WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens

Yan Jiang[1], Xiaoyu Ji[1†], Kai Wang[1], Chen Yan[1], Richard Mitev[2], Ahmad-Reza Sadeghi[2], Wenyuan Xu[1†]
[1]Ubiquitous System Security Lab (USSLAB), Zhejiang University
[2] System Security Lab, Technical University of Darmstadt
{yj98, xji, eekaiwang, yanchen, wyxu}@zju.edu.cn, {richard.mitev, ahmad.sadeghi}@trust.tu-darmstadt.de

***Abstract*—The security of capacitive touchscreens is crucial since they have become the primary human-machine interface on smart devices. To the best of our knowledge, this paper presents WIGHT, the first wired attack that creates ghost touches on capacitive touchscreens via charging cables, and can manipulate the victim devices with undesired consequences, e.g., allowing malicious Bluetooth connections, accepting files with viruses, etc. Our study calls for attention to a new threat vector against touchscreens that only requires connecting to a malicious charging port, which could be a public charging station, and is effective across various power adapters and even USB data blockers. Despite the fact that smartphones employ abundant noise reduction and voltage management techniques, we manage to inject carefully crafted signals that can induce ghost touches within a chosen range. The underlying principle is to inject common-mode noises over the power line to avoid being effectively filtered yet affect the touch measurement mechanism, and synchronize the malicious noise with the screen measurement scanning cycles to place the ghost touches at target locations. We achieve three types of attacks: injection attacks that create ghost touches without users touching the screen, alteration attacks that change the detected legitimate touch position, and Denial-of-Service attacks that prevent the device from identifying legitimate touches. Our evaluation on 6 smartphones, 1 tablet, 2 standalone touchscreen panels, 6 power adapters, and 13 charging cables demonstrates the feasibility of all three type attacks.**

***Index Terms*—Touchscreen, ghost touch, conducted noise**

I. Introduction

As capacitive touchscreens have become essential interfaces for humans to interact with a variety of consumer electronics, e.g., smartphones, tablets, and even vehicles [1], [2], reliable touch operation becomes critical not only for usability but also for security. Several recent news has reported "Ghost Touch", i.e., the touchscreen outputs fake touches and starts to control the device by itself yet users impose no physical contacts on the screen at all [3], [4], [5], [6]. In one case [6], the ghost touches on a charging smartphone booked a presidential suite that cost more than a thousand dollars by itself without raising the user's awareness. To the best of our knowledge, this phenomenon has not been studied before and motivates us to investigate the trustworthiness of capacitive touchscreens as well as their security implication on the victim devices. Particularly, we analyze the underlying causes and investigate whether a malicious attacker can intentionally create ghost touches for device exploitation.

†Xiaoyu Ji and Wenyuan Xu are corresponding authors.

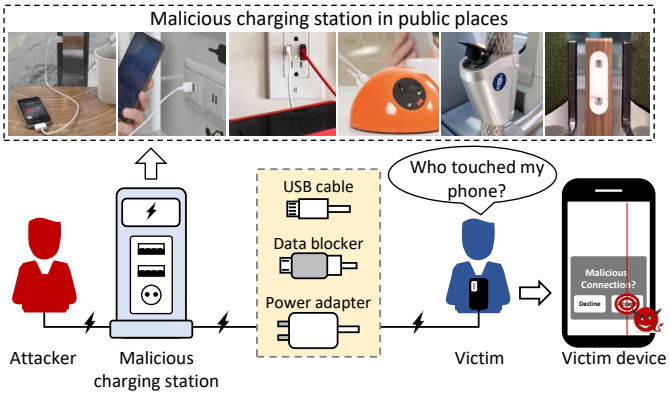


Fig. 1. Illustration of WIGHT attacks. When a user charges his smartphone at a malicious charging station via a charging cable, an attacker can inject elaborate signals to generate ghost touches on the touchscreen or to disable the touch service, even across a power adapter or a USB data blocker.

This paper discovers a new type of threat vector against touchscreens: An attacker injects malicious touches to the touchscreen of a smartphone via its charging cable and power adapter as shown in Fig. 1, instead of via an electric field [7] or electromagnetic (EM) radiation [8]. We call such attacks WIGHT, and we envision that the attack device can be a malicious public charging station as shown in Fig. 1, which is widely used in cafes, hospitals, hotels, etc. [9]. When users charge their devices publicly, the attacker transmits a carefully crafted malicious signal via the power lines to the victim device such that it induces ghost touches on the touchscreen and manipulates the device, e.g., tapping the button to accept a malicious connection. Since such attacks only utilize the power lines as the attack surface, they are harmful even to those security-conscious users who may disable the USB data connection with data blocker gadgets.

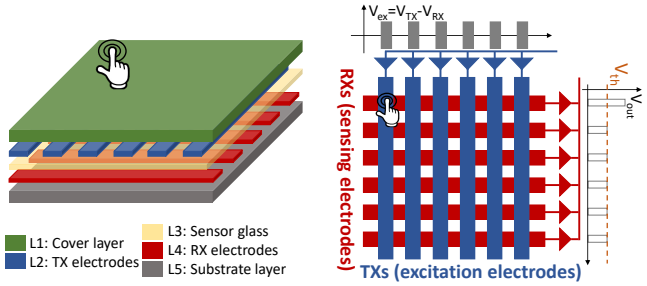
Injecting challenge. Injecting ghost touches via charging cables is difficult. Essentially, the malicious signals injected via charging cables are noises, and modern devices are equipped with abundant noise reduction [10] and voltage management technique [11] to ensure stable power supply and safe operations. Unsurprisingly, technologies ranging from noise filters, voltage converters, and regulators, to power management integrated circuits (PMIC), will eliminate noise. To inject ghost touch successfully, a naive method will be in-

creasing the noise strength large enough such that the injected signals survive these reduction technologies, which, nevertheless, may damage the hardware of devices. To overcome this challenge, we manage to inject a common-mode (CM) signal by applying signals to the GND line of the charging cable. We find that the CM signal can not be filtered completely and can result in a differential-mode (DM) signal due to the asymmetric circuits [12]. The DM signal can interfere with the measurement of the touchscreen capacitance such that it emulates the scenarios as if a user is touching the screen.

Controlling challenge. Controlling the positions of ghost touches via a single charging cable is challenging since attackers have little control over how and where the injected malicious signals traverse over the complicated device circuits. To overcome the challenge, we propose signal enhancement, and synchronization strategies to fulfill desired and controllable ghost touches. Firstly, below the surface of a capacitive touchscreen is an array of parallel electrodes, and the position of a genuine touch is identified by exciting the electrodes sequentially and measuring the capacitance changes. Thus, measuring the excitation signal cycle and synchronizing the malicious signals accordingly may induce ghost touches within the targeted position range. Secondly, touchscreens are designed to be robust against external EMI or electrostatic discharge (ESD) [13], which can be exploited: Applying a strong EMI or ESD can cause the touch service to be temporarily disabled by the ESD-induced soft failures [14]. Thus, by designing the strength, frequency, and timing of the malicious signals, we achieve controllable ghost touch injection.

`WIGHT` achieves three types of attacks: *injection attacks, alteration attacks, and Denial-of-Service (DoS) attacks.* Injection attacks can induce ghost touches along a chosen line on the screen without the user touching the screen. Alteration attacks induce ghost touches along the line that the user touches, i.e., altering the detected touch position. DoS attacks can prevent the device from identifying the user's normal touch operations. The three attacks can be combined to achieve the undesired consequences such as connecting to a malicious Bluetooth connection, etc. We evaluated the performance of `WIGHT` on 6 smartphones, 1 tablet, 2 standalone touchscreen panels, 6 power adapters, and 13 charging cables. The results show that `WIGHT` can achieve three types of attacks (injection attacks, alteration attacks, DoS attacks) at the success rates of 93.33%, 66.67%, and 100%, respectively. We summarize our major contributions as follows:

- We propose `WIGHT`, the first ghost touch attack against capacitive touchscreens by injecting signals via a charging cable (with or without a power adapter). `WIGHT` can inject ghost touches regardless of whether the screen is being touched or not and can disable the touch-based input of victim devices.
- We analyze the underlying principle of successful ghost-touch injection theoretically and experimentally. We find that due to the asymmetric circuits, a CM noise on the power line can be converted into a DM noise, which interferes with the capacitance measurement of the touchscreen and causes ghost touches.
- We validated the feasibility of `WIGHT` on 9 commercial touchscreen devices and proposed countermeasures to mitigate the threat.



(a) Overview of touchscreen. (b) Top view of electrodes.

Fig. 2. A typical structure of capacitive touchscreens.

II. Background

In this section, we introduce the background knowledge of capacitive touchscreen and electromagnetic interference.

A. Capacitive Touchscreen

Capacitive touchscreens sense touch by measuring the capacitance changes induced by physical contacts of a user. Since they can detect multiple touches simultaneously, they become the dominant screens for smartphones and tablets [2], [15], [16]. To detect a touch, a capacitive touchscreen and its auxiliary sensing circuit work together to detect the capacitance variation caused by a touch.

1) Structure of Capacitive Touchscreen: A typical mutual capacitive touchscreen has five layers, as shown in Fig. 2(a): a cover layer, TX electrodes (TXs), a sensor glass, RX electrodes (RXs), and a substrate layer. The critical component of a touchscreen is a conductive electrode matrix consisting of TXs and RXs, forming a mesh of mutual capacitors, whereby each crosspoint of the electrodes forms a parallel-plate mutual capacitor [17], [18], as shown in Fig. 2(b).

To localize a touch, TXs are excited sequentially by the excitation signal with its magnitude being V_{ex}, where $V_{ex} = V_{TX} - V_{RX}$, and V_{TX} and V_{RX} are the potential of TXs and RXs, respectively. The excitation signals are alternating current (AC) signals, e.g., sine or square waves, and will drive the outputs of the sensing circuit, V_{out}, which reflects the capacitance changes proportionally. Since each TX electrode is overlaid with n RX electrodes, the sensing circuit will output n V_{out} with each mapping to the capacitance change at the corresponding crosspoint. Once a user touches a crosspoint on the screen with a finger, the mutual capacitor underneath will change and the V_{out} will exceed the threshold V_{th}. Thus, detecting the location of a touch is equivalent to finding the V_{out} that exceeds the threshold.

2) Sensing Circuit: The main role of the sensing circuit is to convert the capacitance change into the output V_{out} proportionally, which will then be digitized by an analog-digital converter (ADC) and processed by a CPU. A typical

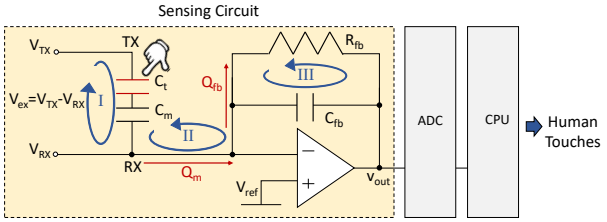


Fig. 3. A typical capacitance sensing circuit. The capacitance variation caused by a finger can be expressed as a voltage output of the sensing circuit, which is further processed by ADC and CPU for detecting the touch event.

schematic diagram of the sensing circuit in the capacitive touchscreen consists of a few capacitors, a resistor, and a non-inverting operational amplifier that connected to the reference voltage V_{ref} [2], as shown in Fig. 3. Since the amplifier has the two properties: no current flows into the inputs of the amplifier, and the voltages at the two inputs are the same, it can be approximately treated as an extremely large resistor. When an excitation signal is applied between the TX and RX electrodes, a current flows through the mutual capacitor C_m and the feedback capacitor C_{fb}, and charges them. At the end of excitation cycle, the charge at the feedback capacitor C_{fb} determines the output voltages V_{out} [2], [19], [20]. When a user touches the screen, the finger acts as an electrode and forms capacitors with the TX and RX electrodes, and we model them with an equivalent capacitor C_t in series with C_m. Note that C_t is typically a negative value [16]. To understand how V_{out} is determined, we borrow the idea of loop analysis methods of electric circuits, and consider the sensing circuit containing three-loop currents in parallel [16], [21], the charging, transferring, and discharging loops.

