Expelliarmus: Command Cancellation Attacks on Smartphones using Electromagnetic Interference

Ming Gao[1,2], Fu Xiao[3,4*], Weiran Liu[1], Wentao Guo[1], Yangtao Huang[1], Yajie Liu[1], Jinsong Han[1,5]
[1] School of Cyber Science and Technology, Zhejiang University, China
[2] ZJU-Hangzhou Global Scientific and Technological Innovation Center, China
[3] School of Computer Science, Nanjing University of Posts and Telecommunications, China
[4] Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, China
[5] Zhejiang Provincial Key Laboratory of Blockchain and Cyberspace Governance, China
{gaomingppm, weiran113, guowentao, yangtaohuang, yajie, hanjinsong}@zju.edu.cn, xiaof@njupt.edu.cn

***Abstract*—Human-machine interactions (HMIs), e.g., touchscreens, are essential for users to interact with mobile devices. They are also beneficial in resisting emerging active attacks, which aim at maliciously controlling mobile devices, e.g., smartphones and tablets. With touchscreen-like HMIs, users can notice and interrupt malicious actions conducted by the attackers timely and perform necessary countermeasures, e.g., tapping the 'Quit' button on the touchscreen. However, the effect of HMI-oriented active attacks has not been investigated yet. In this paper, we present a practical attack towards touch-based devices, namely Expelliarmus. It reveals a new attack surface of active attacks for hijacking users' operations and thus taking full control over victim devices. Expelliarmus neutralizes users' touch commands by producing a reverse current via electromagnetic interference (EMI). Since the reverse current offsets the current change caused by a touch, the touchscreen detects no current change and thus ignores users' commands. Besides this basic denial-of-service attack, we also realize a target cancellation attack, which can neutralize target commands, e.g., 'Quit' without interference in irrelevant operations. Thus, the active attack can be completely performed without interruption from users, even if they are alerted by the abnormal events. Extensive evaluations demonstrate the effectiveness of Expelliarmus on 29 off-the-shelf devices.**

***Index Terms*—Touchscreen, intentional electromagnetic interference, touch cancellation**

I. Introduction

As a typical technique of human-machine interaction (HMI), a touchscreen provides a pleasant user experience. It has become popular on human-centric devices, e.g., smartphones, tablets, and smartwatches [1]. With touchscreens, those devices can reliably detect and implement users' complicated operations from fingers or styluses, including short-taps, long-presses, swipes and the like.

One useful function of HMIs is to defend against emerging physical-layer active attacks [2]–[5]. Such attacks aim at seizing control of victim smartphones and performing covert malicious actions, such as directing the browser to malicious websites, making payments for forged transactions and answering incoming calls for eavesdropping. However, existing attacks mainly rely on injecting false operations and the corresponding events will appear on the user's screen.

* Fu Xiao is the corresponding author.

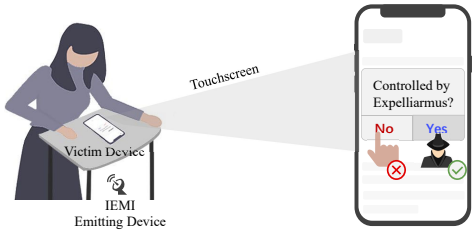


Fig. 1. An illustration of Expelliarmus. The victim smartphone responds merely to the attackers' malicious action and ignores the user's commands.

Once the abnormal events are noticed, the user can easily terminate the attack with the aid of HMIs, e.g., touching the 'Quit' or 'Cancel' button to stop malicious actions and avoid further damage. The touchscreen serves as an essential security blanket. In other words, the effectiveness of existing active attacks on touch-based devices (represented by smartphones) is limited due to their incapability in hijacking users' operations.

A natural question toward active attacks is whether the user's operating command can be remotely hijacked, i.e., cancelling the operation on touchscreens (e.g., on the 'Quit' buttons). We have an interesting observation on touchscreens. In a touch command, the user's finger or a stylus will couple with the capacitive touchscreen, which changes currents in the touchscreen's electrodes [1], [6]. Accordingly, the touchscreen detects and locates this coupling. We consider an intentional electromagnetic interference (IEMI) attack that can remotely manipulate the currents in the victim touchscreens during users' touching. The current changes caused by touches are offset, and the corresponding touch commands are consequentially cancelled. In this cancellation event, the attacker takes over the full control of the touchscreen from the user.

To realize such a cancellation attack, we have to address two challenges: (1) *How to manipulate current in a touchscreen and offset the current change under a touch command?* It is difficult to maliciously control the current in a touchscreen as modern devices typically utilize an anti-EMI design [7] to avoid external interference. Existing attacks [8], [9] could bypass the anti-EMI design under a common assumption of implementing IEMI attacking device nearby [10]–[14]. However, their effects are limited without the ability of controllably hijacking users' commands. To realize practical attacks, we

need to explore the mechanism of IEMI on a touchscreen and exploit an effective scheme for controllable command cancellation. (2) *How to cancel touch commands from various users and capacitor pens on diverse devices through different media?* The attack should be scalable to cover most attacking scenarios. The coupling capacitance on touchscreen varies with users and capacitor pens, and the device diversity should be taken into consideration. The media between IEMI emitting devices and the victim devices also affect the performance of IEMI attacks. Moreover, state-of-the-art (SOTA) touchscreen attacks [8], [9] are with a strong assumption that victim smartphones are placed face-down on a surface (e.g., a table). On the contrary, we consider a more common scenario where users place their devices facing either upward or downward.

We propose a novel IEMI attack, named Expelliarmus. It can cancel users' commands (i.e., touches) on smartphones so that attackers can manipulate victim devices into performing complete malicious actions without being interrupted by HMIs. Based on an in-depth investigation into the mechanism of IEMI, we design new IEMI signals that can inject a reverse current into the victim touchscreens to disable the real touch command, and hence realize a command cancellation attack. Even if the user is aware of such an attack and immediately powers off or reboots the smartphone (e.g., by long-pressing the power button), the time-consuming operation (over 10 seconds)[1], can hardly terminate the malicious actions.

To be more practical, Expelliarmus supports a 'targeted' cancellation. We concentrate the cancelling effect of Expelliarmus onto a targeted region with an accurate screen locator. As illustrated in Fig. 1, Expelliarmus negates the user's touch on the area of the 'No' button, i.e., the prompt box, and chooses the 'Yes' button when the attacker performs SOTA active attacks [2]–[5]. Such a controllable (targeted) cancellation attack is more efficient and stealthier. Our extensive evaluations validate the effectiveness of Expelliarmus under real-world scenarios, with demos of our proof-of-concept attacks presented in [15]. Moreover, we propose preliminary countermeasures to mitigate the impact of IEMI attacks.

Our contributions are summarized as follows:

- We propose Expelliarmus, the first command cancellation attack that can neutralize users' touch commands on touchscreens. It exposes a new attack surface of completely hijacking the devices with a touch-based HMI.
- Expelliarmus enables a targeted attack mode. It can cancel the targeted commands accurately without affecting other operations. An electromagnetic model is established to prove and promote the practicality of Expelliarmus. Those results would facilitate systematical research on the HMIs' security.
- Expelliarmus accomplishes a scalable attack over diverse users, devices, and environments. We evaluate Expelliarmus on 29 COTS devices (including three popular display types, i.e., OLED, IPS, and AMOLED, and three operating systems, i.e., Android, HarmonyOS, and iOS) by successfully cancelling touch commands from 260 human participants and four styluses in real-world scenarios.

