Tap ’n Ghost

A Compilation of Novel Attack Techniques against Smartphone Touchscreens

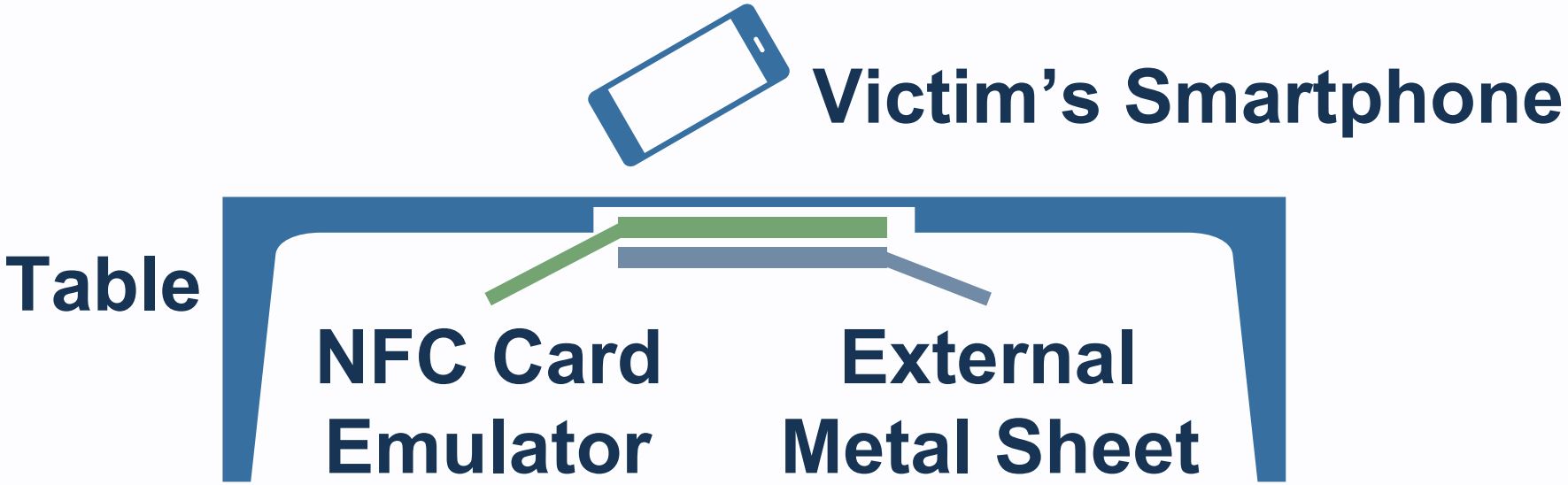
Seita Maruyama [1], Satohiro Wakabayashi [1], Tatsuya Mori [1, 2]

[1] Waseda University, Japan [2] RIKEN AIP, Japan

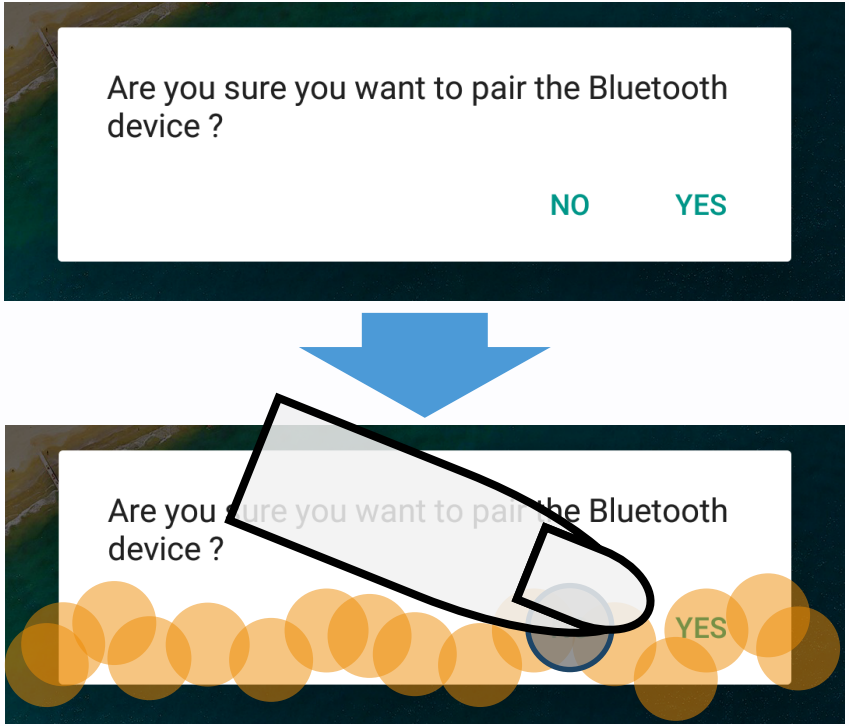
Tap ’n Ghost

- An attack against smartphones
- The attack connects a Bluetooth device or a Wi-Fi access point to the victim's smartphone.
- It consists of two techniques:
  - Attack against NFC-enabled smartphones
  - Attack against Capacitive Touchscreens