(I) *The charging loop*. The goal of this loop is to gain charges from the excitation signals. The charging loop current flows through the capacitor C_m and possibly C_t. When an excitation signal is applied, the capacitors alternate between charging and discharging status as the potentials of the excitation signal alternate between positive and negative values. The stored charge Q_m over the capacitors can be formulated as [18]:

$$NoTouch : Q_m = 2C_m V_{ex} \quad (1)$$
$$FingerTouch : Q_m = 2(C_m + C_t)V_{ex} \quad (2)$$

(II) *The transfer loop*. The goal of this loop is to transfer the charges gained by the charging loop to the feedback circuit. This is designed to improve the precision of the touch detection, as the transferred charges Q_m are accumulated at the feedback capacitor C_{fb} over multiple excitation pulses [2]. According to the law of charge conservation [2], [22], the amount of charges gained from the charging loop equals to the one transferred to C_{fb}, and in case of no touch we have

$$Q_m = Q_{fb} \quad (3)$$
$$2C_m V_{ex} = C_{fb}(V_{ref} - V_{out}) \quad (4)$$

where Q_{fb} is the charge stored in the feedback circuit.

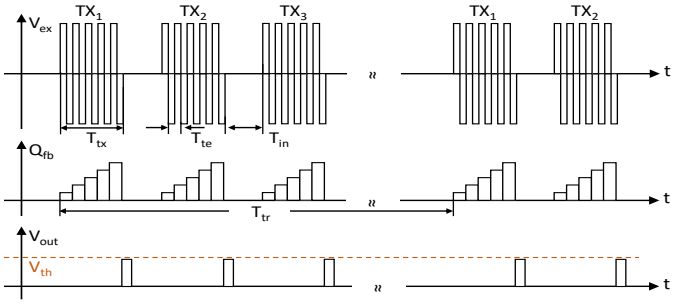


Fig. 4. Waveform diagrams of the time-interleaved sensing method. (a) Top: excitation signal. (b) Middle: charge integral of the sensing circuits. (c) Bottom: output of sensing circuit.

Subsequently, the output of the sensing circuit V_{out} is proportional to the mutual capacitance C_m between TXs and RXs [21] and is

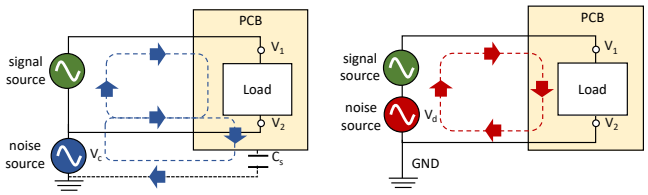
$$NoTouch : V_{out} = V_{ref} - 2C_m V_{ex}/C_{fb} \quad (5)$$
$$FingerTouch : V_{out} = V_{ref} - 2(C_m + C_t)V_{ex}/C_{fb} \quad (6)$$

(III) *The discharge loop*. This loop current flows through the feedback capacitor C_{fb} and the feedback resistor R_{fb}, representing the situation that the charges accumulated over the feedback capacitor are inevitably discharged.

3) Time-Interleaved Sensing Method: The time-interleaved sensing method is widely adopted in mutual capacitive touchscreens, whereby the excitation signals are applied to each TX electrode sequentially in the round-robin style, e.g., each TX electrode is scanned once in each scanning cycle, denoted by T_{tr} [23], [24], [18], [25]. Fig. 4 illustrates the signal waveform of excitation signals, charges at the feedback capacitors, and the output of the sensing circuit in the time-interleaved sensing method. (a) The excitation signal is a series of AC waveform alternating between on and off. The signal is turned on for a duration of T_{tx} to excite each TX electrode, and turned off for an interval of T_{in} to prepare for the next TX electrode. It takes a duration of T_{tr} to scan each TX once, and thus the touch refresh rate $1/T_{tr}$ reflects how sensitive the touchscreen can detect a touch event in terms of time, which is generally in the range of 60 Hz to 200 Hz [19], [26]. For each TX electrode, multiple cycles of AC signals are applied to improve the signal-noise ratio (SNR) of touch identification [19], and we denote T_{te} to be the period of the AC signal, which typically has the frequency in the range of 100 kHz to 500 kHz [26]. (b) The charge stored in the feedback capacitor exhibits a form of staircases over time as a result of multiple cycles of excitation [24]. (c) The output signal of the sensing circuit V_{out} is a sequence of square pulses with a magnitude proportional to the transferred charge. Note that if V_{out} is greater than V_{th}, the touch event will be detected [19].

B. Electromagnetic Interference

Essentially, WIGHT induces ghost touches by injecting Electromagnetic Interference (EMI), which is an electrical noise affecting the performance of electrical circuits [27], [28], [29].



(a) Common-mode EMI. (b) Differential-mode EMI.

Fig. 5. Schematic diagrams of common-mode EMI and differential-mode EMI.

Injected over charging cables, such types of noises are conducted EMI and propagate as a current via physical conductive routes, e.g., power cables, parasitic capacitance, PCB circuits, etc., as compared with its counterpart that is radiated over the air (radiated EMI). Regardless of whether conducted or radiated, any pairs of traces or wires on a printed circuit board (PCB) can experience two types of noises: common-mode (CM) EMI and differential-mode (DM) EMI [28], as illustrated in Fig. 5. Since the key of a successful WIGHT attack is CM-DM conversion [12], [30], [31], we introduce DM and CM EMI below.

(a) *Common-mode EMI*: CM EMI is an electrical noise exhibiting the same magnitude and polarity on two traces or wires on a PCB. As illustrated in Fig. 5(a), the CM EMI source has a voltage of V_c and creates the CM noise flows on both lines in the same direction, and returned to the ground via parasitic capacitance (i.e., a stray capacitor C_s) [27], [32], [33]. Note that the CM current will not flow through the load, as the induced voltage difference between the load is 0 [29], i.e., $V_1 - V_2 = 0$. Considering the load being the sensing circuit, a CM EMI will not be able to affect the total power supply of the sensing circuit, nor will it affect the output.

(b) *Differential-mode EMI*: DM EMI flows through the traces on a PCB in an opposite direction, i.e., through the load and back out, as shown in Fig. 5(b). In terms of the DM EMI source, the induced voltages on each wire are relative to the GND potential, and the voltage difference between the load equals to V_d, which is the voltage of the DM EMI source [28], [32], [33]. Considering the load being the sensing circuit, injecting a DM EMI will change the total power supply to the sensing circuit and thus its output.

III. Threat Model

The attacker's goal is to manipulate the victim's touchscreen by injecting malicious signals into the victim device along the USB charging cable. We make the following assumptions for WIGHT attacks:

- **No data connection:** The victim device equipped with a capacitive touchscreen is charged at a malicious charging station via a charging cable. However, WIGHT does not require the data access permission from the USB cable or physical contact with the touchscreen, which is different from previous work [34], [35], [36], [37].
- **Attacker's knowledge:** The attacker knows the model of the victim device and has done a prior study on the same model before implementing the attack. The device model can be obtained in various ways, e.g., spying through a camera installed on the charging station.
- **Attack setup:** The attack device can be inside a malicious charging station in public places, e.g., markets, hospitals, etc., as shown in Fig. 1. The attacker can provide a normal charging function before launching the attack. In addition, the attacker may launch the attack remotely.

IV. Principle of WIGHT Attack

To understand the touchscreen misbehavior phenomenon reported recently [3] and design WIGHT, we first elaborate on the underlying principles of injecting a noise signal into a touchscreen module with noise filters inside, and then validate the principle with both simulation and real-world experiments.

A. CM-DM Conversion in Asymmetric Circuits

1) How to Trigger a Ghost Touch: Human touches and ghost touches are detected via two distinct causes, although in both cases the output of the sensing circuit V_{out} appears to be larger than a threshold value and the system concludes with a touch being detected. For human touches, the capacitance of the touchscreen is changed due to finger contacts, and thus the output voltage V_{out} reflects the capacitance variation proportionally according to the original design Eq. (6), where the output signal $V_{out} = V_{ref} - 2(C_m + C_t)V_{ex}/C_{fb}$.

To comparison, the attacker cannot touch the screen and cannot change the screen capacitance. Instead, she can affect how the sensing circuit measures the capacitance changes and change the output voltage V_{out} by disturbing the excitation signals. To this end, the attacker can inject a noise signal such that under the superposition of the noise signal and the excitation signal, the deduced output signal is $V_{out} = V_{ref} - 2C_m(V_{ex} + V_{dm})/C_{fb}$, where V_{dm} is the magnitude of the DM signal added to the sensing circuit.

2) How to Inject a DM Signal: Based on the aforementioned analysis, the key to generating ghost touches is to inject a noise signal that can affect the output of the sensing circuit, i.e., a DM signal. In practice, however, it is difficult to directly inject DM signals into electronic devices via charging cables, as most commercial devices are equipped with power management and filter circuits (e.g., DM noise filters, voltage regulators [10], over-voltage protection circuits [38], etc.,) to stabilize the power supply, eliminate noises, and protect the device from electrical damage [39], [40].

To tackle the challenge, we propose a CM-DM conversion strategy that injects a CM noise over the charging cable such that the noise can penetrate the aforementioned filter circuits inside the power management integrated circuit (PMIC) module, and result in a DM noise [12], [30], [31] as the injected signal propagates through the circuit.

CM-DM conversion strategy. Without loss of generality, let $Asin(2\pi ft)$ be a CM signal where A and f are the magnitude and frequency of the signal respectively. Due to the non-linear characteristics of the RLC series circuit [41], a

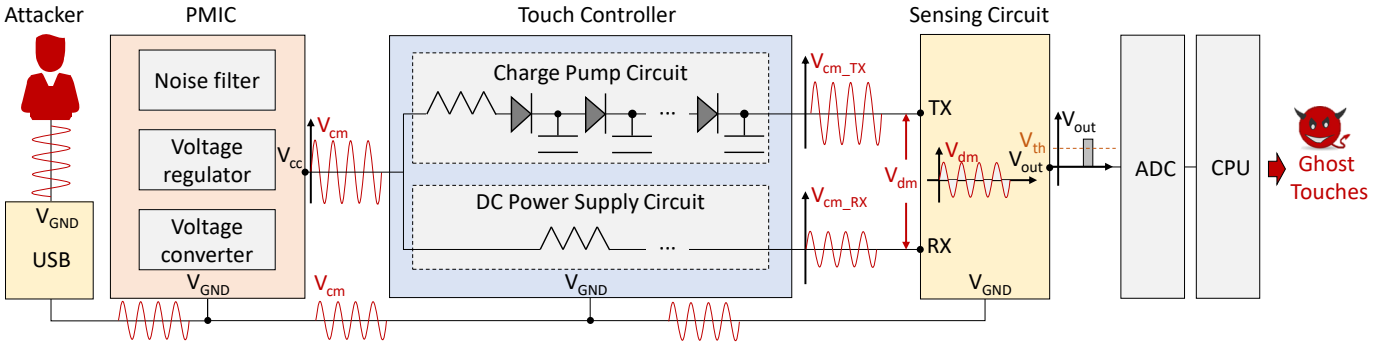


Fig. 6. Overview of the principle of WIGHT attack. Due to the asymmetric circuits in the touch controller, the CM signal injected into the GND line will be converted into a DM signal that interferes with the capacitance measurement. Once the output signal of the sensing circuit exceeds the threshold, the ghost touches will be detected.

CM signal V_{cm} flowing into a circuit with non-linear hardware components will have different phase delay φ and magnitude decay rate β:

$$\varphi = arccos(R/Z) \tag{7}$$
$$\beta = 1/|Z| \tag{8}$$

where $Z = \sqrt{X^2 + R^2}$ is the magnitude of impedance in a standard circuit including capacitors, transistors, and resistors [42]. Z is determined by both the reactance X and the resistance of the circuit, where reactance X is related to the inductors (L) and the capacitors (C), i.e., $X = 2\pi fL - 1/(2\pi fC)$. As a result, the final CM signal is:

$$V_{cm} = \beta A sin(2\pi ft + \varphi) \tag{9}$$

where φ is the phase and β is the magnitude decay rate.

