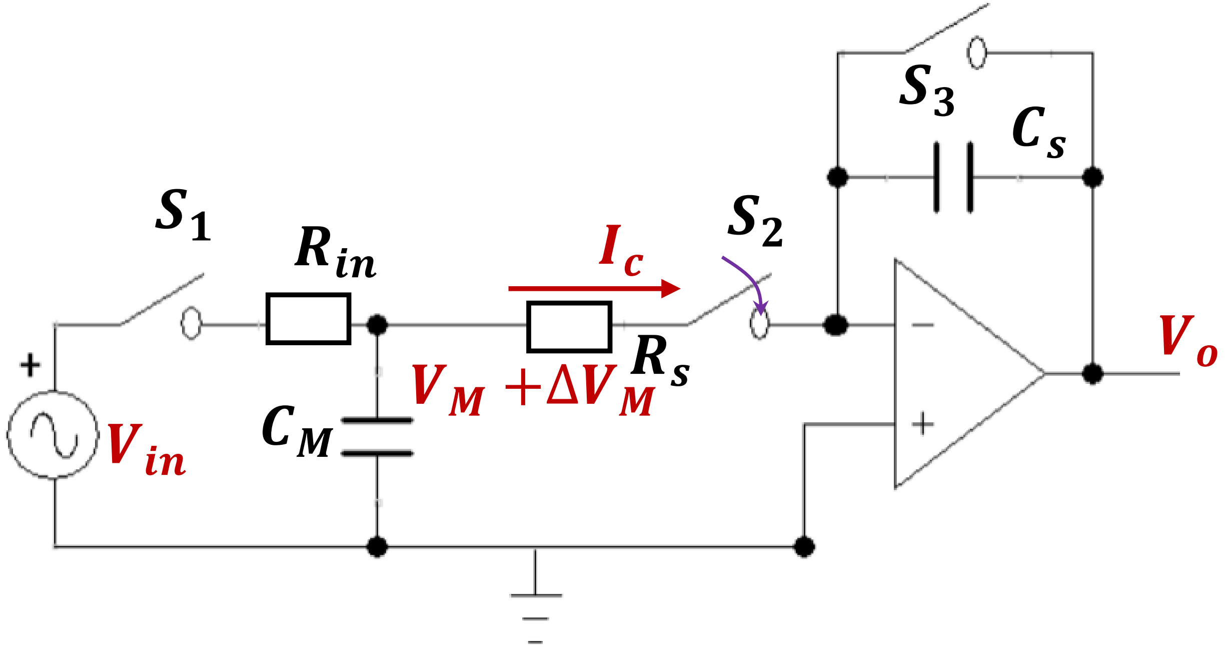
Capacitance 1 μF

Agenda

- Who we are?
- TL;DR
- How touchscreen works?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

Touch Events with IEMI signal



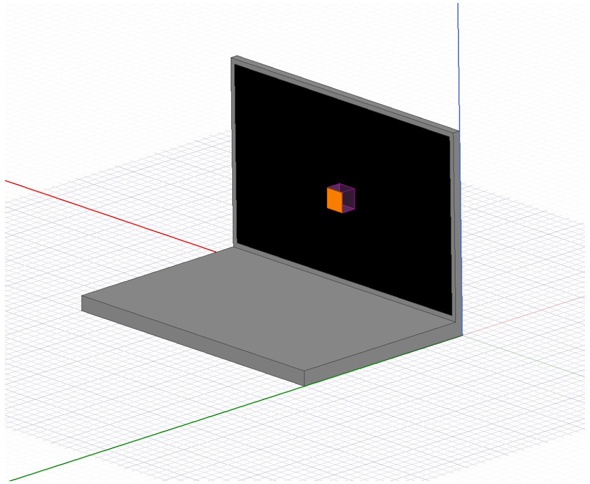


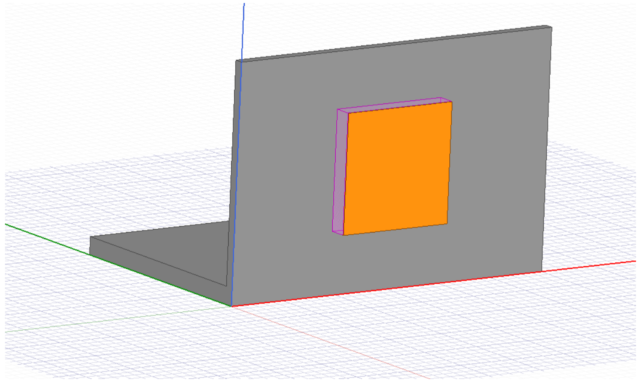
$$\Delta V_M = E_z \cdot d = E \cdot d \cdot \cos\theta$$

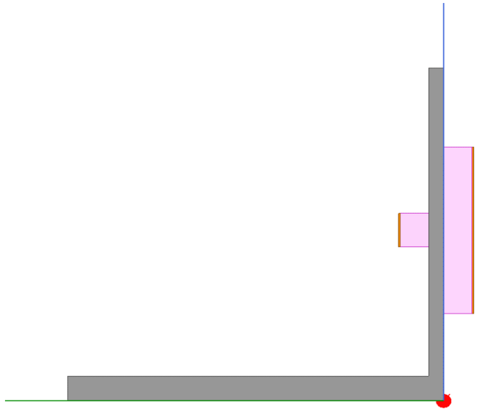
$$V_{oE} = -(V_M + \Delta V_M) \cdot \frac{C_M}{C_S} = V_O + \Delta V o_E$$

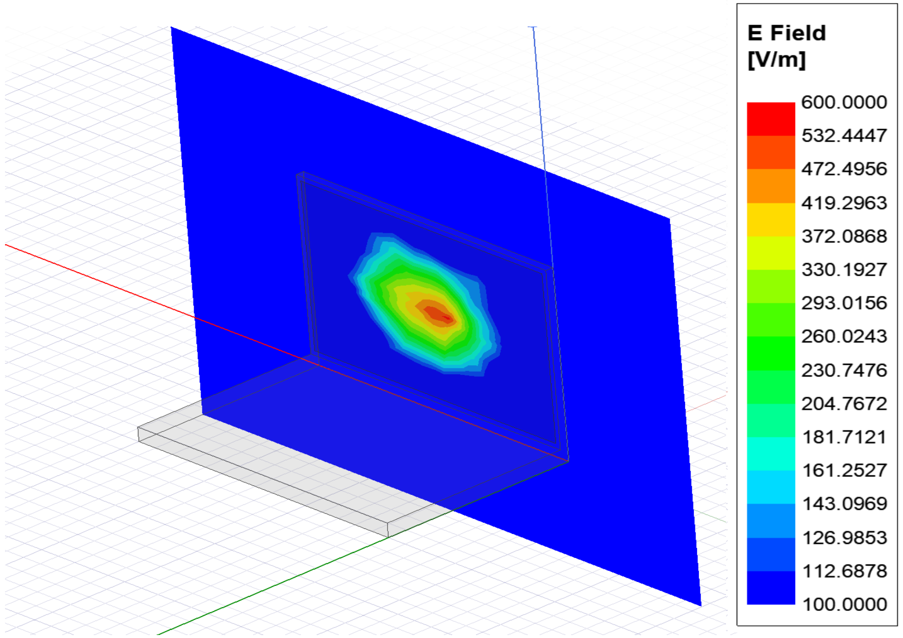
External electric field can lead to increased V_O.

Simulation of External Electric Field

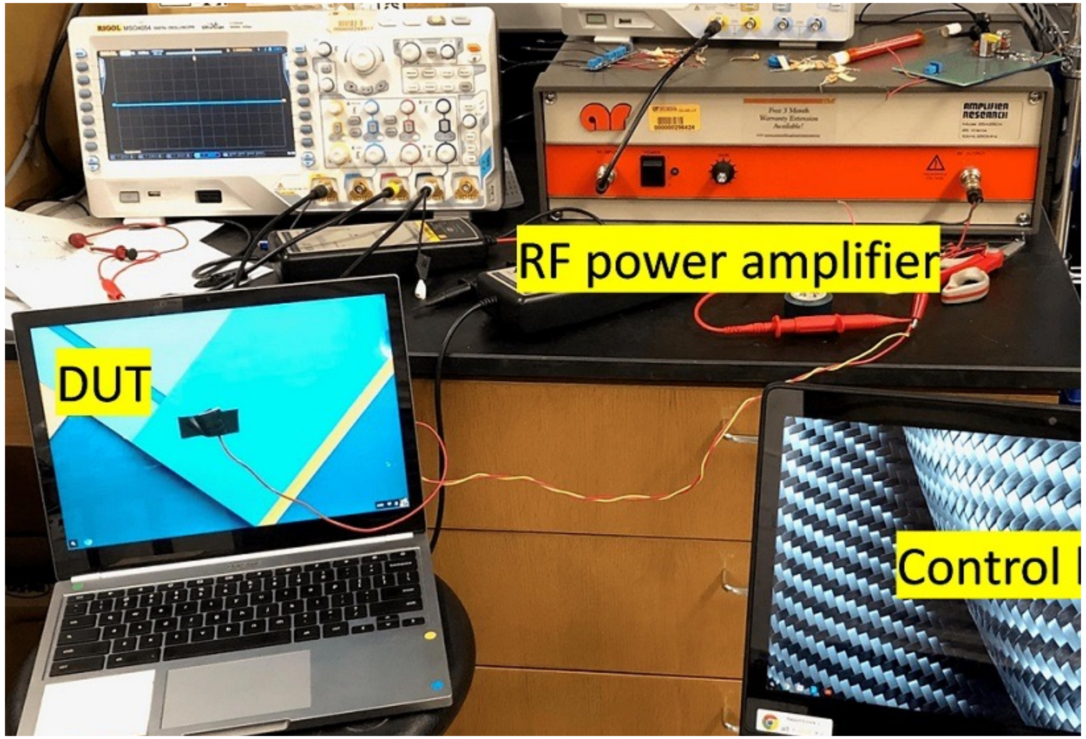




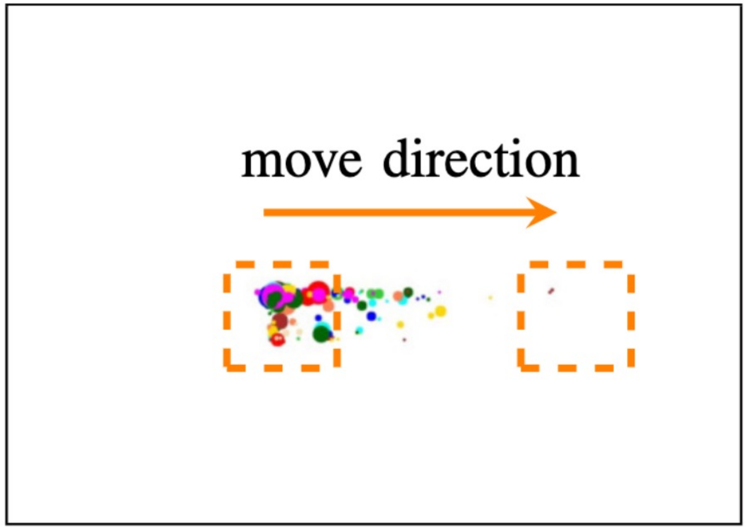


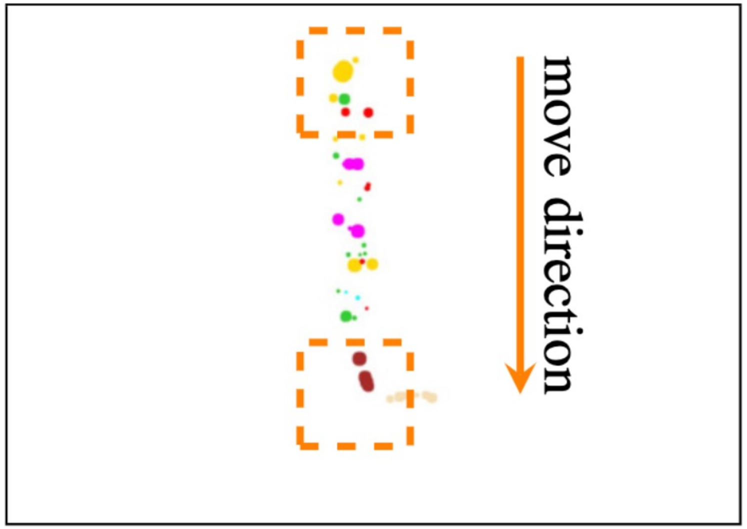


Validation with Preliminary Experiment



Experiment Setup



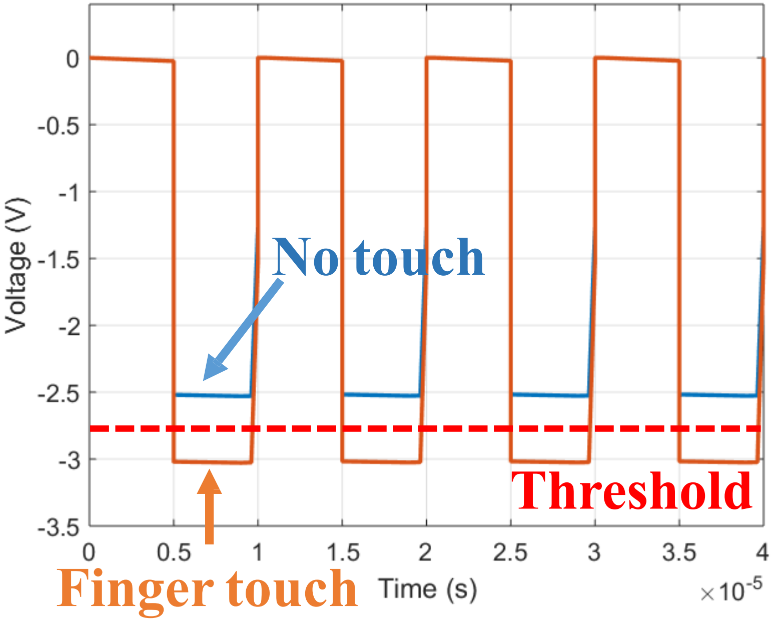


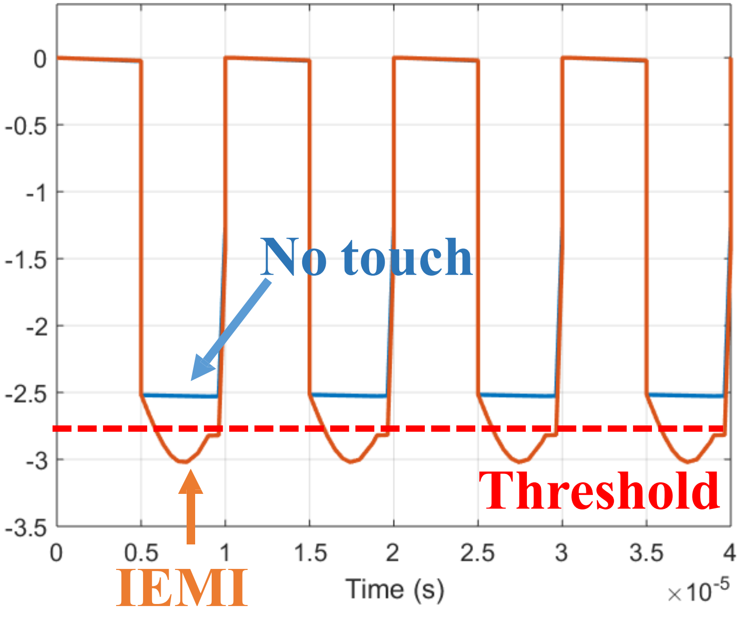
Conditions of Successful Attacks:

- Minimum Electric strength **E_{Zm}**

$$E_{Zm} = \frac{\Delta C_m \cdot V_M}{\varepsilon_r \varepsilon_0 A_{eff}}$$

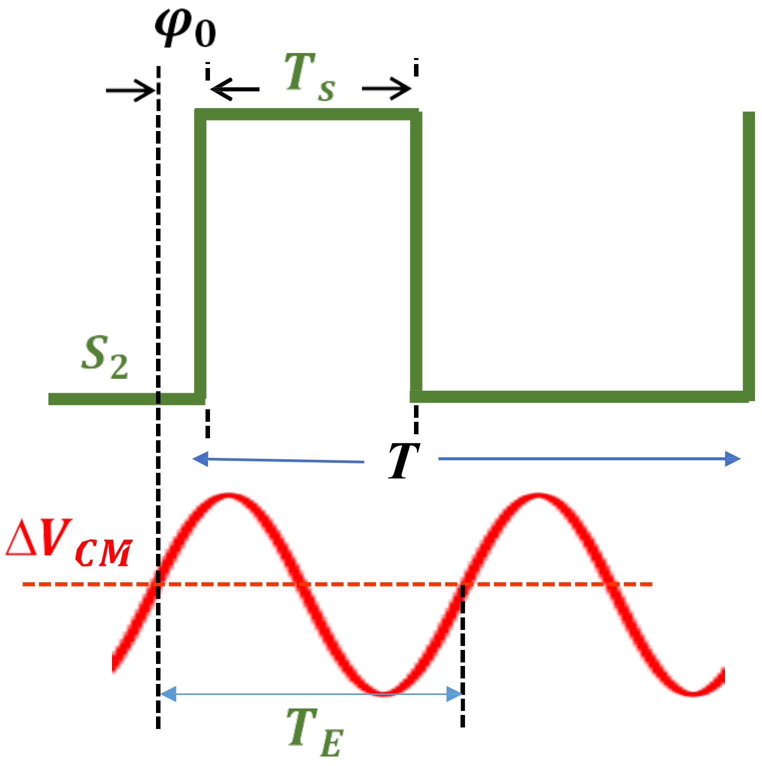
$$E_{Zm} = \frac{C_s \cdot V_{th}}{C_M \cdot d}$$





Conditions of Successful Attacks

- Electric field frequency f_E



The duty cycle D_S is defined as T_S/T, where $T=1/f$ is the period of one full touch sensing

$$\Delta V_{OE} = -\frac{\Delta V_M C_M}{C_S}[\sin(2\pi f_E \cdot T_s + \varphi_0) - \sin\varphi_0]$$

$$\Downarrow$$

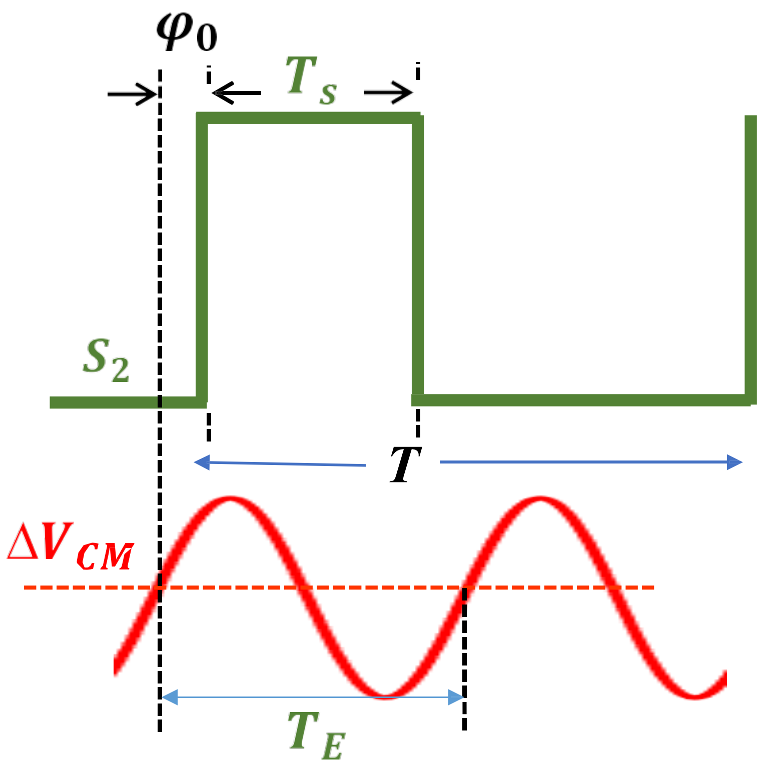
$$\Delta V_{OE} = -\frac{\Delta V_M C_M}{C_S}\left[\sin\left(2\pi D_s \frac{f_E}{f} + \varphi_0\right) - \sin\varphi_0\right]$$

At f_{Emin}, external E-field has no impact:

$$f_{Emin} = \frac{kf}{D_s} \qquad k=1,2,3,4\ldots.$$

Conditions of Successful Attacks

- Minimum required Electric strength at frequency **f_{Emax}**



The duty cycle D_S is defined as T_S/T, where $T=1/f$ is the period of one full touch sensing

$$\Delta V_{OE} = -\frac{\Delta V_M C_M}{C_s}\sum_0^M \left[\sin\left(2\pi D_s\frac{f_E}{f} + \varphi_M\right) - \sin\varphi_M\right]$$

$$\varphi_M = \varphi_0 + 2\pi M \cdot \frac{f_E}{f}$$

Condition 1: frequencies

$$f_E = nf \quad n=0,1,2,3\ldots$$

Condition 2a: The phase angle $\varphi_0=3\pi/2$.

$$f_{Emax} = \frac{f}{4D_S} + \frac{kf}{D_S} \quad k=0,1,2,3\ldots$$

Condition 2b: The phase angle $\varphi_0=\pi/2$.