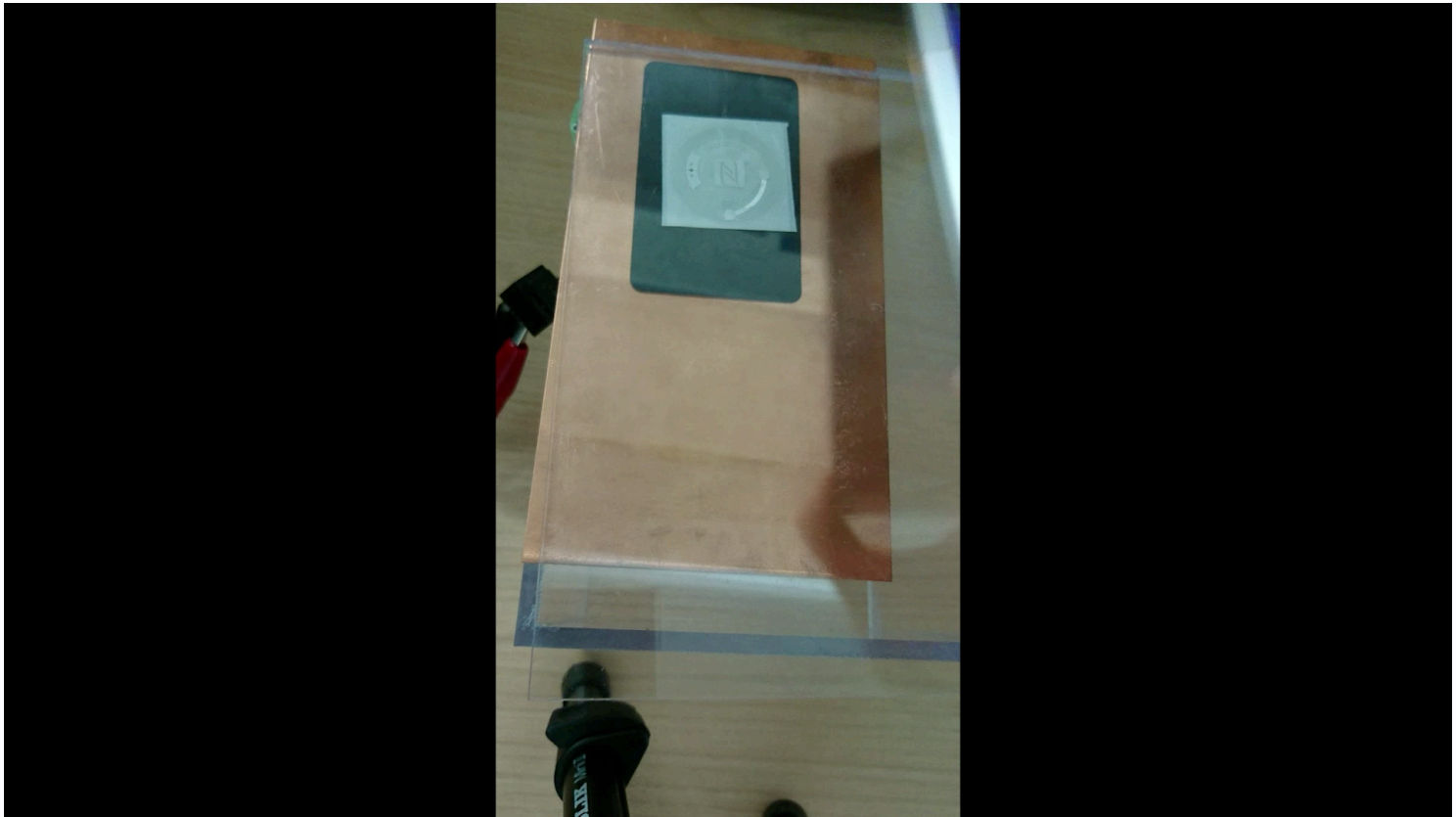
How Our Attack Works



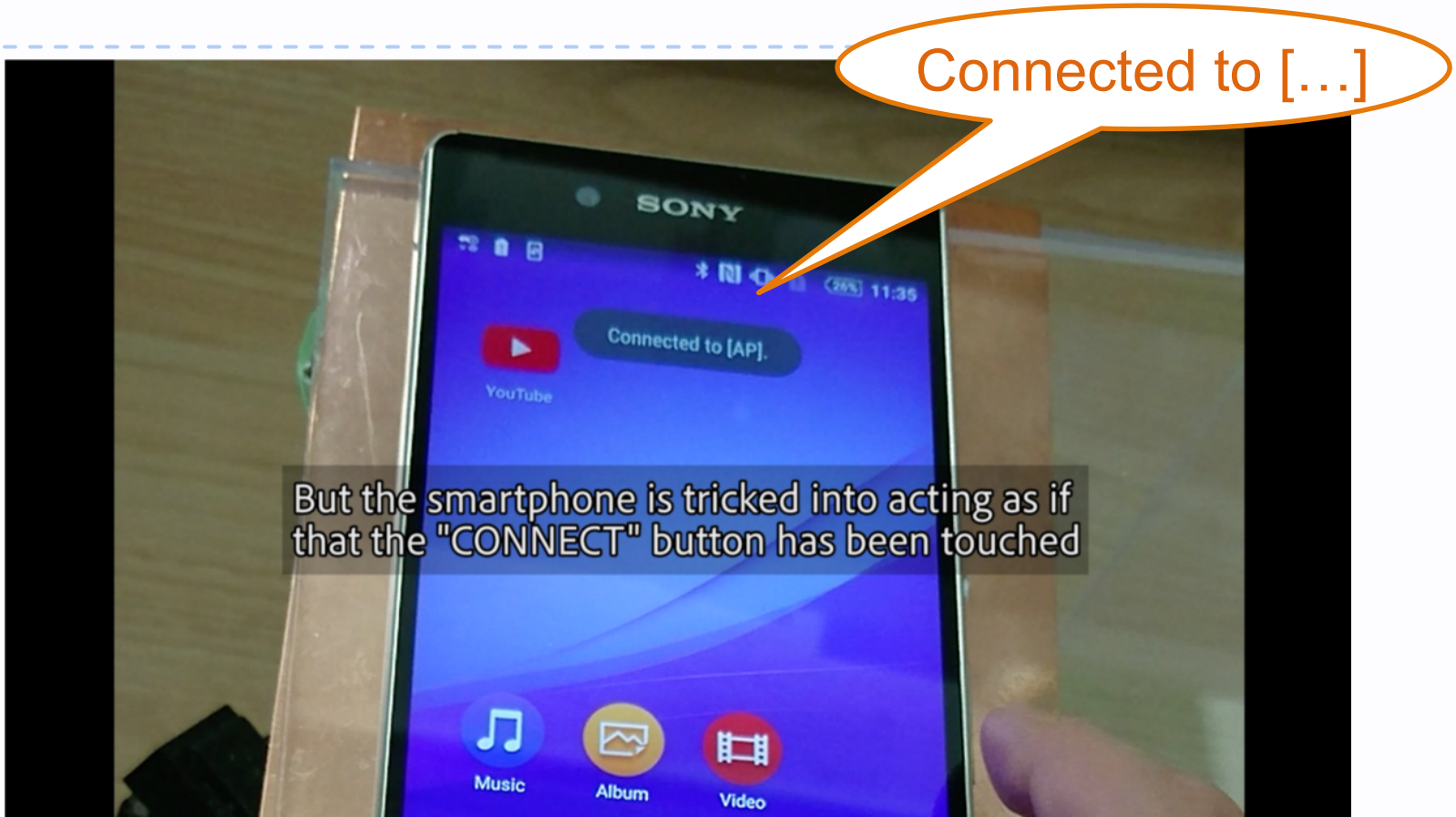
How Our Attack Works



