MagBackdoor: Beware of Your Loudspeaker as A Backdoor For Magnetic Injection Attacks

Tiantian Liu†, Feng Lin†*, Zhangsen Wang†, Chao Wang†, Zhongjie Ba†, Li Lu†, Wenyao Xu‡, Kui Ren†
†Zhejiang University, Hangzhou, Zhejiang, China
‡University at Buffalo, Buffalo, New York, USA
Email: {tiantian,flin,zhangsen,wangchao5001,zhongjieba,li.lu,kuiren}@zju.edu.cn, wenyaoxu@buffalo.edu

***Abstract*—An audio system containing loudspeakers and microphones is the fundamental hardware for voice-enabled devices, enabling voice interaction with mobile applications and smart homes. This paper presents MagBackdoor, the first magnetic field attack that injects malicious commands via a loudspeaker-based backdoor of the audio system, compromising the linked voice interaction system. MagBackdoor focuses on the magnetic threat on loudspeakers and manipulates their sound production stealthily. Consequently, the microphone will inevitably pick up malicious sound generated by the attacked speaker, due to the closely packed arrangement of internal audio systems. To prove the feasibility of MagBackdoor, we conduct comprehensive simulations and experiments. This study further models the mechanism by which an external magnetic field excites the sound production of loudspeakers, giving theoretical guidance to MagBackdoor. Aiming at stealthy magnetic attacks in real-world scenarios, we self-design a prototype that can emit magnetic fields modulated by voice commands. We implement MagBackdoor and evaluate it across a wide range of smart devices involving 16 smartphones, four laptops, two tablets, and three smart speakers, achieving an average 95% injection success rate with high-quality injected acoustic signals.**

I. Introduction

A loudspeaker and a microphone constitute an audio system for audio output and input [1], integrated into commercial electronic devices such as smart speakers, smartphones, laptops, etc. Such a loudspeaker-microphone system satisfies human needs for social interaction and entertainment [2], further evolving into a voice interaction platform for providing service to each human being with different demands, goals, and needs. Motivated by this hands-free human-machine interaction, voice-controlled systems (VCSs) based on loudspeakers and microphones have ubiquitously been installed into electronic devices, e.g., Apple Siri [3], Google Assistant [4], and Amazon Alexa [5].

Recently, the deployment of VCS poses risks of privacy disclosure and property loss, whereby attackers can inject voice commands modulated on sound or light medium into the audio system, triggering malicious tasks. For instance, researchers demonstrate that by utilizing the non-linearity nature of microphones [6], [7], an attacker is capable of delivering arbitrary commands via a modulated ultrasonic wave. However, these attack methods may suffer from at least one of the following limitations: (1) Audible signals crafted by adversarial techniques [8]–[10] tailored to confuse VCSs are easily drowned in ambient noise. (2) Ultrasound-based injection attacks will be rapidly attenuated when penetrating through occlusions like plastic and clothing, due to their weak penetrability [11]. (3) Some methods assemble arrays of attacking facilities for aggressively injection [12], [13], which increases the risk of exposure. (4) Other methods rely on high-cost and unavailable setups, like the Kepler telescope in laser-based attacks [14]. Therefore, it is desirable to propose a novel command injection attack, in an attempt to overcome the above limitations and gain more insight into the vulnerability of audio systems.

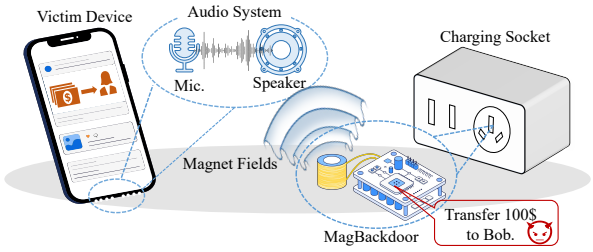


Fig. 1. Attack scenario of MagBackdoor. A self-designed MagBackdoor prototype concealed inside a charging socket emits modulated magnetic fields to induce the loudspeaker of the nearby victim device to utter a sound, further triggering the VCS to execute a malicious command.

Most of the existing injection attacks target microphones directly by transmitting signals using malicious devices. In this paper, we rethink this kind of attack from a new perspective: *Is it possible for adversaries to leverage the benign component in audio systems for command injections, i.e., playing the role as a backdoor for injection attacks?* Based on our investigation, we find that common audio systems are equipped with loudspeakers and microphones, where loudspeakers are in close proximity to microphones out of the need for small form factor and high integration [15]. Once the built-in loudspeaker is forced to speak by an attacker, it can inject malicious commands into the microphone, posing threats to VCSs. However, it is unfeasible to manipulate the loudspeaker stealthily via software implantation, since a malware that compromises loudspeakers cannot pass the system security check such as the APP security review policy [16], [17].