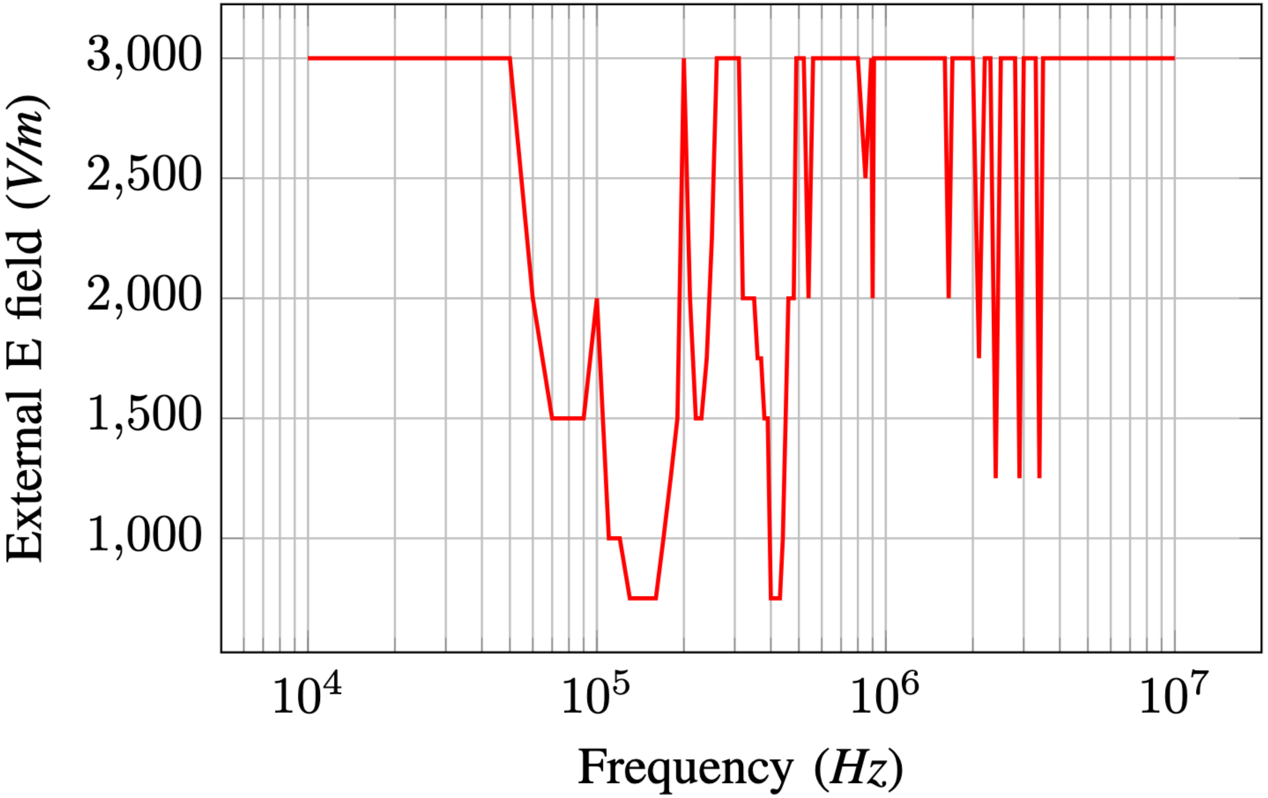
$$f_{Emax} = \frac{3f}{4D_S} + \frac{kf}{D_S} \quad k=0,1,2,3\ldots$$

Theory Validation

Calculated:

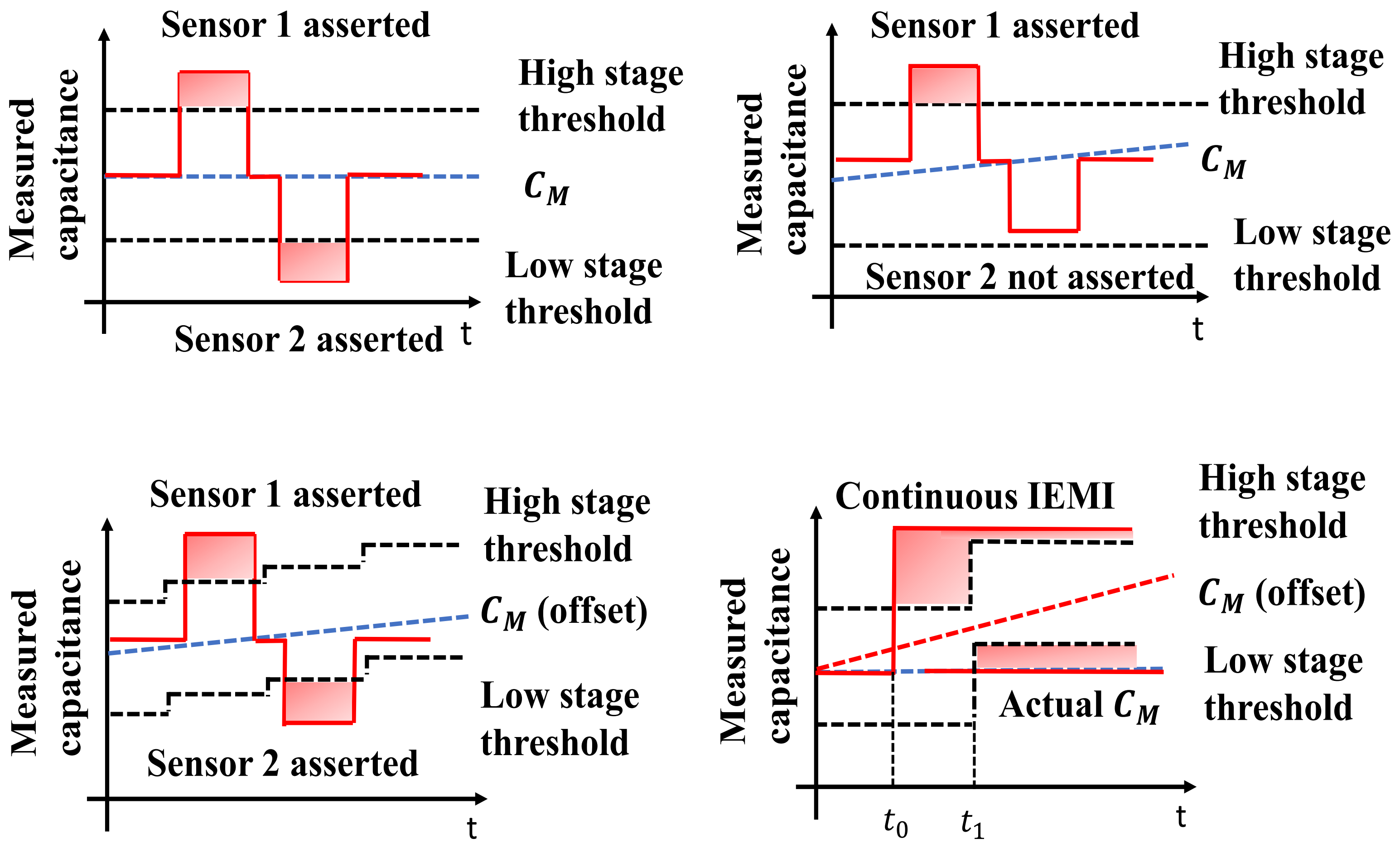
$$f_{Emax} = 140\ kHz, 420\ kHz, 700\ kHz, 980\ kHz$$
$$f_{Emin} = 560\ kHz, 1120\ kHz$$

Measured minimum E-field leading to false touches



Conditions of Successful Attacks

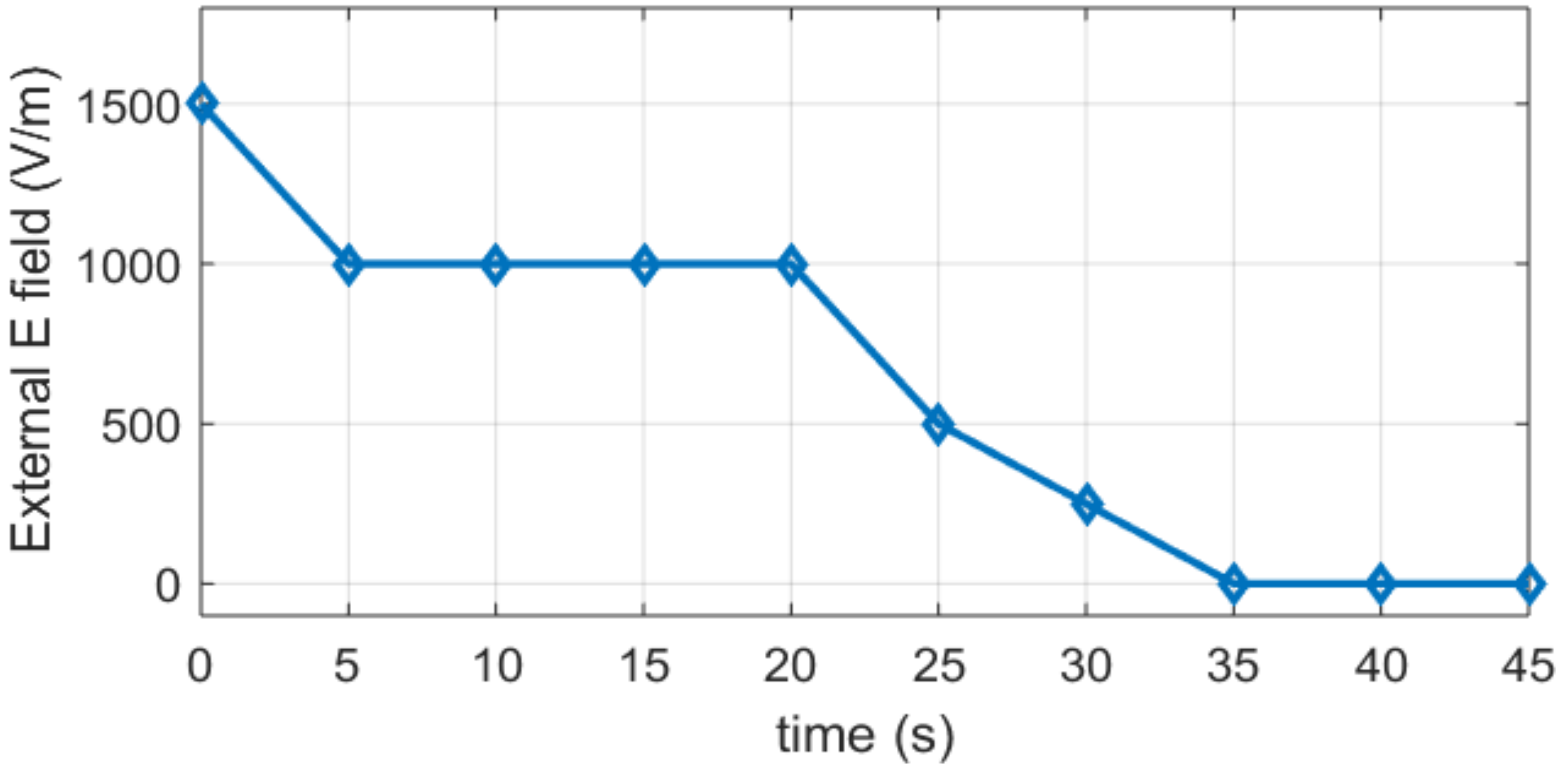
Environmental calibration function:



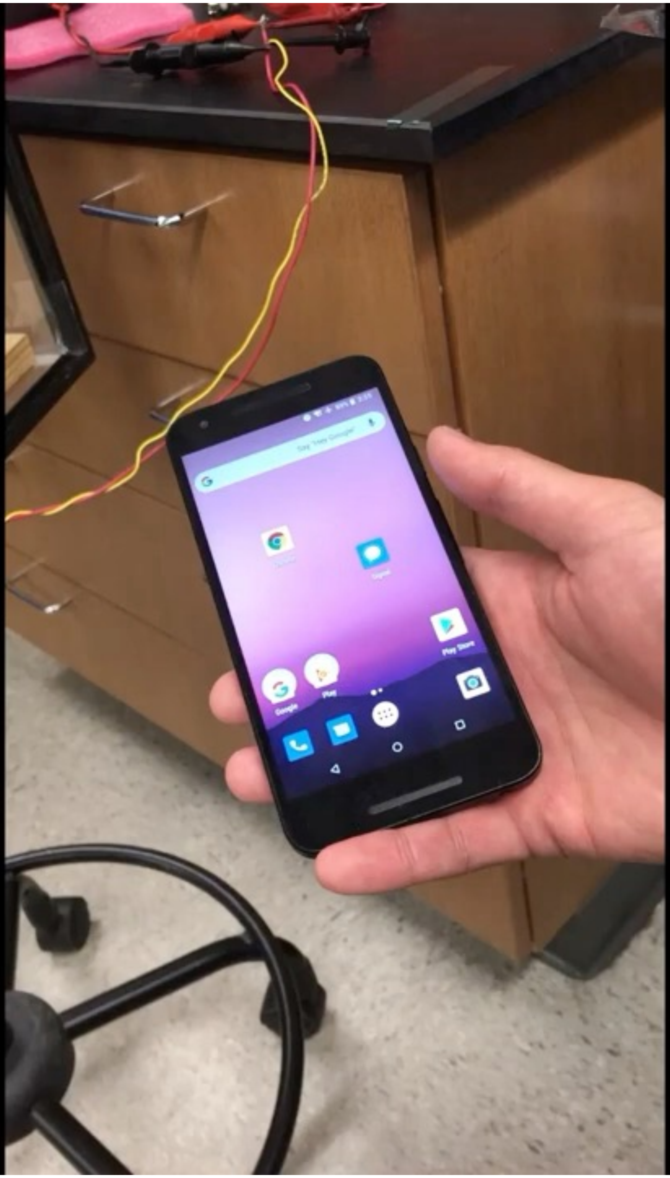
Theory Validation

Impact of environmental calibration as a function of time

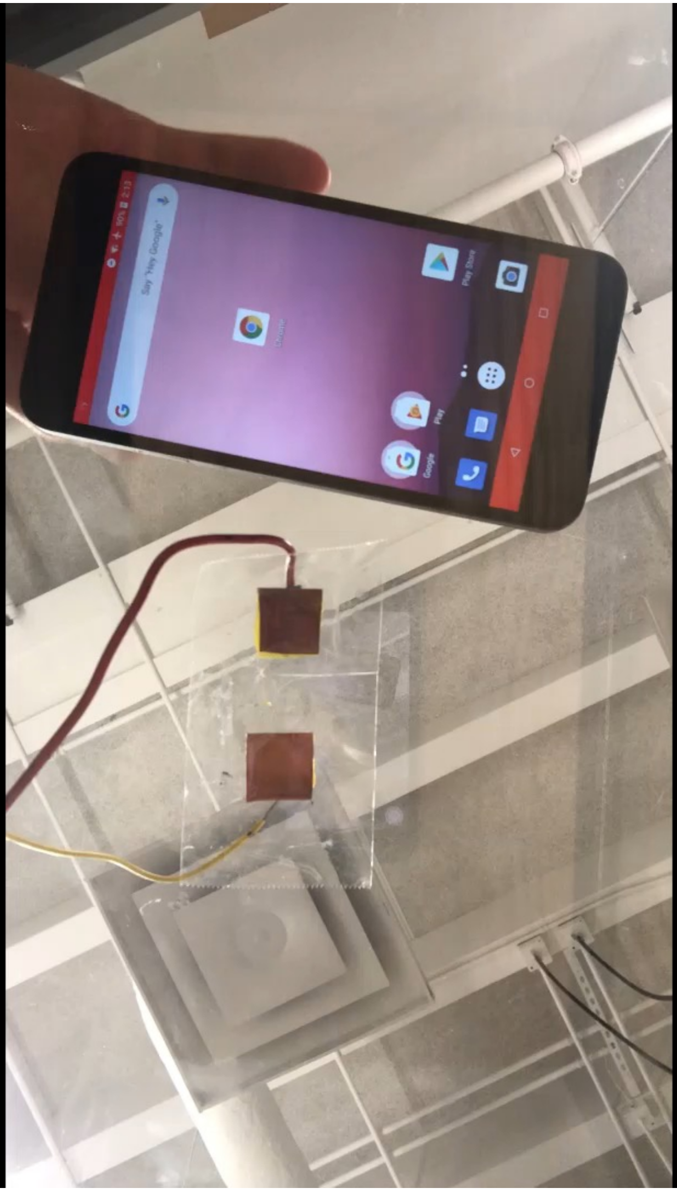
Measured minimum E-field leading to false touches