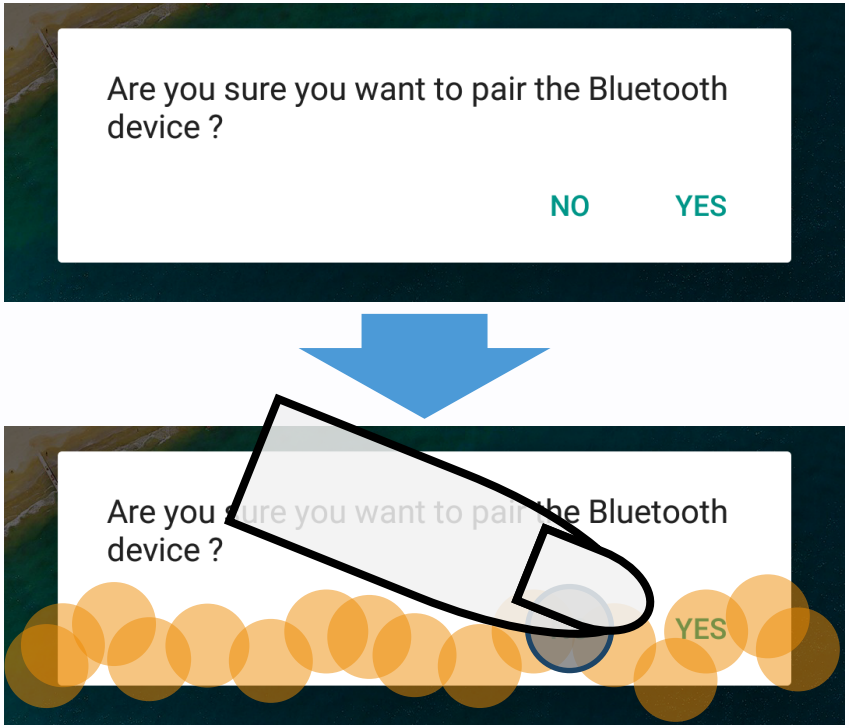
Demo: Overview



Demo: Overview



Two Attack Techniques



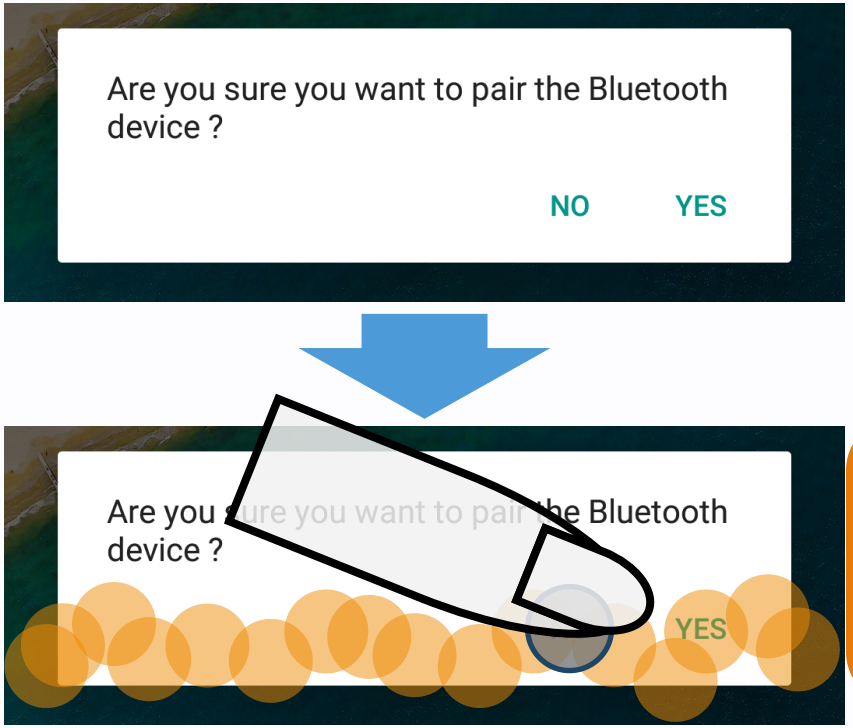
Tag-based Adaptive Ploy:

