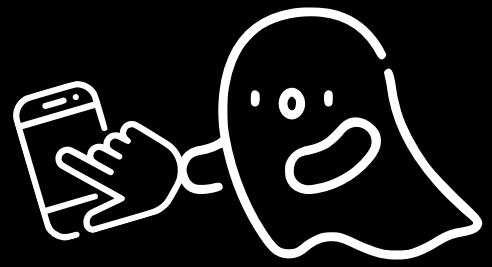
GhostTouch: Attacks on Touchscreens without Physical Touch

Kai Wang[2], Richard Mitev[1], Chen Yan[2], Xiaoyu Ji[2], Ahmad-Reza Sadeghi[1], Wenyuan Xu[2]

[1]System Security Lab, Technical University of Darmstadt, Germany

[2]Ubiquitous System Security Lab, Zhejiang University, China

USENIX Security 2022



System Security Lab

TECHNISCHE UNIVERSITÄT DARMSTADT

Capacitive touch screens are ubiquitous

→ High precision
→ Low wear
→ Multi Touch

Motivation

每经网
www.nbd.com.cn

Enter search keywords

News

Home > News > Main text

related articles

The cell phone being charged automatically booked a ten thousand yuan presidential suite and checked the chat history...

21st Century Business Herald WeChat Official Account 2018-10-08 09:58:19

The Apple mobile phone lying flat on the table was charging, and it automatically clicked the Ctrip APP, browsed the hotel rooms, and booked a presidential suite. All this is done automatically by the mobile phone, as if an invisible person is controlling it.

Nowadays, our lives are almost inseparable from mobile phones. In a
ge amount of personal information, there are

Lenovo SHOP SUPPORT COMMUNITY My Account English Cart

Support

Knowledge Base & Guides

To be sure this content applies to the device you need information on, please enter your serial number or select your product.

Enter serial number or Select Your Product

Help me find my product/serial number

Touch function of Touch Screen cannot run normally under fluorescent light environment

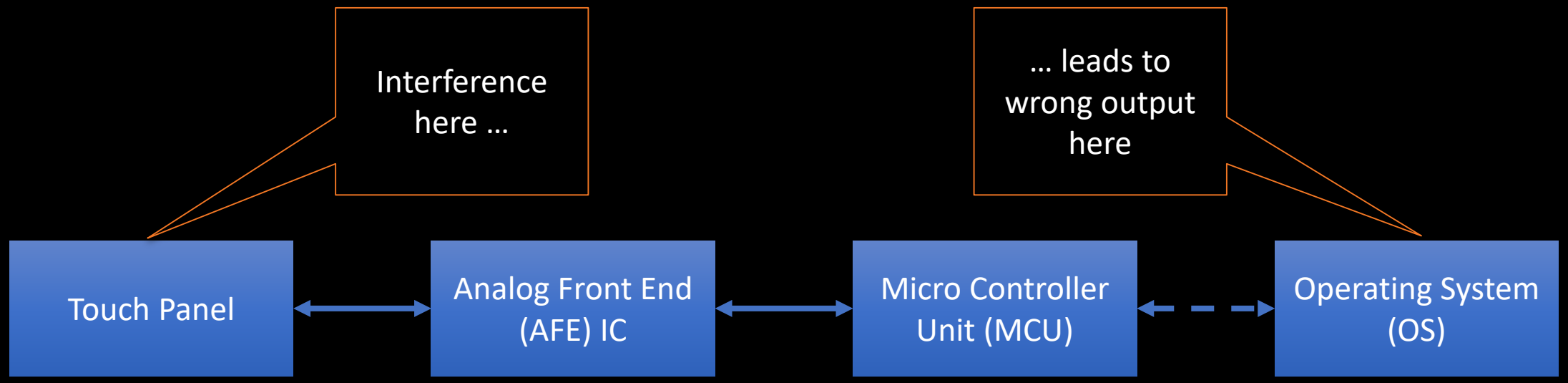
Symptom

Touch function of Touch Screen cannot run normally under fluorescent light environment, while the light is turned off, it will work normally.