In this paper, we aim to explore the new risk of the loudspeaker acting as a backdoor that is used for command injection into VCSs. We propose MagBackdoor, a new mag-

*Feng Lin is corresponding author

netic injection attack that emits magnetic fields to compromise built-in loudspeakers regardless of noise and occlusions. To implement MagBackdoor in practice, we have to address several questions: (1) Whether the loudspeaker can be affected by magnetic force, taking into consideration that there are other internal electronic elements in victim devices, such as cameras and capacitors that may influence the effectiveness of magnetic injection? To investigate this, we conduct a feasibility study to prove that the loudspeaker can be affected by magnetic force, which can turn it into a backdoor for magnetic injection attacks. The feasibility study also proves that other components in the device have negligible impact on the effectiveness. (2) How to accurately manipulate the sound production of loudspeakers to generate voice commands that an attacker wants? We mathematically quantify the impact of external magnetic fields on a loudspeaker. Using the mechanism of electromagnetic induction, the voice coil inside the loudspeaker will vibrate, which will cause sound to emit. Based on it, a varying magnetic field can manipulate the loudspeaker to utter sound consistent with its change. (3) How to launch injection attacks stealthily without the need for hands-on intervention in realistic circumstances? Aiming at stealth magnetic attacks, a MagBackdoor prototype is designed to be concealed inside a charging socket and automatically emits modulated magnetic fields to trigger the malicious task on nearby victim devices, as shown in Figure 1. Knowing that emissive magnetic fields suffer from distortion and attenuation restricted by limited supply space, we exploit the knowledge of integrated hardware design to elaborate the power amplification module. The enhanced intensity of magnetic fields facilitates the wide attacking range of MagBackdoor. Meanwhile, its fine-grained waveform guarantees successful injection with high-quality and high-intelligibility outcomes. Notably, the attacking procedure of the MagBackdoor prototype is operated by hardware instructions without human intervention, whereby an attacker can remotely initiate MagBackdoor with Bluetooth.

The MagBackdoor poses a new threat to electronic devices, not only expanding attack dimensions but also bringing new inspiration to hardware security design. In summary, our contributions are as follows:

- To the best of our knowledge, MagBackdoor is the first magnetic threat on VCS via a loudspeaker-based backdoor.
- We explore the feasibility of magnetic injection attacks and give detailed theoretical guidance with simulations and experiments, further modeling the relationship between external magnetic fields and loudspeakers.
- We design a prototype to implement offline magnetic attacks stealthily, exploiting the integrated system design methodology to promise low-cost and tiny-size attacking setups.
- We implement the prototype of MagBackdoor and evaluate it on 25 voice-enabled devices, including smartphones, tablets, laptops, and smart speakers. Experimental results show that MagBackdoor can achieve an average success rate of 95%, and is almost immune to noise, occlusion, and electromagnetic leakage.

II. Background

A. Magnetic Field

Magnetic field is the field of magnetic forces generated by moving charges, electric currents, and magnets [18]. A magnetic material like iron is subjected to magnetic forces when placed into the magnetic field. The magnetic field can propagate in air and solid mediums, even in a vacuum.

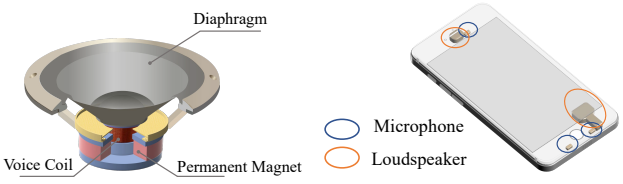
Electromagnet. An electrical conductor such as a wire is coiled into a solenoid around a magnet to induce magnetic fields, which is called an electromagnet [19]. The electromagnet is regarded as the vital source of magnetic fields, where the electric current creates a magnetic field concentrated on the magnet. More specifically, a steady electric current produces a static magnetic field, while a changing current produces a changing magnetic field. The intensity of the magnetic field is proportional to the current intensity but weakens gradually with the increasing distance. The electromagnet plays a key role in electromechanical devices such as transformers, electromotors, electric generators, and loudspeakers [20]. In this paper, the electromagnet is chosen as the critical magnetic field source for magnetic injections due to its low cost, plasticity, and controllability.

Electromagnetic Induction. Electromagnetic induction is the production of an electromotive force (EMF) voltage [21] across electric conductors in varying magnetic fields. The electromagnetic induction uncovers the relationship between magnetism and electricity: 1) When the magnetic field is stationary, the relative motion of the conductor across the magnetic is the cause of EMF voltage in the conductor. If the conductor is closed, an induced current can be generated. 2) When the magnetic field is varying surrounding the conductor, a current will be induced in the closed conductor. 3) The magnitude of EMF voltage or induced current is proportional to the rate of change of the magnetic flux, i.e., magnetic field per unit area. To sum up, electromagnetic induction is the methodology of using magnetic fields to produce currents in a closed circuit.

B. Magnetic Backdoor: Loudspeaker

Magnetism in Loudspeaker. The loudspeaker is an electro-acoustic converter that transforms alternating current signals into corresponding acoustic signals [22]. The most commonly seen structure of the loudspeaker is shown in Figure 2(a). It consists of a diaphragm, a voice coil, and a permanent magnet. The permanent magnet, i.e., an annular pole and another opposite central pole, serves as the base of a loudspeaker to produce fixed magnetic fields. The voice coil rings the central pole and is suspended in the fixed magnetic field. When the altering current flows back and forth in the voice coil, The coil is magnetized into an electromagnet whose polarity changes accordingly. Thus, the voice coil vibrates back and forward along the axis of the center pole since it either attracts or repels the permanent magnet. Whereas the diaphragm is attached to

the coil, the diaphragm will vibrate in line with the variety of currents. With the diaphragm vibrating, the surrounding air is pushed and pulled to create pressure waves called sound. Motivated by the magnetic mechanism of loudspeakers, it is achievable for us to compromise loudspeakers and then manipulate the production of sound via an external magnetic field.



(a) Loudspeaker. (b) iPhone 6s.