In asymmetric circuits, e.g., the touch controller circuits in a touchscreen device (discussed later [42]), the CM signal can be converted into a desired DM signal. As shown in Fig. 6, suppose the CM signal after the PMIC module is V_{cm}, the phase and the magnitude of V_{cm} will change after it traverses the touch controller circuits, and become the desired DM signal and feed into the TX and the RX as inputs. The DM signal can be denoted as

$$V_{dm} = V_{cm\_TX} - V_{cm\_RX} \tag{10}$$
$$= \beta' A sin(2\pi ft + \varphi') \tag{11}$$

where φ' and β' are the resulted phase and magnitude decay rate of the signal by subtracting V_{cm_RX} from V_{cm_TX} (shown in Appendix C Eq. (20), Eq. (21)). After adding V_{dm} onto the excitation signal, the DM signal can interfere with the capacitance measurement to deduce the desired ghost touches.

3) Asymmetric circuits of touchscreens: The success of the CM-DM conversion strategy relies on the assumption that a touchscreen has asymmetric circuits inside and the CM signal injected from the USB cable can flow through the circuits. To investigate, we look into the smartphone touchscreen circuits and depict the key modules starting from the USB module to the touchscreen in Fig. 6.

Notably, the charging current flows through the USB port and enters the PMIC module, which provides the power management function for the touch controller module. Then, the touch controller module adopts a charge pump to generate an elevated voltage for the sensing circuit [18] such that the voltage magnitude feeding into the TX electrodes will be larger than the one directly supplied by the battery [42]. As a result, it reduces the impact of noises on the touchscreen. Finally, the output voltage of the sensing circuit is digitized by the ADC and processed by the CPU to detect touch events.

Analyzing the flowing path of the V_{cm} signal, we find that the charge pump circuit inside the touch controller module is asymmetric compared to the DC power supply circuit. Specifically, the sub-circuits connected to the TX and RX inputs have different nonlinear characteristics and therefore attribute to different phase delays and magnitude decays.

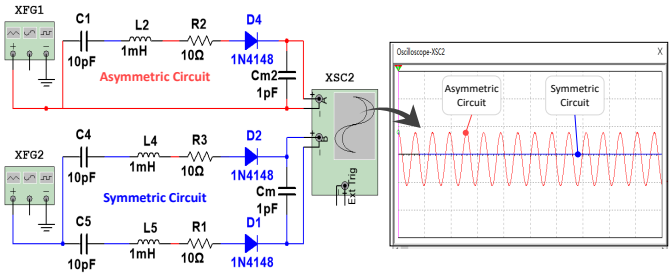
B. Validation by Simulation and Real-world Experiments

To validate the aforementioned CM-DM conversion analysis, we conducted experiments with simulation and real-world experiments.

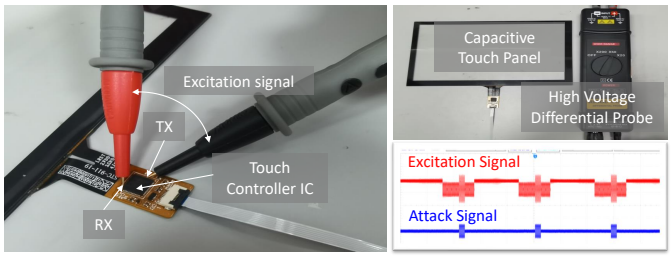
Simulation. The setup of the simulation experiment is shown in Fig. 7(a). We built an asymmetric circuit (top) as well as a symmetric circuit (bottom). Two signal generators and a multi-channel voltmeter are used to power the circuits and monitor the output from both circuits, respectively. We injected a sinusoidal CM signal with a frequency of 300 kHz and root-mean-square (RMS) voltage of 106 V * into both circuits. The output voltages of two circuits shown in the voltmeter validate that the CM signal after the symmetric circuit is 0 (blue line) and become a DM signal (red waveform) in the asymmetric circuit. This experiment confirmed that asymmetric circuits can indeed induce a DM signal.

Touch panel experiment. In addition, we performed an experiment on a commercial touch panel [43], [44] shown in Fig. 7(b). We injected a CM signal from the GND line of the capacitive touch panel and measured the potential difference between the TX electrode and the RX electrode, i.e., the excitation signal applied to the sensing circuit. To improve the measurement accuracy, we utilized an oscilloscope with

*The frequency and magnitude are selected to match those of real touchscreens used in our experiments.



(a) The setup and outputs of the simulation experiment. The CM signal can indeed introduce a DM signal after passing through the asymmetric circuit.



(b) Setup and the outputs of the touch panel experiment. An excitation signal can be monitored after injecting the attack signals from both TX and RX input.

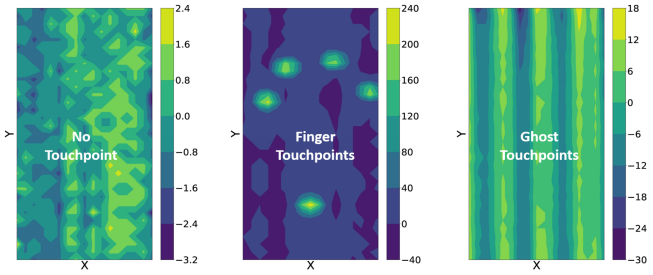
Fig. 7. Validation of the CM-DM analysis by simulation and touch-panel-based experiments.

high voltage differential probes, and the waveform displayed on the oscilloscope is shown in Fig. 7(b), where the red waveform (top, 2.5 V/div) is the excitation signal and the blue one (bottom, 50 V/div) is the injected CM interference. This experiment confirmed that a CM interference can be converted into a DM interference and added to the excitation signal.

Validation on smartphone touchscreen. We validated the attack by displaying the capacitance variations across the entire touchscreen of a Xiaomi Mi MIX2. The contour maps of the capacitance variations are collected by the Android Debug Bridge (ADB) tool [45]. As shown in Fig. 8, in an idle case without any touches, the capacitance variations of the touchscreen shown in Fig. 8(a) have low magnitudes and distributes evenly. In the case of human touches using five fingers, the capacitance variations on the locations with finger contacts have much higher values than the rest ones, indicating the touch events, as shown in Fig. 8(b). In the attack cases, after we injected a CM signal with a frequency of 309 kHz and RMS voltage of 113.1 V into the GND line, the capacitance variations are changed compared to the ones in the idle case, as shown in Fig. 8(c), indicating that the CM signal indeed produces a DM signal that influences the excitation signal and changes the measured capacitance. Although the DM signal can result in capacitance variation, the changes shall be controllable to deduce desired touch events.

V. Attack Design

After clarifying how to inject a CM signal to reshape the desired excitation signal for the sensing circuit of touchscreens in Sec. IV, we introduce how to achieve effective attacks against touchscreens. We design and achieve three kinds of



(a) Idle. (b) Human touch. (c) WIGHT attack.

Fig. 8. Contour maps of capacitance variation when the touchscreen is under different cases (i.e., idle case, human touch case, attack case).

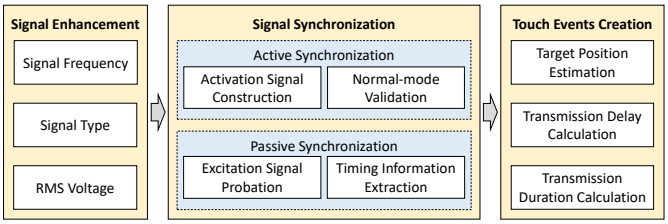


Fig. 9. An illustration of injection attack design. We first select an attack signal for effective signal enhancement and then design the signal for controllable touch events.

attacks, i.e., the injection attack, the alteration attack, and the DoS attack. As the alteration attack and the DoS attack are based on the injection attack, we elaborate on the design of the injection attack from the signal enhancement, synchronization, and touch event generation. The design mechanism of the injection attack can be applied to the other two attacks.

A. Injection Attack

The key insight of WIGHT is to disturb the capacitance measurement process by changing its excitation signal in order to inject ghost touches. In mainstream touchscreens, a TX electrode sends an excitation signal, and all RX electrodes transfer the accumulated charge simultaneously [2], as is discussed in Sec. II, so the injection attack achieves ghost touches along intended TX electrodes. To achieve a successful injection attack, we need to address two key challenges: (a) How to increase the injection intensity to create significant capacitance variation that can exceed the detection threshold for generating ghost touches? (b) How to design the attack signal, including its timing, duration, etc., to generate controllable touch events? In the following, we introduce the key modules of the injection attack, i.e., signal enhancement, signal synchronization, and touch event generation, as shown in Fig. 9.

1) Signal Enhancement: The design of the attack signal should first consider the signal frequency, type, and its RMS voltage to increase the injection intensity.

Signal Frequency: The CM-DM conversion strategy only changes the magnitude and phase delay of the CM signal, without changing the signal frequency. The frequency of the DM attack signal, therefore, should match that of the original excitation signal.

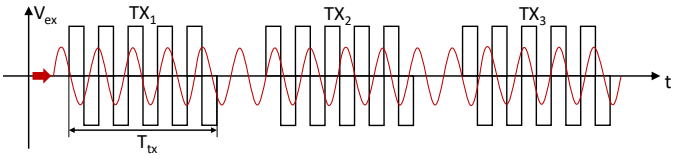
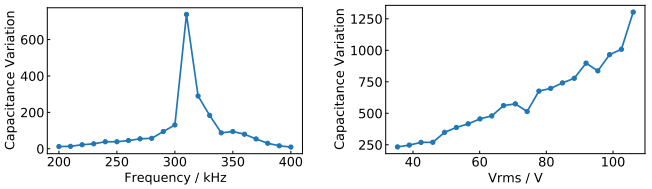


Fig. 10. The schematic diagram of excitation signal (black) and the injected DM signal (red).



(a) Frequency vs. capacitance. (b) RMS voltage vs. capacitance.

Fig. 11. The impact of signal frequency and magnitude on capacitance variation of touchscreens.

Signal Type: As shown in Fig. 10, the original excitation signal (black waveform) is a square-wave signal, and the ideal DM attack signal will be a square-wave signal. However, because the square-wave signal will be filtered by the PMIC module, we use the sin-wave signal as the candidate DM attack signal instead. One question is whether the sin-wave DM signal is strong enough to influence the excitation signal? To analyze, we evaluate the accumulated charge Q_m:

$$Q_m = 2C_m(V_{ex} + V_{dm}) \tag{12}$$

V_{dm} is the magnitude of the DM signal. The larger accumulated charge Q_m is, the stronger interference intensity can be. To achieve maximum interference, the frequency f_d and the initial phase φ_{d0} of the attack signal should be: $f_d = 1/T_{te}$, and $\varphi_{d0} = 0$ or π.

To validate, we conducted a proof-of-concept experiment on Xiaomi Mi Mix2 to verify our analysis. We injected a CM signal with the RMS voltage of 102.5 V and frequencies in the range of 200 kHz to 400 kHz, and then recorded the average capacitance variation per 10 kHz. According to the correlation curve of the signal frequency and the capacitance variation (shown in Fig. 11(a)), the signal with the frequency of 310 kHz demonstrates the largest interference intensity, which is close to the frequency of the excitation signal, i.e., $f_{ex} = 323kHz$.

RMS Voltage: According to Eq. (12), the transferred charge is approximately proportional to the signal intensity. To validate, we performed a validation experiment by injecting CM signals with the frequency of 310 kHz and RMS voltages from 35.35 V to 106 V and then recorded the average capacitance variation per RMS voltage of 3.5 V. The correlation curve of signal magnitude and capacitance variation (shown in Fig. 11(b)) demonstrates proportionality. In practice, the selection of RMS voltage should consider the power limitation and safety issues.

2) Signal Synchronization: To create controllable ghost touches, the attacker was to synchronize the DM attack signal with the touchscreen scanning cycle. We introduce the active and passive synchronization strategies.

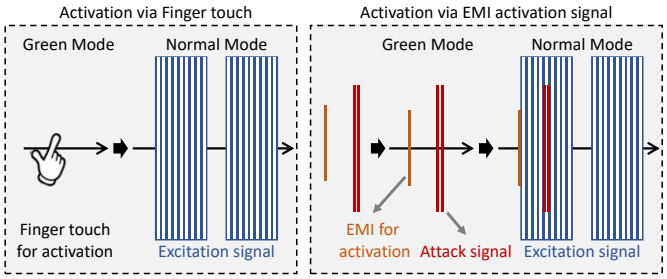


Fig. 12. An illustration of active synchronization. (a) left: the user can activate the excitation signal by touching the screen. (b) right: the attacker can design an EMI activation signal to activate the excitation signal of the touchscreen.