Root cause

Electromagnetic interference will occur when electronic devices work, and it will be affected by others. The electromagnetic interference is not obvious as all devices must pass through electromagnetic compatible testing. Since the working frequency of Capacitive Touchscreen Panel is very similar to light T5's, so T5 has strong electromagnetic interference to it, especially when they share the same socket.

Consequence



→ OS depends on benign touch data for security critical tasks
→ Design sensing circuits to be resilient against unintentional (environment) EMI and intentional (attack) EMI?

Touch screens: a serious security and privacy threat

Wrong input

Wrong output

Banking

Voting

Medical

Is it possible to control touch screens remotely using Electro-magnetic Interference (EMI)?

Selected EMI Attacks

Only very recently EMI is used to attack touch screens

DoS on devices
(e.g., security system)
Sabath et al. GASS 2011

Attack medical devices
(e.g., implants)
Kune et al. S&P 2013

Manipulate temperature reding
(e.g., sensor)
Tu et al. CCS 2019

Scatter touch points
(e.g., phones)
Maruyama et al. S&P 2019

2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019

Fault injection in embedded devices
Degbaoui et al. FDTC 2012

Flip bits in embedded devices
Selvaraj et al. ASIACCS 2018

Inject voice in microphone
Giechaskiel et al. ESORICS 2019

Selected EMI Attacks

Only very recently EMI is used to attack touch screens

Shortcomings of recent related work

- Needs user interaction
- Not targeted (Scatters position of touch randomly)
- Limited attack capabilities (only touch)