Open Application with IEMI



Open Website with IEMI



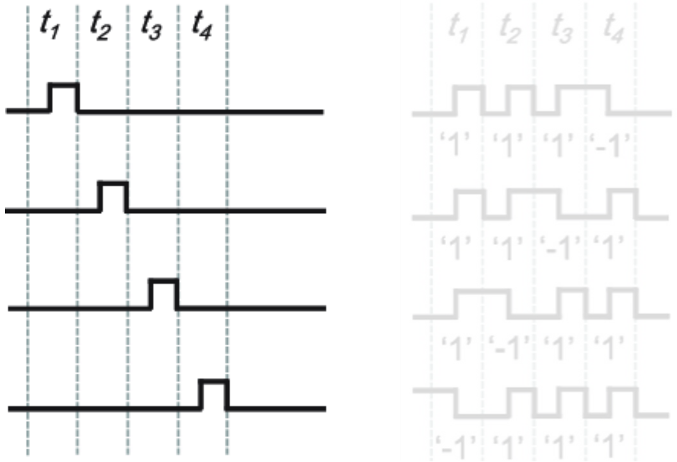
Agenda

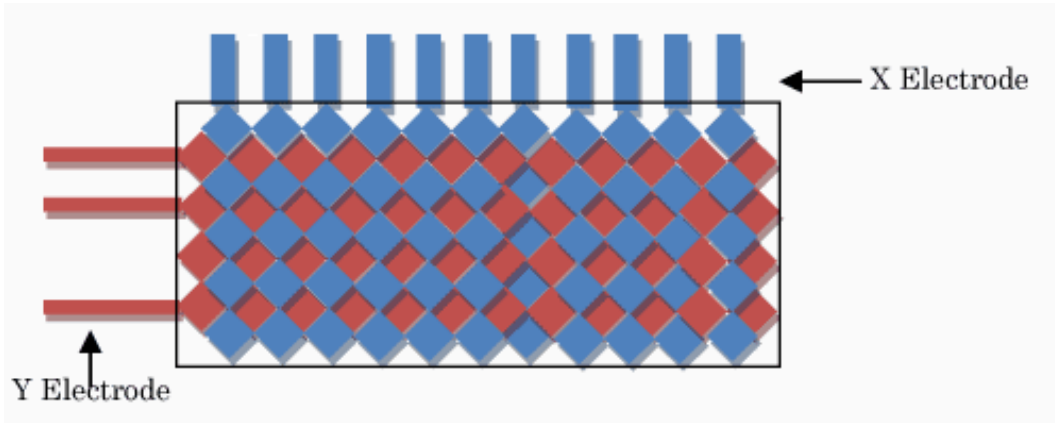
- Who we are?
- TL;DR
- How touchscreen works?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

Precise touch events generation and thorough experiments

Precise Touch Events

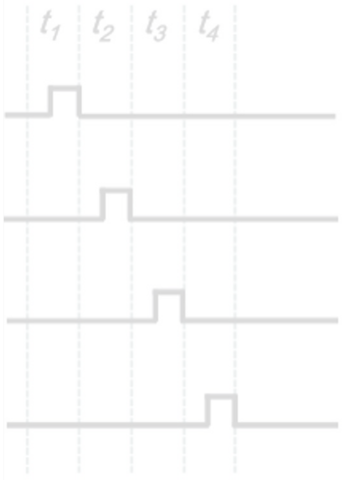
- Challenges?
- Scanning/Driving Methods
  - Sequential scanning
  - Parallel scanning
- Previous approaches

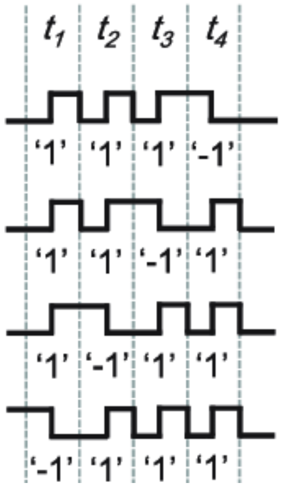


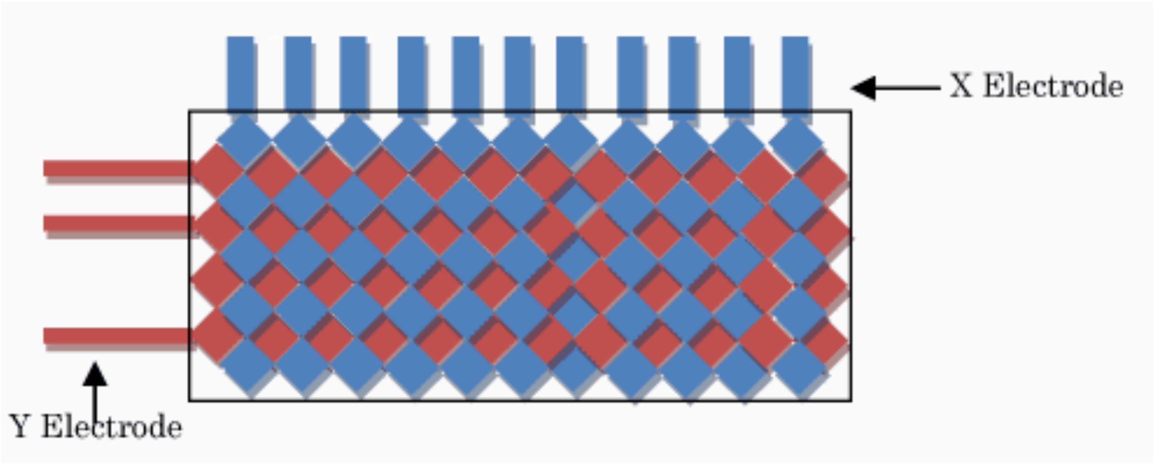


Precise Touch Events

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

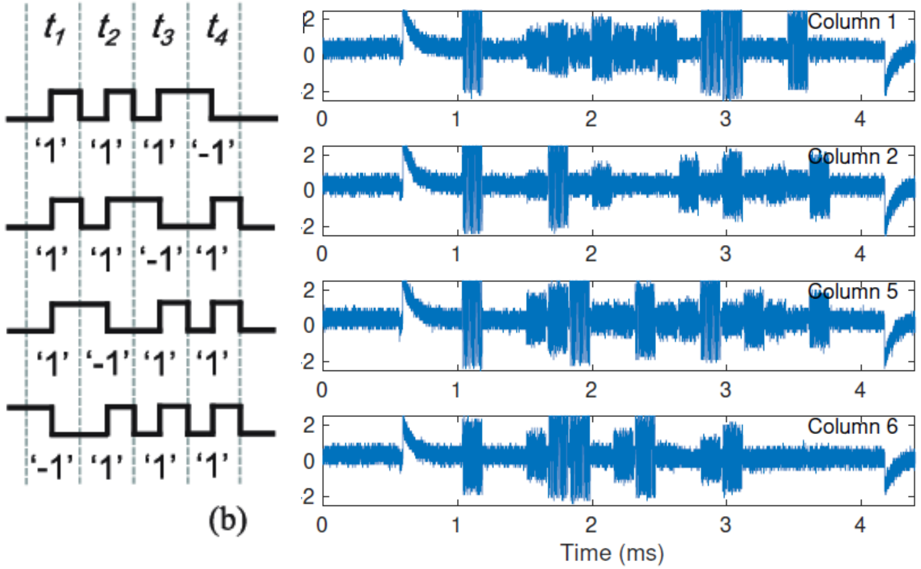




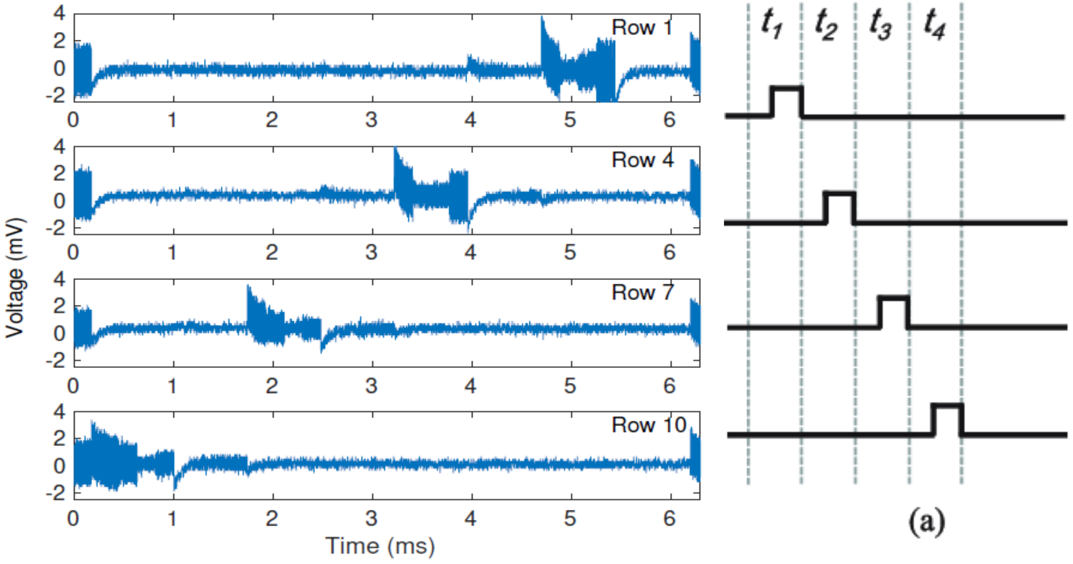


Precise Touch Events

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



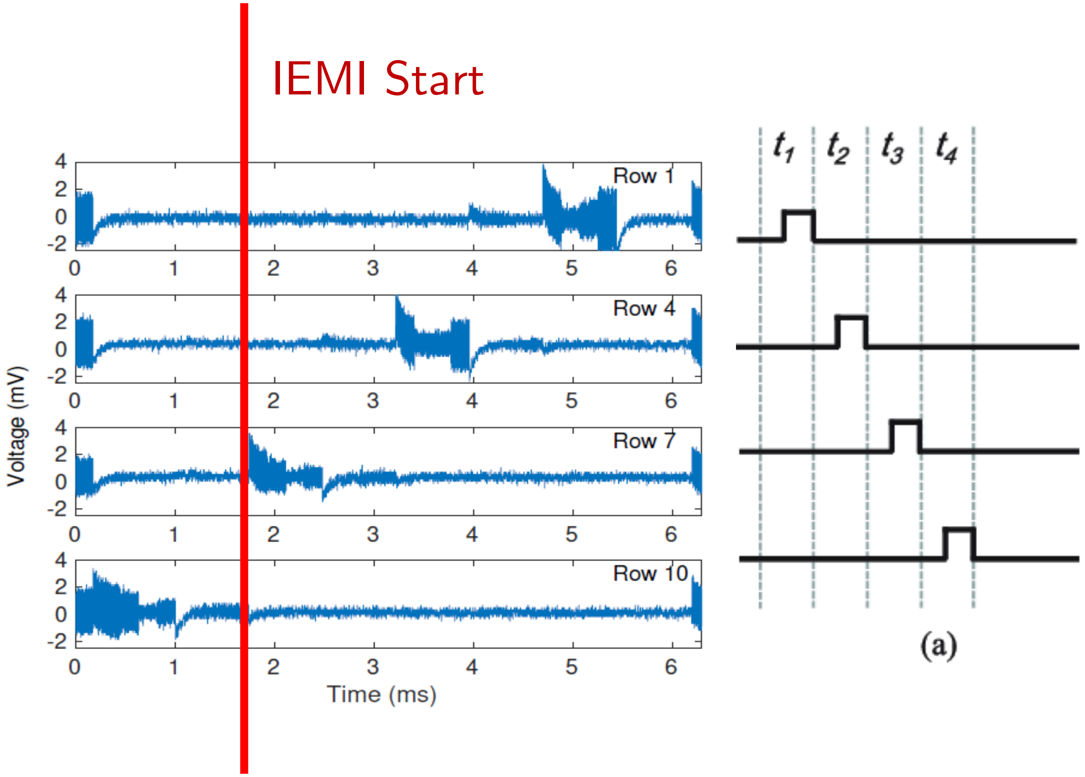
Parallel Driving iPhone 11 Pro



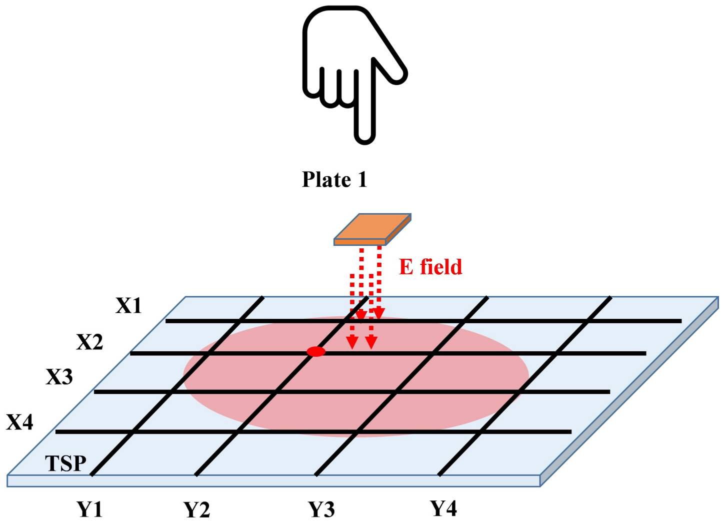
Sequential Driving Pixel 2

Precise Touch Events

- Precise injection time or precise injected location?



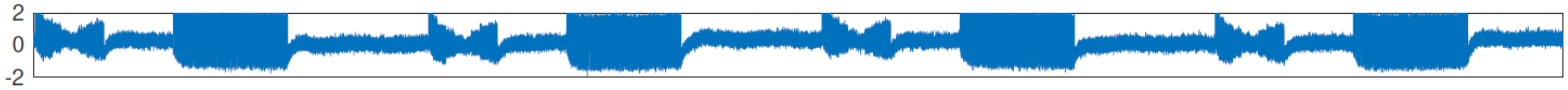
Precise Injection Time



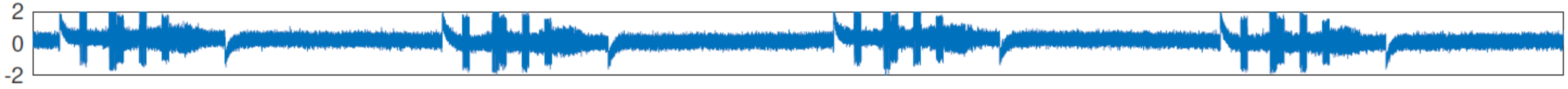
Precise Injection Location

Precise Touch Events

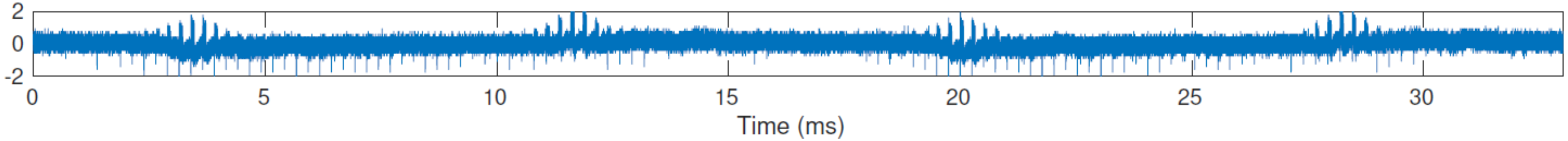
- Challenges from different scanning mechanism (measured on different target devices)



Pixel 2 Touchscreen Driving Signal



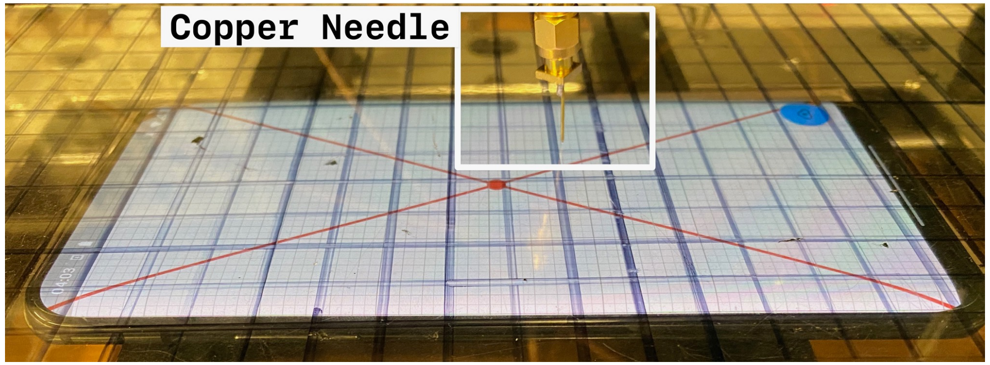
iPhone 11 Pro Touchscreen Driving Signal



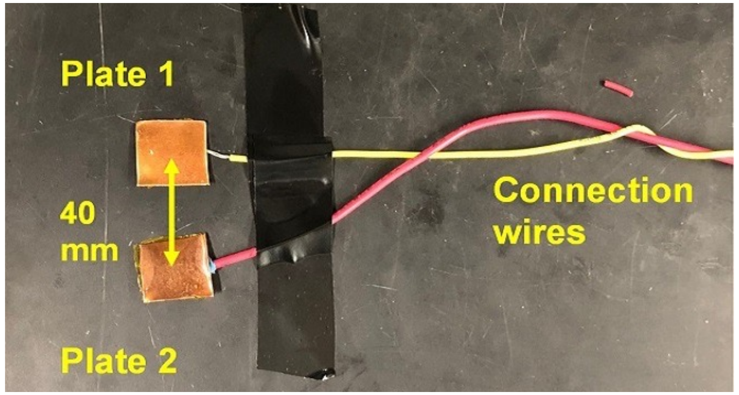
Nexus 5X Touchscreen Driving Signal

Antenna design

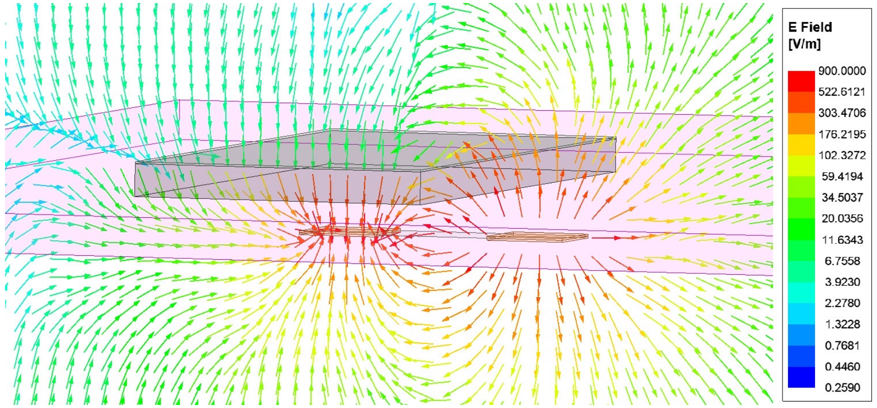
- Spring loaded copper needle vs copper plate