Active Synchronization: To improve the energy efficiency of touchscreens, modern smartphones use adaptive touch sampling frequency scaling algorithm [46], [47]. Specifically, when no touch is detected, the touchscreen will be in "green mode" [48], [49], [50], [44] during which the touch refresh rate is low. For example, the Apple iPhone SE smartphone sets its touch refresh rate to 0.7 Hz in the green mode (Fig. 21(a)). Once a touch is detected, the touchscreen is switched to "normal mode" with a normal refresh rate, e.g., 60 Hz for the Apple iPhone SE smartphone (Fig. 21(b)).

In addition to a genuine touch, the normal mode can be activated by an intentional EMI interference signal [50], [44]. `WIGHT` utilizes the adaptive touch sampling mechanism and crafts an EMI activation signal that simulates the characteristics of users' touch to awaken the touchscreen from the green mode. As a result, the DM signal following the malicious activation signal can be synchronized with the excitation signal. The active synchronization mechanism is depicted in Fig. 12, where the orange signal is the EMI activation signal, the red signal is the DM attack signal, and the blue signal is the excitation signal. In our implementation, the EMI activation signal is a sine-wave signal with a frequency of 20 kHz and an RMS voltage of 70 V.

Passive Synchronization: The activation mechanism actively synchronizes the DM attack signal with the excitation signal. In addition, we propose a passive synchronization strategy to measure the excitation signal scanning cycle.

(a) *Measuring excitation signal:* Excitation signals of touchscreens are AC signals with high frequencies, e.g., 100 kHz to 500 kHz [25], [18], which can be unintentionally leaked in the form of conducted or radiated EMI [8], [51]. Therefore, the attacker can passively receive the leaked EMI signal to extract the timing information. To validate the feasibility, we measured the conducted EMI signal in the GND line through the USB port and collected the radiated EMI signal via an antenna that is above the touchscreen of the Xiaomi Mi Mix2 smartphone. The left figure of Fig. 13 shows the excitation signal trace output from an oscilloscope, in which the bottom waveform is the conducted EMI signal and the top one is the radiated EMI signal, and both of them reflect the excitation

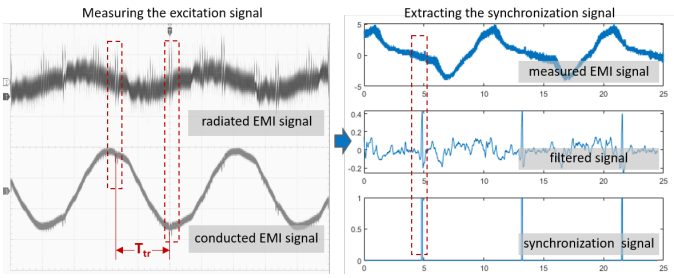


Fig. 13. (a) left: the radiated EMI signal (top) and the conducted EMI signal (bottom) of the smartphone. Both of them reflect the excitation signal of the touchscreen. (b) right: noise filtering and timing information extraction of the measured signal.

signal of the touchscreen. Compared to the measurement of the radiated EMI signal, the measurement at the USB GND port can deduce a more clear signal trace for synchronization.

(b) *Extracting timing information:* To extract timing information from the measured EMI signal, we utilized a DAQ tool [52] to process the signal trace. Then the trace is smoothed by filtering out the power-frequency (i.e., 50 Hz) noise and higher-frequency noises. The right figure of Fig. 13 shows the process of extracting the timing information. we filtered the measured EMI signal (top waveform) and extracted the timing information (bottom) from the filtered signal (middle).

3) Touch Event Generation: To generate controllable touch events, we introduce a synchronization mechanism. The key factors to make a successful touch event include attack execution time and distribution range of the desired ghost touches. Fig. 14 shows the excitation signal (top), the timing information (middle), and the attack signal (bottom). First of all, the attacker calculates the transmission delay T_{de}, the interval between the moments when the scan starts and when the targeted TX is scanned:

$$T_{de} = m(T_{tx} + T_{in}) \tag{13}$$

where m is the number of TXs before scanning the first TXs below the button. As shown in Fig. 14, there is only one TX before scanning the target button, so $m = 1$. Next, the attacker estimates the transmission duration T_{du} of the attack signal:

$$T_{du} = n(T_{tx} + T_{in}) \tag{14}$$

where n is the number of TX electrodes that are covered by a desired ghost touch area, i.e., the button in Fig. 14. To validate the design, we chose attack signals with the transmission duration of 0.5, 1.5, 2, 2.5, 3, and 3.5 ms, and recorded the pixel range of TXs covered by ghost touches on two smartphones (Xiaomi Mi MIX2, LG Nexus 5X). Fig. 15 presents the theoretical TXs range R_{theo} (dashed lines) and the average range of the ghost touches R_{exp} (solid lines) in 3 repeated experiments with various transmission durations. In addition, the deviation D of ghost touches can be given as:

$$D = R_{exp} - R_{theo} \tag{15}$$

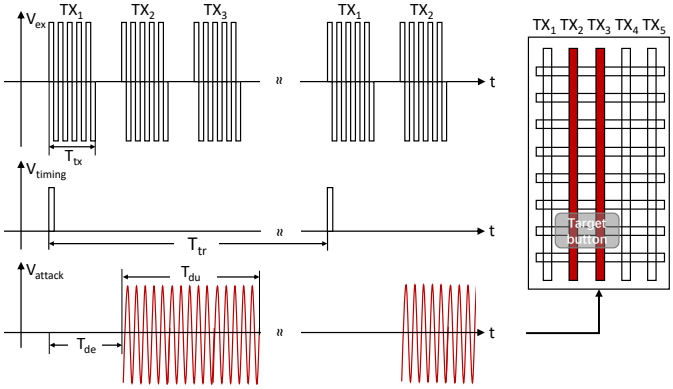


Fig. 14. Attack signal design for injection attack. Referring to the excitation signal and the timing information, an attacker can inject ghost touches into certain TXs.

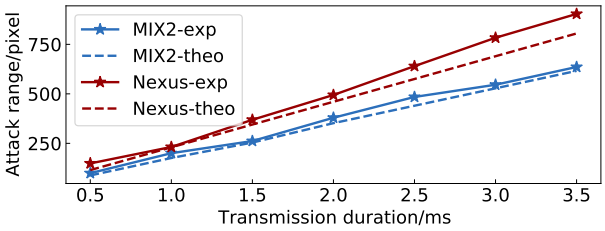


Fig. 15. The experimental (solid lines) and theoretical (dashed lines) range of ghost touchpoints on the touchscreen as the transmission duration of the attack signal increases.

The results validate our design and show that the attack range expanded with the increase in transmission duration. The average deviations of Xiaomi Mi MIX2 and LG Nexus 5X are 21.8 pixels and 52.9 pixels, respectively, which are smaller than the buttons' sizes (169.2*429.1, 186.6*446.3).

Some devices whose TXs are excited partially simultaneously (i.e., the half-sequential driving method) or simultaneously (i.e., the parallel driving method) [24], [23], [21]. For those devices, we can still inject ghost touches according to the timing information but with limited control over the touches' positions. In this paper, injection attacks will have three different outcomes according to the driving methods. (1) Type I: For smartphones adopting the sequential driving method, the attacker can specify any TXs as targets for ghost touches. (2) Type II: For smartphones adopting the half-sequential driving method, the attacker can specify the TXs of limited areas to which ghost touches are injected. (3) Type III: For smartphones adopting the parallel driving method, ghost touches can only appear at certain positions.

B. Alteration Attack

The injection attack works when a victim is not using the smartphone. When a victim is playing with his smartphone, `WIGHT` can achieve an alteration attack to change the locations of the user's touchpoints by influencing the RX. Compared to the injection attack, we use the same method whereby the accumulated charge is changed and the output voltage exceeds

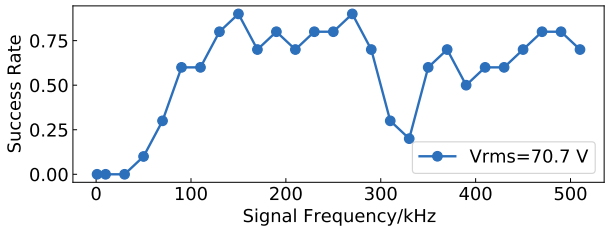


Fig. 16. Success rates of DoS attacks on a range of signal frequencies. The 320 kHz shows a low success rate, indicating that the attack signals should have a different frequency from that of the excitation signal for a better DoS effect.

the detection threshold, but the alteration attack requires the noise signal with smaller magnitudes and slightly different frequencies. In addition, the DM signal in the alteration attack is caused by the users' contact instead of the asymmetric circuits.

When a user touches the touchscreen, the capacitance changes by the touch can be regarded as a parasitic capacitor, which forms a closed loop with the RX electrode [7]. When we inject a CM noise, it will be converted into a DM noise via the closed loop and then change the accumulated charge Q_m of the RX electrode and further change the voltage output. Once the output exceeds the detection threshold, ghost touches will be detected on the crosspoints of TXs and RXs. Noted that the alteration attack does not require synchronization with the excitation signal and the ghost touches do not appear until the victim touches. Thus, the CM noise should be injected before the victim touches the screen, and it takes several hundreds of milliseconds for a human to touch a button while it takes only a few milliseconds for the touch controller to scan the screen. Once the user touches the screen, the ghost touches can appear on any position along the entire RX. As a result, the attacker can use the alteration attack to change what the users have chosen, e.g., clicking "No" but actually "Yes" is clicked.

C. DoS Attack

In addition to actively injecting ghost touches, WIGHT attack can also force to disable the touch service, i.e., the touchscreen does not respond to any user's touch operations.

Typically, when there is an electrostatic discharge (ESD) on the device [53], [14], smartphones will stop reporting the touch events for bypassing accidental touches and self-protection [54], [55], [56]. To simulate the ESD-induced soft failures, the attacker can create an external interference as ESD or EMI [13] by injecting a CM signal to smartphones via the GND line. To avoid generating unexpected ghost touches, it is suggested that the attacker should avoid using the frequency of the excitation signal introduced in Sec. V-A. We conducted experiments on Xiaomi Mi MIX2. If the smartphone does not generate any touchpoints when we touch the screen, we regard it as a successful attack. We swept the attack signal with an RMS voltage of 70.7 V from 10 kHz to 500 kHz with a step size of 20 kHz and recorded the success rate in 10 repeated experiments. The results (shown in Fig. 16) indicate that the attack signal with a frequency range from 125 to 500 kHz, except for the range of excitation signals, can cause effective DoS.

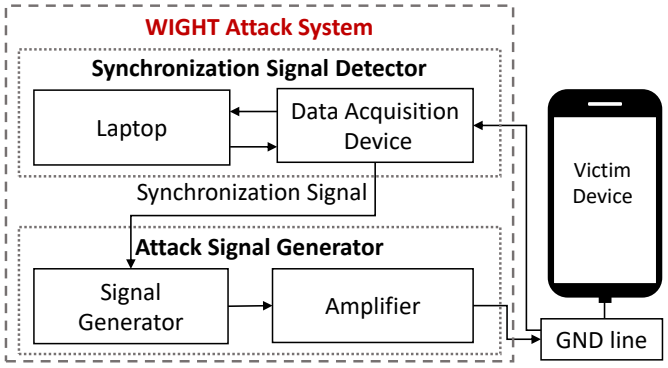


Fig. 17. An illustration of WIGHT attack system.

VI. Evaluation

In this section, we evaluate the overall performance and affecting factors of WIGHT attack and demonstrate its potential real-world threat.

A. Experimental Setup

1) Attack System: The WIGHT attack system includes a *Synchronization Signal Detector* and an *Attack Signal Generator* as illustrated in Fig. 17. The synchronization signal detector comprises a data acquisition device (DAQ) [52] and a laptop. The DAQ senses the touchscreen's excitation signal from the victim device via the charging cable's GND line or a signal probing antenna. The acquired signal is sent to and processed by the laptop in real-time, which extracts the excitation signal cycle and instructs the DAQ to generate a synchronization signal at the right timing to trigger the attack signal generator. The attack signal generator consists of a signal generator [57] and a power amplifier [58]. The signal generator is used to create an elaborate attack signal for the target device, and the amplifier will boost the signal's power before injecting it into the charging cable. Fig. 18 shows the physical implementation of the attack system. The victim device is connected to the attack system disguised as a malicious power socket (shown in Fig. 23) through an ordinary charging cable with or without a power adapter.