Fig. 2. An illustration of the structure of loudspeakers and the distribution of loudspeakers and microphones in smartphones.

Audio System in Commercial Smart Devices. The loudspeaker is always combined with micro-electromechanical system (MEMS) microphones [23] to constitute the audio system in commercial electronic products such as smartphones, smart speakers, laptops, etc. Such a loudspeaker-microphone combination serves for audio capture and audio broadcast, guaranteeing the following voice-controlled module on speech recognition, command execution, and task feedback. Inside the circuit of an electronic product, there is usually a loudspeaker a few millimeters away from the microphone. The reasons for this design are as follows [24]: 1) due to the need for low cost and small size, loudspeakers and microphones often share a sound card and audio codec. 2) Loudspeakers and microphones also share a sound hole. Given an iPhone 6s for example, the front and bottom microphones are adjacent to loudspeakers, as shown in Figure 2(b). The distribution of loudspeakers and microphones in other common smart devices is shown in Appendix A. Due to the proximity of the loudspeaker to microphones, uttered sounds from loudspeakers definitely will be received by microphones. It inspires us to utilize the loudspeaker as a backdoor to inject voice commands into microphones.

III. Threat Model

The attacker's goal is to inject commands into voice-controlled devices equipped with microphones and loudspeakers by using an external magnetic field, ultimately executing malicious actions for privacy and property theft.

Victim Device. The victim devices are common electronic products equipped with loudspeakers and microphones, e.g., smartphones, tablets, and smart speakers, usually installed with VCSs. The attacker cannot alter the device settings or install malware. During the attack, the devices are placed on the surface, e.g., platforms of a cabinet or table. Note that victim devices need to be unlocked for the attack to work.

Attacker's Capability. The attacker can create a magnetic attack device on their own to transmit an altering magnetic field to penetrate the target device and further compromise the built-in loudspeaker. By manipulating the sound production of the loudspeaker, the attacker can inject voice commands to fool voice-enabled devices. Once the setup is deployed, the attacker does not need to get in close proximity to it. The overall attacking manner has no need for human intervention when it is activated, facilitating the deployment and stealthiness of magnetic attacks.

Attack Scenarios. The designed attack device is compact enough to be hidden in an inconspicuous corner, e.g., inside a power socket. With the disguise of an ordinary socket, attackers can use the malicious charging socket at various occasions like cafes and residences. Given that commercial devices like smartphones and smart speakers are placed around the socket for charging, the attack device hidden inside the socket emits malicious commands modulated on magnetic fields. Specifically, the device first injects volume-reducing commands to avoid attention from the surroundings and then sends malicious commands, for instance, purchasing an iPad pro for attacker's personal gain, turning on Bluetooth for information leakage, and accessing apps for espionage.

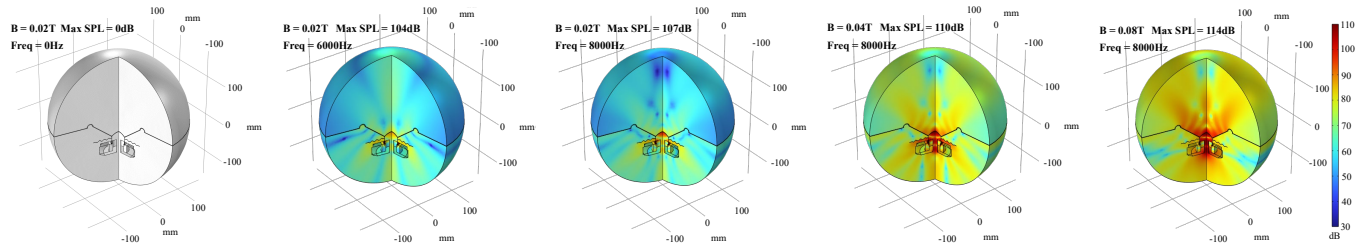
IV. Feasibility Study of Magnetic Attack

In the feasibility study, we first simulate a typical loudspeaker under an external magnetic field to determine the type of emitted magnetic fields. Moreover, we present real-world experiments to verify the feasibility of magnetic injection via a loudspeaker-based backdoor.

A. Static or Dynamic Magnetic Fields?

To carry out a magnetic injection attack, two types of magnetic fields are available: static magnetic fields and dynamic magnetic fields. However, it is uncertain which type of magnetic field would be better to attack loudspeakers. To determine the type of emitted magnetic fields, we design a simulation experiment using COMSOL [25] to investigate the different effects of static and dynamic magnetic fields on loudspeakers. In simulation experiments, a typical loudspeaker is placed in a uniformly distributed magnetic field. The magnetic field passes through its diaphragm from top to bottom. We modify the frequency and amplitude of the magnetic field to create either a static magnetic field or multiple varying magnetic fields, to interfere with the loudspeaker. The parameter setting of the simulation experiment is listed in Table I. We estimate the frequency and sound pressure level (SPL) of sound emitted from the loudspeaker under different external magnetic fields.

The measured sound fields are presented in Figure 3. From the simulation result, the loudspeaker will correspondingly emit 6kHz and 8kHz sound in a varying magnetic field with the applied frequency of 6kHz and 8kHz, respectively. In terms of the strength of emitted sound, we calculate the maximum SPL of the sound field distribution. When the amplitude of magnetic fields increases from 0.02T to 0.08T, the maximum SPL successively increases from 107dB to 114dB. This phenomenon implies that the amplitude of the magnetic-generated sound is positively correlated with the amplitude of



(a) Sound fields in 0.02T static magnetic fields.