[1]The normal 'power off' and 'reboot' that takes up only 3 seconds cannot be realized because it requires the double check with a touch command on the touchscreen, which is also cancelled by Expelliarmus

II. Background And Threat

A. Background of Touchscreen

Touchscreens have become one of the most popular HMIs. They are deployed in various fields, including consumer electronics (e.g., smartphones), public facilities (e.g., automated teller machines), industrial devices [16], autonomous vehicles [17], and medical facilities [18]. Touchscreens recognize touch commands by detecting electric field changes. Among various touch sensing techniques, the mutual capacitive touchscreen prevails due to its low cost and high accuracy [2]. Before presenting the attacking model, it is necessary to explore the working principle of mutual capacitive touchscreens.

A capacitive touchscreen is typically layered on the inner side of the glass in the screen. It comprises two layers of indium tin oxide (ITO), a transparent conductive material. One consists of a grid of transmitting (TX) electrodes and the other of receiving (RX) electrodes, which are arranged orthogonally [2]. These electrodes are mutually coupled with a mutual capacitance C_M. With each touch, a finger or a stylus will couple with the touchscreen, which introduces a capacitance change ΔC in a duration of Δt. However, ΔC cannot be directly measured. Considering the excitation signals in TX electrodes are typically square wave signals with a constant voltage V_{TX}, the capacitance change ΔC would introduce a charge signal $\Delta Q(= \Delta C \cdot V_{TX})$ in RX electrodes. A capacitance to digital converter (CDC) [19] is utilized for measuring the current change $\Delta i(= \Delta Q/\Delta t)$ in RX electrodes and then calculating ΔC as follows,

$$\Delta C = \frac{\Delta Q}{V_{TX}} = \frac{\Delta i \cdot \Delta t}{V_{TX}}. \tag{1}$$

If $\Delta C \geq C_{gate}$ (i.e., $|\Delta i| \geq i_{gate}$) where C_{gate} and i_{gate} are preset thresholds, the touchscreen detects a touch command.

Particularly, a micro controller unit (MCU) drives one TX electrode to send excitation signals successively and measures Δi from RX electrodes in turn [8]. Thus, it supports error-free multi-touch. We mainly analyze the performance of Expelliarmus on the mutual capacitance touchscreens. Our attacks also work on other kinds of touchscreens.

B. Conventional Touchscreen Attacks

Existing attacks on touchscreens can be broadly divided into two groups: the passive mode and the active mode.

Passive Attacks. Attackers can extract private information from the victim touchscreens via electromagnetic leakage, including password or keystroke inference [20], [21] and display reconstruction [22]–[24]. Moreover, side channels, e.g., acoustic [23], magnetic [25], and mmWave [24] signals, are also exploited for the passive attacks.

Active Attacks. Different from the passive ones, active attacks are performed for malicious control. Existing approaches usually inject false touches into touchscreens using an IEMI

attack [2]. Two recent works [8], [9] realize target attacks that are able to remotely assign the location of these false touches.

However, existing attacks pose little influence on users' commands. Touchscreens always execute users' touch commands reliably. Even if existing active attacks (not only on touchscreens [2], [8], [9] but also on others, e.g., voice assistants [3], [5], [11] and NFC [2]) have successfully launched malicious actions on the victim devices, users can interrupt them or avoid further damage via their own commands, i.e., tapping the 'Cancel' or 'Quit' buttons. In other words, users can always maintain absolute control of their devices via touchscreens. Therefore, for complete hijacking, the potential threats of active attacks have not been fully investigated.

Our Insight. We observe that a touchscreen would perform diverse responses to different IEMI signals. The frequency, amplitude, and modulation of the IEMI signals would pose a significant influence on the responses of touchscreens. Along these lines, we present a modulation scheme on the IEMI signals so that our proposed attack can offset the current change in the victim touchscreens (i.e., making $|\Delta i|<i_{gate}$ in Eq. 1). In this way, we are able to cancel the touch commands.

C. Threat Model

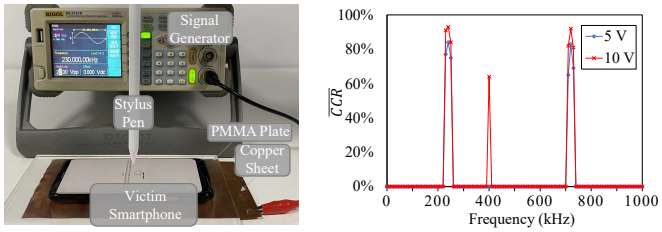
The cancellation attack can not only be independently conducted, but also jointly performed with other attacks, for example, a malware and prior active smartphone attacks [2]–[5], [8], [9], [11], [26]–[29]. Therefore, the attackers can accomplish complete control over the victim devices. Here, we define the attackers' capabilities as follows.

- **Victim Device:** Expelliarmus is mainly targeted at touch-based device, represented by smartphones. In SOTA touchscreen attacks [8], [9], the victim device is supposed to be placed face-down on a surface (e.g., a table), which is impractical. Moreover, the touchscreens of industrial devices and autonomous vehicles use specific layouts that are always face-up [17]. Different from those impractical assumptions, we consider a more common scenario where users place their devices either upward or downward.
- **Attack Setup:** We make the common assumption of the EMI attack setup [10]–[14], in which attackers can hide the IEMI attacking device approaching the victim smartphone (e.g., under the table where the smartphone is placed).
- **Attackers' Capability:** Attackers can synthesize any low-power IEMI signals. Nevertheless, they can neither hurt the victim device using high-power EMI nor physically touch the victim device. Additionally, it is *unnecessary* for attackers to know the model of the victim device beforehand.

III. Feasibility Investigation

Before digging into detailed design, we conduct pilot study to explore the feasibility of touch command cancellation based on the observation on diverse performances of a touchscreen under different IEMI signals.

Pilot Study. We first validate the possibility of touch command cancellation using IEMI with different frequencies. An effective way to generate radiated IEMI signals is using



(a) Setup. (b) CCR against a stylus

Fig. 2. Pilot experiment and results.

electrodes. The experimental setup is shown in Fig. 2(a). A metal (copper) electrode plate (200 × 100 × 0.1 mm) is placed under a face-up smartphone (HUAWEI P10) of 145 × 69 × 7 mm. A polymethyl methacrylate (PMMA) plate (of 5 mm thickness) serves as a shielding layer. The total distance from the malicious copper electrode plate to the victim touchscreen is 12 mm. A signal generator drives the copper electrode plate with a sinusoidal signal whose frequency sweeps from 10 kHz to 500 kHz at a step of 10 kHz. The IEMI amplitude is set as 4 V, 5 V, and 6 V respectively. We manipulate a mechanical arm into holding a stylus (Stylus Pen [30]) to swipe on a touchscreen following an identical track repeatedly. An APP 'Screen Test Pro' [31] is used to track and record touches.

Metric. To describe the performance of cancellation, we define a metric named average cancellation-to-command ratio (CCR). It represents the average proportion of the cancelled commands taking account for all testing commands on victim smartphones. To be specific, we measure the number of cancelled taps compared to the total number and the lost length proportion in swipes on average. In particular, CCR=0 indicates that the touchscreen operates normally, while CCR=1 means the complete cancellation.