Attack technique against NFC-enabled smartphones

Ghost Touch Generator:

Attack technique against Capacitive Touchscreens

Two Attack Techniques



Tag-based Adaptive Ploy:

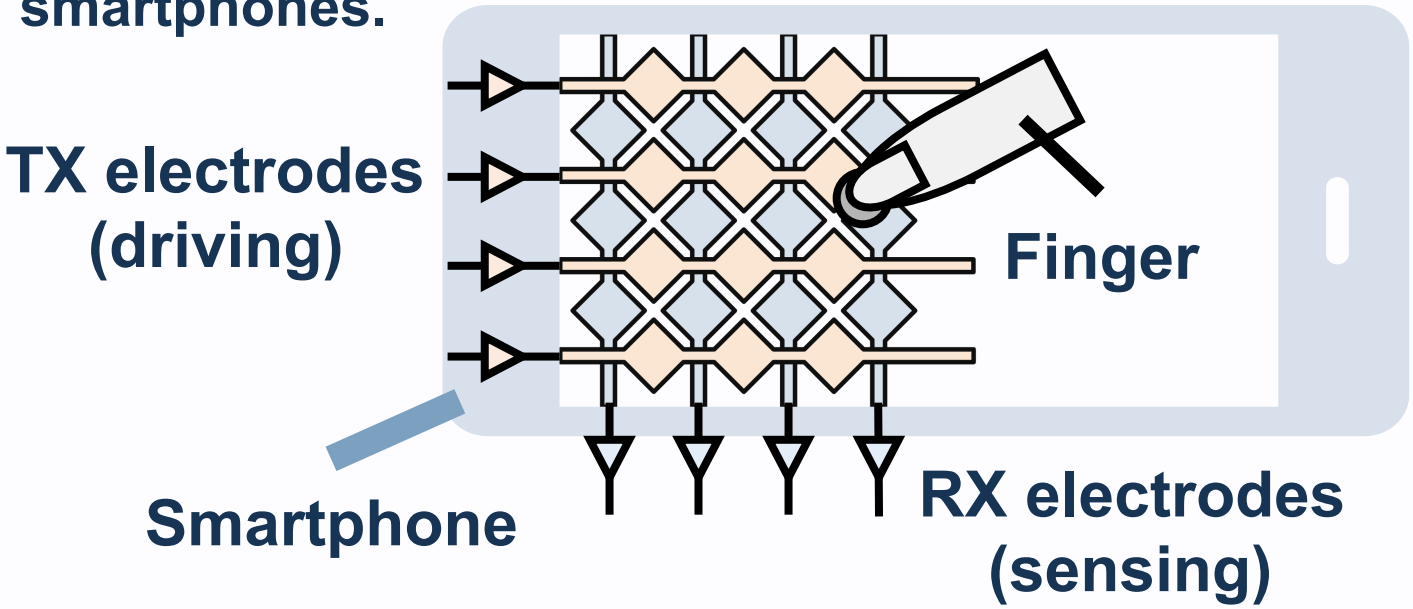
Attack technique against NFC-enabled smartphones

Ghost Touch Generator:

Attack technique against Capacitive Touchscreens

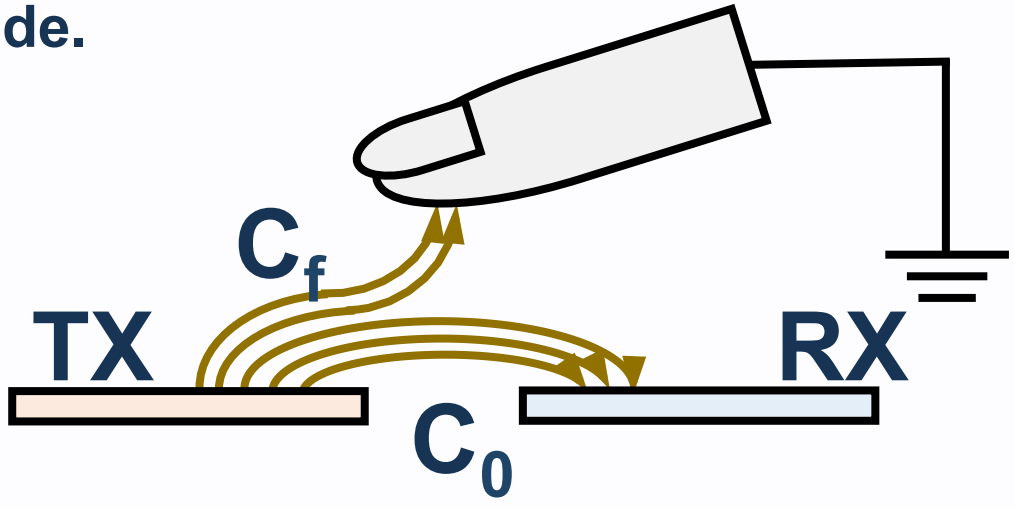
How Touchscreens Work

- Capacitive touchscreens are widely used in smartphones.