(b) Sound fields in 6kHz and 0.02T magnetic fields.

(c) Sound fields in 8kHz and 0.02T magnetic fields.

(d) Sound fields in 8kHz and 0.04T magnetic fields.

(e) Sound fields in 8kHz and 0.08T magnetic fields.

Fig. 3. The simulation results of estimated sound from the loudspeaker in different frequencies and amplitudes of magnetic fields.

TABLE I
SIMULATION PARAMETERS OF THE LOUDSPEAKER IN A MAGNETIC FIELD

Device	Element	Parameter	Value
Loudspeaker	Magnet	Remanent flux density	0.4T
	Voice coil	Number of turns	100
	Voice coil	Relative permeability	1 H/m
	Diaphragm	Young's modulus	2GPa
Magnetic field	Intensity	Frequency	0Hz
			6kHz
			8kHz
Magnetic field	Intensity	Amplitude	0.02T
			0.04T
			0.08T

the magnetic field. However, when the loudspeaker is under a static magnetic field as shown in Figure 3(a), it cannot produce a sound. It is indicated that a dynamic magnetic field can compel a loudspeaker to emit sound, while a static magnetic field cannot. According to the simulation result, we select the dynamic magnetic field as the aggressive signal.

B. Realistic Experiment

We conduct two real-world experiments to further prove the feasibility of injecting acoustic signals via altering magnetic fields and answer the following two critical research questions (RQ):

- **RQ1:** What are the effects on loudspeakers and microphones when a varying magnetic field is applied?
- **RQ2:** Do other electronic elements contained in the device have an impact on the attacking results of magnetic fields?

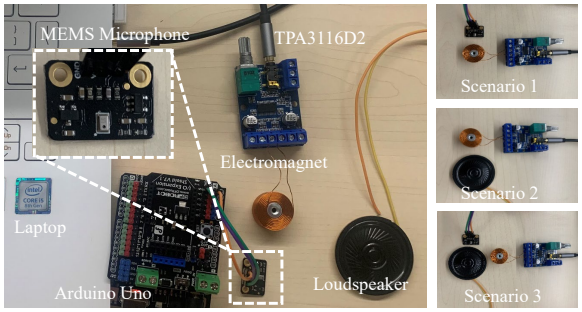


Fig. 4. The setup of Experiment I and three experimental scenarios where a separate microphone, a separate loudspeaker, and a combination of the two in a varying magnetic field.

1) Experiment I: External microphones and loudspeakers: In this experiment, we focus on whether magnetic fields can induce acoustic signals on individual loudspeakers, individual microphones, or a combination of microphone and speaker.

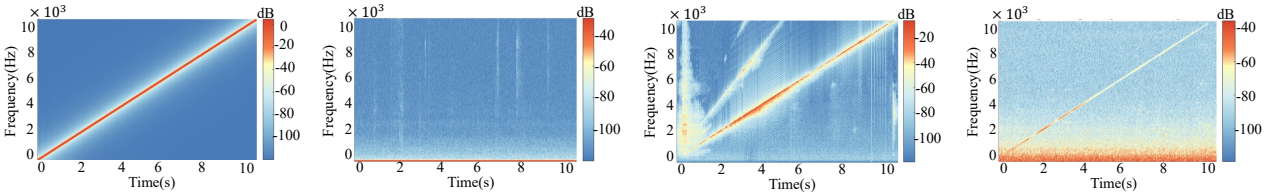
Setup. The overall setup of Experiment I is shown in Figure 4. The TPA3116D2 board [26] is linked to the sound card of a laptop, driving the electromagnet to produce a magnetic field. We control the laptop to produce an altering magnetic field consistent with the variance of the 0-10kHz chirp signal, to cause interference with a MEMS microphone or a loudspeaker. In Experiment I, we design three scenarios where the generated magnetic field applies the magnetic force on a separate microphone, a separate loudspeaker, and a combination of the two, respectively. An Arduino Uno [27] is directly connected to the MEMS microphone and the loudspeaker to capture raw sound data. Note that the electromagnet is placed within 5 mm to the target.

Results. We measure the spectrum of recorded audio from the microphone and spoken audio from the loudspeaker using the three experimental scenarios. The experimental result is shown in Figure 5. It is evident that a MEMS microphone in magnetic fields cannot receive chirp signals but only noise, whereas the loudspeaker can emit entire chirp signals. Interestingly, when the loudspeaker gets close to the microphone, the microphone will record the chirp signals, results shown in Figure 5(d). Notably, if the loudspeaker is positioned away from the microphone, the intensity of recorded audio from the microphone will become growing fainter and even disappear.

> **Answer 1:** Given a modulated magnetic field, the loudspeaker will utter expected sounds. Although a magnetic field cannot directly inject signals into microphones, it can achieve acoustic injection attacks on microphones with the help of nearby loudspeakers.

2) Experiment II: Commercial smart devices: In commercial smart devices, various electronic elements, e.g., capacitors and cameras, are soldered onto a circuit where the audio system, that is, loudspeakers and microphones, is also mounted. To illustrate the impact of other existing electronic elements, we conduct magnetic injections on an iPhone 6s under two conditions. One where the iPhone 6s is stripped of all loudspeakers, and the other where all the components are intact.