2) Target Device: We evaluate the attack on 6 smartphones, 1 tablet, and 2 standalone capacitive touch panels listed in Table I. All these devices have capacitive touchscreens and can be plugged into the malicious charging socket via a charging cable in the experiments.

3) Test Interface: To measure ghost touches, we developed an Android application named *WIGHT Test* (shown in Fig. 24(a)), which can customize the number, size, shape, and position of buttons, record the timestamps of touch events, and provide feedback for touch interaction. Following the typical design of touchscreen buttons [59], we set the buttons to appear in rectangle shapes and medium sizes (2.5cm$*$1cm

TABLE I. Parameters and success rates of injection attacks on 9 target devices.

#	device model	spec.	year	dir.	ref./Hz	exc./kHz	Injection Attack			
							type	f./kHz	vrms./V	succ.
1	Xiaomi Mi Mix 2	USB-C	2017	V	119.7	323	I	309	109.6	19/30
2	Huawei nova 2	USB-C	2017	V	116.2	140.7	II	18.83	158.4	14/30
3	Apple iPhone SE	Lightning	2020	H	60	303	III	12	106.0	17/30
4	Apple iPhone 7	Lightning	2016	H	60	120	III	12	81.3	19/30
5	Samsung Galaxy S20 FE	USB-C	2020	H	118.12	416	II	420	106.0	13/30
6	LG Nexus 5X	USB-C	2015	H	120	278	I	278	106.0	25/30
7	Asus Google Nexus 7	Micro	2013	H	120	129	II	300	99.0	13/30
8	CAPATIVATE-PHONE	Micro	2019	V	30	120	I	120	106.0	29/30
9	9-inch touch panel	USB-A	2020	V	70	185	II	185	106.0	19/30

Note: (a) *spec.* is the USB connectors' specification. (b) *year* is the manufacturing date of the device. (c) *dir.* is the direction of TX electrodes, and *V* is vertical and *H* is horizontal. (d) *ref.* is the touch refresh rate (Hz) of the devices. (e) *exc.* is the frequency of the excitation signal (kHz). (f) *f.* and *vrms.* indicate the frequency (kHz) and the RMS voltage (V) of the attack signal respectively. (g) *succ.* is the success rate of the attack.

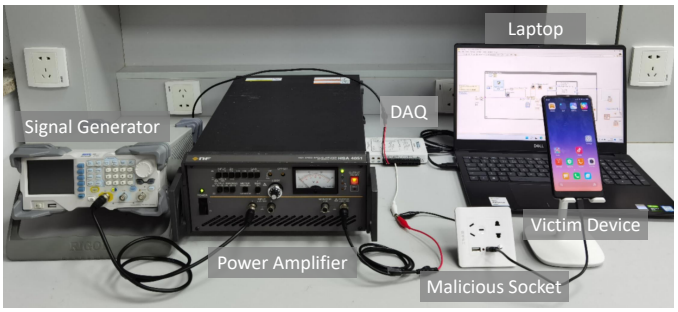


Fig. 18. Physical implementation of the attack system.

on Huawei nova2 and 3cm∗1cm on other Android devices). The buttons are aligned vertically or horizontally. For Apple devices and standalone touch panels, we used off-the-shelf applications or built-in system interfaces, e.g., calculators or the pop-up windows of Bluetooth connection.

B. Overall Performance

We evaluate the overall performance of injection attacks, alteration attacks, and DoS attacks using two main metrics, the attack's success rate and response time.

- *Success rate.* For injection and alteration attacks, we consider an attack successful if the target button is touched at least once within three seconds since the attack starts and no other buttons are touched. DoS attacks are successful if the device fails to respond to any human touches.
- *Response time.* Response time is the time duration between the start of an attack to the moment it succeeds.

1) Injection Attacks: We divide the target devices into three types according to their driving methods as introduced in Sec. V-A. Because ghost touches appear in different positions on various types of devices, we customized the test interface based on the possible attack outcomes of each device type, i.e., placing buttons in the area where ghost touches may appear. We repeated the attack 30 times on each device and measured the success rate.

We found injection attacks successful on all devices. The detailed attack parameters and success rates are reported in Table I. The overall success rate averaged over the 9 devices is 62.2%, and the success rate on individual devices can reach up to 83.3% on a Nexus 5X smartphone and 93.3% on a TI CAPTIVATE-PHONE touch panel. As a case study, we measured the response time of 40 successful injection attacks on two smartphones (Xiaomi Mi Mix 2 and Nexus 5X). To compare with the response time of normal human touches, we recruited 20 participants including 4 females and 16 males aged between 20 and 50, and asked them to press a random button as soon as possible after seeing the prompt in *WIGHT Test*. We recorded the response time of 2 trials for each participant. Fig. 22 shows the cumulative distribution function (CDF) of response time for attacks and humans. The result indicates that `WIGHT` attack can inject ghost touches in around 0.5-1s, which is faster than human touches (around 1-2s).

2) Alteration Attacks: We evaluated the success rate of alteration attacks with 30 repeated trials on each device. As this experiment requires human participants to physically touch the device while we launch the attack, we have carefully followed safety regulations and applied safety measures to protect human participants despite the absence of the local Institutional Review Board (IRB). For example, we limited the duration and current of the attack signal within the safety boundaries [60], [61], [62]. The experiment risks and protection methods are described in Appendix A. Table II shows the attack parameters and success rates of alteration attacks on each device. The success rate is 47% on average and can reach up to 66.7% on the Xiaomi Mi Mix 2 smartphone.

3) DoS Attacks: We evaluated DoS attacks using the setups and safety measures similar to alteration attacks. We measured the success rates of DoS attacks while the participants were performing eight common touch services including single-tap, double-tap, stretch, pinch, swipe up, swipe down, swipe left, and swipe right. Similarly, we repeated the trials 30 times on each device and found the attack successful on all devices and types of touch services. The results in Table II show an

TABLE II. Parameters and success rates of alteration attacks and DoS attacks on 9 target devices.

#	Alteration Attack			DoS Attack		
	f.	vrms.	succ.	f.	vrms.	succ.
1	322	77.8	20/30	230	21.2	30/30
2	133	88.4	16/30	130	116.7	10/30
3	120	106.0	11/30	20	77.8	30/30
4	120	70.7	10/30	300	70.7	28/30
5	416	24.7	18/30	416	81.3	30/30
6	290	38.9	9/30	290	70.7	30/30
7	129	10.6	14/30	85	95.4	30/30
8	120	46.0	13/30	300	91.9	28/30
9	185	24.7	16/30	243	91.9	16/30

TABLE III. The success rates of injection attacks at various signal magnitudes.

vrms./V	53	71	88	110	113
Xiaomi Mi MIX2	0%	0%	0%	50%	65%
LG Nexus X5	0%	80%	85%	90%	90%

average success rate of 85.9% and 100% success rate of DoS attacks on 5 devices.

C. Factors Affecting WIGHT Attack

We evaluate the impact of signal magnitude and charging cables/power adapters on the performance of WIGHT attack.

1) Signal magnitude: As discussed in Sec. V-A, a stronger attack signal may cause a greater interference on touchscreens. To evaluate the impact of signal magnitude on the attack's success rate, we tested injection attacks on two smartphones (Xiaomi Mi Mix 2 and LG Nexus 5X) at various levels of RMS voltages (53V, 71V, 88V, 110V, and 113V) and repeated the trials 20 times on each device. The results in Table III show that the success rate of injection attacks generally increases with higher signal magnitudes.

2) Charging Cables and Adapters: We evaluated the impact of 13 charging cables and 6 power adapters shown in Fig. 24(b). Referring to the measurement method of CM voltage [63], we used the evaluation setup in Fig. 25. We injected a sinusoidal signal with a frequency of 300 kHz and an RMS voltage of 106.0 V into the charging cables or power adapters and used an oscilloscope to measure the signal that flowed into the charging cable. We found that the signal magnitude is reduced after transmission while the signal frequency remains the same. We quantify the signal attenuation with a signal transmission efficiency E_f:

$$E_f = Vp_1/Vp_0 \tag{16}$$

where Vp_1 and Vp_0 are the signal's magnitudes after and before transmitting through the charging cable and adapter. In addition, we also measured the success rate of injection attacks on 3 devices (Nexus 5X, Nexus 7, and iPhone SE) connected with different charging cables and power adapters using the setup in Fig. 26. The results in Table IV indicate that WIGHT attack is effective with most charging cables and even across power adapters, which we assume is due to the high signal transmission efficiency of charging cables and power adapters. Though the voltage converters in power adapters are physically isolated, we believe the CM signal can go through the parasitic capacitors of the isolation transformer to the GND port [63]. We also found that a few charging cables and power adapters that have low signal transmission efficiencies typically render a lower attack success rate. As discussed earlier, we believe the success rates can be increased with higher signal magnitudes.

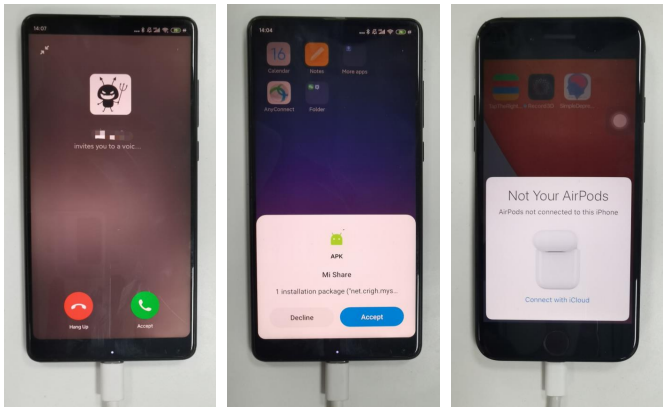


Fig. 19. An illustration of three practical scenarios of the injection attack: picking up an eavesdropping phone call, receiving malicious files, and approving the Bluetooth connection request.

D. Potential Attack Scenarios

To demonstrate the potential real-world threat of WIGHT attack, we evaluate three real-world scenarios including controlling devices, misdirecting options, and blocking operations.

1) Controlling Devices: In this scenario, an attacker can surreptitiously control the victim device by injecting ghost touches when the user is not using the device. Fig. 19 shows three typical scenarios of injection attack: picking up an eavesdropping phone call, accepting malicious files, and approving a Bluetooth connection request. (1) An attacker can make a phone call to the victim device and then inject ghost touches to pick up the eavesdropping phone call. In Fig. 27, when the Xiaomi Mi Mix 2 was called, the attacker transmitted the attack signal with transmission period $T_{tr} = 8.354ms$, transmission delay $T_{de} = 5.6ms$, and transmission duration $T_{du} = 1.2ms$. As a result, the touchpoints were injected into the right side of the touchscreen, and then the phone call was picked up. We have successfully picked up the phone call 6 times in 10 trials. (2) Similarly, the attacker may also implant malware via file sharing. As shown in Fig. 28, we could transfer a malicious file to the victim's smartphone and inject ghost touches to accept the file. (3) In addition, WIGHT can approve a Bluetooth connection request. Fig. 29 shows the process of connecting AirPods by injecting ghost touches. If the Bluetooth service of Apple products is available when the attacker approaches with an AirPods, the victim device will pop up a "Connect" button on the screen [64]. The attacker

TABLE IV. The signal transmission efficiency and attack success rates of various charging cables and power adapters.