Results. Although the touchscreen has gone through a thorough electromagnetic compatibility test with anti-EMI designs, the tested smartphone is still vulnerable to IEMI. As shown in Fig. 2(b), the CCR can reach up to 100% using a 6 V, 240 kHz IEMI signal. In general, it is susceptible to IEMI signals of specific frequencies, and a higher IEMI amplitude would indicate better cancellation performance.

Distribution of Cancellation. The cancelling effect is distributed almost uniformly over the touchscreen. The distribution is independent from the amplitude and frequency of IEMI signals. It mainly relies on the shape of the IEMI electrode as analyzed in Sec. IV and Sec. V-C1.

The pilot experiment confirms that IEMI can produce the cancelling effect on users' commands on smartphones. As the next steps, we will exploit methods to expand cancellation on users' fingers and transfer the cancellation distribution around the whole touchscreen into a controllable cancellation attack.

IV. Modeling IEMI Effect on a Touchscreen

We establish an electromagnetic model to analyze the IEMI effect on a touchscreen. The model acts as the guidance in designing practical cancellation attacks. As illustrated in Fig. 3, we consider a touchscreen and its equivalent resistance-

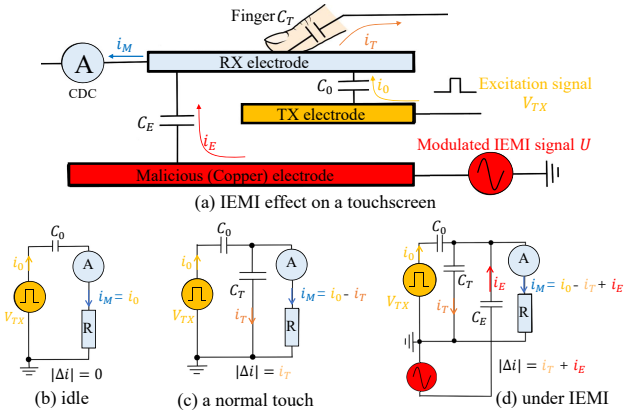


Fig. 3. Illustrations of (a) IEMI effect on a touchscreen, and equivalent circuits when the screen is (b) idle, (c) touched normally, and (d) affected by IEMI.

capacitance (RC) circuit, and analyze the characteristic of the circuit when being touched and interfered in.

In an idle touchscreen, i_0 is the steady-state current through the capacitance of TX-RX electrodes (denoted as C_0), where R is an equivalent resistance. The CDC (denoted as Ⓐ) measures the current $i_m = i_0$ in Fig. 3(b).

In a touch command, a finger or a stylus will introduce a coupling capacitance C_T, along with an additional current i_T. The measured current i_m changes from i_0 in Fig. 3(b) to $i_0 - i_T$ in Fig. 3(c). When the current change $|\Delta i| = i_T$ exceeds i_{gate} (i.e., the detected capacitance change $|\Delta C| = C_T > C_{gate}$), the touchscreen detects the touch command.

We assume an IEMI electric field, denoted as $\boldsymbol{E}$. According to Maxwell's equation [8], the IEMI coupling is

$$\oint_{\boldsymbol{l}} \boldsymbol{E} d\boldsymbol{l} = -\iint_{\boldsymbol{S}} \frac{\partial \boldsymbol{B}}{\partial t} d\boldsymbol{S}, \tag{2}$$

where $\boldsymbol{l}$ is a closed contour bounding a surface $\boldsymbol{S}$, and $\boldsymbol{B}$ is the electro-magnetic field. The time-varying $\boldsymbol{B}$ exerts an electromotive force in a touchscreen (as $\boldsymbol{S}$ here), which injects a current i_E through the coupling capacitance C_E. By appropriate modulation, the current i_E will keep reverse to i_T, as shown in Fig. 3(d). We have

$$|\Delta i| = i_T - i_E. \tag{3}$$

Correspondingly, the detected capacitance change in a touchscreen is reduced to $|\Delta C| = C_T - C_E$. If it meets $|\Delta C| < C_{gate}$, the touchscreen detects no touch and thus the user's command is cancelled. Based on experimental observations, we infer that C_{gate} is approximately 100 pF.

V. Attack Design

We propose the design of Expelliarmus with the goal of neutralizing users' operations (e.g., taps, presses, and swipes), especially in a target area through a controllable way. Expelliarmus is composed of four modules, as illustrated in Fig. 4.

A. Effective Cancellation

We exploit the fundamental factors that affect the efficiency of touch command cancellation in terms of the electrode design, frequency determination, and intensity selection.

An intuitive scheme for generating an IEMI electric field is to utilize a copper electrode plate. The electrode has high electrical conductivity and serves as a near-field antenna [9]. If being driven by a sinusoidal malicious signal $U(t) = Usin(2\pi ft)$, where U and f are the amplitude and frequency respectively, the electrode will generate an IEMI electric field with the intensity of $E = U/2d$, where d is the distance to the touchscreen. In practice, the attacker can inconspicuously attach a copper thin plate to the desired place, e.g., the region on the underside of the table where a victim smartphone is placed. The area of such a plate is much larger than that of the touchscreen. The electrode will couple with the RX electrodes in the touchscreen [8], and we have,

$$i_E = K_0 \varepsilon \frac{\partial \boldsymbol{E}}{\partial t} = \frac{K\varepsilon U}{d}, \tag{4}$$

where ε and d are the dielectric constant of the medium and the distance between the copper electrode and the touchscreen, K_0 and K are constant.

According to Eq. 4 and Fig. 2(b), we can conclude that the higher U, the stronger the interference effect with a bigger i_E. Note that a simple increase of IEMI strength cannot always lead to better performance. An IEMI of over 2000 V/m may hurt the touchscreen permanently, in which case the touchscreen may detect commands with wrong locations, detect false touches, or ignore touch commands randomly even after being away from the high-power IEMI. Therefore, we cannot simply jam the touchscreens using high-power EMI, which may damage the victim smartphones, and meanwhile, the desired malicious actions cannot be conducted or completed.

To address the above issue, we leverage the fact that the frequency of the malicious signal plays an essential role in cancellation attacks. As a typical RC circuit, the touchscreen presents various responses to the frequency of external IEMI signals. It is most sensitive to a specific frequency, i.e., resonant frequency [32]. The resonant frequency f_r of a touchscreen when being touched (the equivalent RC circuit as Fig. 3(d)) can be represented as follows,

$$f_r = \frac{1}{2\pi(C_0 + C_T)R}. \tag{5}$$

Moreover, the touchscreen's response reaches a peak at the harmonics of the resonant frequency, i.e., at kf_r $k \in \mathbb{N}$. Figure 2(b) demonstrates this relationship, in which the victim smartphone is the most vulnerable to IEMI signals at 240 kHz, 400 kHz (approaching twice 240 kHz), and 720 kHz (triple 240 kHz). In this case, driven by malicious signals of kf_r, we can generate a power IEMI electric field with an effective current i_E injected into the victim touchscreen. Furthermore, we provide a positive voltage bias for the malicious signals to guarantee that i_E always flows from the copper electrode (with a relatively high voltage) to the victim touchscreen (with a relatively low voltage). Thus, i_E maintains to be reverse to i_T, and $|\Delta i|$ is significantly reduced.