Setup. The experimental device to generate magnetic fields



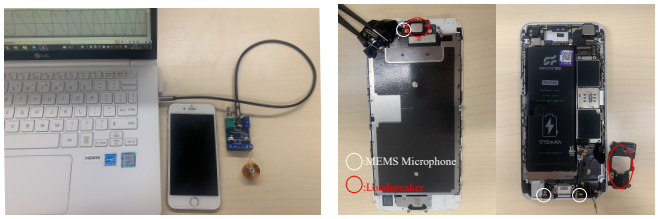
(a) The original chirp. (b) The sound of microphone in scenario 1. (c) The sound of loudspeaker in scenario 2. (d) The sound of microphone in scenario 3.

Fig. 5. The measured spectrum of sampled sound from the microphone or loudspeaker in Experiment I. Figure 5(a) shows the spectrum of original chirp signals loaded on the electromagnet.

is still the same as Experiment I, consisting of a TPA3116D2 board, a laptop, and an electromagnet, as shown in Figure 6(a). We utilize the electromagnet driven by the TPA3116D2 board to produce a magnetic field with 0-10 kHz chirp variation. An iPhone 6s is selected as a victim of magnetic injection attacks. In the first injection scenario, we remove all internal loudspeakers in an iPhone 6s as presented in Figure 6(b). In the second scenario, the iPhone 6s remains intact. We start the recorder inside iPhone 6s to collect the sound received by the microphone. In both experimental scenarios, the victim iPhone 6s is 5mm away from the electromagnet.

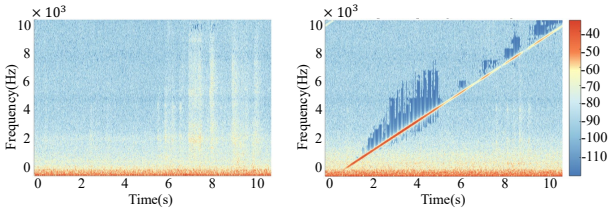
Results. The results for injected signals into the iPhone 6s in two different states are shown in Figure 7. For the removed-loudspeaker iPhone 6s, the built-in microphone is unable to receive any signal. Conversely, the iPhone 6s with loudspeakers receives the chirp signals distinctly, showing a solid spectrum trace from 0Hz to 10kHz. The only difference between the two experimental conditions is the loudspeaker. Furthermore, we compare the signal to noise ratio (SNR) between the injected signal in iPhone 6s and the MEMS microphone in Figure 5(d). The SNRs in those two cases are -4.4dB and -6.8dB, respectively. It is reasonable to speculate that other electronic elements in devices have negligible positive or negative effects on magnetic attacks.

Answer 2: Other interior electronic elements have a negligible influence on the magnetic injection. Only loudspeakers can serve as a magnetic backdoor aiming at injecting acoustic signals into smart devices.



(a) Setup of Experiment II. (b) Loudspeaker removed from iPhone 6s.

Fig. 6. The setup of Experiment II, where the iPhone 6s has no loudspeaker or maintains intact, respectively in two experimental scenarios.



(a) Non-loudspeaker iPhone 6s. (b) Intact iPhone 6s.

Fig. 7. The measured spectrum of injected signals received by the microphone in a non-loudspeaker iPhone 6s and intact iPhone 6s, respectively.

V. MagBackdoor Design

The basic idea of magnetic attack is to inject magnetic fields into built-in audio systems and trigger command execution by a hacked loudspeaker. Aiming at the concealment means of attack, we design MagBackdoor, the first magnetic attack prototype against audio systems on commercial smart devices. The overall framework of MagBackdoor is illustrated in Figure.8. In the design of MagBackdoor, we face the following technical challenges:

(1) How to generate magnetic fields in agreement with malicious voice commands in a flexible and high-integrated manner? According to our theoretical analysis, when the magnetic force impacts loudspeakers, the sound from a loudspeaker compromised by malicious magnetic fields is determined by the current flowing on the electromagnet. Therefore, MagBackdoor uses a hardware decoding circuit decoding the digital audio file of voice commands to output aggressive currents, which will be loaded on an electromagnet to emit the corresponding magnetic field.

(2) How to facilitate a powerful magnetic injection attack? Although our feasibility study confirms the feasibility of magnetic injection, the attacking distance in our experiment is no more than one centimeter. To emit powerful magnetic fields over a longer distance, we urgently need to improve the energy of the output magnetic fields. Moreover, to satisfy the stealthiness of attack, the size of the designed setup should be as small as possible. We leverage the knowledge of analog circuits to design a small-sized specialized power amplification module, which is responsible for amplifying currents while synchronously preserving the fine-grained analog waveform.

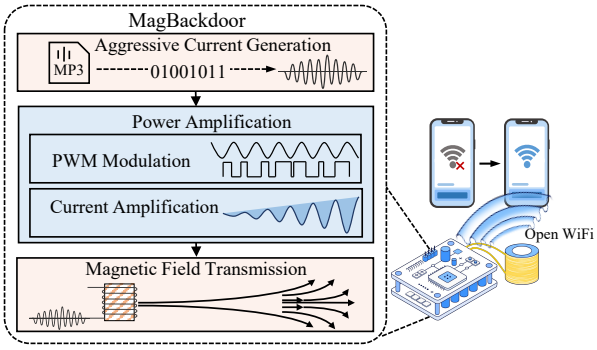


Fig. 8. The system overview of MagBackdoor, a prototype consisting of three hardware module owning different functions to promise a effective magnetic attack.