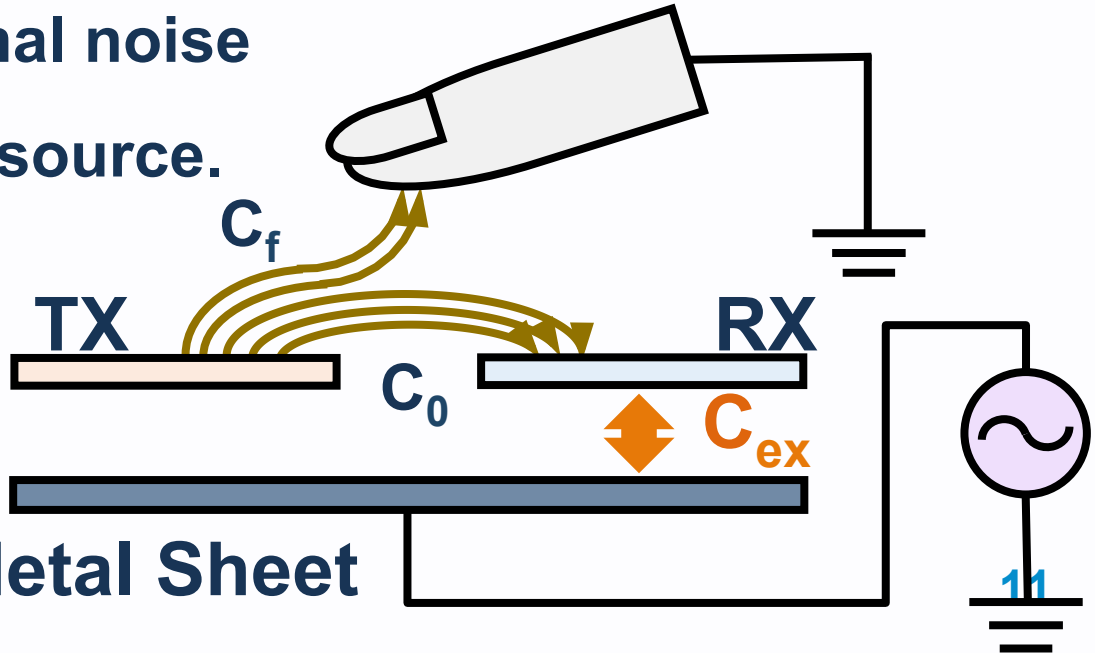
How Touchscreens Work

- Bringing a finger close to the intersection will decrease electrical current flowing into the RX electrode.



Ghost Touch Generator

- The attacker can cause false touch events by injecting intentional noise from an external source.



Demo: Ghost Touch Generator

Ghost Touch Generator

- It causes “false touches” on the 5/7 models.
- The characteristic frequencies vary by model.

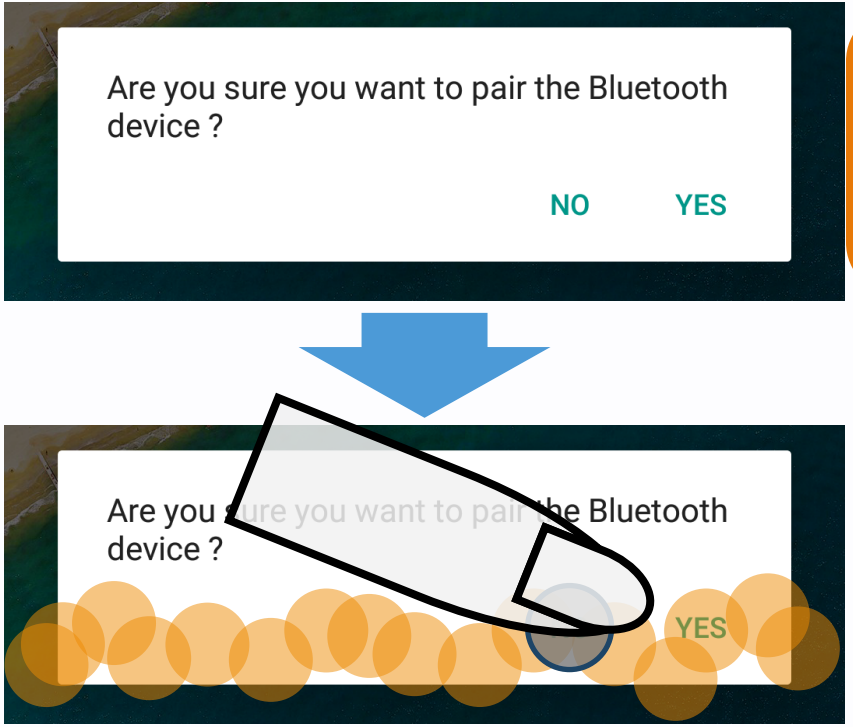
Device	Manufacture	Success false touches	Frequency [kHz]
Nexus 7	ASUS	✓	128.2
ARROWS NX F-05F	FUJITSU		—
Nexus 9	HTC	✓	280.9
Galaxy S6 edge	SAMSUNG		—
Galaxy S4	SAMSUNG	✓	384.5
AQUOS ZETA SH-04F	SHARP	✓	202.0
Xperia Z4	SONY	✓	218.0

Summary of Ghost Touch Generator

1. This attack technique scatters false touches on touchscreens.

2. The attacker needs to identify the smartphone model in advance.

Two Attack Techniques



Tag-based Adaptive Ploy:
Attack technique against NFC-enabled smartphones

Ghost Touch Generator:
Attack technique against Capacitive Touchscreens

NFC

- NFC is a short-range (~10 cm) wireless communication technology

Credit Card

Smartphones

Smart Posters

pocketnow, https://pocketnow.com/android-nfc-app-reveals-contactless-credit-card-details-should-you-be-worried
androidcentral, https://www.androidcentral.com/samsung-pay-uk-everything-you-need-know
nfc Direct, https://nfcdirect.co.uk/44-social-media-nfc-smart-posters