In short, we redesign the malicious signal as follows,

$$U(t) = \sum_{k=1}^{3} Usin(2\pi k f_r t) + \frac{U}{2}, \tag{6}$$

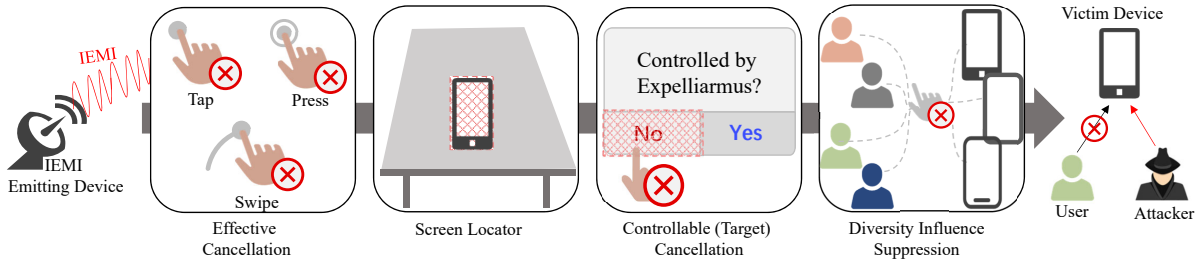
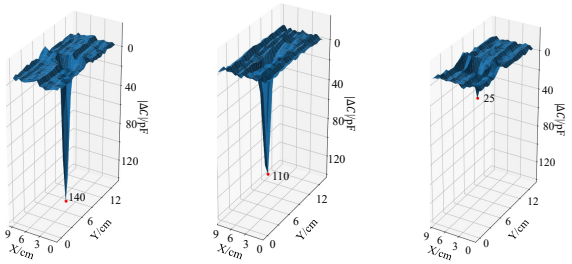


Fig. 4. Expelliarmus, a practical and scalable active attack on touch-based devices, can cancel users' commands using IEMI. It supports a controllable cancellation on target areas with an accurate screen locator. It is able to take over the complete control of touchscreens from users.



(a) No IEMI. (b) E=21.4 V/m. (c) E=214 V/m.

Fig. 5. The detected capacitance change ΔC caused by touches from a user's finger under our designed IEMI. Under 214 V/m, ΔC drops down to merely 25 pF, with few touches detected.

where we adopt k =1, 2, 3 (with $E = \frac{3U}{2d}$) in the consideration of attacking cost, because emitting IEMI of super high frequencies requires an expensive signal generator. Empirically, such a setting can improve CCR by 9.8% on average compared to using the single-frequency signal with the identical IEMI intensity. Figure 5 presents the performance of our proposed attack on cancelling user's finger touches under the same setup in Sec. III. The attack deceives the victim smartphone into sensing little capacitance change by injecting reverse currents. Using the malicious signal with multiple frequencies, a 2 V supply can reduce the detected capacitance change ΔC in a finger touch from 140 pF (the C_T of the user's finger) to 110 pF (i.e., $C_T - C_E$), with nearly half of touches lost. Increasing the voltage supply to 20 V, the detected capacitance change ΔC significantly drops down to merely 25 pF, in which few touches can be detected with the CCR of high up to 99.9%.

B. Screen Locator

The basis of a controllable cancellation lies in an accurate screen locator that senses the position of the victim touchscreen. It has been reported that the screen of a smartphone will leak an electromagnetic signal [21] that can be collected using small antennas under the touchscreen, while the antennas away from the touchscreen can barely detect such a leakage due to attenuation. The possible ambient interference mainly consists of the leakage of electric networks, whose frequencies are typically 50 Hz or 60 Hz, and their harmonics. We place additional copper needle antennas at four corners of the table to measure and eliminate the ambient interference by utilizing an adaptive filter. In practice, we can place a matrix of small copper plates (of 1×1 cm) serving as both the sensing antennas and the IEMI emitting electrodes (not simultaneously, as detailed in Sec. V-C3). After obtaining the screen position, we can infer the positions of the target buttons and implement the following controllable cancellation.

C. Controllable Cancellation

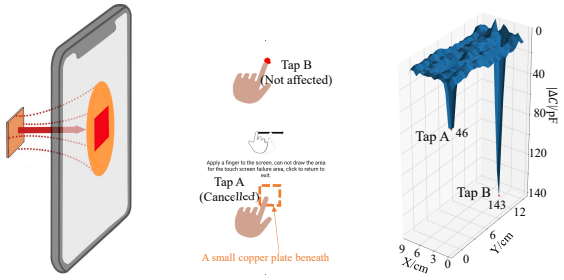
To realize a controllable cancellation, we explore the possibility of generating the required IEMI electric field in a small target area without leakage into other areas on the touchscreen. We exploit a matrix of small copper plate antennas to replace a big plate and drive the antennas under the target area for the target cancellation. We model the IEMI electric field generated by a small copper plate. Accordingly, we design a practical attacking device for the controllable cancellation.

1) Theoretical Analysis: We revisit the model proposed in Sec. IV and analyze the effect of the IEMI electric field generated by a small copper plate on a touchscreen. Therefore, we deduce the theoretical attacking coverage in this scene.

We assume a square antenna of l at the distance of d away from a victim touchscreen, as illustrated in Fig. 6(a). In the area towards the antenna (i.e., the red zone in Fig. 6(a)), the electric field maintains $E = \frac{U}{2d}$ with i_E following Eq. 4. Out of this area, the electric field attenuates gradually [33]. Nevertheless, it still poses a cancelling effect on the neighboring area (i.e., the orange zone in Fig. 6(a)). Empirically, a 1×1 cm antenna at 12 mm away can cover an area of approximately 1.5×1.5 cm. In short, an antenna can induce the cancelling effect in and around the area it directly faces.

2) Preliminary Experiment: We validate the cancelling effect on a target area. We place a small plate of 1×1 cm under the victim smartphone, whose position is directly opposite to such an area on the touchscreen as the orange dotted rectangle in Fig. 6(b). The attacking distance is 12 mm. A user taps twice on the touchscreen simultaneously, one over the plate (the 'Tap A' in Fig. 6(b)) and the other out of it (the 'Tap B' in Fig. 6(b)). The screenshot is shown in Fig. 6(b) with the detected capacitance change ΔC in Fig. 6(c). The 'Tap A' is cancelled. Here, the detected capacitance change ΔC is merely 46 pF, lower than C_{gate} (of about 100 pF). In comparison, the 'Tap B' works normally, of which the ΔC keeps 143 pF as usual. Using an antenna array composed of multiple copper plates, we can cancel touch commands on an arbitrary area without disturbing the others on a touchscreen.

3) Practical Attacking Device Design: We design an antenna array for realizing practical target cancellation. The antenna array acts as both the IEMI emitting antennas and the receiving antennas for capturing the electromagnetic leakage from the screen for the locator in Sec. V-B. It consists of 8×10



(a) (b) (c)

Fig. 6. The working principle and preliminary experiment of the controllable cancellation. (a) An illustration of the IEMI electric field generated by a small copper plate and its influencing scope on a touchscreen. Experimentally, the tap over a small copper plate can be cancelled with (b) the screenshot of the victim smartphone and (c) the detected capacitance change ΔC. Our method can cancel touch commands on a target area without influence on the others.

copper plate antennas (of $1\times1\times0.01$ cm). The interval between the antennas is 1 cm. The attacking coverage of the array is 17×21 cm and can be enlarged by increasing the antenna number according to the requirements of different attacking scenes. We adopt programmable relays to control up to the 80 antennas independently so that only the desired antenna is powered. In addition, we use the standard shielded signal cables to avoid mutual interference among antennas.