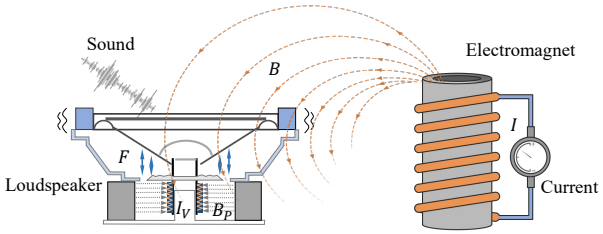


Fig. 9. The mathematical model: a varying magnetic field from an electromagnet to induce current on the voice coil of the loudspeaker and cause sound generation.

A. Aggressive Current Generation

To output a specified variation of the magnetic field, we mathematically model the relationship between the magnetic field and the loudspeaker, to find the rules for manipulating magnetic fields and the ensuing sound from the loudspeaker. Since vital components of loudspeakers are the voice coil and permanent magnet, the internal loudspeakers can be simplified as Figure 9. MagBackdoor enables a standard electromagnet that can be manipulated by modifying currents on the electromagnet, to craft magnetic fields around the loudspeaker. The strength of magnetic field B at position r is proportional to the loaded current I [28], whose relationship can be formulated as:

$$B(r) = N_M \frac{\mu I}{4\pi} \int_C \frac{dl \times (r-l)}{|r-l|^3}, \tag{1}$$

where dl is a vector along the path C whose amplitude is the length of the differential element of the wire in the current direction, l is the position vector of the current element, $r-l$ is the total displacement vector from the conductor element to the calculated field point r, N_M is the number of turns in the electromagnet, and μ is the permeability of the electromagnet. Once the magnetic field $B(r)$ alters, an EMF voltage will be generated in the voice coil, known as electromagnetic induction. According to Faraday's law of induction [29], the induced EMF E can be calculated as:

$$E = N_V \frac{d\Phi}{dt} = N_V N_M \frac{\mu A}{4\pi} \int_C \frac{dl \times (r-l)}{|r-l|^3} \cdot \frac{dI}{dt}, \tag{2}$$

where N_V is the number of turns in the voice coil and A is the surface area of magnetic flux. The magnetic flux on the coil is denoted by Φ. Thus, the induced current I_V on the voice coil can be calculated by using the following formula:

$$I_V = \frac{E}{R} = \frac{1}{R} N_V N_M \frac{\mu A}{4\pi} \int_C \frac{dl \times (r-l)}{|r-l|^3} \cdot \frac{dI}{dt}. \tag{3}$$

Considering that the coil is immersed in a strong permanent magnetic field, the voice coil will be forced by Ampere force, which is defined as:

$$F = B_P I_V L = \frac{B_P L}{R} N_V N_M \frac{\mu A}{4\pi} \int_C \frac{dl \times (r-l)}{|r-l|^3} \cdot \frac{dI}{dt}, \tag{4}$$

where L is the length of the voice coil and B_P represents the strength of the permanent magnetic field in loudspeakers. Note that the Ampere force is derived from the internal permanent magnet rather than the external electromagnet. This is because the Ampere force from external magnetic fields cannot push or pull the diaphragm of loudspeakers, considering that its direction is perpendicular to the diaphragm's axis. According to Eq.4, the induced Ampere force is proportional to the variation of the current flowing on the adversarial electromagnet, since all parameters except the current I are constant. The Ampere force renders the coil's vibration and thereon enables the diaphragm accessed by the coil to generate sound. That is, the generated sound is determined by the current on the electromagnet.

> **Rules for manipulating magnetic fields.** Based on the model, the varying current modulated in the electromagnet enables a correspondingly varying magnetic field. Due to magnetic impact on the internal structure of loudspeakers, the frequency and intensity of sound from loudspeakers depend on the frequency and amplitude of modulated current signals flowing through the electromagnet.

Therefore, to perform injection attacks, MagBackdoor can generate the current whose amplitude corresponds to the variation of voice commands that attackers want to inject. The generated current is then loaded on the electromagnet to emit corresponding magnetic fields, interfering with the loudspeaker. For ease of deployment, the audio that attackers want to inject is pre-stored in an SD card of the system. MagBackdoor uses a hardware decoding circuit equipped with a digital to analog converter (DAC) to decode digital files of malicious commands, producing an aggressive current consistent with the expected audio.

B. Power Amplification

Though acquiring the aggressive current via the aforementioned module, its attenuated amplitude cannot induce efficient magnetic fields to attack devices. Unfortunately, using amplifiers directly to amplify the audio signal will introduce excessive distortion. Thus, this part of hardware design aims to amplify the analog signal meanwhile maintaining fine-grained human voice. We adopt a two-stage amplification strategy involving PWM modulation and current amplification.

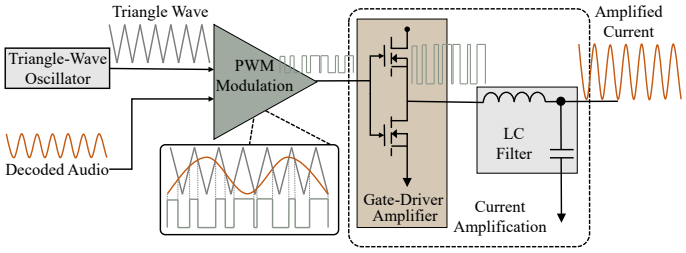


Fig. 10. The signal processing flow of Power Amplification.