NFC and Android

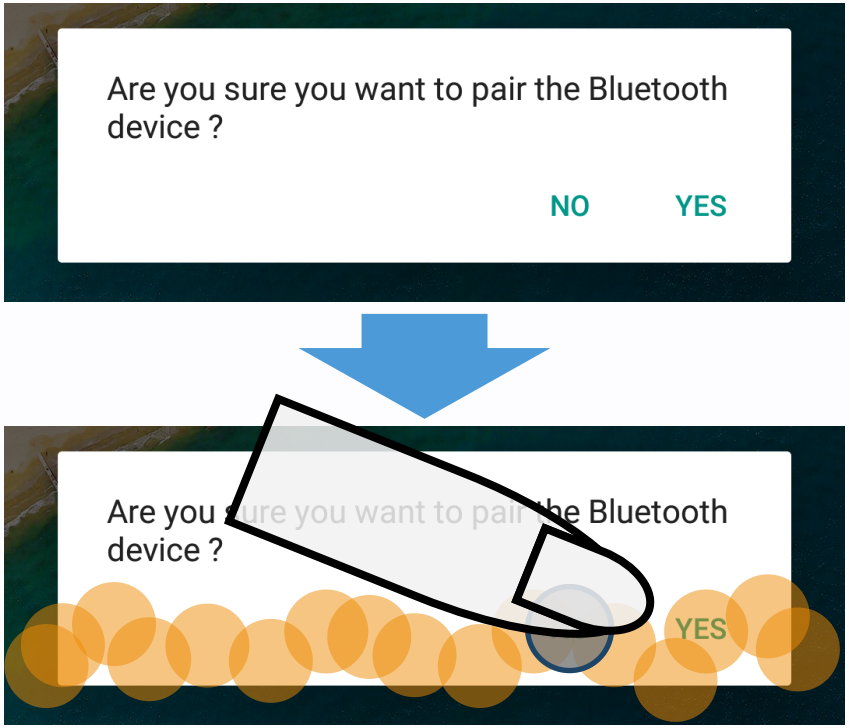
- Android smartphones always look for nearby NFC tags and read it.
- The following operations are launched depending on the NFC tag record:
  - Opening a website
  - Connecting a Wi-Fi access point (with confirmation)
  - Pairing a Bluetooth device (with confirmation)

Tag-based Adaptive Ploy

- NFC emulation enables to emulate an NFC tag, and dynamically change its content.

1. Request to open an attacker's website & identify the smartphone model
2. Request to pair an attacker's Bluetooth device

Summary of Two Attack Techniques



Tag-based Adaptive Ploy:

Attack technique against NFC-enabled smartphones

Gets info & Shows dialog box

Ghost Touch Generator:

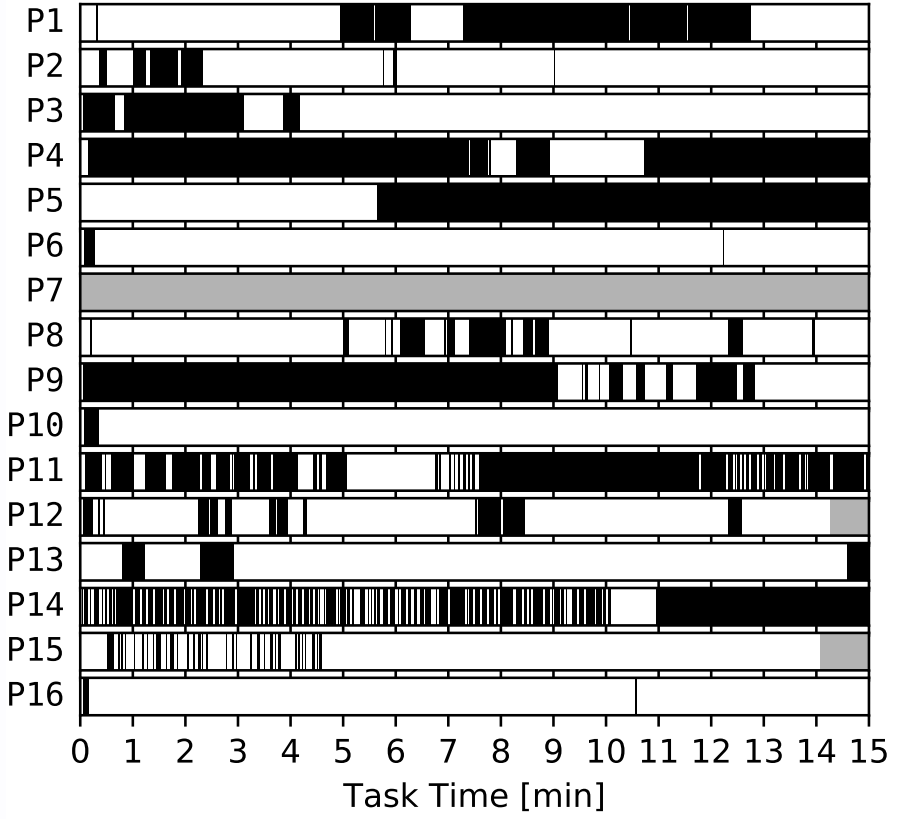
Attack technique against Capacitive Touchscreens