Scatter touch points
(e.g., phones)
Maruyama et al. S&P 2019

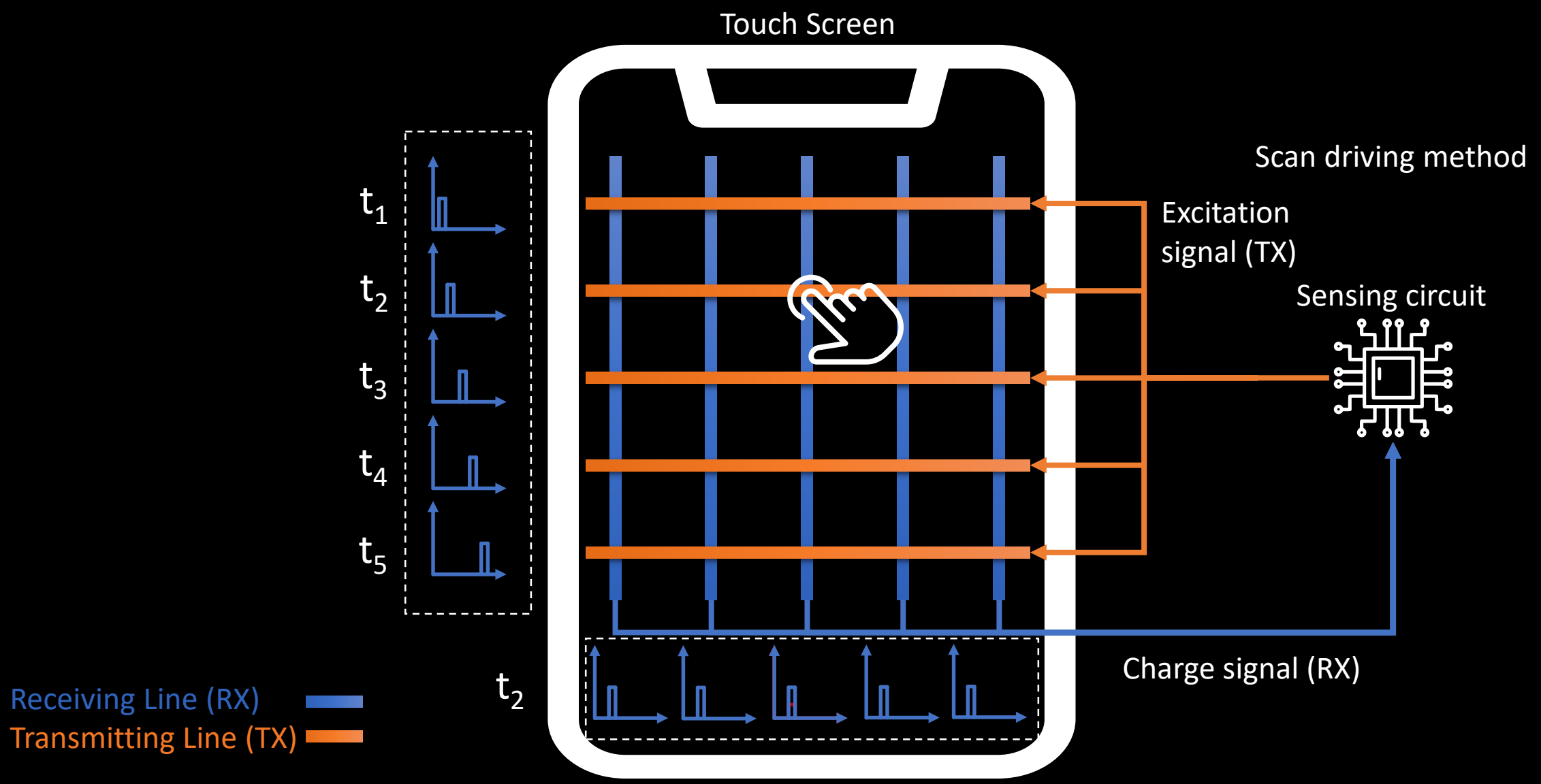
2018 2019

ect voice in microphone
haskiel et al. ESORICS 2019

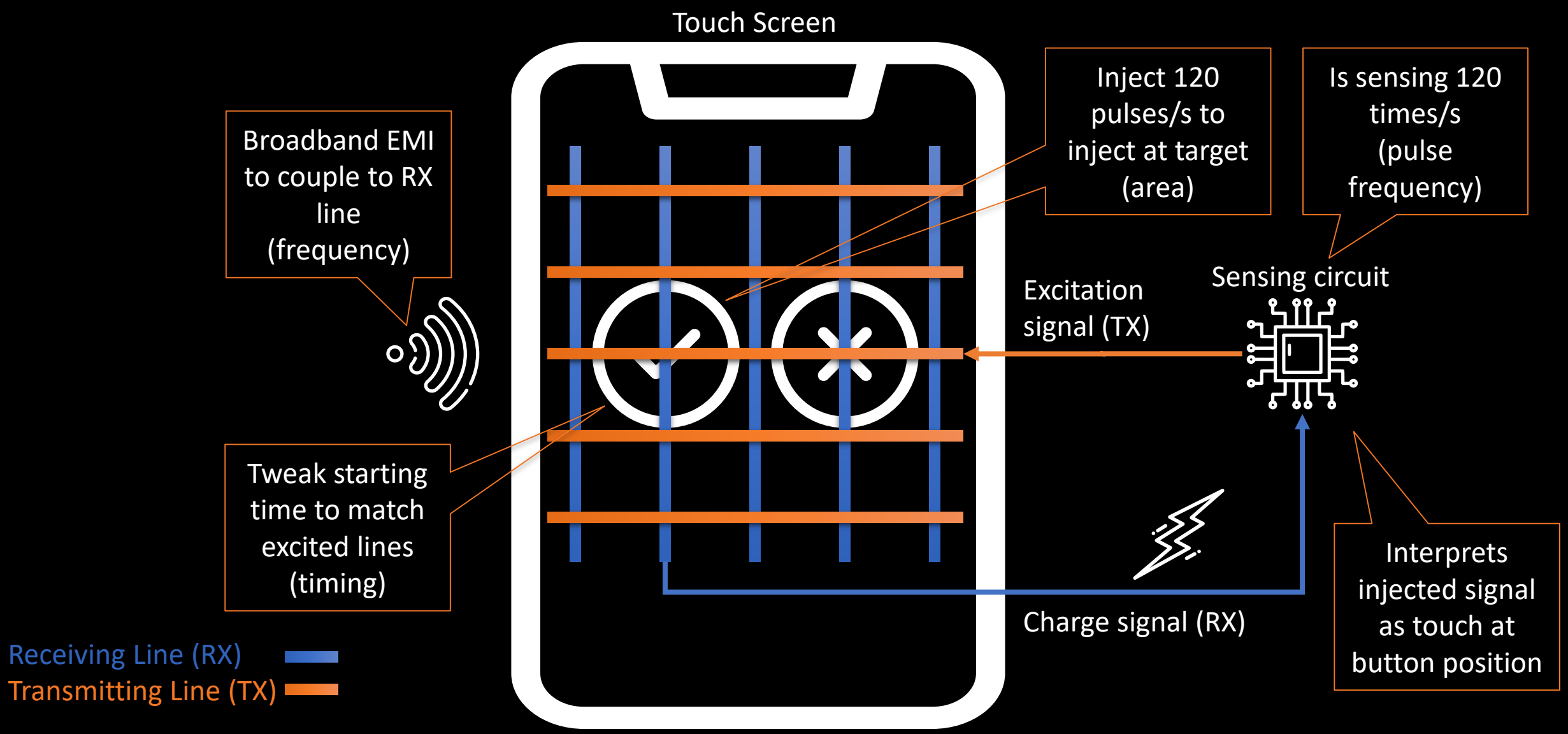