Copper Needle



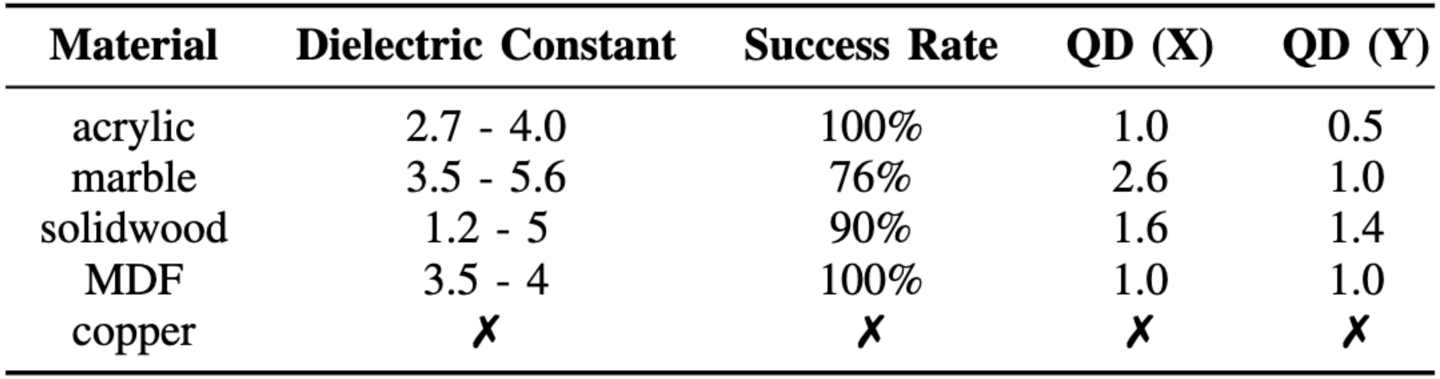
Copper Plates



Copper Plates Antenna E-Field Simulation

Table Material

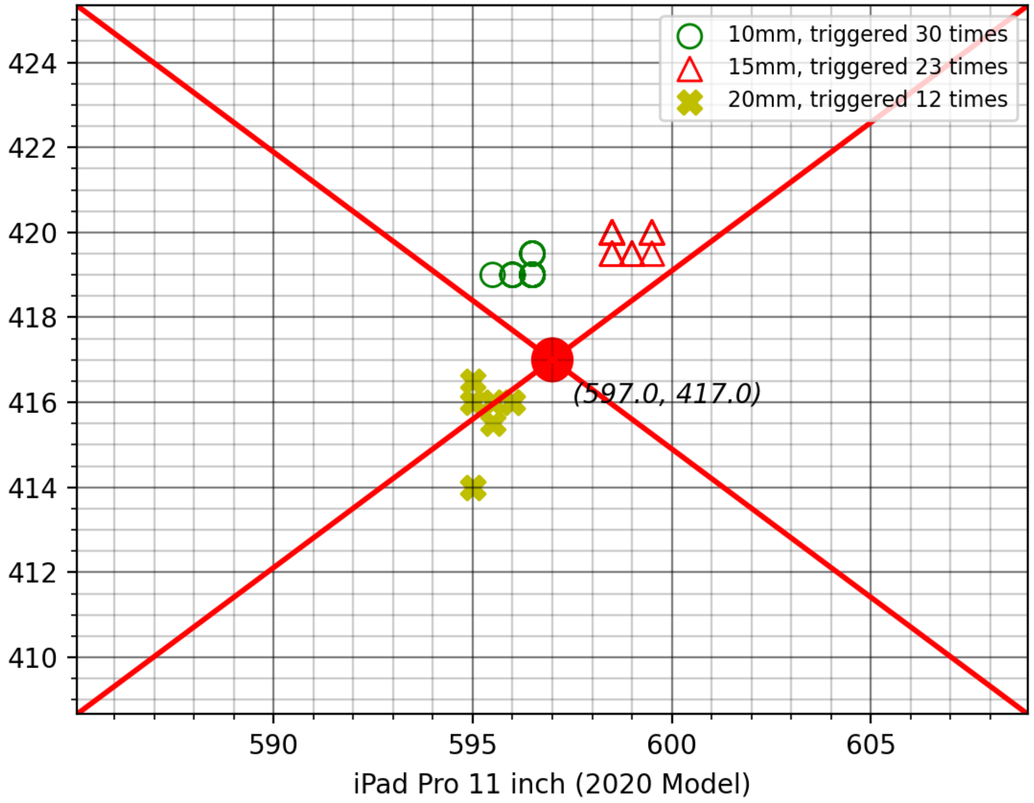
- Common material
  - Medium density fiberboard(MDF)
  - Solid wood
  - Acrylic
  - Marble
  - Copper
- Difference?
  - Dielectric Constant



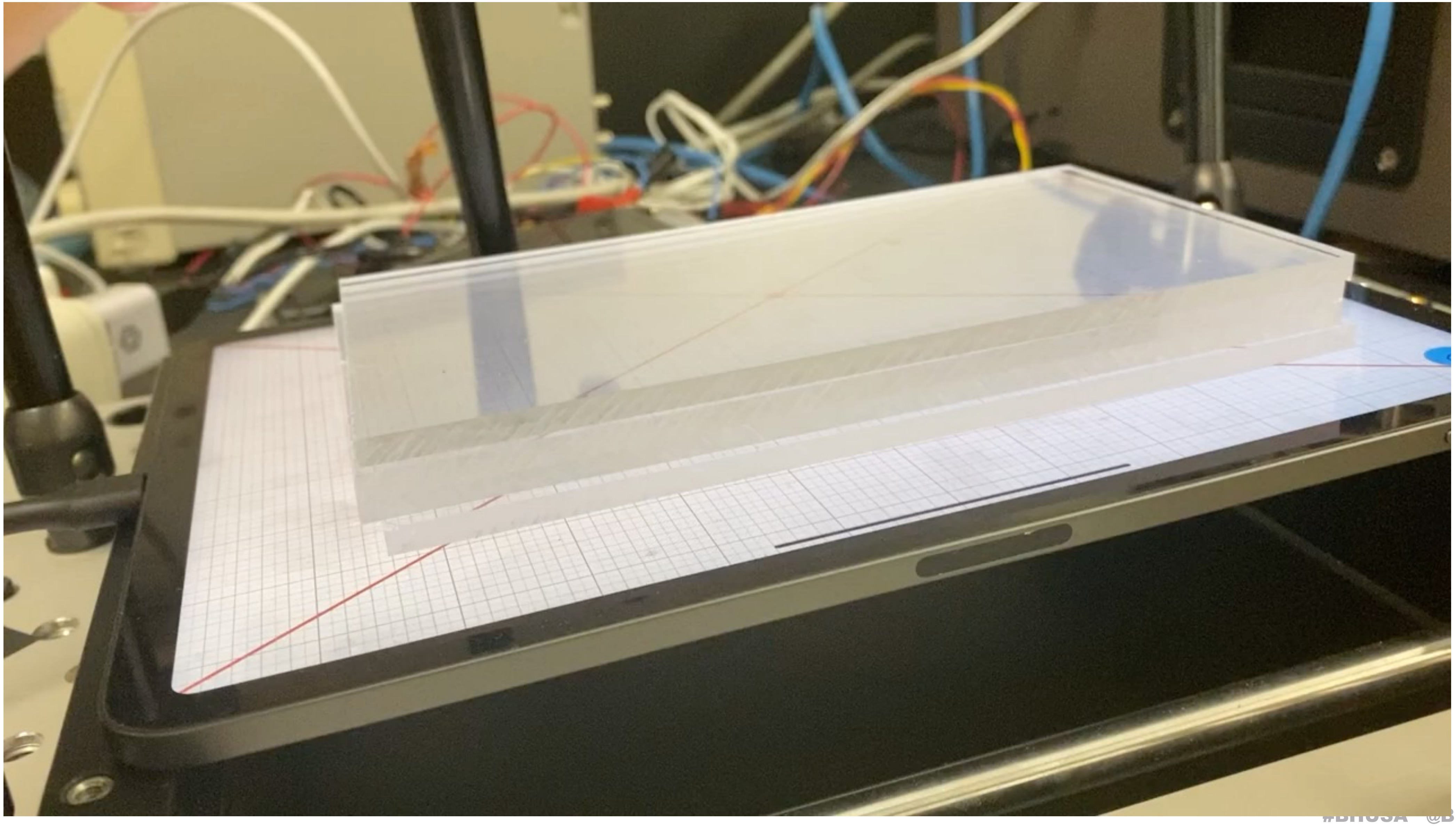
Material	Dielectric Constant	Success Rate	QD (X)	QD (Y)
acrylic	2.7 - 4.0	100%	1.0	0.5
marble	3.5 - 5.6	76%	2.6	1.0
solidwood	1.2 - 5	90%	1.6	1.4
MDF	3.5 - 4	100%	1.0	1.0
copper	✗	✗	✗	✗

Table Thickness

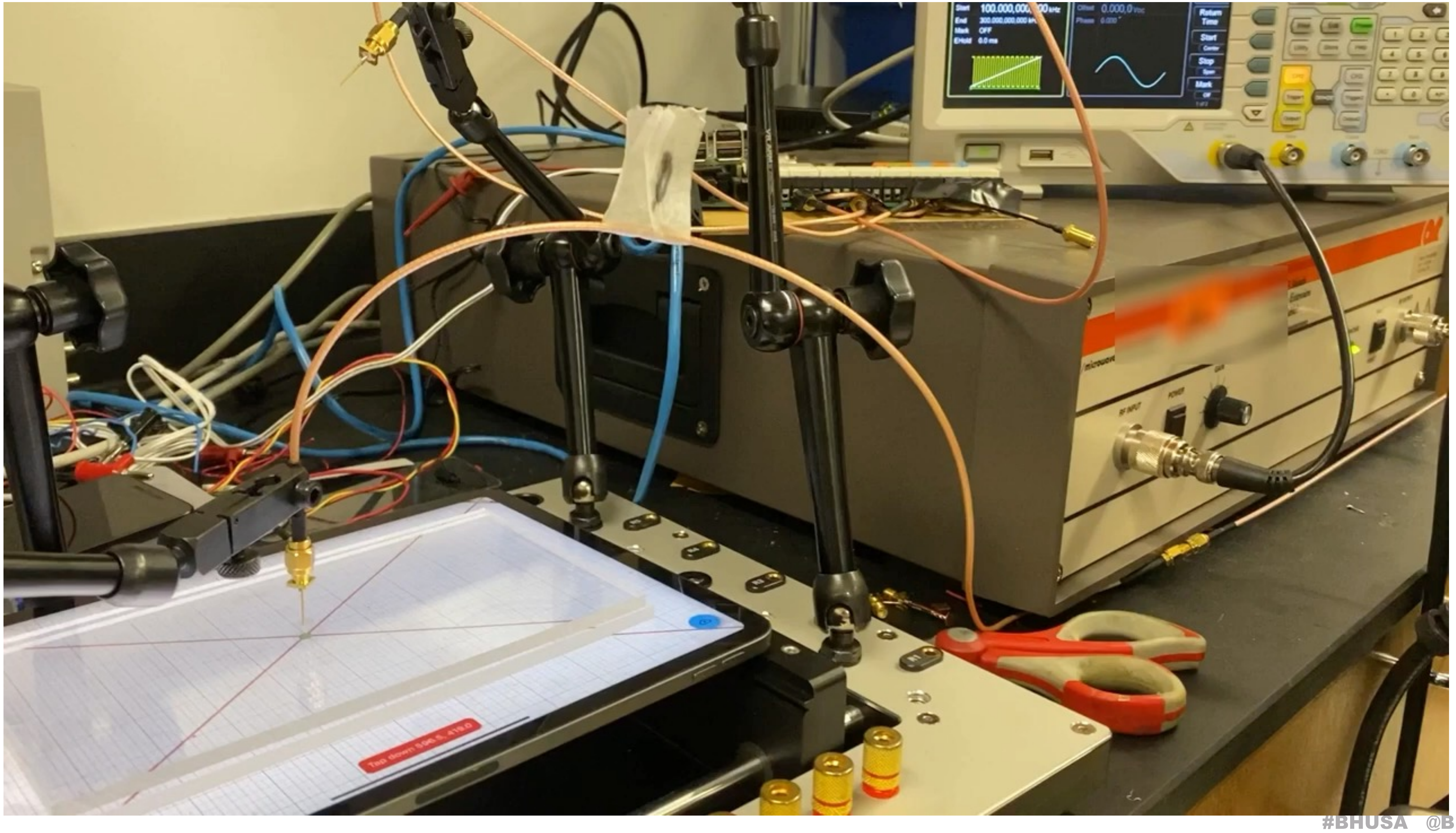
- Importance of the tabletop thickness
  - Finger size copper plate antenna
  - Acrylic sheet
  - iPad Pro
  - Repeat 30 times
  - 40% success rate
- Real tabletop thickness
  - 1/2 inch, 5/8 inch



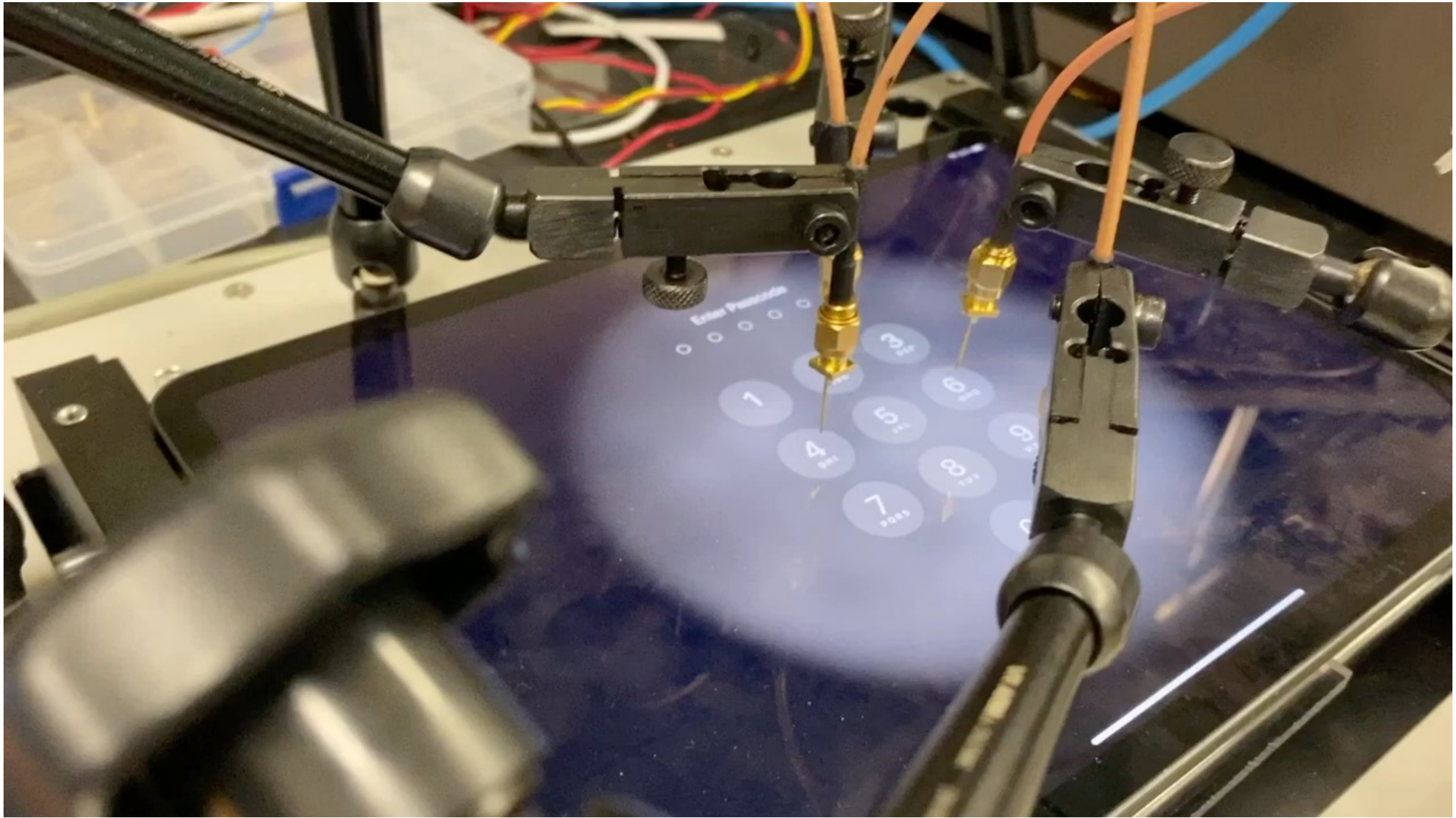
Precise Touch Injection (2cm away)