D. Diversity Influence Suppression

We consider the diversity of users, devices, and environments to explore the scalability of IEMI cancellation attacks.

1) User Diversity: The coupling capacitance on touchscreen varies with users [34], which determines the resonant frequency f_r according to Eq. 5. Fortunately, we experimentally observe that the diversity of users' coupling capacitance C_T has a limited impact on the resonant frequency f_r. Among 260 volunteers (aged from 18 to 50, 130 males and 130 females), C_Ts are always in the range of [115, 150] pF. Compared with C_0, whose typical value is around 2000 pF, the diversity of users can bring at most 1.65%(=$\frac{150-115}{2000+115}$) drift to f_r. Such a slight frequency drift hardly affects the cancellation performance. For example, the fundamental resonant frequency f_r for human fingers is about 320 kHz on a VIVO S6 experimentally, and it is vulnerable against IEMI in a band of about 20 kHz, i.e., from 310 kHz to 330 kHz. Even though a drift of 5.2 kHz (=1.65%$\times$ 320 kHz) alters its f_r from 320 kHz to 325.2 kHz, a malicious signal of 320 kHz is still in its vulnerable frequency band of 325.2$\pm$10 kHz. In practice, we recruit 10 volunteers to measure the resonant frequency f_r of a model of smartphones beforehand and adopt the average value as the f_r in a real attack. Experimental results in Sec. VI show that the adopted f_rs perform well among 260 volunteers and four styluses on 29 COTS devices.

2) Device Diversity: The diversity of devices results in twofold impacts. The resonant frequency f_r varies with devices due to diverse C_0 according to Eq. 5. On the other hand, the reverse current i_E also depends on the model of the victim device as ε in Eq. 4 is affected by the device itself. Attackers can employ the same model device as the victim one to experimentally determine appropriate f_r and U in advance.

Fig. 7. Prototype of the designed attacking device.

We consider three popular display types, i.e., OLED, IPS, and AMOLED, and three operating systems, i.e., Android, HarmonyOS, and iOS. An interesting observation is that the resonant frequencies of touchscreen are close to several typical values, supported by experiments in Sec. VI-D1. Accordingly, the attack can be expanded to cancel unseen devices by emitting IEMI signals modulated on all these typical values. Therefore, Expelliarmus overcomes the device diversity.

3) Environment Diversity: Environmental factors are also influential when conducting a cancellation attack, e.g., the table on which the victim devices are placed. Specifically, the thickness of the table determines the distance between the attacking device and the victim screen (i.e., d in Eq. 4) and the table material serves as the medium of the coupling capacitance C_T, whose dielectric constant (i.e., ε in Eq. 4) also impacts the cancelling effect. To compensate for the change of i_E caused by these environmental factors, attackers can adjust the signal intensity (i.e, U in Eq. 4). Practical evaluations on the environment diversity including table materials and thickness are presented in Sec. VI-E1 and Sec. VI-E2 respectively.

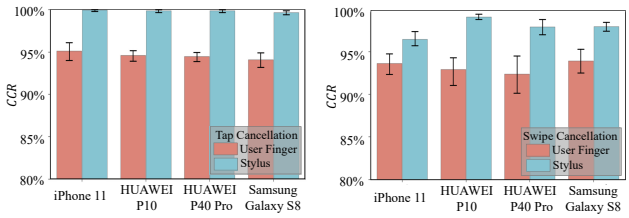
VI. Evaluation

We implement Expelliarmus and evaluate its cancellation performance on COTS devices in real-world scenes. All experiments in this paper follow the IRB protocol approved.

A. Setup

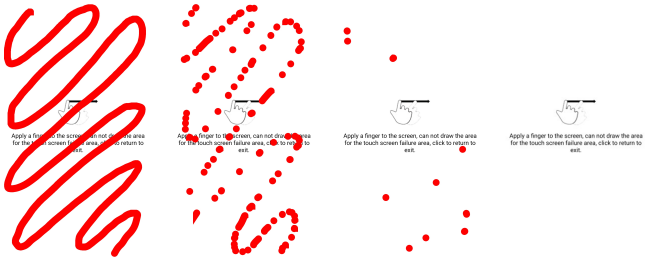
We implement the prototype of Expelliarmus as shown in Fig. 7. The size of the designed attacking device is 15×19 cm. It can be squeezed into a box (the IEMI antenna array is also fixed in this box) and attached to the back of a table. Programmable relays serve as the antenna channel controller. The size can be miniaturized into an extremely small size after customized manufacture, and hence Expelliarmus will be more suitable for practical attacks. An all-in-one instrument (Ni VituralBench 8012) serves as the arbitrary waveform generator and the oscilloscope, connected to a laptop. It supplies the antenna array with IEMI signals (amplified by a power amplifier AIGTEK ATA2021H) and receives the electromagnetic leakage from touchscreens collected by the array. The CCR defined in Sec. III serves as the metric.

We recruit 260 volunteers (aged from 18 to 50, 130 males and 130 females) in total and ask them to tap and swipe on 29 devices (including 24 smartphones, three tablets, and two smartwatches) with different display types (OLED, IPS, and AMOLED) and different operating systems (Android, HarmonyOS, and iOS). Four kinds of styluses (including a Stylus Pen, a NANK pencil, an Adonit Snap 2 Pen and a Maglus Pen) are involved in the experiments.



(a) Tap cancellation. (b) Swipe cancellation.

Fig. 8. Cancellation of touch commands on four smartphones.



(a) No IEMI. (b) E=100 V/m. (c) E=1000 V/m. (d) E=1500 V/m.

Fig. 9. Swipes are cancelled as the IEMI intensity increases.

B. Overall Performance

Expelliarmus successfully cancels taps and swipes on four smartphones (HUAWEI P10, HUAWEI P40 Pro, Samsung Galaxy S8, and iPhone 11).

1) Tap Cancellation: We first consider the tap cancellation. We ask 100 volunteers to tap on the four smartphones 200 times respectively (i.e., the number of finger taps is 100×4×200=80,000 totally). The positions of taps are random. We present the CCRs of cancelling finger taps in Fig. 8(a). Expelliarmus achieves an average CCR among different devices and users of high up to 94.5%. In particular, Expelliarmus can cancel at most 95.5% of taps on the iPhone 11 from the 100 volunteers. Moreover, we also use the four styluses. Each stylus is held by 10 volunteers respectively to tap on each smartphone 200 times (i.e., the total number of stylus taps is 10×4×4×200=32,000), while merely 12 tap commands are recognized by these smartphones. Expelliarmus achieves a CCR of over 99% against stylus taps. Such results indicate that users should cost more time interrupting a malicious action in a real attack. The increase in time consumption is approximately 14.4 seconds on average. Considering that the attacker can usually inject a malicious command within 10 seconds [8], [9], users cannot tap successfully on the 'Cancel' button in the prompt box of malicious action warning before the attacker chooses the 'Yes' button. As a result, the users fail to stop the attacker from hijacking their devices.