Our attack: GhostTouch

First work to use EMI to inject precise touch points without user interaction

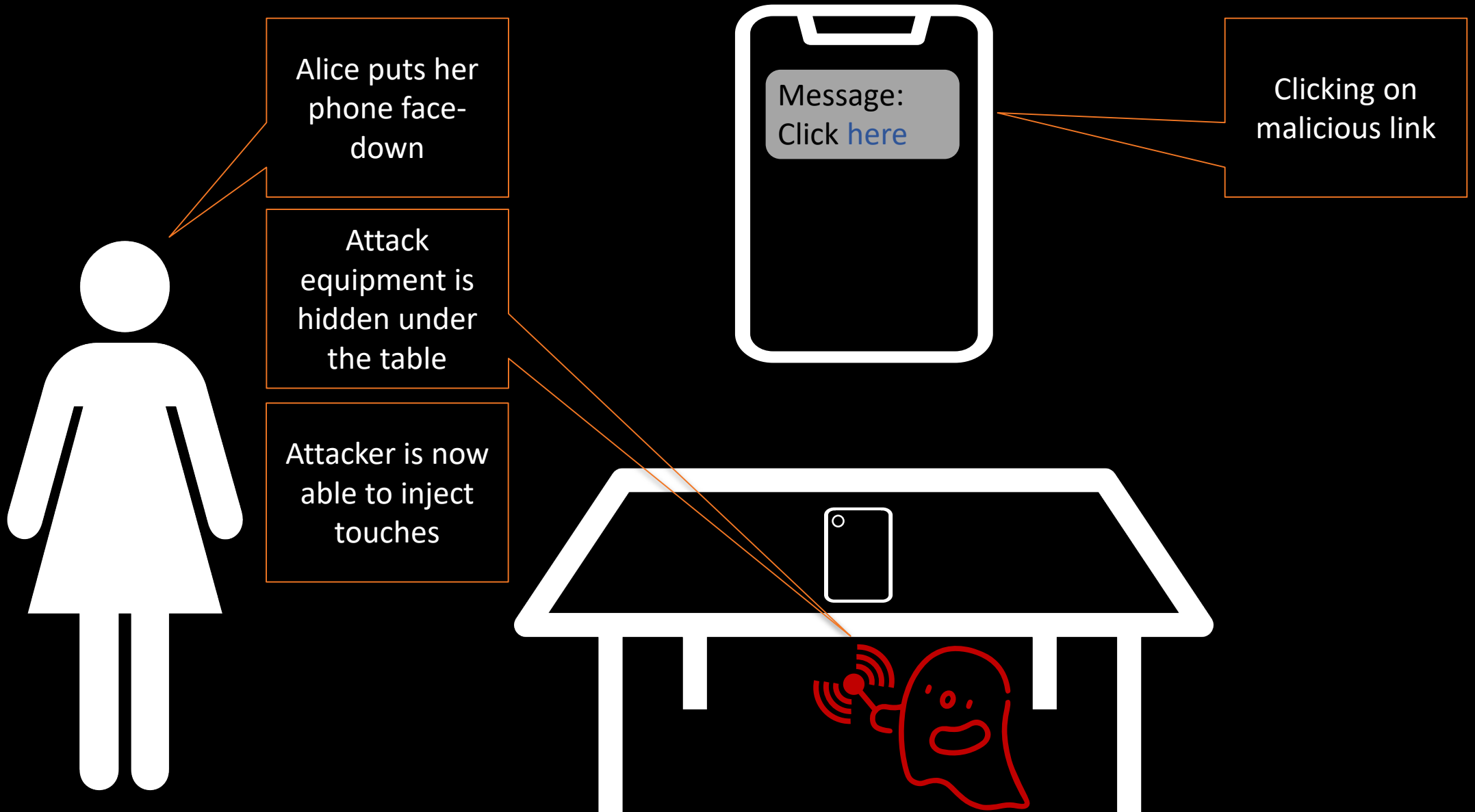
Background on touch screens