Generates false touches

Feasibility of the Threat

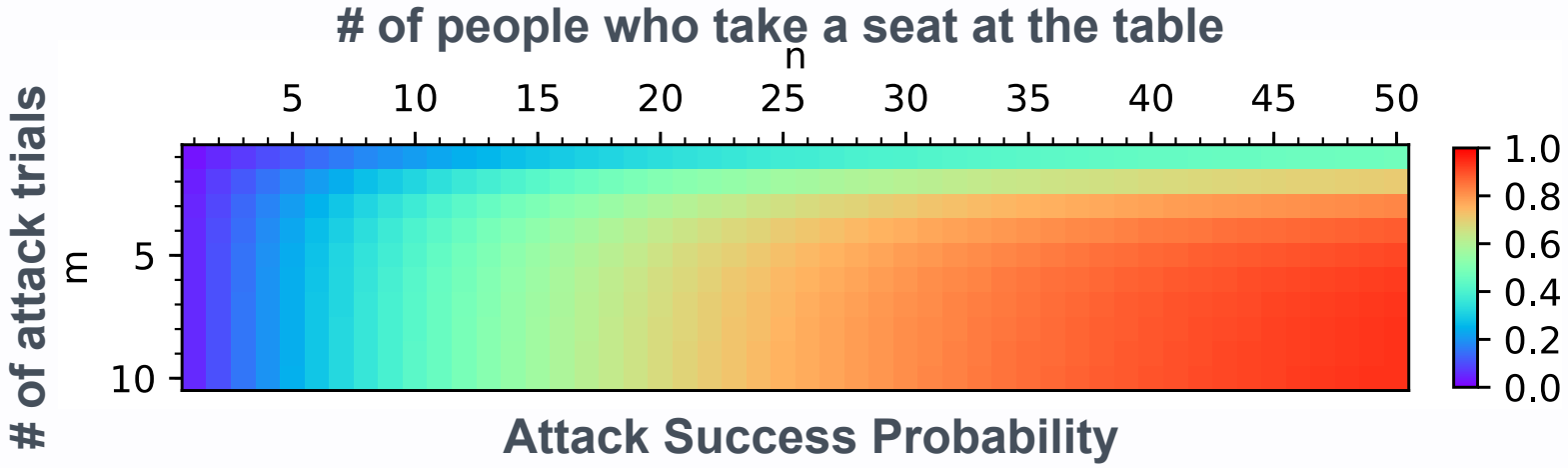
- The attack succeeds only if the victim uses their smartphone within the NFC communication range.
  (NFC communication range < Ghost Touch Generator attack range)
- We conducted a deceptive study to investigate how often the victim's smartphone came within the attack range of the Malicious Table.
  - ➡ 15 out of the 16 participants were attackable.

User Study


P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Task Time [min]

Overall Attack Success Rate

- Overall attack success rate is 71%,
  if 30 people take a seat at the Table and
  the attacker can retry attack 3 times for each person.



Countermeasures

- Add the user approval processes before Android OS launches every operations recorded in a NFC tag (cf. iPhone XS, XS Max, and XR)

- Detect the malfunction on touchscreens
  - Add idle time to TX electrodes, and check noise on RX electrodes
  - Identify the characteristic patterns of false touches

Responsible Disclosure

- With the aid of JPCERT/CC, we have contacted several smartphone manufacturers.

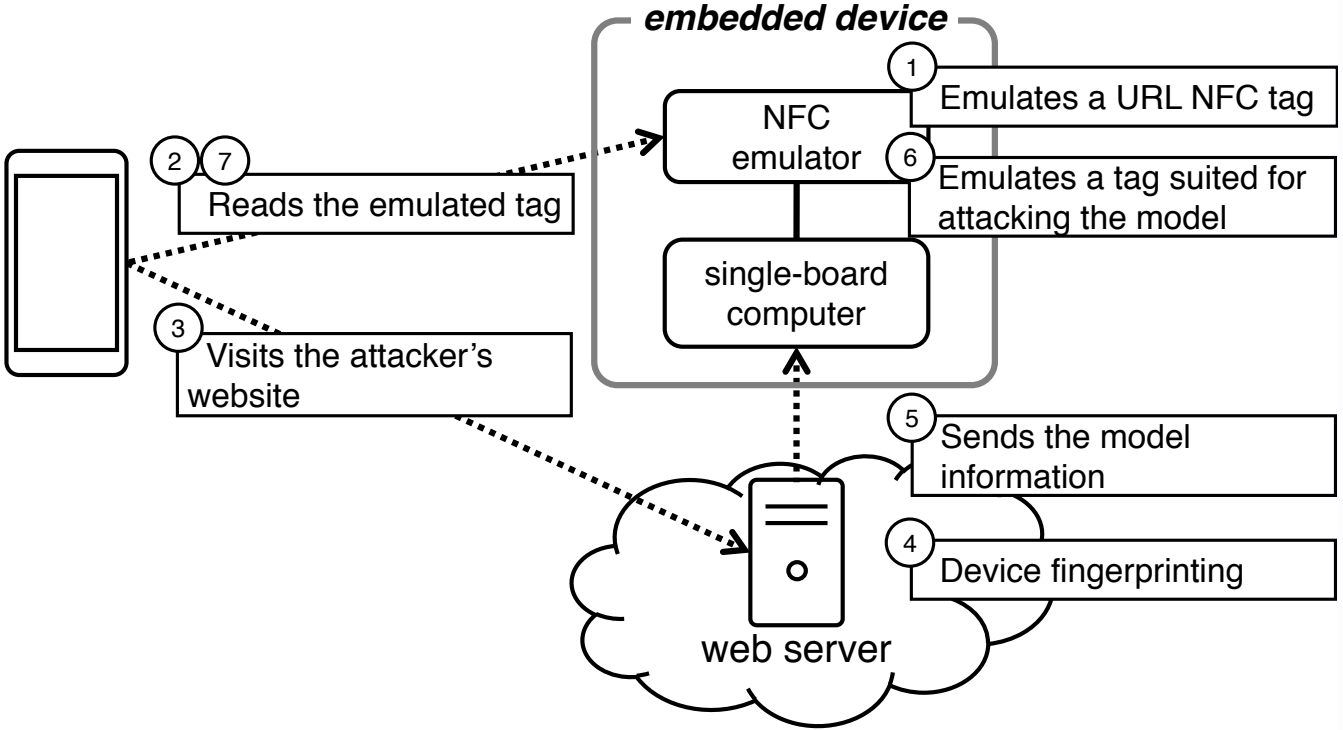
- We demonstrated the attack to them and confirmed that the attack is applicable their latest model.