PWM Modulation. The frequency band of audio is particularly prone to distortion after a common analog amplification. To address it, we resort to pulse width modulation (PWM) technology that uses a rectangular pulse wave to modulate the decoded audio signal, whose pulse width varies proportionally to the instantaneous amplitude of audio. The wide band of rectangular pulse waves can completely preserve and reinforce the 20-20,000Hz frequency band of acoustic characteristics. Furthermore, the PWM technology as frequency modulation, gives anti-noise performance against most forms of noise amplitude variations. For the sake of speed and stability, MagBackdoor resorts to integrated analog circuits to implement PWM modulation. The signal modulation process is plotted in Figure 10, indicating the transformation of input signals. A triangle-wave oscillator produces a periodical triangle wave $c(t)$. The $c(t)$ and decoded audio $a(t)$ are fed into the PWM generator. The PWM generator mainly relies on a comparator circuit that compares the two inputs and outputs the analog voltage $\delta(t)$ accordingly. The resulting $\delta(t)$ can be modelled as follows:

$$\delta(t) = sgn\left(a(t) - v(t)\right) = \begin{cases} 1, & a(t) > c(t), \\ 0, & a(t) \leq c(t). \end{cases} \tag{5}$$

When the audio is instantaneously higher in voltage than the triangular wave, the comparator outputs a maximum positive voltage. Otherwise, the comparator outputs a maximum negative voltage. The resulting modulation is a chain of pulses whose duty cycle is proportional to the audio amplitude.

Current Amplification. The second stage is the amplification, which accepts the modulated PWM signal with low power and produces a high-current driven signal with no distortion. The fast edge rates and high switching frequencies of the modulated signal require the amplifier to handle rapid switching between positive and negative voltages. We adopt a gate-driver amplifier, whose output states only include maximum positive and negative voltage like a switch. After amplifying the PWM signal, the modulated audio signal will be boosted similarly without signal distortion. The next step is to retrieve the original audio, which will be loaded into an electromagnet to activate the corresponding magnetic field. Recalling the PWM signal $\delta(t)$, we expand it into a Fourier series, allowing us to observe the audio current signal $a(t)$ from frequency domain. The Fourier series can be calculated as follows:

$$\delta(t) = a(t) + \sum_{k=1}^{\infty} \frac{2(-1)^k}{\pi k} sin(\pi k a(t)) cos(2\pi f_c k t), \tag{6}$$

where f_c is the frequency of triangle waves. Note that for ease of reading, the theoretical derivation of Eq.6 is placed in the Appendix B. Based on Eq.6, it is clear that the low-frequency band of δ only contains the desired audio, owing to the bandwidth of $a(t)$ less than f_c. Therefore, to recover the desired audio, MagBackdoor utilizes a low-pass filter such as an inductor-capacitor circuit to filter out the useless PWM signal and extract the expected current.

C. Magnetic Field Transmission

After decoding, modulating, and amplifying, it is time to apply the amplified current signal on an electromagnet to drive a constant stream of magnetic field generation. In addition to the loaded current, the magnetic property of the electromagnet affects the strength of emitted magnetic fields. We customize a cylindrical electromagnet that generates external magnetic fields with a wide elliptic distribution, extending the attack range of MagBackdoor. To acquire the powerful magnetism of the electromagnet, we consider the following four design parameters.

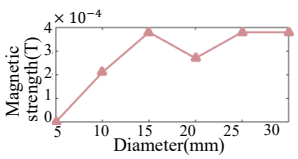


Fig. 11. Measured magnetic strength under different diameters.

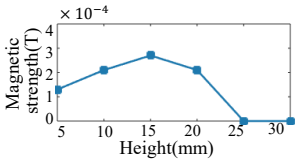


Fig. 12. Measured magnetic strength under different heights.

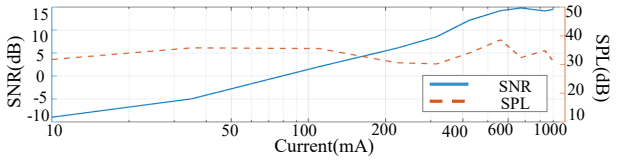


Fig. 13. The estimated SNR of injected signals and SPL of around the target when currents of different strengths are loaded on the electromagnet.

Diameter of magnet. The diameter of the inserted core determines magnetic field intensity and density at the center and outside of the electromagnet. We proceed to choose a suitable diameter of the inserted magnet, which can generate the strongest possible magnetic fields. Thus, we customize six cylindrical magnets with diameters varying from 5mm to 30mm, as shown in Appendix C. All of them are made of soft iron with the same height of 10mm. We wrap 20 turns of coils around them and run a ten mA current on them equally. We use a Teslameter to measure the average magnetic field strength at the center and side of the six electromagnets, respectively. According to the measured results in Figure 11, the 15mm diameter magnet is chosen.

Height of magnet. Another design factor that affects the magnetism of the electromagnet in attacks is its height. Six

electromagnets are fabricated into different heights from 5mm to 30mm, and their magnetic strengths are measured by Teslameter. Note that all six electromagnets possess the same 10mm diameter and 20 turn coil in a 10mA current. According to the measured result in Figure 12, MagBackdoor sets the height of magnet as 15mm.

Number of Coil Turns. The number of coil turns determines the electromagnet's magnetic strength and the corresponding spreading distance. In most cases, the magnetic strength is proportional to the number of turns, in alignment with the fundamental characteristic discovered long ago. In the MagBackdoor, the attacker winds a 400-turn coil around the electromagnet.