#	charging cable	L/m	I/A	spec.	eff.	succ.	#	power adapter	eff.	succ.
C1	HUAWEI CP51	1	3	USB-C	62%	8/10	**A1**	OPPO VCA7GACH	116%	7/10
C2	HUAWEI AP71	1	5	USB-C	100%	7/10				
C3	HUAWEI CC790	1	6	USB-C	99%	7/10	**A2**	RECCI RCT-N02C	97%	9/10
C4	QOOVI CC-500C	1	2	USB-C	47%	7/10				
C5	SmartDevil A51-104	0.25	5	USB-C	100%	8/10	**A3**	QOOVI C213	96%	9/10
C6	SmartDevil A51-106	0.5	5	USB-C	100%	7/10				
C7	SmartDevil A51-110	1	5	USB-C	100%	8/10	**A4**	HUAWEI-050200	88%	7/10
C8	ZMI	1.5	5	USB-C	100%	8/10				
C9	HUAWEI AP70	1	2	Micro	93%	3/10	**A5**	Xiaomi A319-050100U	53%	6/10
C10	iPhone	1	1	Lightning	100%	8/10				
C11	PISEN LS-TC09-2000	2	5	USB-C	16%	0/10	**A6**	SKK-S258	97%	7/10
C12	QOOVI CC-022A	1.2	2	C/M/L	50%	0/10				
C13	Remax	1.2	2	C/M/L	57%	0/10				

Note: (1) *L* is the cable length. (2) *I* means the rated current of charging cables. (3) *eff.* represents the signal transmission efficiency of the cables/adapters.

can perform injection attacks to tap the button and connect the AirPods, which can be used as a stepping stone to activate and control the voice assistant by double-tapping the AirPods [65].

2) Misdirecting Options: By performing alteration attacks, the attacker can misdirect the victim user's touchpoint to ghost touches on the same RX electrode. For example, when the attacker sends a link that contains malicious files, two buttons will appear at the bottom of the screen, prompting users to click a button to open the link or not. If the user clicks the "Decline" button, the fast-moving ghost touches along the RX can tap the "Accept" button with a success rate of around 50%. Clicking a malicious link may enable a virus [66] and damage the user's privacy. The attacker may also connect malicious NFC tags in a similar way [67].

3) Blocking Operations: A DoS attack can disable touch services and block the victim user's touch operations. We envision that an attacker can combine injection attacks and DoS attacks. For example, if the user finds his/her phone is performing an unintended operation caused by injection attacks, e.g., loading malware, he/she cannot interrupt the process in the presence of DoS attacks. DoS attacks can also be used to intentionally degrade the user experience, e.g., causing interruptions while the user is playing a delay-sensitive game.

VII. Discussion

In this section, we discuss the safety recommendations, limitations, and potential countermeasures of `WIGHT` attack.

A. Safety Recommendations

In practice, a user may physically touch the victim device while an attacker is injecting attack signals into the charging cable. Considering that the attack signal is an alternating current with a high voltage, we seriously recommend that researchers should conduct experiments under the supervision of safety professionals, and the laboratory needs to be equipped with standard electrical protective devices, e.g., the earth leakage circuit breaker (ELCB) [68], to prevent electric shock and potential injury to humans.

B. Limitations

Limited by the driving method of the victim touchscreen, `WIGHT` attack cannot control ghost touches to appear at any position of the screen. For example, injection attacks may at most inject ghost touches along any TX electrode or at fixed areas/positions, and alteration attacks can only cause ghost touches along the RX electrode that the user touches. Therefore, in most cases, the ghost touches may appear randomly on a vertical or horizontal line of the screen. If two buttons are aligned horizontally on the electrode where ghost touches appear, the success rate of taping a specific button will be around 50%. We envision that future work could investigate the feasibility of more fine-grained control of ghost touches.

C. Potential Countermeasures

`WIGHT` attack manipulates devices by injecting ghost touches into the touchscreens via the charging cable. Therefore, it is difficult to defend against this attack using traditional methods such as data blockers [34], [36], [37]. To mitigate the threat, we propose potential countermeasures from three perspectives: hardware-based suppression, software-based detection, and authentication.

1) Hardware-based Suppression: `WIGHT` attack relies on the mechanism that a CM interference of high intensity can be converted into a DM interference in asymmetric circuits. Therefore, we propose a hardware defense named *Ghost Blocker* that can suppress or even prevent the attack signal's transmission. The key component is a CM choke that can create an opposing field of magnetic flux to suppress the CM noises traveling in the same direction on a group of lines [69]. We design the CM choke's inductor with an inductance $L_{cm} = X_L/(2f\pi)$, where X_L is the resistance of the load, and f is the frequency of the touchscreen's excitation signal (around 100 kHz to 500 kHz). Therefore, to maximize the suppression effect, the inductance in practice needs to be around $0.77X_L$ to $1.59X_L$ μH. To verify the effectiveness, we simulate two identical asymmetric circuits in Fig. 20. The

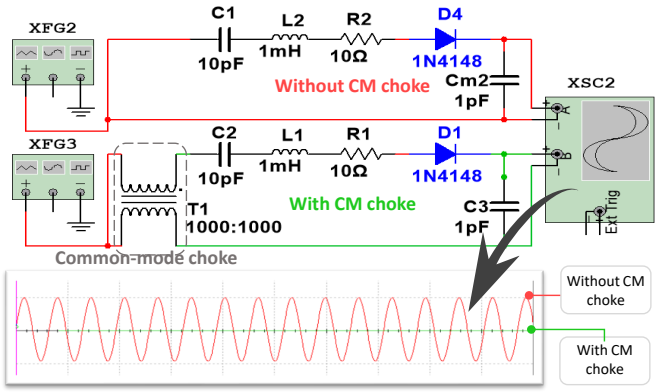


Fig. 20. The simulation of CM choke. The output voltage (green waveform) of the bottom circuit is close to 0, indicating that a CM choke can effectively mitigate the attack signal.

bottom circuit is equipped with a CM choke while the top circuit is unprotected. The results displayed in the voltmeter show that the CM choke can effectively suppress the CM interference, therefore eliminating DM interference that causes ghost touches.

2) Software-based Detection: We propose a software-based detection method that exploits capacitance variation and touch features such as pressure, touch size, etc., to differentiate human touches and ghost touches. The defender first collects touch data of humans and ghost touches using touchscreens and additional pressure sensors [54], [55], [70]. The dataset can be given as $D = [d_1, d_2, d_3, d_4, d_5]$, where d_1 is the capacitance variation, d_2 is the number of simultaneous touches, d_3 is the touch duration, d_4 is the touch size, and d_5 is the touch pressure. Based on the collected dataset, the defender can train a classifier, which we envision can effectively detect the attacks because ghost touches are very different from human touches on these features.

3) Authentication: We suggest building a collaborative database of trustworthy public charging stations. The defender may exploit hardware fingerprinting methods [71] with the authentication chips in touchscreen devices to verify secure charging stations. If an authorized charging station is hijacked by an attacker, its hardware fingerprints will become invalid and the authentication chip can alert the user.

VIII. Related Work

We summarize the related work on touchscreen attacks as well as charging-based and USB-based attacks.

A. Touchscreen Attacks

Research in recent years has shown that an attacker can manipulate a device by attacking its touchscreen. Shwartz et al. [72] first presented a touch injection attack by replacing the touchscreen driver. This attack can accurately inject any touch-point into a victim device. Nevertheless, a practical challenge is that the attacker needs to tamper with the victim device's hardware in advance. In comparison, other studies focused on attacking the touch sensing circuits using physical signals. Maruyama et al. [7] proposed Tap'n Ghost, an alteration attack that can change the detected touch position when a user is touching the screen. This attack is achieved by generating an electric field that interferes with the RX electrodes of touch-screens. Wang et al. [8] presented GhostTouch, an injection attack that can inject ghost touches into targeted positions of the screen by emitting an electromagnetic interference (EMI). Both of the attacks require the victim device to be placed on a table where the attack device is hidden underneath. In this work, we present `WIGHT`, the first wired attack on capacitive touchscreens that can achieve injection, alteration, and DoS outcomes via the charging cable and even across power adapters.

B. Charging-based and USB-based Attacks

Universal Serial Bus (USB) has become the de-facto standard for both charging and data transfer on modern devices [73]. Many vulnerabilities have been found in the USB interface. For example, several studies have demonstrated that sensitive information including passwords to unlock smartphones [74], critical keys in cryptographic systems [75], information of the browsed webpage [76], display content of a screen [35], data traffic [77] etc., can be extracted through USB power cables. Esteves et al. [78] demonstrated that EMI signals conducted through charging ports could be used to inject voice commands into smartphones. Due to the trust-by-default nature of the USB ecosystem [34], malicious USB peripherals have emerged in recent years. Some USB peripherals can be used to eavesdrop on signals, such as BadUSB Hubs [36], KeyGrabber [79], and CottonMouth [80], and others can be used to inject signals, such as USBee [81], USB Killer [82], and TURNIPSCHOOL [83]. Different from these USB-based attacks, our attack does not rely on the data lines and therefore cannot be defended using the traditional data blocking techniques [37].

IX. Conclusion

In this paper, we present `WIGHT`, the first wired attack on capacitive touchscreens via charging cables. `WIGHT` can inject ghost touches regardless of whether the screen is being touched or not and can disable the touch service of victim devices. We analyze the underlying principle of ghost touches theoretically and experimentally and find that due to the asymmetric circuits, a common-mode noise on the power line can be converted into a differential-mode noise that interferes with the capacitance measurement. We have validated the effectiveness of `WIGHT` on 9 commercial touchscreen devices, 13 charging cables, and 6 power adapters and proposed both hardware and software countermeasures to mitigate the threat.

Acknowledgements

We thank the anonymous reviewers and our shepherd for their valuable feedback. This research was supported by the National Natural Science Foundation of China Grant 62071428, 61925109.

REFERENCES

[1] G. M. Insights, "Touch screen display market size, covid-19 impact analysis, regional analysis, application development, competitive landscape forecast, 2021–2027," https://www.gminsights.com/industry-analysis/touch-screen-display-market, 2021.

[2] H. Nam, K.-H. Seol, J. Lee, H. Cho, and S. W. Jung, "Review of capacitive touchscreen technologies: Overview, research trends, and machine learning approaches," *Sensors*, vol. 21, no. 14, p. 4776, 2021.

[3] AndroidCentral, "Why does my touch screen go crazy while charging?" https://forums.androidcentral.com/google-nexus-7-tablet-2012/497397-why-does-my-touch-screen-go-crazy-while-charging.html, 2019.

[4] Slane35, "Touchscreen problems while charging," https://forum.xda-developers.com/showthread.php?t=1784773, 2012.

[5] User1950278, "Glitchy touchscreen caused by charger [closed]," https://electronics.stackexchange.com/questions/77631/glitchy-touchscreen-caused-by-charger, 2013.

[6] NBD, "The cell phone being charged automatically booked a ten thousand yuan presidential suite and checked the chat history." http://www.nbd.com.cn/articles/2018-10-08/1260630.html, 2018.

[7] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap 'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *Proceedings of 2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 620–637.

[8] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "GhostTouch: Targeted attacks on touchscreens without physical touch," in *Proceedings of 31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[9] DISPLAYS2GO, "The value of phone charging stations," https://www.displays2go.com/Article/The-Value-Phone-Charging-Stations-97, 2018.

[10] Y. Choi, N. Chang, and T. Kim, "DC–DC converter-aware power management for low-power embedded systems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 26, no. 8, pp. 1367–1381, 2007.

[11] Z. Li, *Power management integrated circuits design, functionality analysis and applications*. The University of Texas at Arlington, 2005.

[12] P. S. Crovetti and F. Fiori, "Distributed conversion of common-mode into differential-mode interference," *IEEE transactions on microwave theory and techniques*, vol. 59, no. 8, pp. 2140–2150, 2011.

[13] S. Yang, B. Orr, Y. Guo, Y. Zhang, D. Pommerenke, H. Shumiya, J. Maeshima, T. Sekine, Y. Takita, and K. Araki, "Measurement techniques to predict the soft failure susceptibility of an IC without the aid of a complete software stack," in *Proceedings of IEEE International Symposium on Electromagnetic Compatibility (EMC)*. IEEE, 2016, pp. 41–45.

[14] J. Zhou, Y. Guo, S. Shinde, A. Hosseinbeig, A. Patnaik, O. H. Izadi, C. Zeng, J. Shi, J. Maeshima, H. Shumiya *et al.*, "Measurement techniques to identify soft failure sensitivity to ESD," *IEEE transactions on electromagnetic compatibility*, vol. 62, no. 4, pp. 1007–1016, 2019.

[15] Synaptics, "Latest advances in touch and display integration for smartphones and tablets," https://www.synaptics.com/sites/default/files/touch-display-integration-smartphones-tablet.pdf, 2014.