Stable Repeatable Clicks

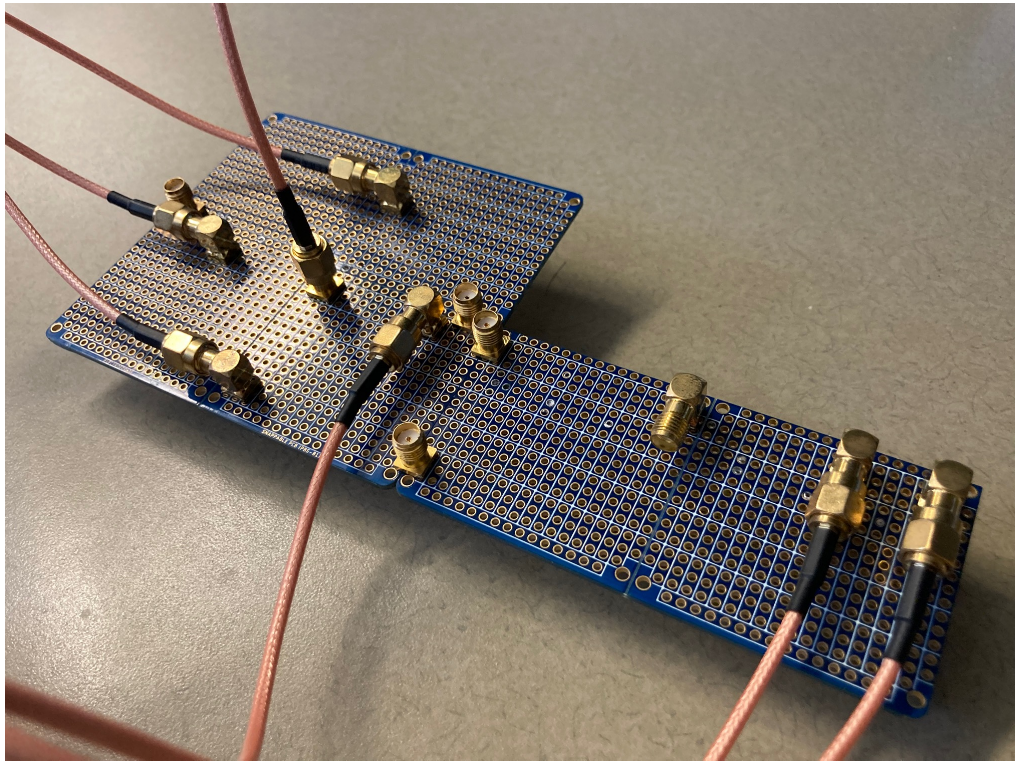


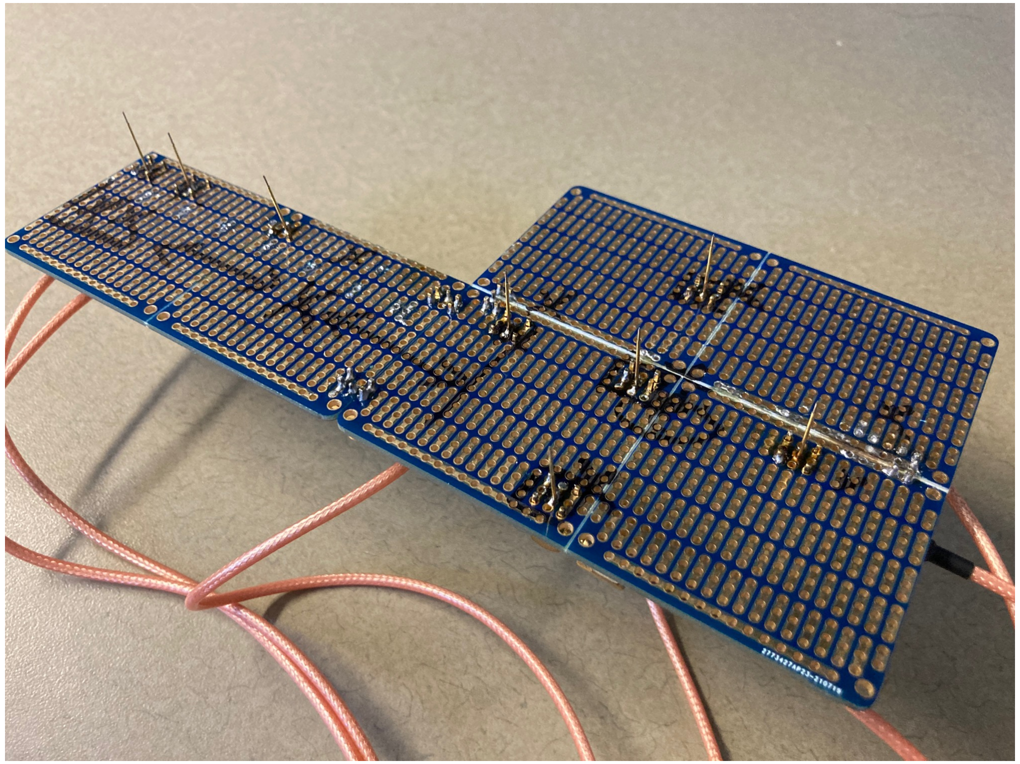
Unlock iPad with Simple Clicks



Utilization of Clicks

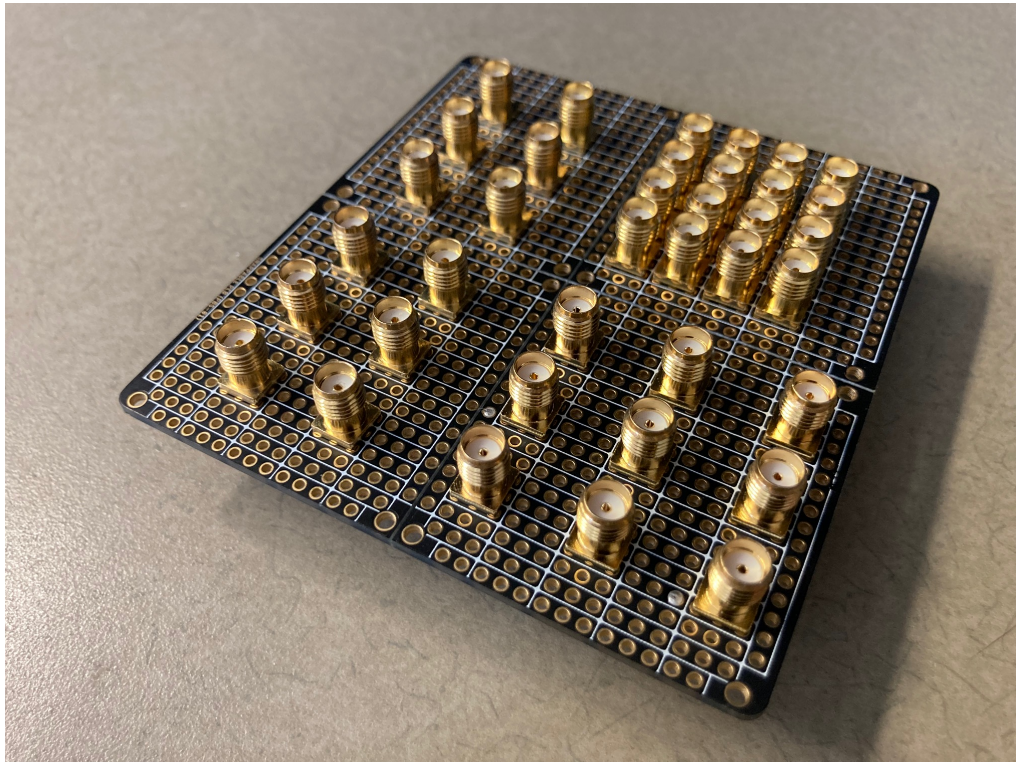
- Sparse antenna array

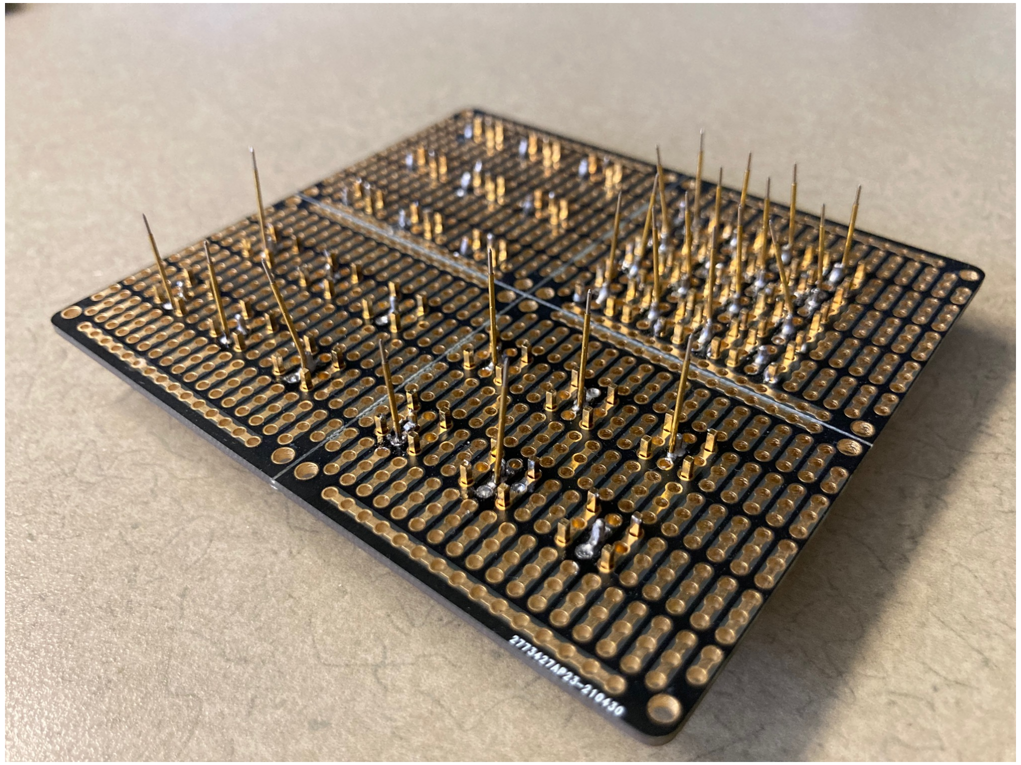




Utilization of Clicks

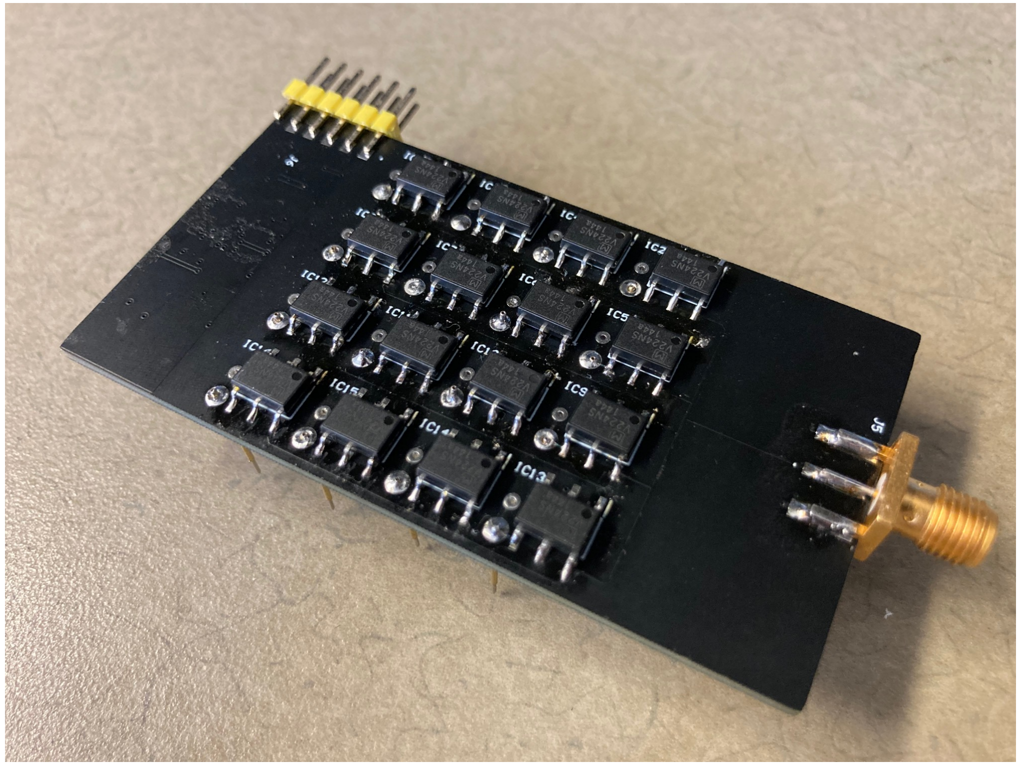
- Dense antenna array
  - Interference between antennas? 6mm minimum distance

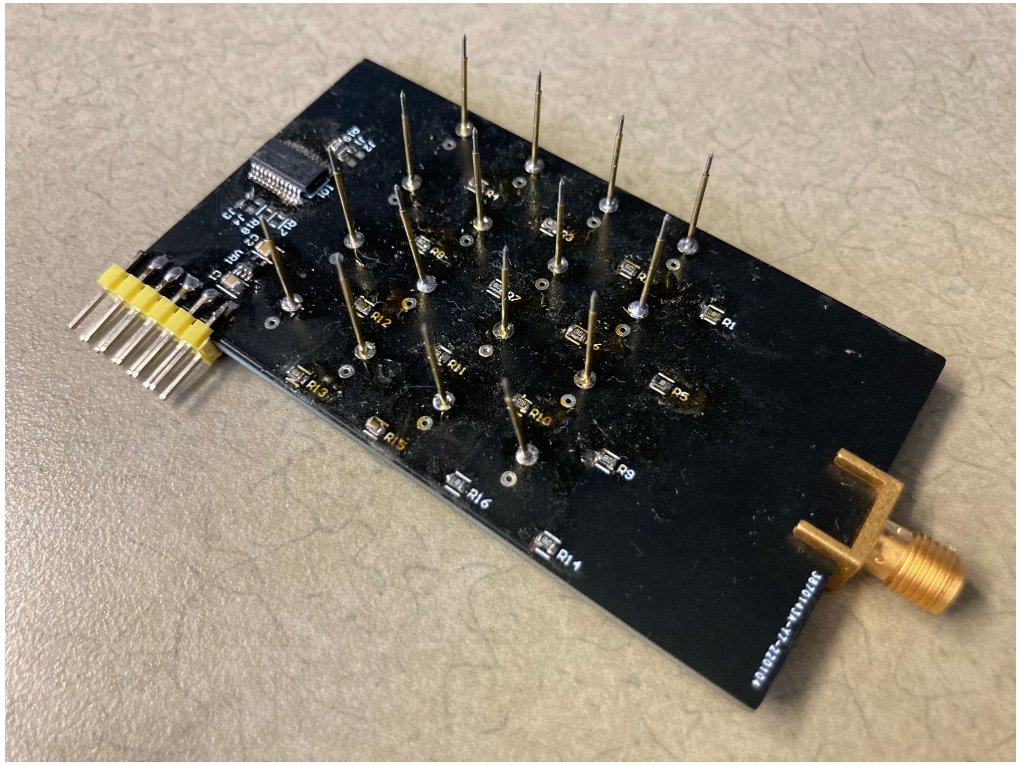




Utilization of Clicks

- Modularized antenna array
  - Programmable controlled antenna array





Precise Touch Events

			Quartile Deviation (pixels)		Gestures		
DEVICE	DRIVING	SUCCESS RATE	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)

Precise Touch Events

			Quartile Deviation (pixels)			Gestures	
DEVICE	DRIVING	SUCCESS RATE	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	✓	✗	✗

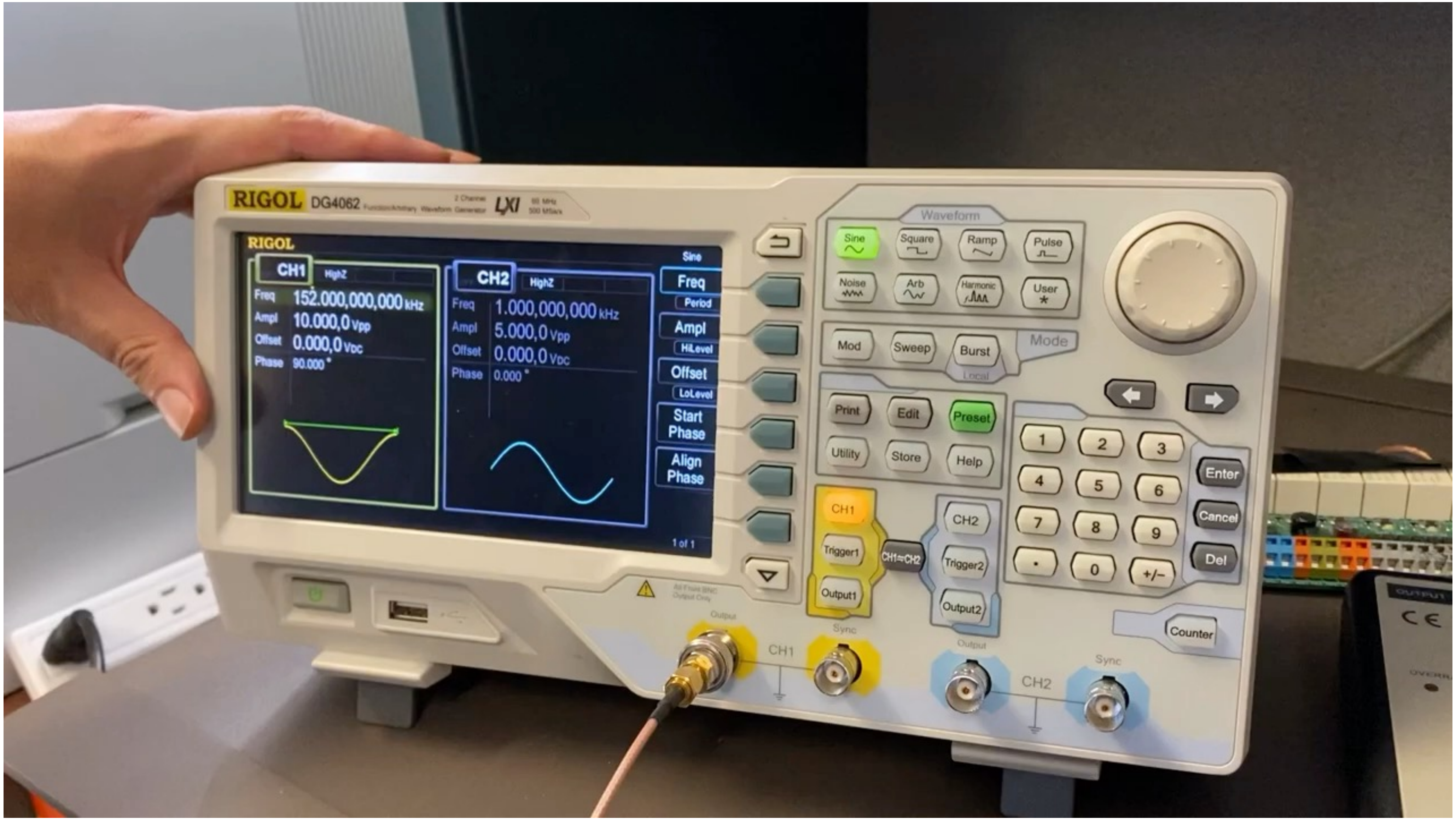
Driving method: P (Parallel), S (Sequential)

Precise Touch Events

			Quartile Deviation (pixels)		Gestures		
DEVICE	DRIVING	SUCCESS RATE	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)

