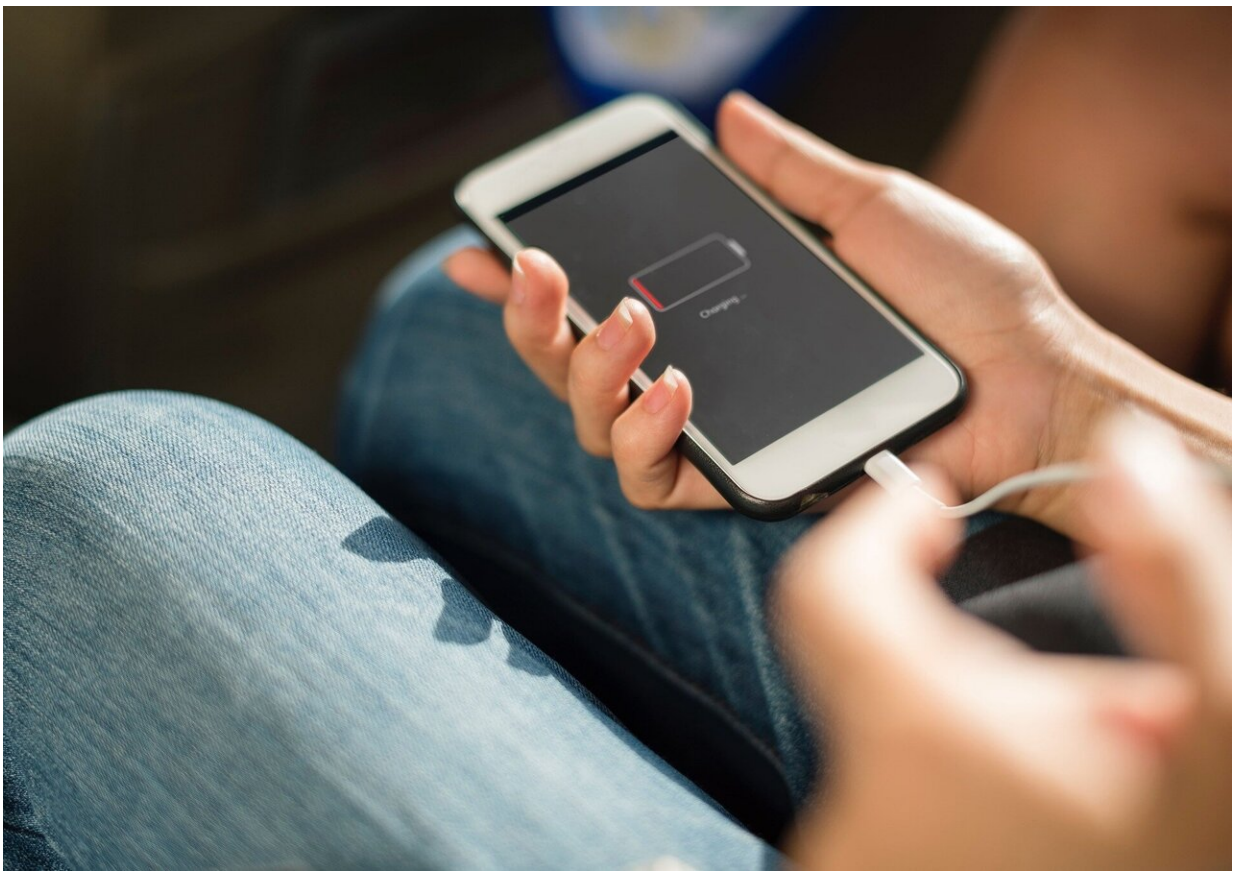
Thwarting attacks from the charging socket: Team explores protecting mobile device touchscreens from 'ghost touch'

July 20 2022, by Silke Paradowski



Credit: CC0 Public Domain

Touch screens on mobile devices can be attacked and manipulated via

charging cables and power supply units. This is what researchers at the System Security Lab at TU Darmstadt have discovered together with a Chinese research team. Several smartphones and standalone touchscreen panels could be compromised in practical tests by simulated touches, the "ghost touches." The results were presented at this year's IEEE Symposium on Security and Privacy.

The researchers from TU Darmstadt and Zhejiang University in Hangzhou carried out attacks on capacitive touchscreens via charging cables and power adapters, revealing a new way to attack mobile devices. Similar to their previous research project, "GhostTouch," the researchers were able to create false touches, called "Ghost Touches," on multiple touchscreens and manipulate the device via them.

The international research team had to overcome two main challenges. The first was to affect the capacitive touchscreens via a charging-only cable without damaging the hardware. Electronic devices are usually equipped with resistive filters in the circuits to ensure a stable power supply. It was necessary to design an attack that would work even if users were using a charging-only cable without a data channel, which is typically used in public spaces for privacy and security reasons. Second, the touch points had to be specifically controlled in order to manipulate the device. This was necessary so that—for example—malicious Bluetooth connections could be established, users could be tapped by a phone call, or malware could be received.

In the test setup, a compromised public charging station was assumed to be the starting point of the attack. A manipulated USB charging socket, whose power supply could be controlled remotely, was used. Such publicly accessible charging stations are often found in cafés, in hospitals, hotels or at airports and train stations. Anyone who charges their smartphone or tablet at this charging station initiates the attack, which is initially disguised as a normal charging signal. The attacker

measures the sampling frequency of the touchscreen via the charging connection in order to adapt the attack signal. Beyond that, no data connection is necessary.

A sophisticated attack signal is injected into the GND line, i.e. the ground line, via the charging line. The attack signal, which is injected via the USB interface, affects the power supply and is converted into a noise signal due to the lack of filtering. With the help of these noise signals, three different attack effects can be achieved, which are related to the typical structure of capacitive displays.

The main component of a touchscreen is a matrix of rows and columns of conductive electrodes (TX) and sensing electrodes (RX), whose crossing points are called mutual capacitance. When one touches the screen, the finger forms an additional capacitance with the electrodes and changes the equivalent capacitance, creating a touch event and allowing the smartphone to be controlled.

The researchers were able to achieve targeted ghost touches along both the TX electrodes and the RX electrodes without physical contact. Furthermore, the screen could be manipulated in such a way that it no longer responded to real touches.

In addition to the attack scenarios, the international research team also describes possible software-based and hardware-based countermeasures in their paper, which was published at the IEEE Symposium on Security and Privacy 2022. Looking further to a hardware-based functional tool that disrupts the common-mode attack signal, software-based measures can be used to detect altered capacity or to identify reliable charging stations in a manner similar to the fingerprint mechanism.

More information: Yan Jiang et al, WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens, *2022 IEEE Symposium on Security*

and Privacy (2022). DOI: 10.1109/SP46214.2022.00108
www.computer.org/csdl/proceedi … 1600b537/1CIO7Ic5kR2