Conclusion

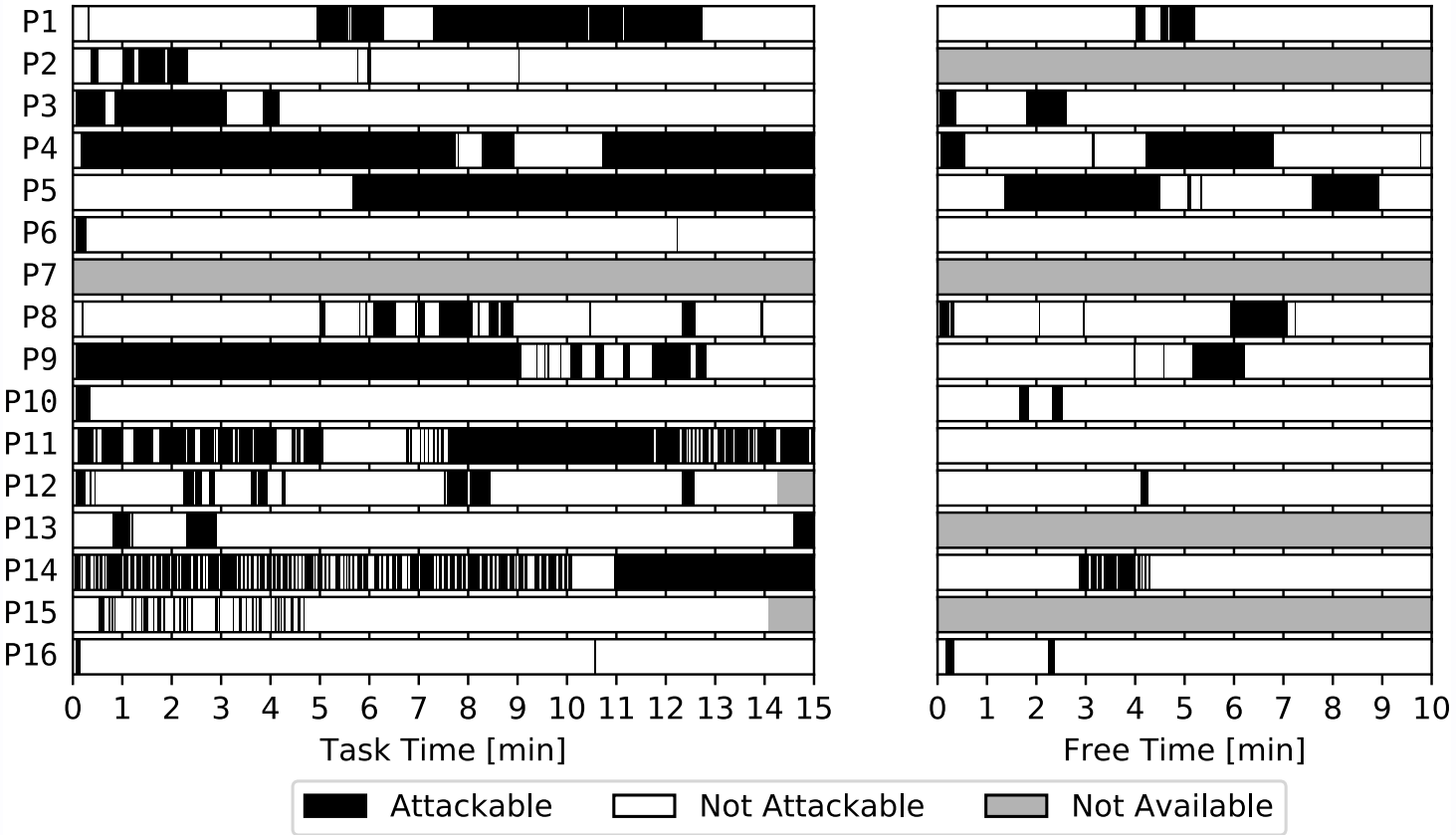
- We presented the new attack “Tap ’n Ghost,” which exploits the NFC and the touchscreen of the victim’s smartphone.
- We demonstrated the attack is feasible.
- We provide possible countermeasures.

Appendix

Tag-based Adaptive Ploy (TAP)



User Study


P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Task Time [min]
0 1 2 3 4 5 6 7 8 9 10
Free Time [min]
Attackable
Not Attackable
Not Available

Attack Conditions

- **Success rate of a single attack:** 3%

- **Following Conditions must be satisfied:**
  - a smartphone comes with Android OS.
  - a smartphone is equipped with NFC.
  - a victim has enabled the NFC functionality.
  - a smartphone's touchscreen controller is attackable with Ghost Touch Generator.
  - a victim has unlocked the smartphone
    when s/he brings it close to the Malicious Table.
  - Ghost Touch Generator attack has succeeded.

Overall Attack Success Rate

- Overall attack success rate is 71%,
  if 30 people take a seat at the Table and
  the attacker can retry attack 3 times for each person.