2) Swipe Cancellation: We cancel swipes from the 100 volunteers and the four styluses with the CCRs shown in Fig. 8(b). The average CCR reaches 93.2% on swipes of volunteers and that of styluses is 97.9%. Swipe commands are almost completely cancelled. To be intuitive, we ask a volunteer to repeat the identical swipes as much as possible on a Samsung Galaxy S20 Pro for four times, with the screenshots shown in Fig. 9. The results demonstrate swipe cancellation under different IEMI intensities. Even if some points in a swipe are detected, as shown in Fig. 9(c), the swipe has been degraded into taps. In this case, users cannot perform swipe commands (e.g., swiping left or right from the edge to go back or quit, and swiping up from the bottom to the home screen). Therefore, users gradually lose control of their devices.

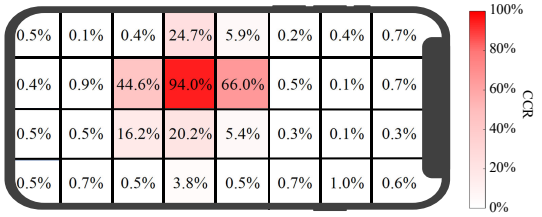


Fig. 10. Controllable cancellation performance. Here the attack targets on the typical position of the 'Cancel' button in a prompt box.

C. Controllable (Target) Cancellation

For practical attacks, we implement controllable cancellation on target areas with an accurate screen locator.

1) Screen Locator: We place the four smartphones randomly on a table. Expelliarmus realizes an accurate screen location. The average location error is 3.9 mm with a maximum error of 9.2 mm. The contact area of a finger with a touchscreen is about 5 mm × 5 mm and the area of a 'Cancel' or 'Quit' button is over 20 mm × 10 mm [35]. In a controllable cancellation, we prefer to generate an IEMI electric field with an area slightly larger than that of the target button to guarantee the cancelling effect. In this case, an error of 3.9 mm can meet the requirement of practical attacks.

2) Cancellation in a Target Area: We successively conduct the controllable cancellation attack on the four smartphones. An App is developed which highlights a point randomly on the screen and volunteers are asked to tap on it. The App also records these touch commands for measuring CCR. We activate the cancelling effect on the screen and record touch commands. We ask the 100 volunteers to tap on the typical position of the 'Cancel' button in a prompt box (at the left of the touchscreen centre). The distribution of CCRs on different areas is shown in Fig. 10. We achieve the CCR of 94.0% in the target area while the commands in the other areas are detected by the touchscreen normally without disturbance. We repeat attacks on the other areas and obtain similar performance. In a real attack, Expelliarmus can adjust the target coverage to deal with various interface designs of 'Cancel' buttons.

D. Diversity of User and Device

We evaluate the scablability of Expelliarmus by testing on more users and devices.

1) Impact of Touchscreen: We implement Expelliarmus on other 25 COTS touch-based devices, including 20 smartphones (carrying Android, HarmonyOS, and iOS), three tablets, and two smartwatches. All devices are vulnerable with CCRs of at least 90%, 16 of which are listed in Tab. I. The detailed information of all 29 tested devices can be found in [36]. An interesting observation is that the resonant frequencies of all tested devices are close, around 240 kHz, 280 kHz or 330 kHz. Accordingly, our proposed attacks can be expanded to cancel

TABLE I
PERFORMANCE OF CANCELLATION ATTACKS ON DIVERSE DEVICES

Device	OS	Screen			Resonant Frequency f_r (kHz)	IEMI Intensity E (V/m)	CCR
		Manufacturer	Display	Size (inch)			
HUAWEI P40 Pro	HarmonyOS	BOE, Samsung	OLED	6.57	310∼340	1500	94.4%
HUAWEI P10	Android	Japan Display Inc.	JDI IPS	5.10	220∼260	1250	94.6%
iPhone 11	iOS	LG	IPS	6.1	220∼245	1100	95.5%
iPhone 13	iOS	BOE	OLED	6.1	230∼250	535	94.9%
Samsung Galaxy S20 Pro	Android	Samsung	AMOLED	6.2	280	1750	95.1%
Samsung Galaxy S8	Android	Samsung	AMOLED	5.8	180∼200	550	94.0%
Samsung Galaxy Fold Z Flip	Android	Samsung	Eco2 OLED	6.7	220∼250	1000	91.7%
OPPO Reno3 Pro	Android	Unknown	AMOLED	6.4	330	950	92.5%
VIVO S6	Android	Samsung	AMOLED	6.44	300-330	800	93.9%
Mi 10	Android	CSOT	AMOLED	6.67	280-300	1040	94.4%
OnePlus 9	Android	Samsung	AMOLED	6.55	280	1600	92.0%
iPad Pro 2020	iPadOS	LG	IPS	11	220∼240	820	94.1%
iPad Air 2	iPadOS	Unknown	IPS	7.76	130	630	90.2%
HUAWEI MatePad Pro	HarmonyOS	BOE	IPS	10.8	210∼380	250	97.9%
Apple Watch Series 5	WatchOS	LG	LTPO OLED	1.78	280∼300	600	89.9%
HUAWEI Band 6	LiteOS	Unknown	AMOLED	1.47	220	760	91.1%

devices with unseen models. Attackers can adopt three IEMI signals as Eq. 6 with the f_rs set as 240 kHz, 280 kHz and 330 kHz respectively. Such a method can improve the practicality of Expelliarmus in real-world scenarios.

2) Impact of User and Stylus: Experiments in Sec. VI-B involving 100 volunteers have demonstrated the scalability of Expelliarmus among various users. We further recruit 160 other volunteers and ask them to tap and swipe on tested smartphones. We achieve an average CCR of 94.1% of the 260 volunteers in total.

We notice that COTS styluses in our experiment are more vulnerable than users' fingers to Expelliarmus. A possible reason is that the IEMI signals couple with the styluses additionally. Therefore, the i_T caused by touch commands from the styluses drops. However, our attacks fail in cancelling commands from Apple Pencil 1/2 generations on an iPhone or iPad that is connected with the Pencil via Bluetooth, in which case the Bluetooth provides an additional channel to transmit commands. Although a Bluetooth-connected stylus could eliminate the cancelling effect, Expelliarmus still threatens common human users and their devices.

E. Impact of Environment

To evaluate the robustness of Expelliarmus, we test tables with different materials and thicknesses in different scenes.

1) Medium (Table Material): We evaluate it with respect to the CCR using different table materials, of which the dielectric constants impact Expelliarmus. We select five popular materials, i.e., PMMA (ε=2.7∼4.0), plastic (ε=1.8∼2.5), solid wood (ε=1.2∼5), medium density fiberboard (MDF, ε=3.5∼4.0), and paper (ε=2.5). The thickness of each material is 5 mm. We repeat attacks on the four tested smartphones in Sec. VI-B, with results shown in Fig. 11. In addition, we consider metal materials (including copper, iron, and aluminium), through which Expelliarmus fails with CCRs of 0, i.e., the touchscreens work normally. Those metal materials serve as electromagnetic shielding here. Nevertheless, Expelliarmus is capable to pass through non-metal tables and perform cancellation attacks.

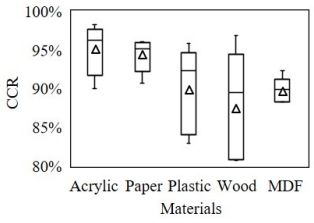


Fig. 11. Impact of material.