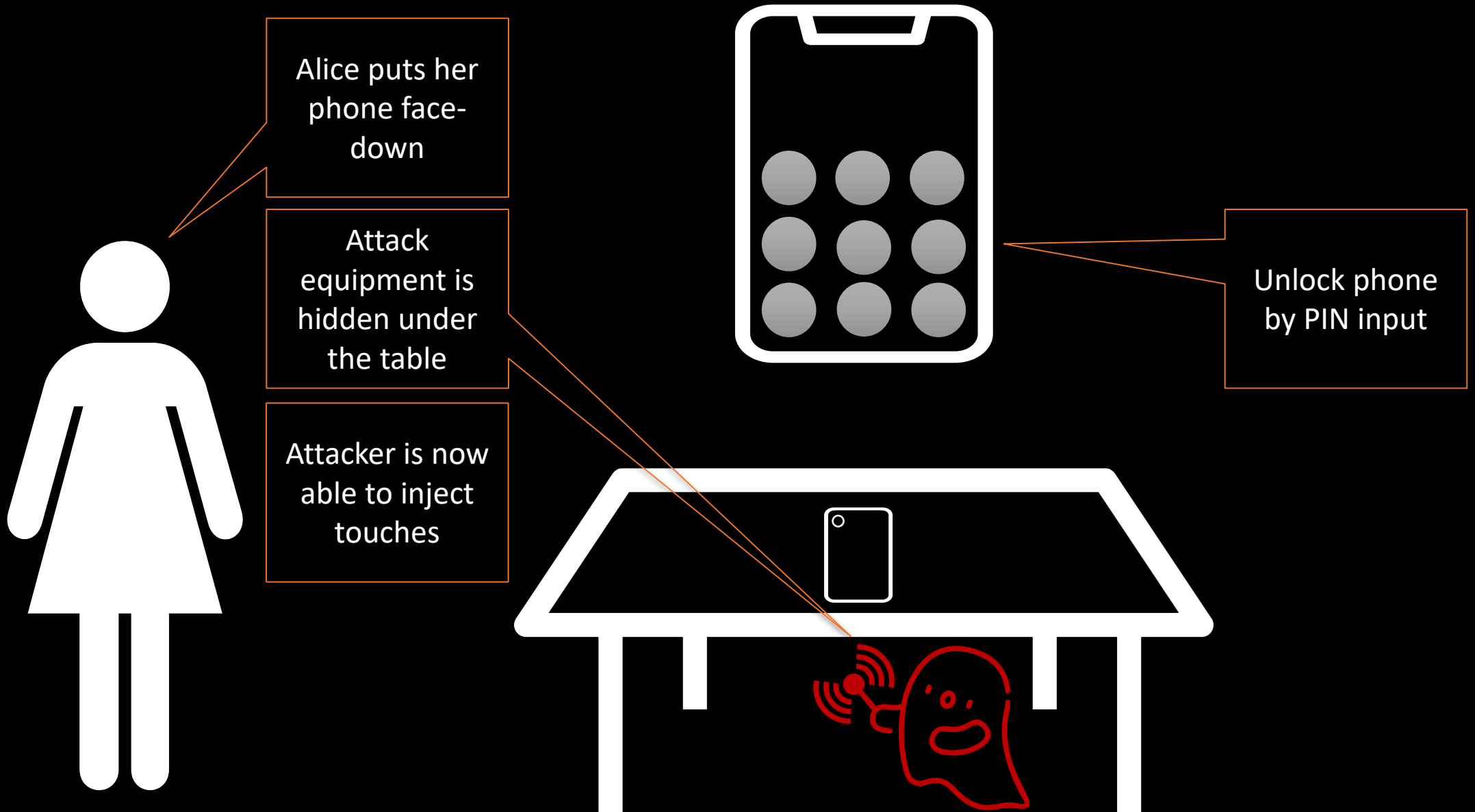
Our Attack


Touch Screen
Broadband EMI to couple to RX line (frequency)
Inject 120 pulses/s to inject at target (area)
Is sensing 120 times/s (pulse frequency)
Sensing circuit
Excitation signal (TX)
Tweak starting time to match excited lines (timing)
Charge signal (RX)
Interprets injected signal as touch at button position
Receiving Line (RX)
Transmitting Line (TX)