Omni-directional Swipe

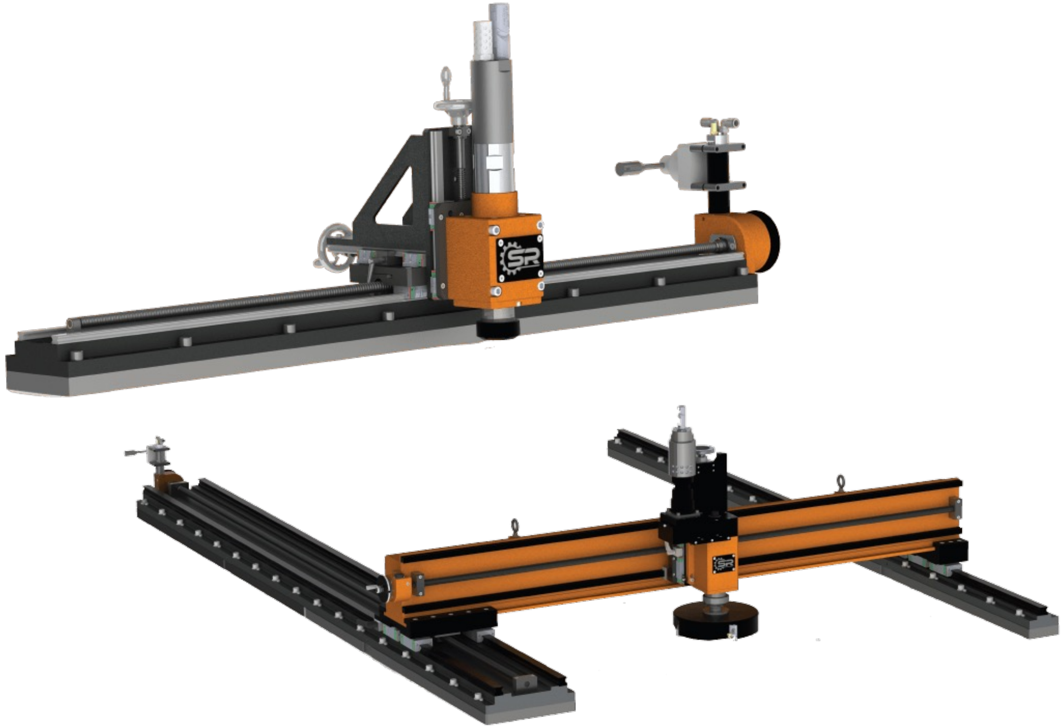


CH1 HighZ
Freq 152.000,000,000 kHz
Ampl 10.000,0 Vpp
Offset 0.000,0 Vdc
Phase 90.000 °

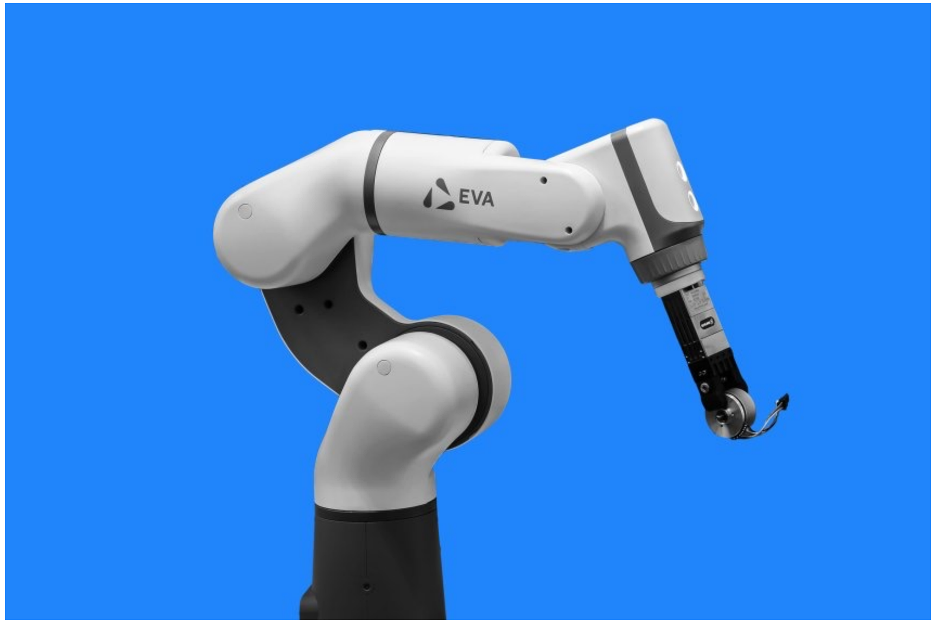
CH2 HighZ
Freq 1.000,000,000 kHz
Ampl 5.000,0 Vpp
Offset 0.000,0 Vdc
Phase 0.000 °

Utilization of Swipes

- Linear gantry mills/Robot arm



@sprtool.com



@MIT Tech Review

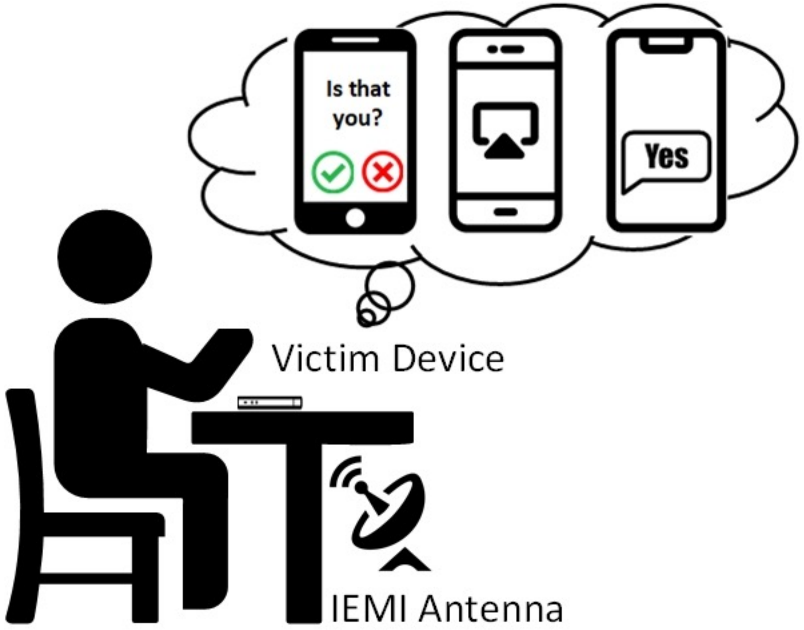
Agenda

- Who we are?
- TL;DR
- How touchscreen works?
- A theoretical attack on touchscreen
- Precise touch events generation
- Road to practical touchscreen attacks.
- Q&A

Complete practical attack vectors

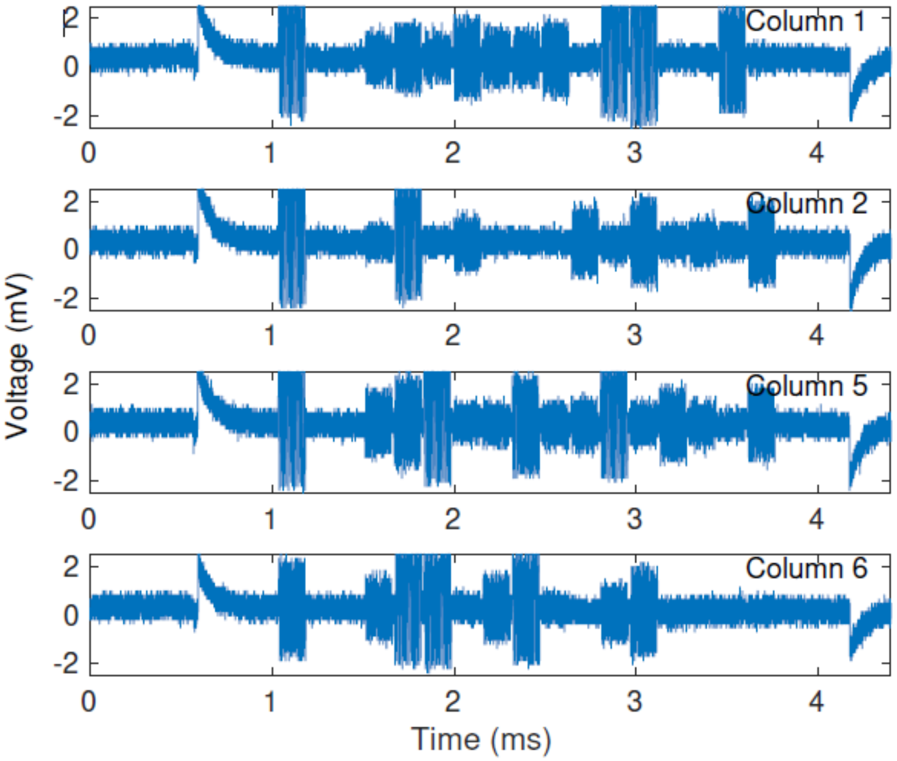
Now what?

- 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

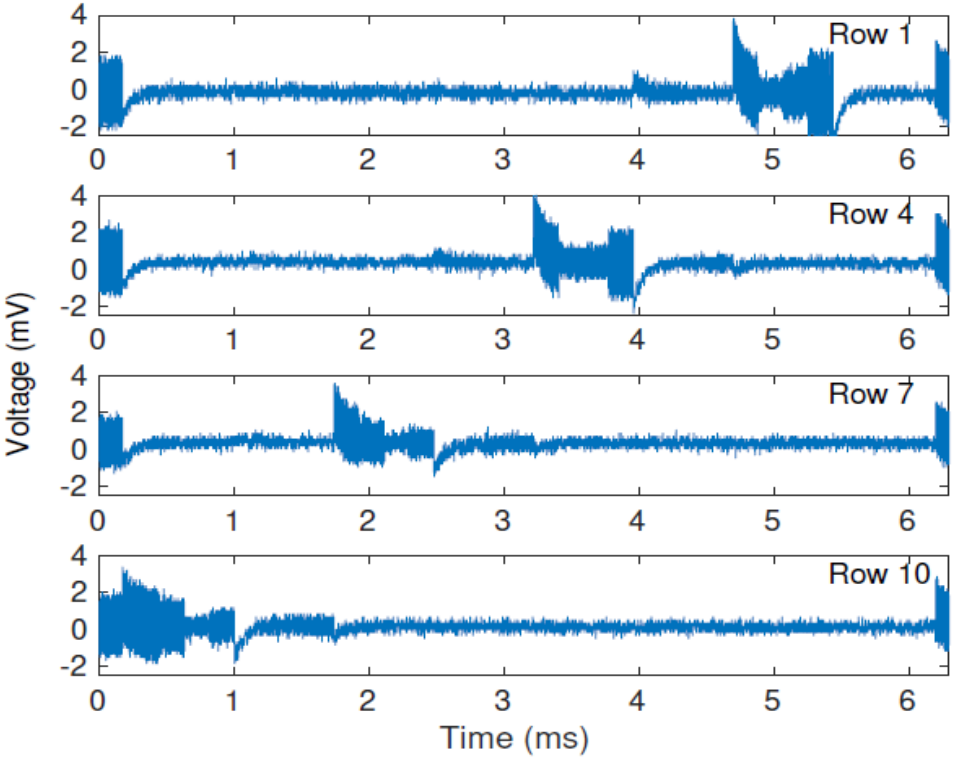


Phone Locator

- 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



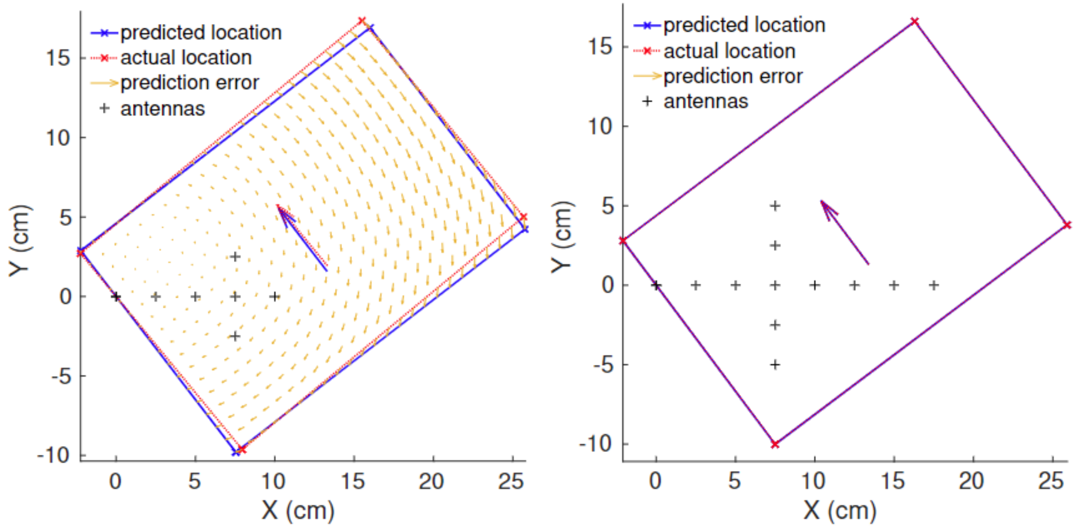
Sequential Scanning Pixel 2

Phone Locator

- A quick but reliable KNN classifier

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

Antenna location/screen location transformation matrix



(a) Screen location detected using 7 antennas

(b) Screen location detected using 12 antennas

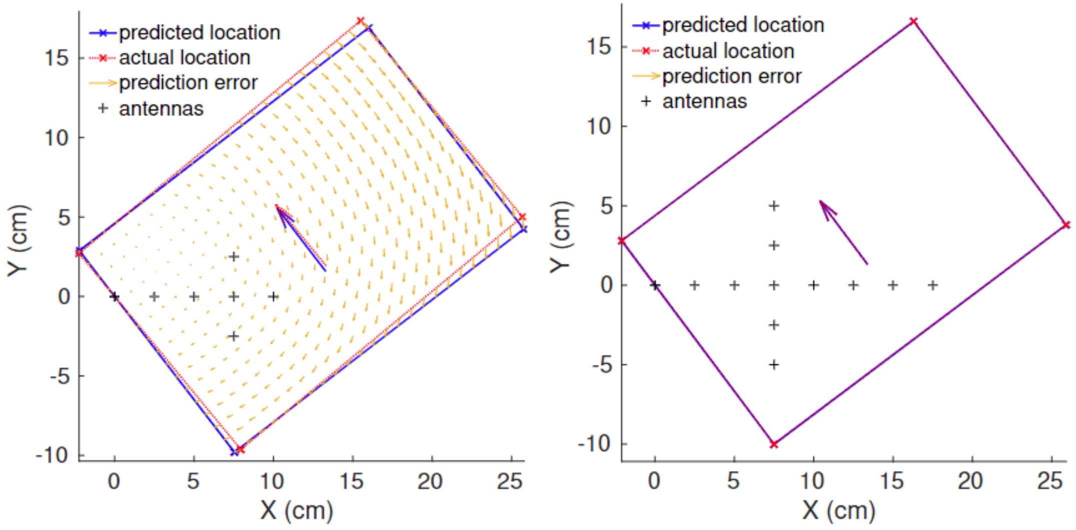
Evaluation using iPad Pro 2020

Phone Locator

- A quick but reliable KNN classifier

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

Antenna location/screen location transformation matrix



(a) Screen location detected using 7 antennas

(b) Screen location detected using 12 antennas

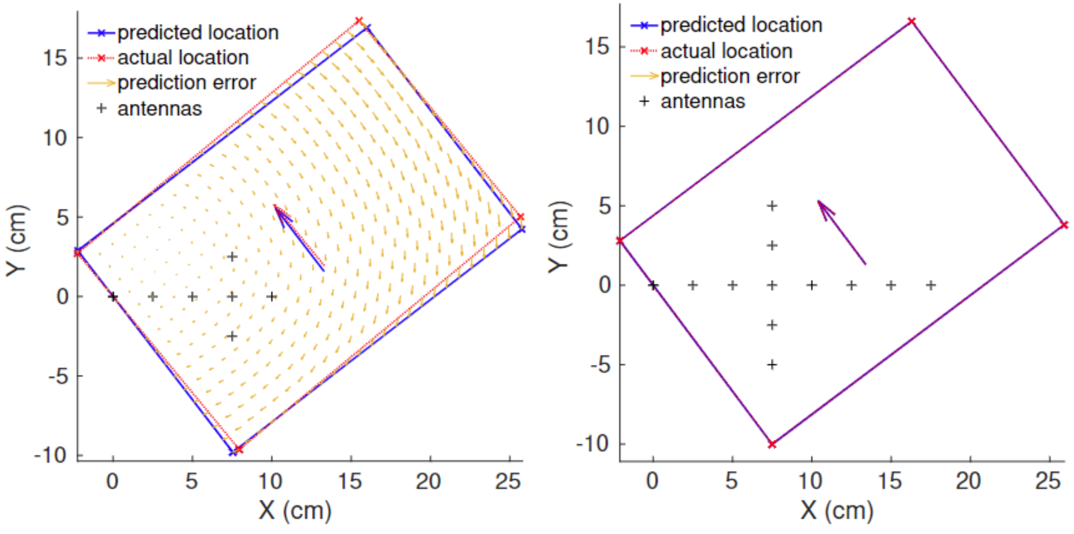
Evaluation using iPad Pro 2020

Phone Locator

- A quick but reliable KNN classifier

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

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

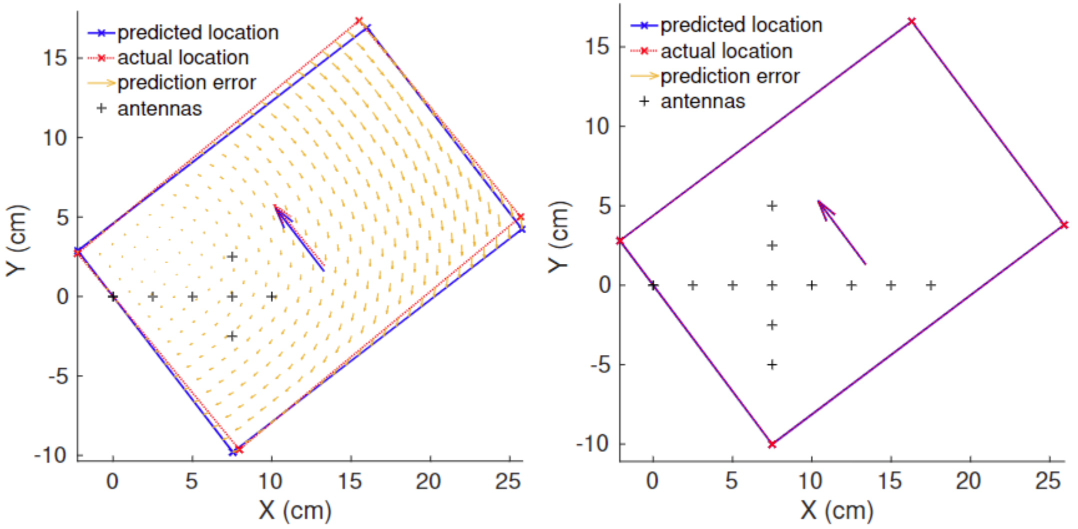
Phone Locator

- A quick but reliable KNN classifier

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

Antenna location/screen location transformation matrix

Device	Driving Method	Sample Rate	Error	Time
Nexus 5X	SDM	50MSa/s	0.42 cm	N/A
Google Pixel 2	SDM	50MSa/s	0.51 cm	N/A
iPhone 11 Pro	PDM	1MSa/s	0.3 cm	0.08s
OnePlus 7 Pro	PDM	2MSa/s	0.06 cm	0.14s
iPad Pro	PDM	1MSa/s	0.18 cm	0.17s