[16] T. Vu, A. Baid, S. Gao, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, and J. Walling, "Capacitive touch communication: A technique to input data through devices' touch screen," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 4–19, 2013.

[17] J.-Y. Ruan, P. C.-P. Chao, and W.-D. Chen, "A multi-touch interface circuit for a large-sized capacitive touch panel," in *Proceedings of IEEE SENSORS*, 2010, pp. 309–314.

[18] Y. Yoo and B.-D. Choi, "Readout circuits for capacitive sensors," *Micromachines*, vol. 12, no. 8, p. 960, 2021.

[19] H. Shin, S. Ko, H. Jang, I. Yun, and K. Lee, "A 55db snr with 240hz frame scan rate mutual capacitor $30\times$ 24 touch-screen panel read-out ic using code-division multiple sensing technique," in *Proceedings of IEEE International Solid-State Circuits Conference Digest of Technical Papers,2013*. IEEE, 2013, pp. 388–389.

[20] C.-J. Lee, J. K. Park, C. Piao, H.-E. Seo, J. Choi, and J.-H. Chun, "Mutual capacitive sensing touch screen controller for ultrathin display with extended signal passband using negative capacitance," *Sensors*, vol. 18, no. 11, p. 3637, 2018.

[21] G. Schwarz, "Development of a Parallel and Time Interleaved Multi-Channel Capacitance Measurement System," *Institute of Electrical Measurement and Measurement Signal Processing*, vol. 10, 2016.

[22] S. Aoki, T. Onogi, and S. Yokoyama, "Charge conservation, entropy current, and gravitation," 2021.

[23] M. Miyamoto, M. Hamaguchi, and A. Nagao, "A 143×81 mutual-capacitance touch-sensing analog front-end with parallel drive and differential sensing architecture," *IEEE Journal of Solid-State Circuits*, vol. 50, no. 1, pp. 335–343, 2014.

[24] M. G. A. Mohamed and H. Kim, "Concurrent driving method with fast scan rate for large mutual capacitance touch screens," *Journal of Sensors*, vol. 2015, 2015.

[25] S. P. Hotelling, C. H. Krah, and B. Q. Huppi, "Multipoint touch surface controller," 2017, uS Patent 9,547,394.

[26] A. Ng and P. H. Dietz, "39.3: the need for speed in touch systems," in *Proceedings of SID Symposium Digest of Technical Papers*, vol. 44, no. 1. Wiley Online Library, 2013, pp. 547–550.

[27] M. Kaur, S. Kakar, and D. Mandal, "Electromagnetic interference," in *Proceedings of 3rd International Conference on Electronics Computer Technology*, vol. 4. IEEE, 2011, pp. 1–5.

[28] M. Miloudi, A. Bendaoud, and H. Miloudi, "Common and differential modes of conducted electromagnetic interference in switching power converters," *Revue Roumaine Science Technique–Électrotechnique. et Énergétique*, vol. 62, no. 3, pp. 246–251, 2017.

[29] J. Gaboian, "A statistical survey of common-mode noise," *Analog Applications*, 2000.

[30] A. Jaze, B. Arhambaul, and S. Conno, "Mode conversion due to asymmetric gnd via configuration," in *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. IEEE, 2012, pp. 363–368.

[31] A. Jaze, B. Archambeault, and S. Connor, "Differential mode to common mode conversion on differential signal vias due to asymmetric gnd via configurations," in *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. IEEE, 2013, pp. 735–740.

[32] K. Mainali and R. Oruganti, "Conducted emi mitigation techniques for switch-mode power converters: A survey," *IEEE Transactions on Power Electronics*, vol. 25, no. 9, pp. 2344–2356, 2010.

[33] S. N. EMC, "Differential mode noise and common mode noise causes and measures," https://techweb.rohm.com/knowledge/emc/s-emc/01-s-emc/6899, 2018.

[34] J. Tian, N. Scaife, D. Kumar, M. Bailey, A. Bates, and K. Butler, "Sok:" plug & pray" today–understanding usb insecurity in versions 1 through c," in *Proceedings of IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 1032–1047.

[35] T. Shiroma, Y. Nishio, and H. Inoue, "A threat to mobile devices from spoofing public usb charging stations," in *Proceedings of IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2017, pp. 88–89.

[36] K. Nohl and J. Lell, "Badusb-on accessories that turn evil," *Black Hat USA*, vol. 1, no. 9, pp. 1–22, 2014.

[37] Y. Kumar, "Juice jacking-the usb charger scam," *Available at SSRN 3580209*, 2020.

[38] F. Noack, J. Pospiech, R. Brocke, and J. Schonau, "Reliable overvoltage protection of electronic devices in low-voltage power systems," in *Proceedings of International Symposium on Electromagnetic Compatibility (IEEE Cat. No. 99EX147)*. IEEE, 1999, pp. 298–301.

[39] Y.-C. Chuang and Y.-L. Ke, "A novel high-efficiency battery charger with a buck zero-voltage-switching resonant converter," *IEEE Transactions on Energy Conversion*, vol. 22, no. 4, pp. 848–854, 2007.

[40] F. Shearer, *Power management in mobile devices*. Elsevier, 2011.

[41] Y. Kpomahou, C. Midiwanou, R. Agbokpanzo, and L. H. D. Adjaï, "Nonlinear resonances analysis of a rlc series circuit modeled by a modified van der pol oscillator," *European Journal of Physics*, vol. 43, no. 3, p. 035204, 2022.

[42] J.-M. Baek, D.-J. Seo, J.-H. Chun, and K.-W. Kwon, "A dual charge pump for quiescent touch sensor power supply," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 11, pp. 780–784, 2012.

[43] ALiExpress, "Capacitive touchscreen panel," https://de.aliexpress.com/item/32917864063.html?gatewayAdapt=glo2deu, 2022.

[44] GOODIX, "5-point capacitive touch controller for small-sized mid," https://www.distec.de/fileadmin/pdf/produkte/Touchcontroller/DDGroup/GT911_Datasheet.pdf, 2015.

[45] GoogleDevelopers, "Android debug bridge (adb)," https://developer.android.com/studio/command-line/adb, 2021.

[46] A. W. Min, K. Han, D. Hong, and Y.-j. Park, "Adaptive touch sampling for energy-efficient mobile platforms," in *Proceedings of IEEE Systems Conference (SysCon) Proceedings*. IEEE, 2015, pp. 754–757.

[47] S.-M. Kim, H. Cho, M. Nam, S.-G. Choi, and K. Cho, "Low-power touch-sensing circuit with reduced scanning algorithm for touch screen panels on mobile devices," *Journal of Display Technology*, vol. 11, no. 1, pp. 36–43, 2015.

[48] M. Y. Malik, "Power consumption analysis of a modern smartphone," *arXiv preprint arXiv:1212.1896*, 2012.

[49] S. Electronics, "Green mode," https://www.sunpower-uk.com/glossary/what-is-green-mode/, 2019.

[50] MANUALZZ, "S7817 touch controller datasheet specification," https://manualzz.com/doc/26546841/s7817-touch-controller-datasheet, 2021.

[51] H. Kim and B.-W. Min, "A study on emi generation from a capacitive touch screen panel," in *Proceedings of Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*. IEEE, 2017, pp. 344–346.

[52] N. INSTRUMENTS, "NI myDAQ," https://www.ni.com/zh-cn/shop/hardware/products/mydaq-student-data-acquisition-device.html, 2021.

[53] J.-M. Tsai, Y.-J. Chuang, S.-S. Liao, and S.-Y. Yuan, "Improve ESD protection on mobile phone with capacitive touch screen," in *Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, vol. 1. IEEE, 2011, pp. 295–298.

[54] H. Lu and Y. Li, "Gesture on: Enabling always-on touch gestures for fast mobile access from the device standby mode," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 3355–3364.

[55] W. McGrath and Y. Li, "Detecting tapping motion on the side of mobile devices by probabilistically combining hand postures," in *Proceedings of the 27th annual ACM symposium on User interface software and technology*, 2014, pp. 215–219.

[56] J. Schwarz, R. Xiao, J. Mankoff, S. E. Hudson, and C. Harrison, "Probabilistic palm rejection using spatiotemporal touch features and iterative classification," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 2009–2012.

[57] RIGOL, "RIGOL DG1022," https://www.batronix.com/shop/waveform-generator/Rigol-DG1022.html, 2021.

[58] Micronix, "NF HSA4015," https://eshop.micronix.eu/measurement-equipment/electrical-quantities/nf-corporation-instruments/high-speed-bipolar-amplifiers/hsa-4051.html, 2013.

[59] D. Tao, J. Yuan, S. Liu, and X. Qu, "Effects of button design characteristics on performance and perceptions of touchscreen use," *International Journal of Industrial Ergonomics*, vol. 64, pp. 59–68, 2018.

[60] I.-S. S. Board, "IEEE guide for safety in ac substation earthing grounding," https://www.powerandcables.com/wp-content/uploads/2017/12/IEEE-Guide-for-Safety-In-AC-Substation-Earthing-Grounding.pdf, 2000.

[61] H. TURNER, "Human responses to electricity: A literature review(physiological and pathological responses of humans exposed to electricity)," 1972.

[62] C. F. Dalziel and W. R. Lee, "Reevaluation of lethal electric currents," *IEEE Transactions on industry and general applications*, no. 5, pp. 467–476, 1968.

[63] R.-L. Lin, J.-Y. Guo, and C.-M. Chang, "Study of common-mode voltage measurements for iec62684," in *Proceedings of IEEE Industry Applications Society Annual Meeting*. IEEE, 2013, pp. 1–8.

[64] Apple, "Connect your airpods and airpods pro to your iphone," https://support.apple.com/en-us/HT207010, 2021.

[65] ——, "Connect and use your airpods max," https://support.apple.com/en-us/HT211883, 2021.

[66] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *Proceedings of international conference on computing, communication and automation (ICCCA)*. IEEE, 2016, pp. 537–540.

[67] C. Miller, "Don't stand so close to me: an analysis of the nfc attack surface," in *Proceedings of Briefing at BlackHat USA. Las Vegas*, 2012.

[68] P. Abirami and M. L. George, "Electronic circuit breaker for overload protection," in *Proceedings of International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*. IEEE, 2016, pp. 773–776.

[69] C. Dominguez-Palacios, J. Bernal, and M. Prats, "Characterization of common mode chokes at high frequencies with simple measurements," *IEEE Transactions on Power Electronics*, vol. 33, no. 5, pp. 3975–3987, 2017.

[70] S. Hwang, A. Bianchi, and K. Wohn, "Micpen: pressure-sensitive pen interaction using microphone with standard touchscreen," in *CHI'12 Extended Abstracts on Human Factors in Computing Systems*, 2012, pp. 1847–1852.

[71] C. M. Ahmed and A. P. Mathur, "Hardware identification via sensor fingerprinting in a cyber physical system," in *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2017, pp. 517–524.

[72] O. Shwartz, A. Cohen, A. Shabtai, and Y. Oren, "Shattered trust: When replacement smartphone components attack," in *Proceedings of 11th USENIX Workshop on Offensive Technologies (WOOT 17)*, 2017.

[73] Z. Wang and A. Stavrou, "Exploiting smart-phone usb connectivity for fun and profit," in *Proceedings of the 26th Annual Computer Security Applications Conference*, 2010, pp. 357–366.

[74] P. Cronin, X. Gao, C. Yang, and H. Wang, "Charger-Surfing: Exploiting a power line Side-Channel for smartphone information leakage," in *Proceedings of 30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 681–698.

[75] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Powerhammer: Exfiltrating data from air-gapped computers through power lines," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1879–1890, 2019.

[76] S. S. Clark, H. Mustafa, B. Ransford, J. Sorber, K. Fu, and W. Xu, "Current events: Identifying webpages by tapping the electrical outlet," in *Proceedings of European Symposium on Research in Computer Security*. Springer, 2013, pp. 700–717.

[77] Y. Su, D. Genkin, D. Ranasinghe, and Y. Yarom, "USB snooping made easy: Crosstalk leakage attacks on USB hubs," in *Proceedings of 26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1145–1161.

[78] J. L. Esteves and C. Kasmi, "Remote and silent voice command injection on a smartphone through conducted iemi: Threats of smart iemi for information security," *Wireless Security Lab, French Network and Information Security Agency (ANSSI), Tech. Rep*, 2018.