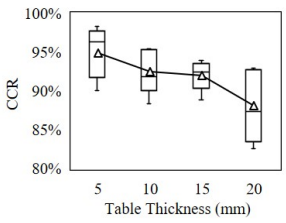


Fig. 12. Impact of table thickness.

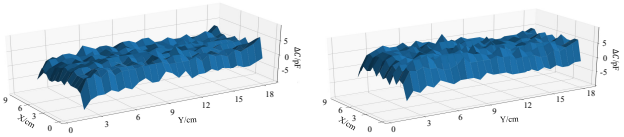
2) Attacking Distance (Table Thickness): To understand the practicality of Expelliarmus, we evaluate the impact of the distance between the attacking device and the touchscreen of a victim device. The distance is determined by the thickness of the table on which the victim device is placed. The table (PMMA) thickness is set as 5, 10, 15, and 20 mm. The devices are attacked 50 times respectively at each distance, with the results shown in Fig. 12. Note that the attacking distance is the sum of the thickness of the table and the device itself in our setup. The CCR drops to 92.0% when the table thickness is 15mm, while it eventually drops to 87.9% through the 20 mm table. In a real attack, an attacker may know the information of the table thickness and accordingly increase IEMI intensity. We can improve the CCRs to 91.9% on the smartphones through the 20 mm table. In particular, the attacking distance is able to extend high up to 47 mm. Due to the typical table thickness of 1/2 inch (12.7 mm) or 5/8 inch (15.9 mm), such an attacking distance can cover most real-world scenarios.

VII. DEFENSES

We summarize existing countermeasures against EMI attacks and propose two effective solutions. We have reported the cancellation attack and potential defenses to manufacturers.

A. Existing methods

EMI attacks have raised a wide concern about security. High-power EMI can cause denial of service (DoS) [37], while low-power EMI can be leveraged for false injections



(a) No IEMI. (b) E=1000 V/m.

Fig. 13. The detected capacitance change ΔC without touches. No reverse current i_E can be detected for defense.

into smartphones [10], microphones [11], and embedded systems [12]–[14]. Defending methods against EMI attacks can be divided into hardware, software, and hybrid ones. However, existing means hardly offer efficient protection.

Hardware Defenses. Hardware anti-EMI methods, represented by shielding [10], [11] and EMI filters [38], have been widely deployed on industrial infrastructure. They effectively safeguard industrial safety. However, such hardware methods cannot be applied to devices that communicate via wireless signals e.g., Wi-Fi, Bluetooth, and ZigBee, because such hardware defenses also cause serious interference to wireless communication. In particular, manufacturers may reinforce the touchscreen by increasing the excitation signal V_{TX} and thus increasing i_T, as well as the required intensity of IEMI for cancellation. Such reinforcement reduces the cancellation success rate to some degree. However, it costs more energy and cannot protect existing devices.

Software Defenses. The difference between real and false signals under EMI enables the software-based detection algorithms. Inspired by this, an intuitive scheme is to detect the reverse current i_E. Unfortunately, such a detection barely works. During the cancellation of a touch, the RX electrodes cannot distinguish the affected current $i_T - i_E$ from the normal one i_E because the two currents are generated under the same principle (i.e., due to the coupling capacitance). Moreover, Expelliarmus barely affects the victim touchscreen without touches. Figure 13 compares the detected capacitance in an idle victim smartphone. The normal operation owns an average ΔC of 1.32 pF with a standard deviation of 2.41 pF and a range of ± 7.00 pF, while ΔC under IEMI is 1.6 pF on average with a standard deviation of 2.45 pF and a range of ± 6.50 pF. Observing no significant difference, software methods fail in the detection of Expelliarmus. Another software-based defense is to reduce the thresholds C_{gate} and i_{gate}, while it degrades the user experience due to mistouch, and increases the risk of being vulnerable against false touch injections [8], [9].

Hybrid Defenses. As a representative of hybrid defenses, power-switching [39], [40] is a recently proposed anti-EMI technique. Its basic idea is to detect abnormal responses generated by EMI when the power supply of the victim device is off. It requires switching the power randomly. However, this countermeasure can hardly be applied to touchscreens due to the requirement of display and high-speed response.

B. Our Suggestions

We propose two suggestions against Expelliarmus-like attacks from the perspectives of users and manufacturers.

Conductive Accessory. We notice that when being connected with a conductor via the USB (e.g., to a PC), the smartphones can be less vulnerable to Expelliarmus. The possible reason lies in that the conduction transfers the malicious reverse current and thus protects the touchscreen. Based on this observation, we suggest the use of conductive accessories for dust plugs on the smartphone USB. Instead of a metal cover or Faraday Fabric recommended in [9], which is harmful to wireless communication quality, our proposed method can mitigate IEMI attacks without any side effects.

Redundancy-base Method. It is almost impossible to visually detect Expelliarmus because it is hidden under tables and can be further embedded into physical tables. Nevertheless, the IEMI would generate an electromagnetic field in a large range. An addition small antenna can easily detect this field. We suggest that manufacturers equip touchscreens with an additional electrode to detect and mitigate EMI attacks.

VIII. Related Work

HMIs on Smartphones. Modern smartphones carry diverse HMIs via various sensors, e.g., voice interaction via voice assistants (VAs) [41]–[43], gestures via cameras [44], and augmented reality (AR) via motion sensors [45]. Moreover, ultrasound [46], motion sensors [47], [48], and eye-tracking [49] are also utilized for detecting users' commands. Nevertheless, the touchscreen is the primary and most widely used one. It is fundamental for smartphones and their security.

Active Attacks on HMIs. Besides touchscreens, other HMIs have been reported to be vulnerable. VAs are suffering from electromagnetic attacks [11], [28], adversarial attacks [4], [29], and ultrasonic non-linear attacks [3], [5], [26], [27]. Motion sensors can be spoofed by acoustic transduction attacks [50]. To our best knowledge, Expelliarmus is the first work to cancel touch commands. It exploits the possibility of fully hijacking smartphones.

IX. Conclusion

We realize Expelliarmus, a novel command cancellation attack, which reveals a new attack surface of active attacks for hijacking users' operations and taking full control over smartphone-like touch-based devices. An IEMI modulation scheme promotes its scalability in reality. Such a vulnerability exists among almost all touch-based devices, and appeals to people for necessary countermeasures to resist its threat.

Acknowledges

This paper is partially supported by the National Key R&D Program of China (2021QY0703), National Science Fund for Distinguished Young Scholars of China under grant No.62125203, National Natural Science Foundation of China under grant U21A20462, 61932013, and 62032021, Research Institute of Cyberspace Governance in Zhejiang University, and Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (Grant No. 2018R01005).

REFERENCES

[1] L. Du, "An overview of mobile capacitive touch technologies trends," 2016.

[2] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap 'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *Proceedings of IEEE S&P*, 2019.

[3] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of ACM CCS*, 2017.

[4] X. Yuan, Y. Chen, Y. Zhao, Y. Long, X. Liu, K. Chen, S. Zhang, H. Huang, X. Wang, and C. A. Gunter, "Commandersong: A systematic approach for practical adversarial voice recognition," in *Proceedings of USENIX Security*, 2018.

[5] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, "Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves," in *Proceedings of NDSS*, 2020.

[6] 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, 2014.

[7] M. Mathur, J. K. Rai, and N. Sridhar, "Electromagnetic compatibility analysis of projected capacitive touch technology based panel computer for military application," *Journal of Electromagnetic Waves and Applications*, vol. 30, no. 13, pp. 1689–1701, 2016.