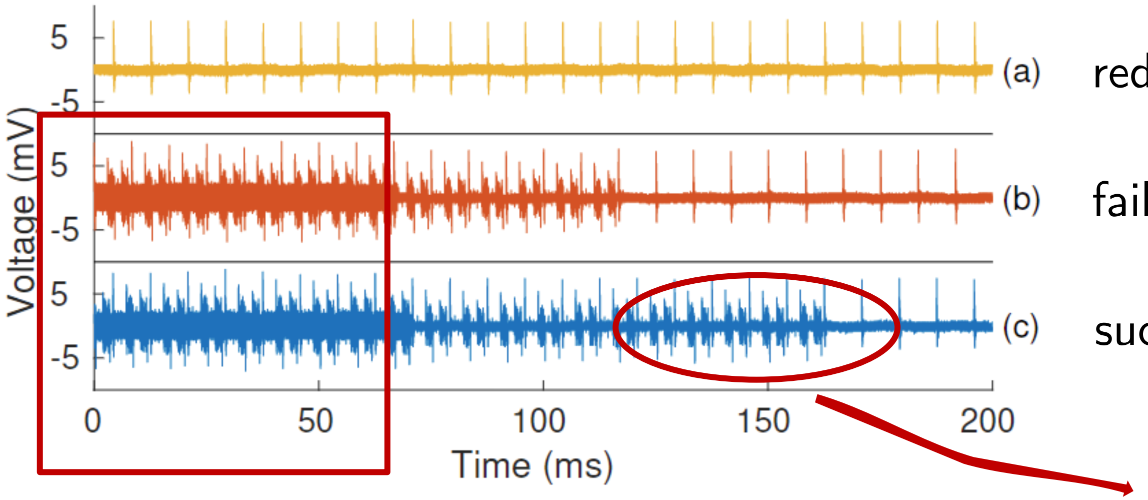
(a) Screen location detected using 7 antennas

(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



reduced scan without IEMI

failed IEMI attack

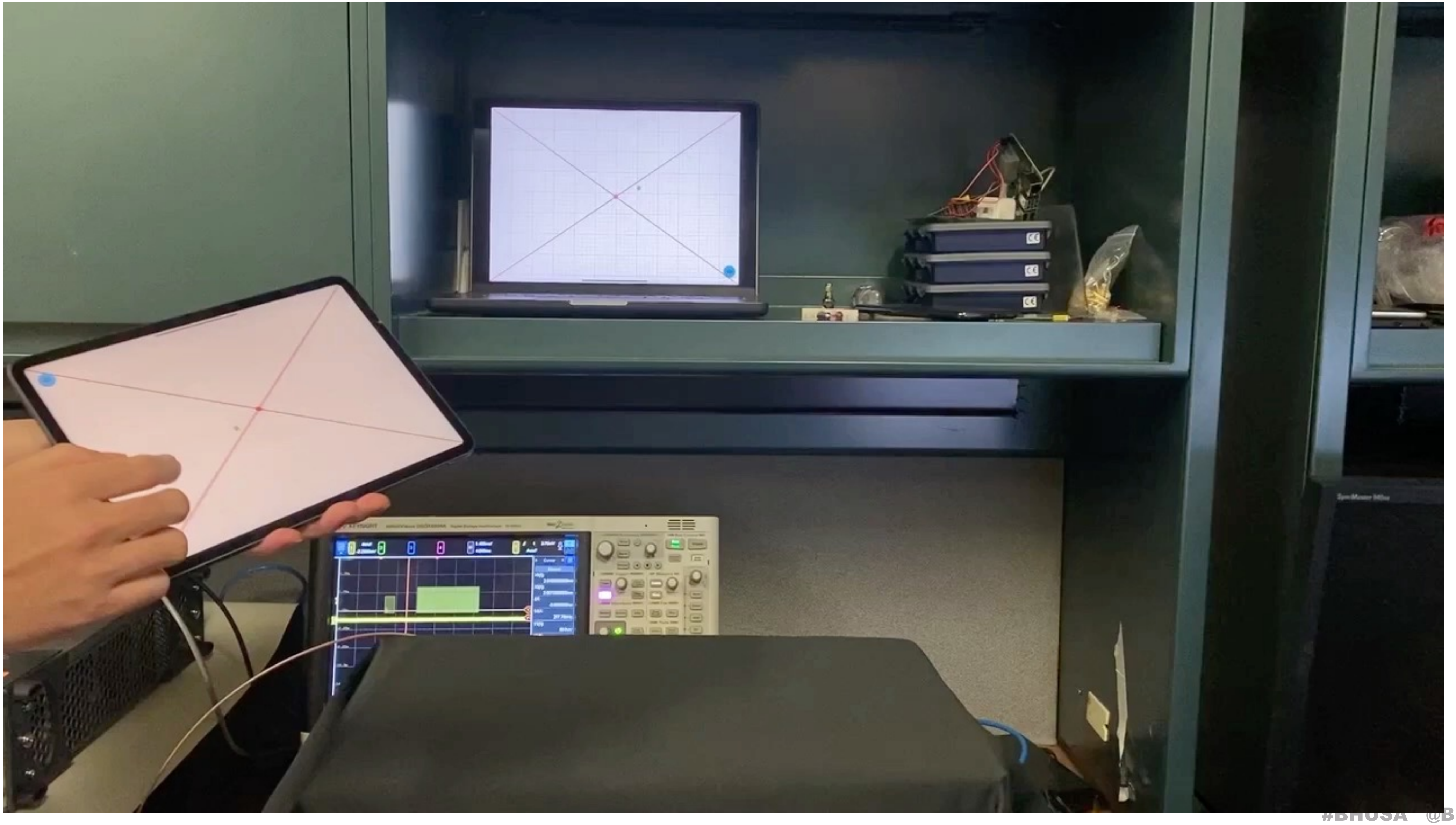
successful IEMI attack

Extra active scanning

IEMI Signal

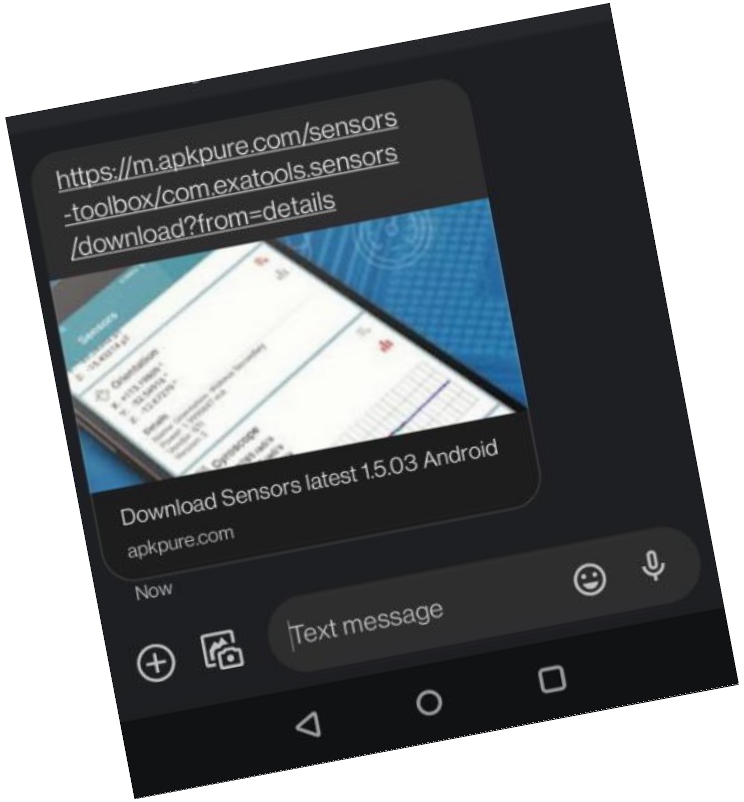
iPad Pro 2020

End-to-End Attack



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)



https://m.apkpure.com/sensors-toolbox/com.exatools.sensors/download?from=details

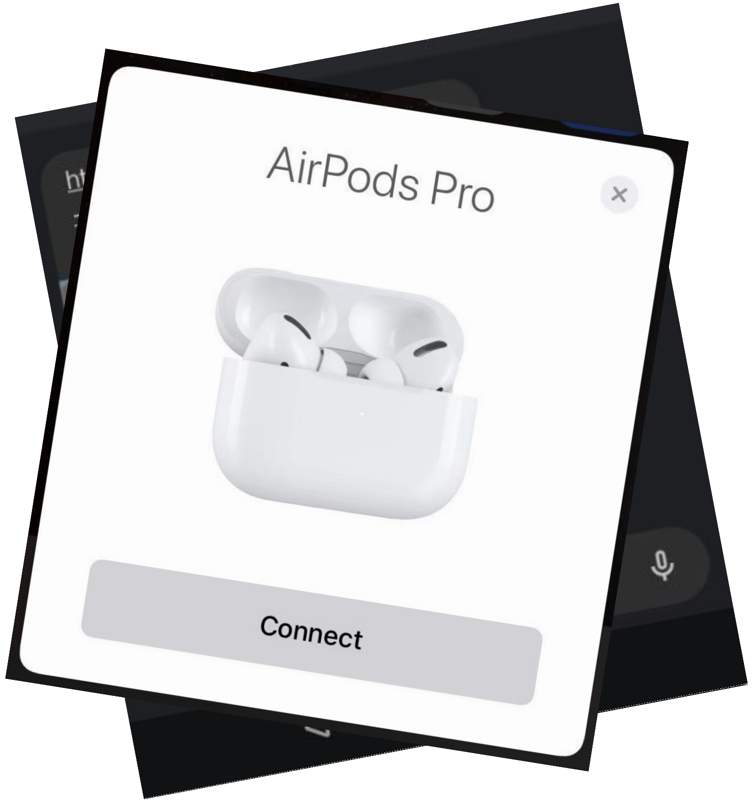
Download Sensors latest 1.5.03 Android

apkpure.com

Now

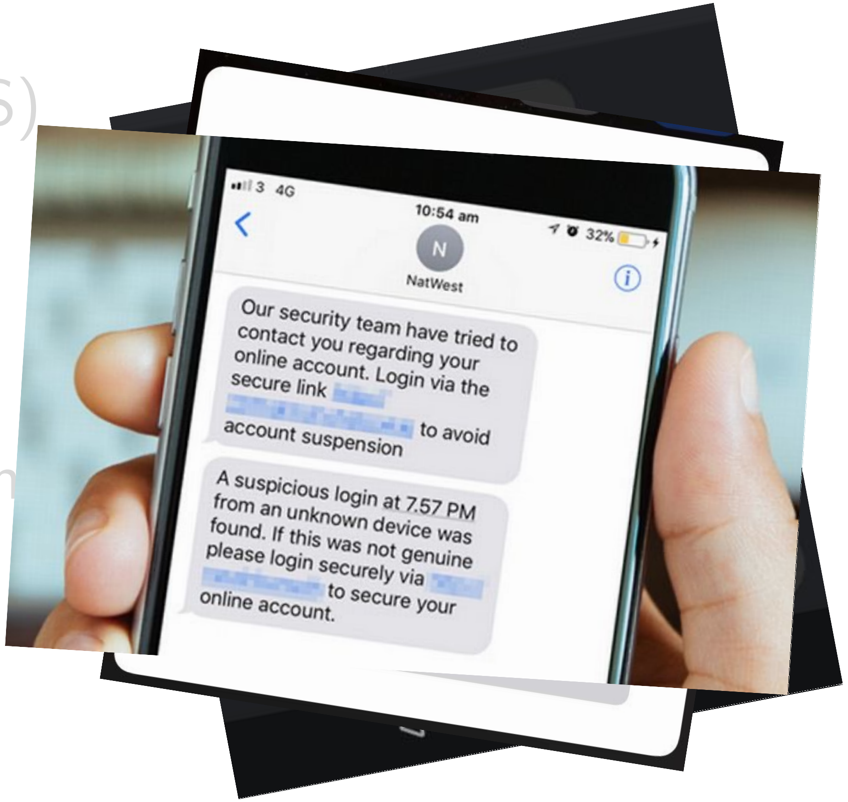
Attack Scenarios

- 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 unlockin



Our security team have tried to contact you regarding your online account. Login via the secure link [redacted] to avoid account suspension

A suspicious login at 7.57 PM from an unknown device was found. If this was not genuine please login securely via [redacted] to secure your online account.

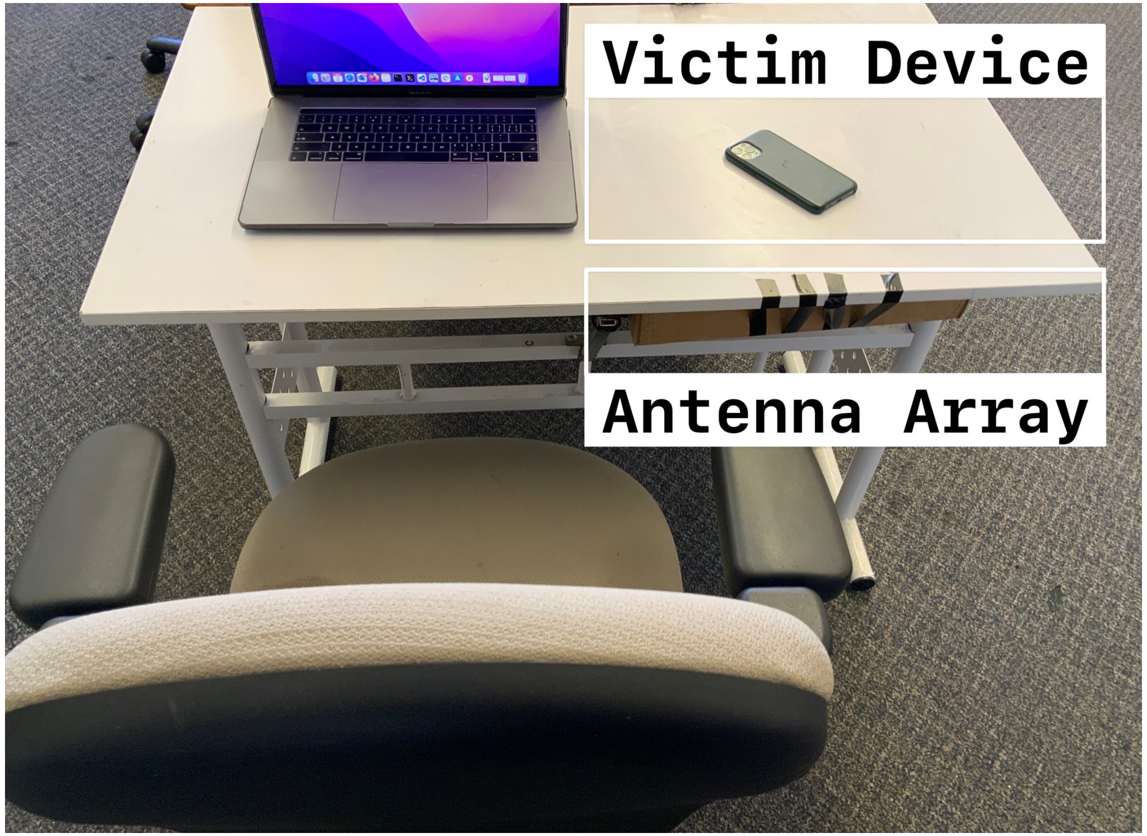
Attack Scenarios

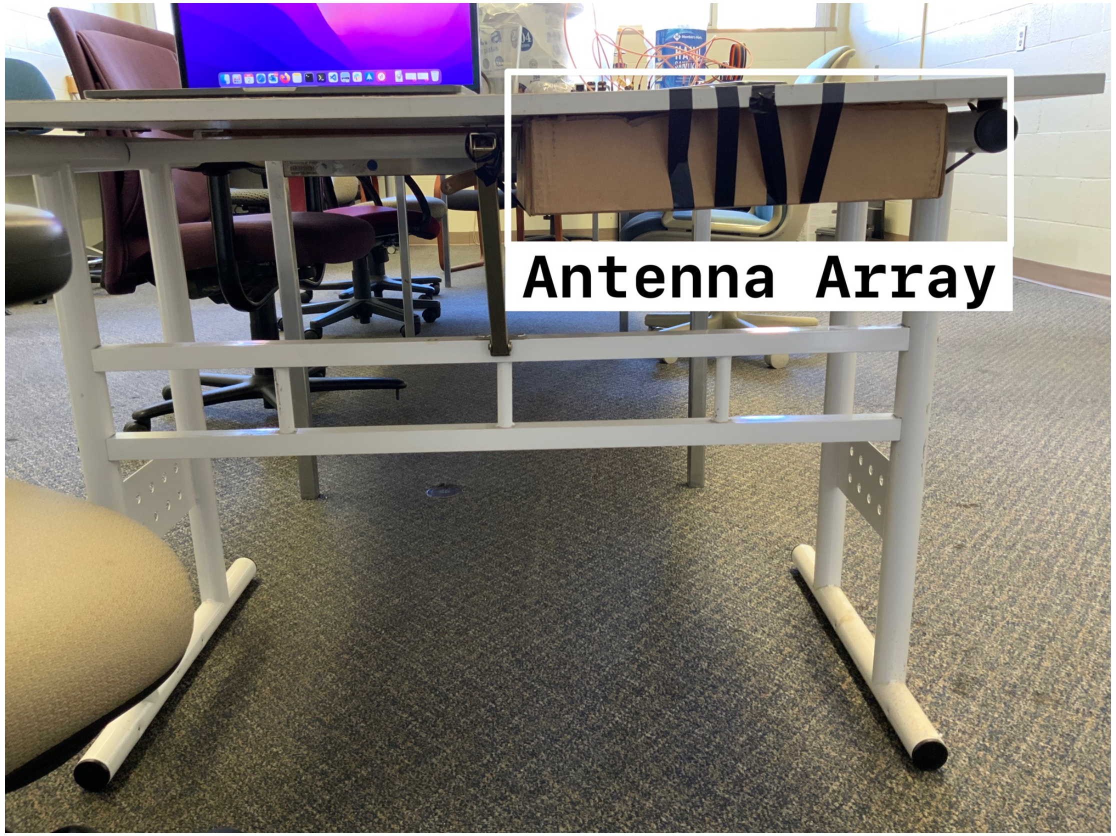
- Click based attack
  - Malicious application installation (Android)
  - Malicious Bluetooth peripheral connection (iOS)
- Gesture based attack
  - Send messages (bank fraud message)
  - Send money (press-and-hold on PayPal icon)
  - Unlock phone (omnidirectional gesture unlockin