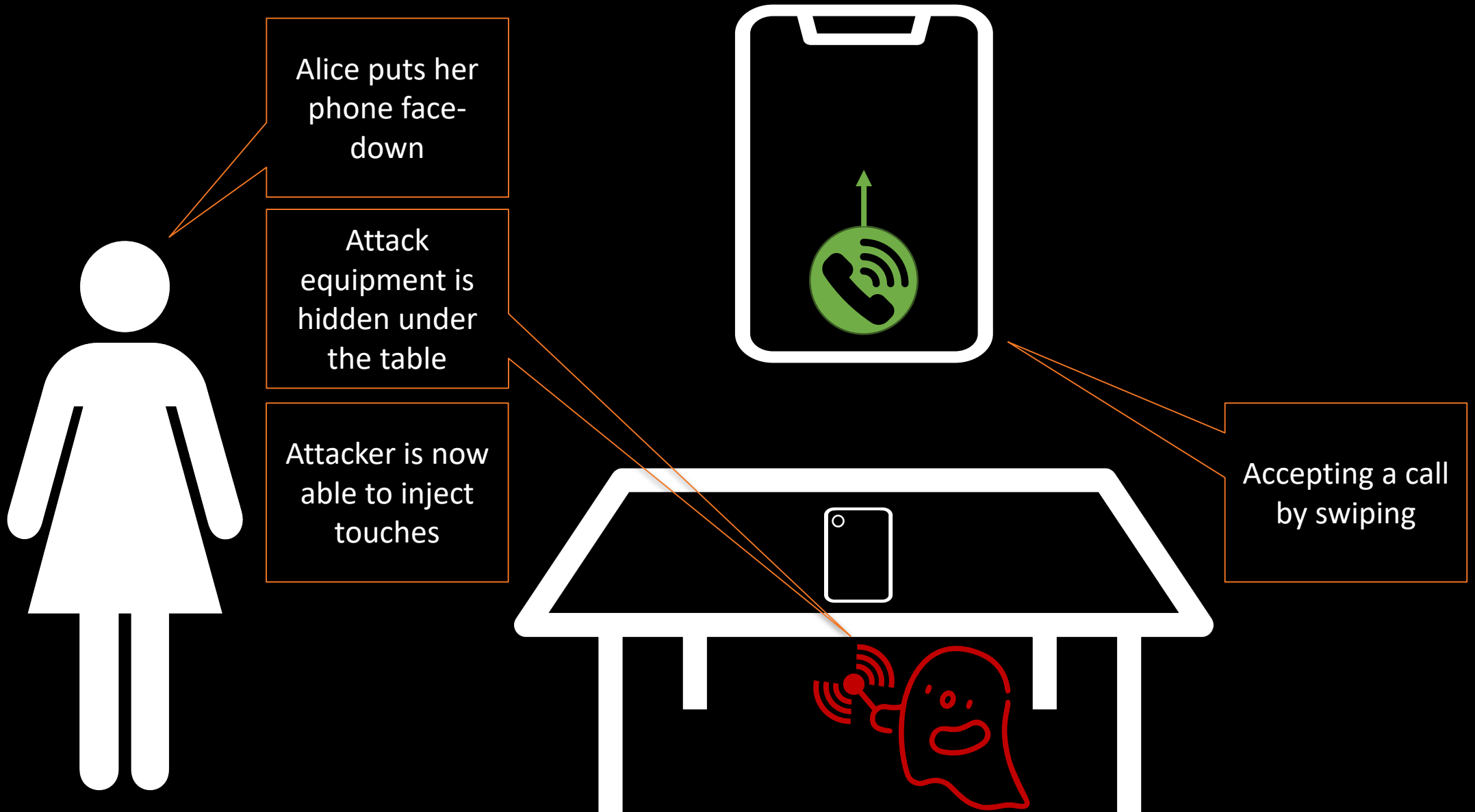
Scenario


Alice puts her phone face-down
Attack equipment is hidden under the table
Attacker is now able to inject touches
Message: Click here
Clicking on malicious link

Scenario

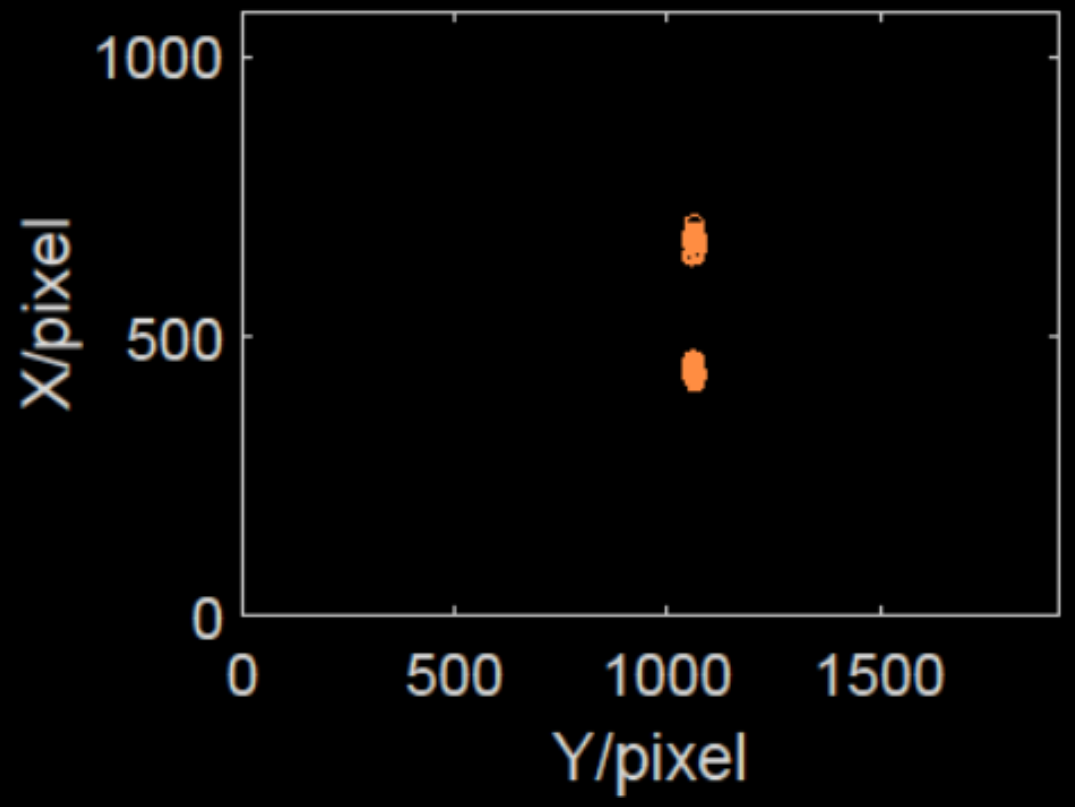

Alice puts her phone face-down
Attack equipment is hidden under the table
Attacker is now able to inject touches
Unlock phone by PIN input

