Tap ’n Ghost
A Compilation of Novel Attack Techniques against Smartphone Touchscreens

Seita Maruyama¹, Satohiro Wakabayashi¹, Tatsuya Mori¹,²

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

Victim’s Smartphone

Table

NFC Card Emulator

External Metal Sheet
How Our Attack Works

Are you sure you want to pair the Bluetooth device?

NO YES

Are you sure you want to pair the Bluetooth device?

YES
Demo: Overview
Demo: Overview

Connected to […]

But the smartphone is tricked into acting as if that the "CONNECT" button has been touched
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**
Capacitive touchscreens are widely used in smartphones.

- TX electrodes (driving)
- RX electrodes (sensing)

Finger on smartphone
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.

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

*For reference, the full results are shown in Table C.3 (Appendix).*
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 is a short-range (~10 cm) wireless communication technology.

[Images of a credit card, smartphones, and NFC-enabled posters with a Facebook Like button.]
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
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 to 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)

1. Emulates a URL NFC tag
2. Reads the emulated tag
3. Visits the attacker’s website
4. Device fingerprinting
5. Sends the model information
6. Emulates a tag suited for attacking the model
7. Embedded device
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.