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 unlockin

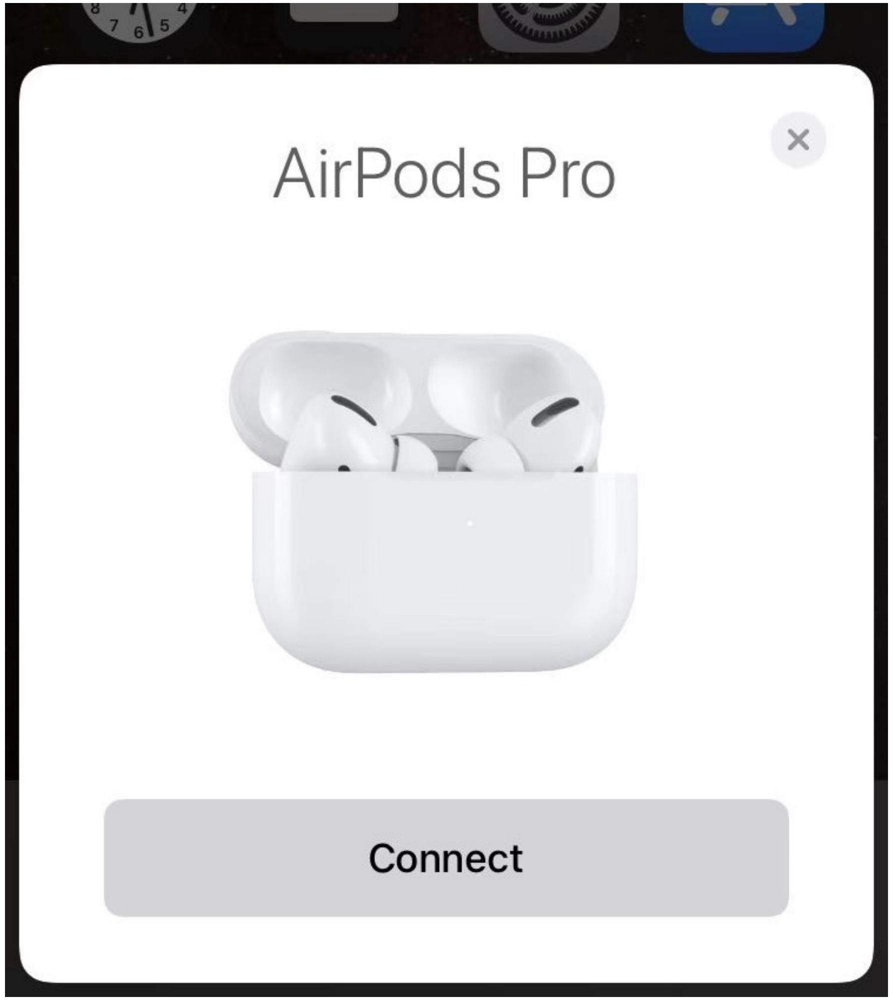
Attack Setup





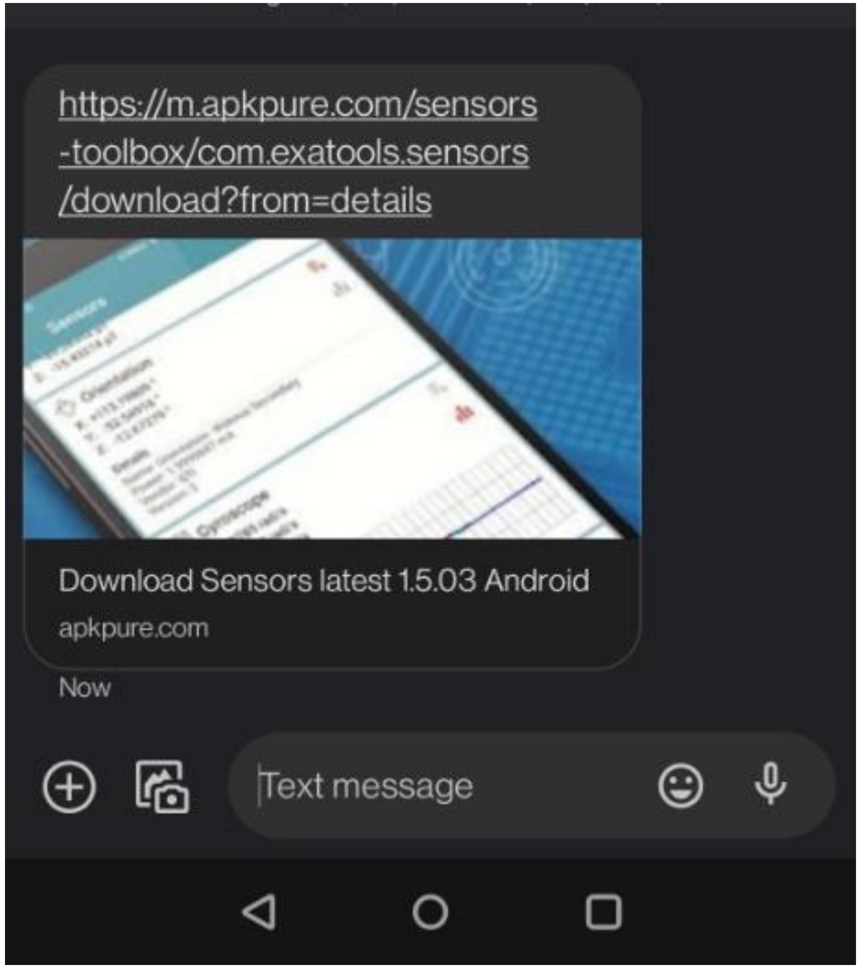
Attack Evaluation

- Only 4 antennas needed for locating the phone
- Malicious Siri on iOS devices
  - iPad Pro 2020, 6/10 success rate, less than 12 seconds
  - iPhone 11 Pro, 9/10 success rate, less than 9 seconds



Attack Evaluation

- Only 4 antennas needed for locating the phone
- Malicious application installation on Android devices
  - Oneplus 7 Pro, 3/10 success rate
  - We should click on OKAY but instead we clicked on CANCLE
  - Denser array design can fix this issue



https://m.apkpure.com/sensors-toolbox/com.exatools.sensors/download?from=details

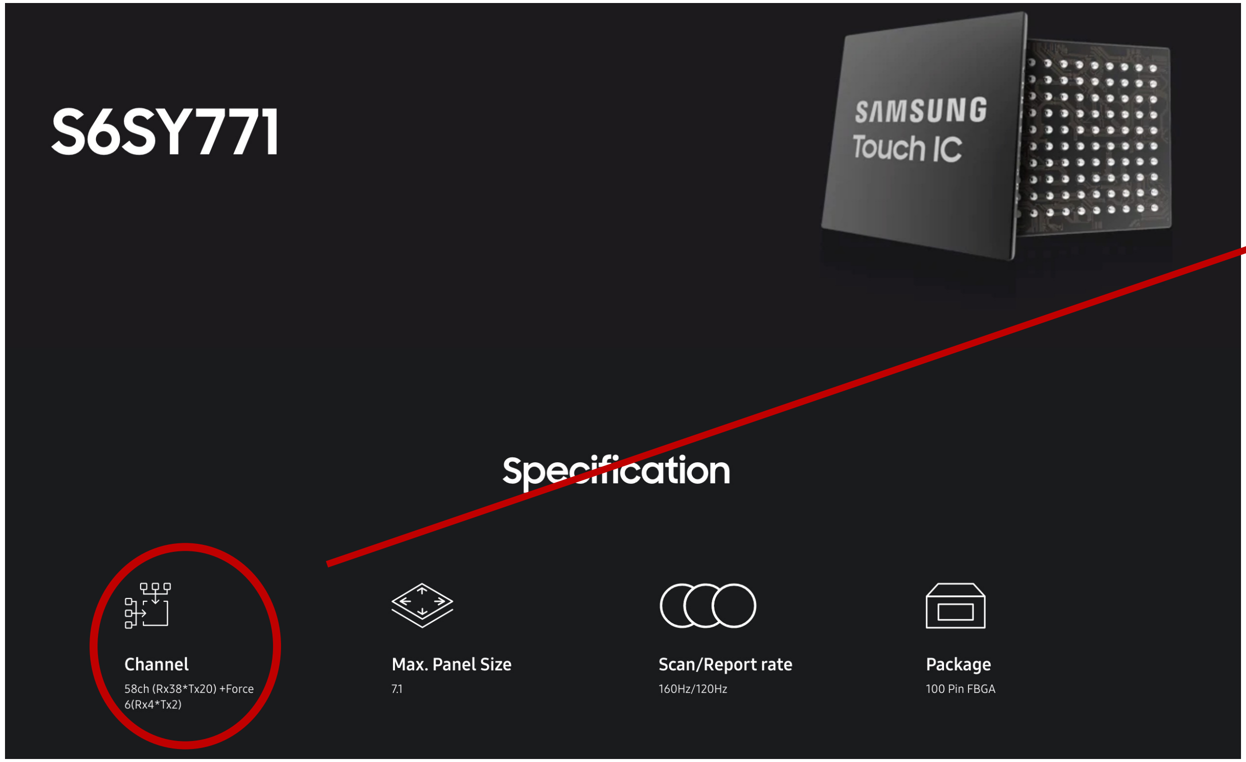
Download Sensors latest 1.5.03 Android

apkpure.com

Now

Mitigations

- Pressure/Force detection (Vendors)



S6SY771

Specification

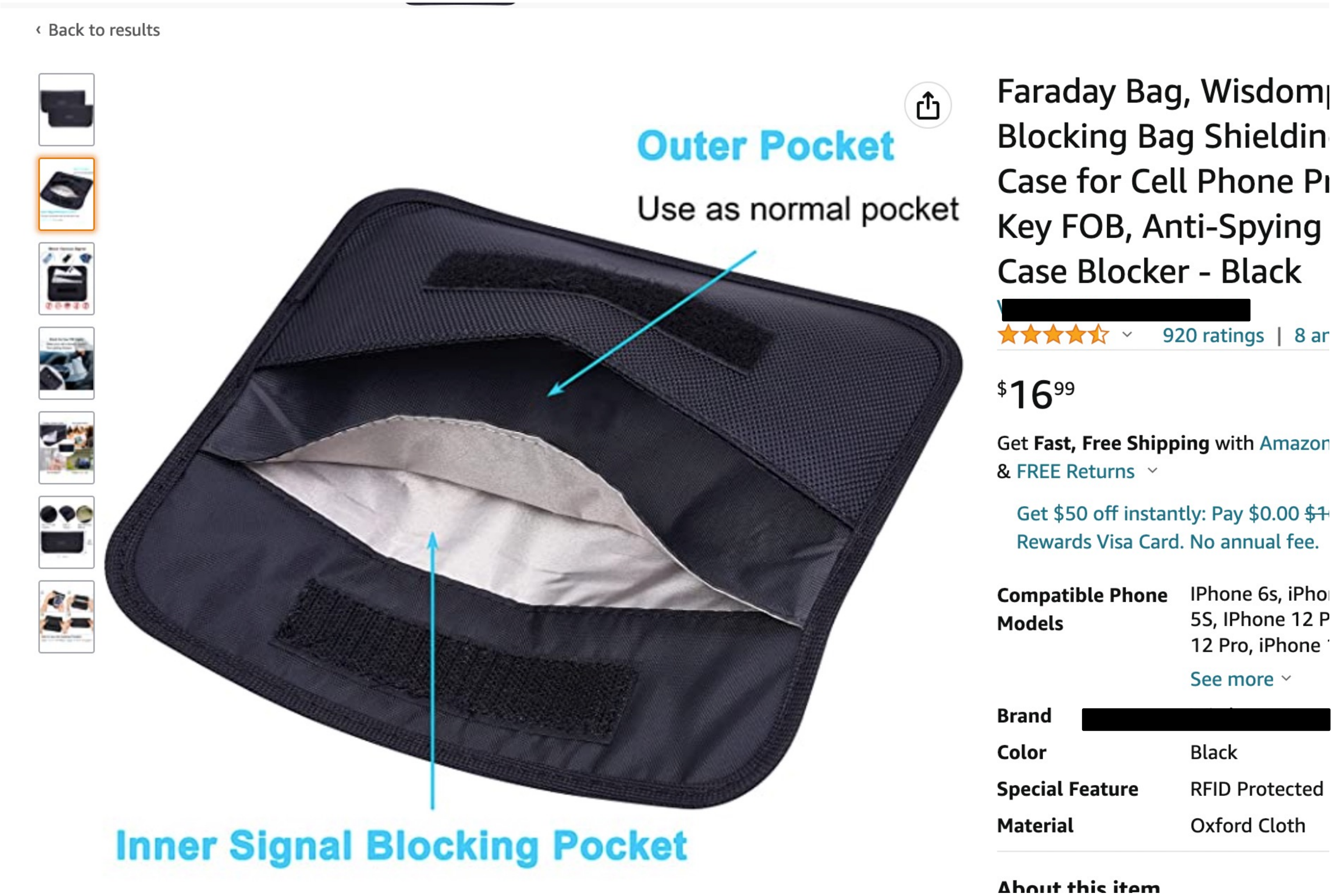
Channel	Max. Panel Size	Scan/Report rate	Package
58ch (Rx38*Tx20) +Force 6(Rx4*Tx2)	7.1	160Hz/120Hz	100 Pin FBGA

Channel

58ch (Rx38*Tx20) +Force 6(Rx4*Tx2)

Mitigations

- Faraday Bag/Pouch (Customers)



‹ Back to results

Faraday Bag, Wisdom
Blocking Bag Shieldin
Case for Cell Phone P
Key FOB, Anti-Spying
Case Blocker - Black

[redacted]

★★★★☆ 920 ratings | 8 ar

$16 99

Get **Fast, Free Shipping** with Amazon
& FREE Returns

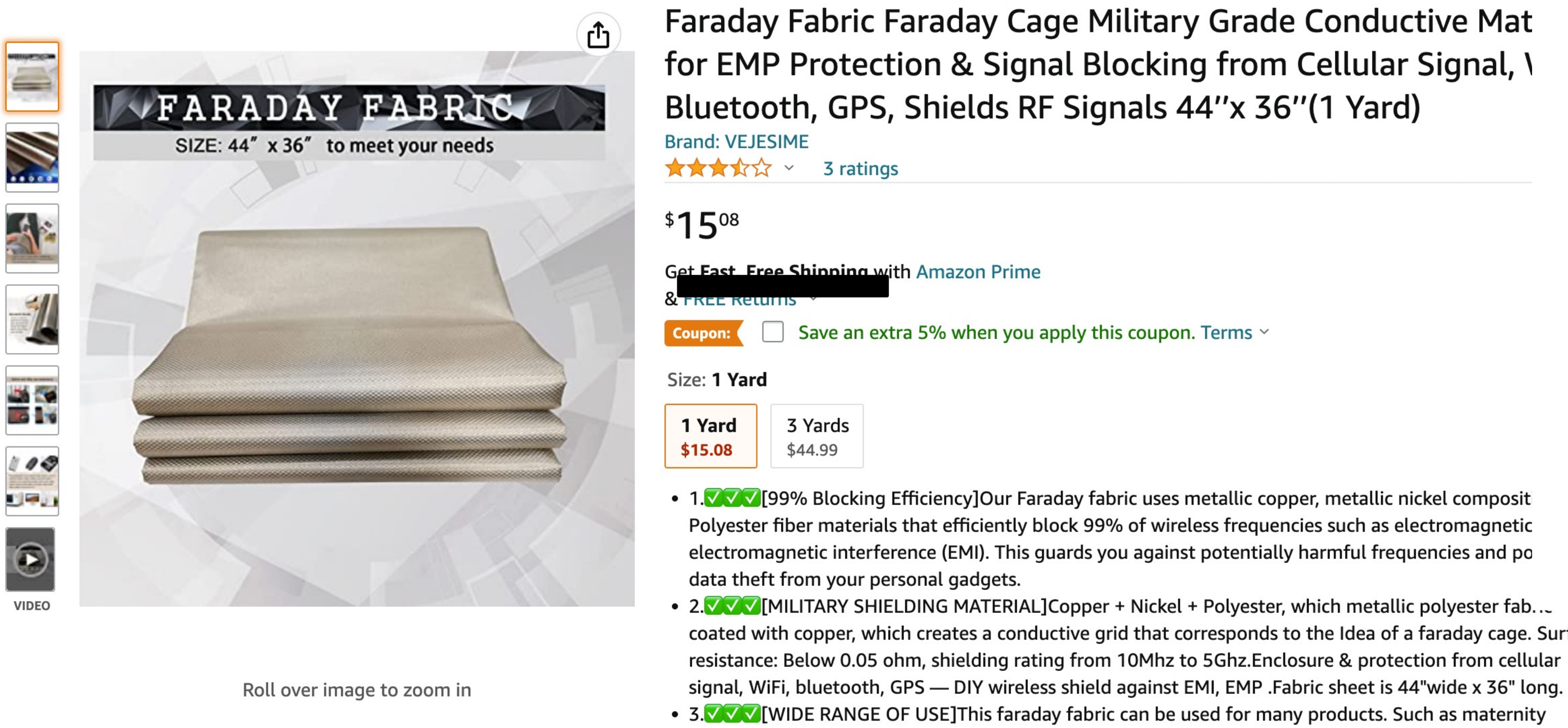
Get $50 off instantly: Pay $0.00 ~~$1~~
Rewards Visa Card. No annual fee.

Compatible Phone Models	IPhone 6s, iPho 5S, IPhone 12 P 12 Pro, iPhone See more
Brand	[redacted]
Color	Black
Special Feature	RFID Protected
Material	Oxford Cloth

About this item

Mitigations

- Faraday Fabric + Case with cover (Customers)


FARADAY FABRIC
SIZE: 44" x 36" to meet your needs
VIDEO
Roll over image to zoom in

Faraday Fabric Faraday Cage Military Grade Conductive Mat for EMP Protection & Signal Blocking from Cellular Signal, \ Bluetooth, GPS, Shields RF Signals 44''x 36''(1 Yard)

Brand: VEJESIME

★★★☆☆ 3 ratings

$15.08

Get Fast, Free Shipping with Amazon Prime
& [redacted]

Coupon: □ Save an extra 5% when you apply this coupon. Terms

Size: 1 Yard

1 Yard $15.08 | 3 Yards $44.99

- 1.✅✅✅[99% Blocking Efficiency]Our Faraday fabric uses metallic copper, metallic nickel composit Polyester fiber materials that efficiently block 99% of wireless frequencies such as electromagnetic electromagnetic interference (EMI). This guards you against potentially harmful frequencies and po data theft from your personal gadgets.
- 2.✅✅✅[MILITARY SHIELDING MATERIAL]Copper + Nickel + Polyester, which metallic polyester fab... coated with copper, which creates a conductive grid that corresponds to the Idea of a faraday cage. Surface resistance: Below 0.05 ohm, shielding rating from 10Mhz to 5Ghz.Enclosure & protection from cellular signal, WiFi, bluetooth, GPS — DIY wireless shield against EMI, EMP .Fabric sheet is 44"wide x 36" long.
- 3.✅✅✅[WIDE RANGE OF USE]This faraday fabric can be used for many products. Such as maternity

Q&A

Questions?

🏠 https://invisiblefinger.click

🐦 @Zeropwnedlol

✉ haoqi.shan@ufl.edu
shuo.wang@ece.ufl.edu