[79] R. Divya and S. Muthukumarasamy, "Visual authentication using qr code to prevent keylogging," *International Journal of Engineering Trends and Technology*, vol. 20, no. 3, pp. 149–154, 2015.

[80] "Cottonmouth," https://nsa.gov1.info/dni/nsa-ant-catalog/usb/index.html#COTTONMOUTH-I, 2008.

[81] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb," in *Proceedings of 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 264–268.

[82] O. Angelopoulou, S. Pourmoafi, A. Jones, and G. Sharma, "Killing your device via your usb port." in *Proceedings of HAISA*, 2019, pp. 61–72.

[83] N. playset, "Turnipschool," http://www.nsaplayset.org/.

APPENDIX

A. EXPERIMENT RISKS AND PROTECTION METHODS

Before conducting the trial, we inform the participants with the following information: the background and significance of our research, eligibility criteria, experimental design and methods, allowance and compensation, the potential risks, and preventive measures. In addition, the participants can terminate the trial at any time.

Experiment Procedures. The detailed experiment procedures for participants are as follow. (1) First, check the environment of the charging station, plug in the phone, and place it on the table; (2) Then, tap the button according to the popup prompt, and repeat 4 trials; (3) After each trial, participants are required to fill in a questionnaire about whether the target button is clicked successfully. The whole experiment lasts about 5 minutes, and each participant will earn $8 for the experiment.

Informed Risks. Our experiments require participants to press a button in two scenarios: without attacks and with attacks, i.e., injecting ghost touches. During the test, the participants may have a subtle sensation when they tap the button due to a static buildup on the touchscreen. To reduce such likelihood, we have used a copper plate to absorb the static electricity by contacting the touchscreen after each trial. Additionally, in a rare and extreme case, the participant may experience a momentary electric shock if he/she holds the metal frame of the phone and the ground simultaneously. To protect the participants, we have 3 protection mechanisms: (1) Limit the pulse duration to be less than 2ms so that the current flows into the human body will be less than the safety boundary if the circuit ever shorts. (2) Install a current-limitation fuse. (3) We request participants to place the phone on the table and do not pick up the phone during the experiment.

B. RESPONSIBLE DISCLOSURE

We have informed the product security teams about the vulnerability reported in this paper, including the vulnerable products, a detailed description of the vulnerability, and proof of concept. In addition, we also introduced the experimental steps so that they can reproduce a simple version of the attack. What's more, we provided our expected correct behavior and workaround.

C. FORMULA DERIVATION FOR SIGNAL TRANSMISSION

As introduced in Sec. IV-A, let V_{cm_TX} and V_{cm_RX} be the potential of TX and RX that are caused by the injected CM signal respectively.

$$V_{cm\_TX} = \beta_1 A sin(2\pi f t + \varphi_1) \tag{17}$$
$$V_{cm\_RX} = \beta_2 A sin(2\pi f t + \varphi_2) \tag{18}$$

Due to the different non-linear characteristics in the asymmetric circuit, the magnitude decay rate β and phase φ vary from TX and RX. Then the desired DM signal V_{dm} that is fed into the TX and RX can be denoted as:

$$\begin{aligned} V_{dm} &= V_{cm\_TX} - V_{cm\_RX} \\ &= \beta_1 A sin(2\pi f t + \varphi_1) - \beta_2 A sin(2\pi f t + \varphi_2) \\ &= (\beta_1 + \beta_2) sin(\frac{\varphi_1 - \varphi_2}{2}) cos(2\pi f + \frac{\varphi_1 + \varphi_2}{2}) \\ &+ (\beta_1 - \beta_2) cos(\frac{\varphi_1 - \varphi_2}{2}) sin(2\pi f + \frac{\varphi_1 + \varphi_2}{2}) \end{aligned}$$

Further the formula can be derived as Eq. (11):

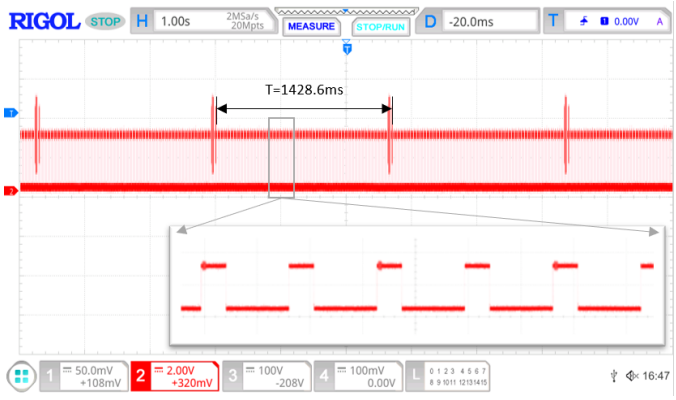
$$V_{dm} = \beta' A sin(2\pi f t + \varphi') \tag{19}$$

where

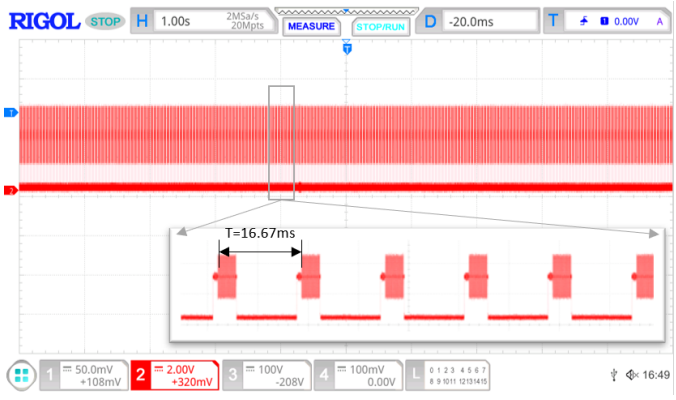
$$\beta' = \sqrt{((\beta_1 - \beta_2) cos(\frac{\varphi_1 - \varphi_2}{2}))^2 + ((\beta_1 + \beta_2) sin(\frac{\varphi_1 - \varphi_2}{2}))^2} \tag{20}$$

$$\varphi' = \frac{\varphi_1 + \varphi_2}{2} + arctan(\frac{(\beta_1 + \beta_2) sin(\frac{\varphi_1 - \varphi_2}{2})}{(\beta_1 - \beta_2) cos(\frac{\varphi_1 - \varphi_2}{2})}) \tag{21}$$

D. EXCITATION SIGNAL UNDER DIFFERENT WORK MODES



(a) Green mode.



(b) Normal mode.

Fig. 21. The excitation signal of the Apple iPhone SE(2020) under normal mode and green mode, displayed in the oscilloscope.

E. Response time of ghost touches and human touches.

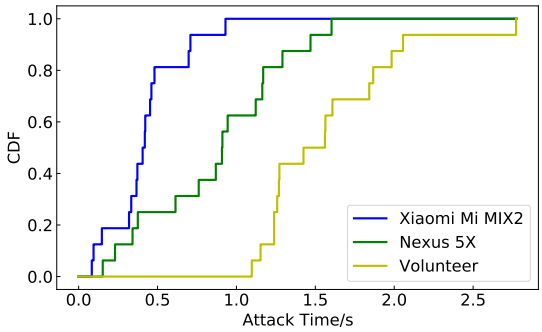
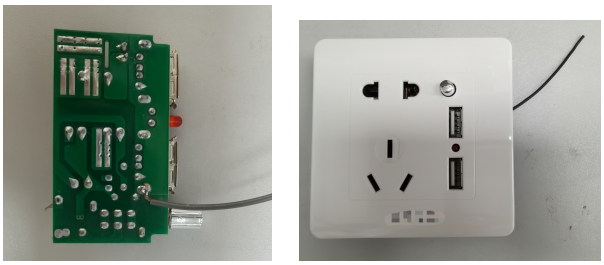


Fig. 22. The CDF plots about the response time of WIGHT attack and volunteers. The average response time of WIGHT on Xiaomi Mi MIX2 is 0.420 s and on LG Nexus 5X is 0.872 s, on volunteers is 1.523 s.

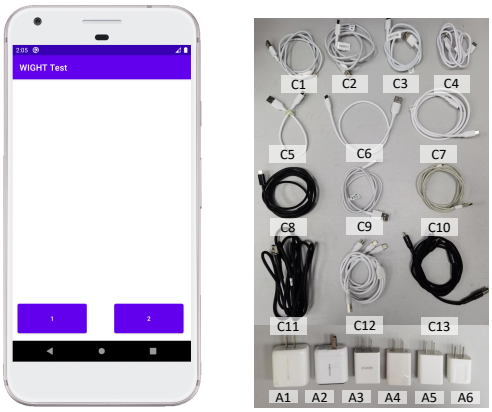
F. Malicious USB socket



(a) PCB circuit. (b) Outlook.

Fig. 23. The attacker flies the GND line from the USB socket.

G. WIGHT Test application and charge cables and adapters.



(a) *WIGHT Test* application. (b) cables and adapters.

Fig. 24. (a) A graphical interface of *WIGHT Test* application. (b) The charging cables and adapters used for evaluation.

H. Setup of the evaluation on charge cables and power adapters

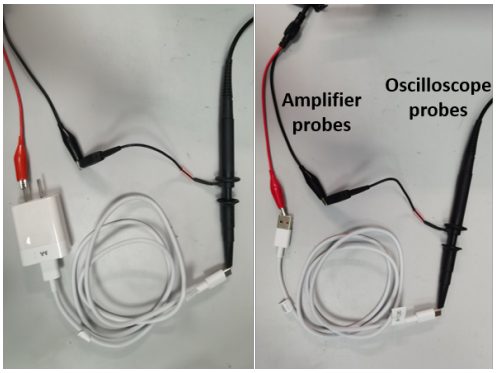


Fig. 25. Evaluation setup of signal transmission efficiency.

Fig. 26. Evaluation setup of success rate with different charging cables or power adapters.

I. Practical attack scenarios of the injection attack.

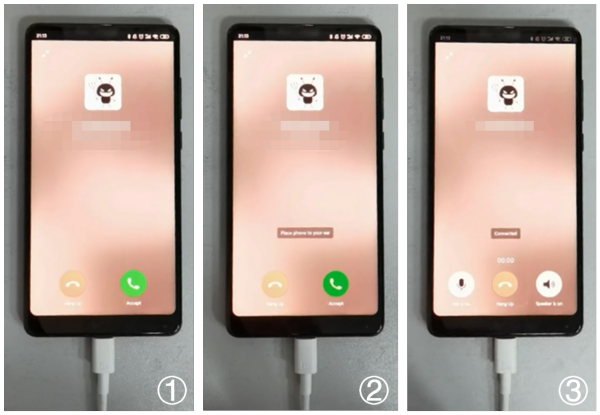


Fig. 27. Picking up an eavesdropping phone call. Step1: the attacker calls the victim; Step 2: the call is picked up by the ghost touches; Step3: the attacker can remotely eavesdrop on the conversations of the victims.

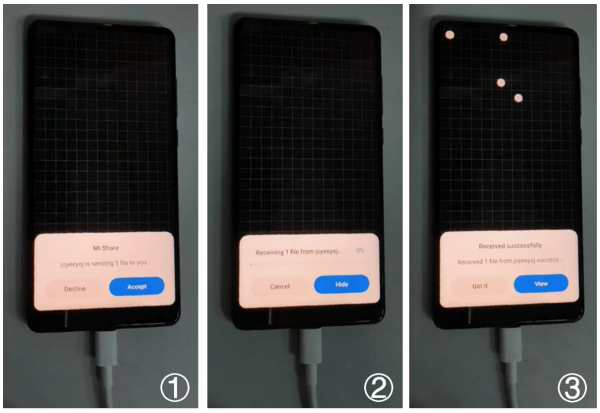


Fig. 28. Accepting a malicious file. Step1: the attacker uses the MiShare tool to send a file request to the victim device; Step 2: the request button is clicked by the ghost touches and then the victim device starts to receive the file; Step3: the malicious file is accepted by the victim device.

Fig. 29. Approving the Bluetooth connection. Step1: the attacker approaches the victim device with an Airpod and then there will be a connection request on the victim device; Step 2: the request button is clicked by the ghost touches; Step3: the attacker's Airpod is connected to the victim device.