[8] "GhostTouch: Targeted attacks on touchscreens without physical touch," in *Proceedings of USENIX Security*, 2022.

[9] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin, "Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices," in *Proceedings of IEEE S&P*, 2022.

[10] C. Kasmi and J. Lopes Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.

[11] D. F. Kune, J. D. Backes, S. S. Clark, D. B. Kramer, M. R. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Proceedings of IEEE S&P*, 2013.

[12] J. Selvaraj, G. Y. Dayanikli, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of AsiaCCS*, 2018.

[13] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or heat?: Manipulating critical temperature-based control systems using rectification attacks," in *Proceedings of ACM CCS*, 2019.

[14] M. Mishali and Y. C. Eldar, "From theory to practice: Sub-nyquist sampling of sparse wideband analog signals," *IEEE J. Sel. Top. Signal Process.*, vol. 4, no. 2, pp. 375–391, 2010.

[15] Expelliarmus Demos, "A video demonstration of expelliarmus - cancelling touch commands on smartphones.." https://youtu.be/DYdLjGM1gXw, 2022.

[16] Xenarc Technologies Inc., "Industrial capacitive touch screen.." https://www.xenarc.com/industrial-capacitive-touchscreen/, 2021.

[17] TESLA Inc., "Tesla model s.." https://www.tesla.com/models, 2021.

[18] FOCUS LCDs, "Touch screens for use in medical instrument displays.." https://focuslcds.com/journals/touch-screens-for-use-in-medicalinstrument-displays/, 2019.

[19] Analog Inc., "AD7745." https://www.analog.com/en/products/ad7745.html, 2010.

[20] F. Maggi, S. Gasparini, and G. Boracchi, "A fast eavesdropping attack against touchscreens," in *Proceedings of IEEE IAS*, 2011.

[21] W. Jin, S. Murali, H. Zhu, and M. Li, "Periscope: A keystroke inference attack using human coupled electromagnetic emanations," in *Proceedings of ACM CCS*, 2021.

[22] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, "A threat for tablet pcs in public space: Remote visualization of screen images using EM emanation," in *Proceedings of ACM CCS*, 2014.

[23] D. Genkin, M. Pattani, R. Schuster, and E. Tromer, "Synesthesia: Detecting screen content via remote acoustic side channels," in *Proceedings of IEEE S&P*, 2019.

[24] Z. Li, F. Ma, A. S. Rathore, Z. Yang, B. Chen, L. Su, and W. Xu, "Wavespy: Remote and through-wall screen attack via mmwave sensing," in *Proceedings of IEEE S&P*, 2020.

[25] Y. Liu, K. Huang, X. Song, B. Yang, and W. Gao, "Maghacker: eavesdropping on stylus pen writing via magnetic sensing from commodity mobile devices," in *Proceedings of ACM MobiSys*, 2020.

[26] Y. He, J. Bian, X. Tong, Z. Qian, W. Zhu, X. Tian, and X. Wang, "Canceling inaudible voice commands against voice control systems," in *Proceedings of ACM Mobicom*, 2019.

[27] N. Roy, S. Shen, H. Hassanieh, and R. R. Choudhury, "Inaudible voice commands: The long-range attack and defense," in *Proceedings of USENIX NSDI*, 2018.

[28] X. Ji, J. Zhang, S. Jiang, J. Li, and W. Xu, "Capspeaker: Injecting voices to microphones via capacitors," in *Proceedings of ACM CCS*, 2021.

[29] T. Chen, L. Shangguan, Z. Li, and K. Jamieson, "Metamorph: Injecting inaudible commands into over-the-air voice controlled systems," in *Proceedings of NDSS*, 2020.

[30] StylusPen Inc., "Apple stylus pen." https://styluspen.cn/, 2021.

[31] Google Play, "Screen test pro.." https://play.google.com/store/apps/details?id=com.thjh.screeninfo&gl=US&adlt=strict&toWww=1&redig=DD342CEDADC64F1B8A576C5B2B7D80D8, 2022.

[32] A. Paidimarri, D. Griffith, A. Wang, G. Burra, and A. P. Chandrakasan, "An rc oscillator with comparator offset cancellation," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 8, pp. 1866–1877, 2016.

[33] S. Naik, B. Bag, and K. Chandrasekaran, "Electrical field analysis of different structure conductors using fem," in *Proceedings of IEEE ICAECT*.

[34] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui, "Rf-mehndi: A fingertip profiled RF identifier," in *Proceedings of IEEE INFOCOM*, 2019.

[35] Stackoverflow, "How to dismiss the dialog with click on outside of the dialog?." https://stackoverflow.com/questions/8384067/how-to-dismiss-the-dialog-with-click-on-outside-of-the-dialog, 2012.

[36] Anonymous-Expelliarmus, "Vulnerable devices against expelliarmus." https://github.com/Anonymous-Expelliarmus/Vulnerable-devices-against-Expelliarmus, 2022.

[37] F. Sabath, "What can be learned from documented intentional electromagnetic interference (iemi) attacks?," in *Proceedings of URSI General Assembly and Scientific Symposium*, pp. 1–4, 2011.

[38] J. Gago, J. Balcells, D. GonzÁlez, M. Lamich, J. Mon, and A. Santolaria, "Emi susceptibility model of signal conditioning circuits based on operational amplifiers," *IEEE Transactions on Electromagnetic Compatibility*, vol. 49, no. 4, pp. 849–859, 2007.

[39] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of ACM CCS*, 2015.

[40] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *Proceedings of IEEE S&P*, 2020.

[41] A. Graves, A.-r. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013.

[42] K. Sun and X. Zhang, "Ultrase: single-channel speech enhancement using ultrasound," in *Proceedings of ACM MobiCom*, 2021.

[43] Q. Zhang, D. Wang, R. Zhao, Y. Yu, and J. Shen, "Sensing to hear: Speech enhancement for mobile devices using acoustic signals," in *Proceedings of ACM UbiComp/IMWUT*, 2021.

[44] HUAWEI Inc., "Conduct your tunes, direct your leisure." https://consumer.huawei.com/en/emui-11/tips/get-familiar-list/article18/, 2020.

[45] Embedded, "Working with motion sensors in ar and vr designs." https://www.embedded.com/working-with-motion-sensors-in-ar-and-vr-designs/, 2019.

[46] K. Sun, T. Zhao, W. Wang, and L. Xie, "Vskin: Sensing touch gestures on surfaces of mobile devices using acoustic signals," in *Proceedings of ACM MobiCom*, 2018.

[47] J. Hou, X. Li, P. Zhu, Z. Wang, Y. Wang, J. Qian, and P. Yang, "Signspeaker: A real-time, high-precision smartwatch-based sign language translator," in *Proceedings of ACM MobiCom*, 2019.

[48] R. Xiao, J. Liu, J. Han, and K. Ren, "Onefi: One-shot recognition for unseen gesture via COTS wifi," in *Proceedings of ACM SenSys*, 2021.

[49] Z. Jiang, J. Han, C. Qian, W. Xi, K. Zhao, H. Ding, S. Tang, J. Zhao, and P. Yang, "VADS: visual attention detection with a smartphone," in *Proceedings of IEEE INFOCOM*, 2016.

[50] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proceedings of Usenix Security*, 2015.