GhostTouch: Attacks on Touchscreens without Physical Touch

Kai Wang², Richard Mitev¹, Chen Yan², Xiaoyu Ji², Ahmad-Reza Sadeghi¹, Wenyuan Xu²

¹System Security Lab, Technical University of Darmstadt, Germany
²Ubiquitous System Security Lab, Zhejiang University, China

USENIX Security 2022
Capacitive touch screens are ubiquitous

→ High precision
→ Low wear
→ Multi Touch
Motivation

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

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 order to protect a large amount of personal information, there are...

Knowledge Base & Guides

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 T5s, 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
Is it possible to control touch screens remotely using Electromagnetic 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 reading (e.g., sensor)**
  Tu et al. CCS 2019

- **Inject voice in microphone**
  Giechaskiel et al. ESORICS 2019

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

- **Flip bits in embedded devices**
  Selvaraj et al. ASIACCS 2018

- **Fault injection in embedded devices**
  Degbaoui et al. FDTC 2012
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)
Our attack: GhostTouch

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

- Charge signal (RX)
- Excitation signal (TX)
- Scan driving method
- Sensing circuit
- Receiving Line (RX)
- Transmitting Line (TX)
Our Attack

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

Receiving Line (RX)  - Blue
Transmitting Line (TX) - Orange
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

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Success</th>
<th>Price</th>
<th>Injection Speed</th>
<th>Direction</th>
<th>Std/ Pixel</th>
<th>Std/mm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Y</td>
</tr>
<tr>
<td>Galaxy A10s</td>
<td>✓</td>
<td>$</td>
<td>3.5</td>
<td>Vertical</td>
<td>158.9</td>
<td>111.9</td>
</tr>
<tr>
<td>Huawei P30 Lite</td>
<td>✓</td>
<td>$$</td>
<td>2.0</td>
<td>Vertical</td>
<td>182.0</td>
<td>189.0</td>
</tr>
<tr>
<td>Honor View 10</td>
<td>✓</td>
<td>$$$</td>
<td>0.3</td>
<td>Vertical</td>
<td>41.4</td>
<td>4.9</td>
</tr>
<tr>
<td>Nexus 5X</td>
<td>✓</td>
<td>$$</td>
<td>8.2</td>
<td>Vertical</td>
<td>14.6</td>
<td>19.2</td>
</tr>
<tr>
<td>Redmi Note 9S</td>
<td>✓</td>
<td>$</td>
<td>2.5</td>
<td>Horizontal</td>
<td>73.3</td>
<td>210.2</td>
</tr>
<tr>
<td>Nokia 7.2</td>
<td>✓</td>
<td>$$</td>
<td>8.7</td>
<td>Vertical</td>
<td>36.5</td>
<td>156.3</td>
</tr>
<tr>
<td>Redmi 8</td>
<td>✓</td>
<td>$</td>
<td>1.5</td>
<td>Horizontal</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Galaxy S20 FE 5G</td>
<td>✓</td>
<td>$$</td>
<td>2.8</td>
<td>Vertical</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>iPhone SE (2020)</td>
<td>✓</td>
<td>$$</td>
<td>1.0</td>
<td>Vertical</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>iPhone 12</td>
<td>×</td>
<td>$$$</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Huawei Mate 40 Pro</td>
<td>×</td>
<td>$$$</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>