Scenario

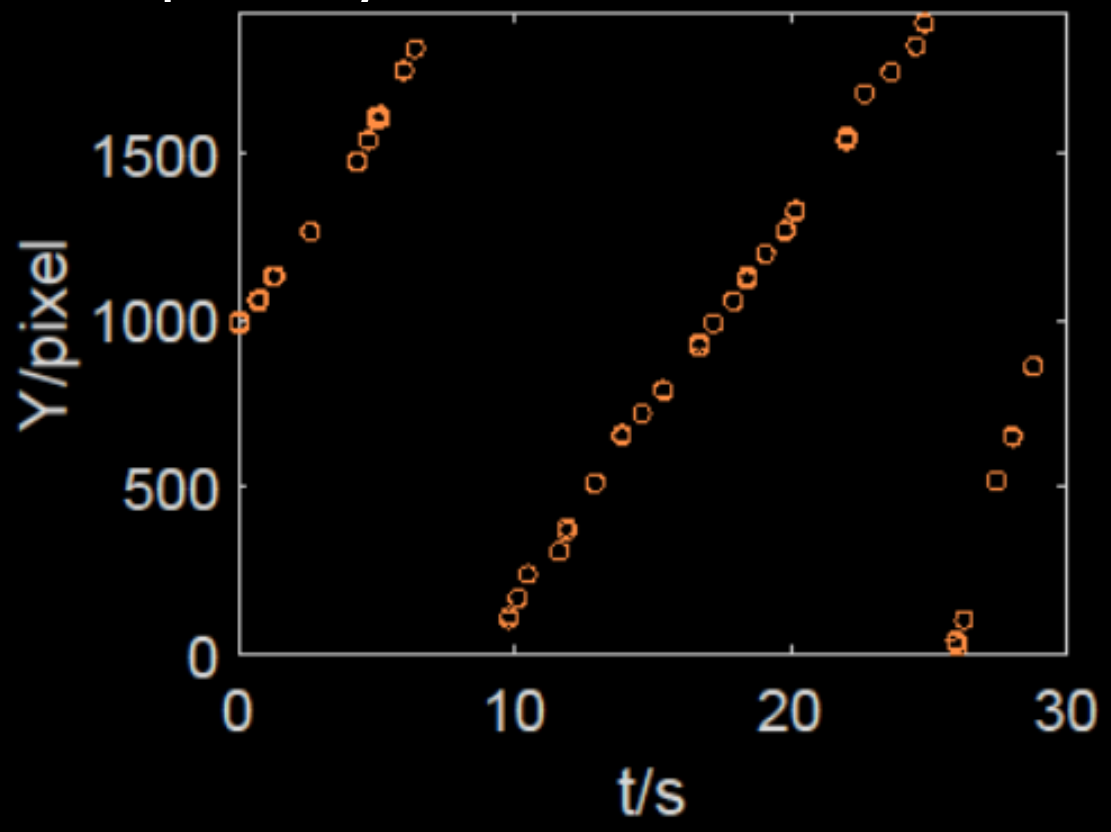

Alice puts her phone face-down
Attack equipment is hidden under the table
Attacker is now able to inject touches
Accepting a call by swiping

Results: Injection

Touch points are consistently injected only at two RX lines



Spaced points are interpreted as "swipes" by the OS



Results: Phones

Phone Model	Success	Price	Injection Speed	Direction	Std/Pixel		Std/mm	
					X	Y	X	Y
Galaxy A10s	✓	$	3.5	Vertical	158.9	111.9	14.9	10.5
Huawei P30 Lite	✓	$$	2.0	Vertical	182.0	189.0	11.1	11.6
Honor View 10	✓	$$$	0.3	Vertical	41.4	4.9	1.3	0.6
Nexus 5X	✓	$$	8.2	Vertical	14.6	19.2	0.9	1.1
Redmi Note 9S	✓	$	2.5	Horizontal	73.3	210.2	4.7	12.5
Nokia 7.2	✓	$$	8.7	Vertical	36.5	156.3	2.3	9.9
Redmi 8	(✓)	$	1.5	Horizontal	N/A	N/A	N/A	N/A
Galaxy S20 FE 5G	(✓)	$$	2.8	Vertical	N/A	N/A	N/A	N/A
iPhone SE (2020)	(✓)	$$	1.0	Vertical	N/A	N/A	N/A	N/A
iPhone 12	×	$$$	N/A	N/A	N/A	N/A	N/A	N/A
Huawei Mate 40 Pro	×	$$$	N/A	N/A	N/A	N/A	N/A	N/A