Flowing Current. The current generated from power amplification module described in Section 5.2, will flow on the selected electromagnet to activate varying magnetic fields. As an injection attack, the range of current strength should satisfy the two principles: (1) the current amplitude should not be so weak that it fails to inject; (2) nor too large that the induced audio propagates outside the device, alerting the user. To determine a reasonable current value, we adjust the current output of the MagBackdoor prototype and repeatedly perform injection attack experiments on an iPhone 6s. During the experiment, MagBackdoor outputs magnetic fields modulated with a 1kHz tone at a distance of 5mm from the target. We calculate the SNR of injected signals in iPhone 6s to assess the injection effects. Furthermore, to measure the soundwave amplitudes of the injection technique to the human ear, we use a DELIXI sound level meter [30] to measure the SPL around the device. According to Figure 13, the SNR is positively correlated to current in the beginning, but will level off in the end. We speculate that the built-in loudspeaker has a limited speaking ability within its fixed hardware parameters. Considering the voice activity detection (VAD) of VCSs requiring SNR is above -5dB [31], the current strength should be larger than 40mA. Meanwhile, the measured SPL fluctuates between 30dB and 40dB, equivalent to the ambience noise of a quiet bedroom at night. Furthermore, we conduct a live experiment to further prove the inaudible characteristic of MagBackdoor, as discussed in Section VII-G.

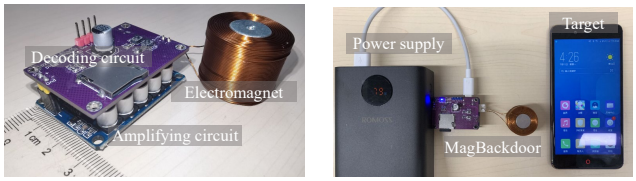
VI. Implementation

In this section, we discuss the actual hardware construction of MagBackdoor prototype using off-the-shelf electrical components. Our prototype includes two major circuits, i.e., a decoding circuit and an amplifying circuit, and an electromagnet. In order to reduce the size of the prototype, the decoding and amplifying circuits are individually layered into the top and bottom layers, as shown in Figure 14(a).

Decoding circuit. The key core of the decoding circuit is a system on chip (SoC) to decode and convert the digital signal into the corresponding analog signal. We choose BK3266 SoC [32] integrating Bluetooth communication and hardware decoder, soldered on a printed circuit board (PCB) printed with a Bluetooth baseband antenna. Four general-purpose input/outputs (GPIOs) of BK3266 serve as input digital signal pins to read data from an SD card for decoding pre-stored audio files of voice commands. The attacker can communicate with BK3266 via Bluetooth 4.2 to activate the decoding function. Afterward, the converted analog signal flows through the pin header and is fed to the bottom amplifying circuit.

Amplifying circuit. The amplifying circuit incorporates the TDA8932B [33], a class-D amplifier, which is used to execute the modulation and amplification. Five parallel polarized capacitors are connected to the power supply side of TDA8932B for power filtering. To further enhance the power of output currents, the two output channels of TDA8932B are united into one channel, whereby two current signals are superimposed simultaneously to generate the final output signal. Two 10μH inductors linked to film capacitors are configured as low-pass filters to remove unwanted PWM signals from the output current. The amplified current passes through the customized electromagnet to emit malicious magnetic fields.

As for the power supply, the CH224K [34] quick charging chirp is employed to support USB power delivery with USB Type-C, which can output a maximum power of 65W. The total size of MagBackdoor is $6cm \times 3cm \times 1.5cm$ with a cost of less than $5.



(a) MagBackdoor prototype. (b) Attack scenario.

Fig. 14. The implementation of MagBackdoor.

VII. Evaluation

A. Setup

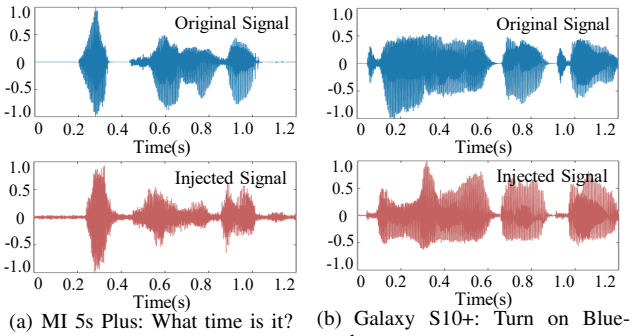
We evaluate MagBackdoor on commercial electronic devices, including smartphones, smart speakers, laptops, and smart tablets. These victim devices contain loudspeakers and microphones, whose manufacturers involve mainstream giants such as Apple, Google, Samsung, Huawei, and Xiaomi. The prototype of MagBackdoor is shown in Figure 14(b), aiming at a victim device to inject malicious commands. We use Google Text-to-Speech (TTS) API [35] to generate the audio of voice commands. The malicious commands in MP3 format with a 16k sampling rate are pre-stored in an SD card of decoding module. Appendix D lists the text of malicious commands. Note that all devices are not specially pre-trained by their owners' voice, nor by malicious audio. In magnetic injection attacks to a specific device, each command is appended to the corresponding wake word, e.g., Hey Siri. The MagBackdoor prototype can be linked to a power socket to charge directly via USB Type-C. The power supply is 12V 1A.

B. Metrics

We define three metrics to comprehensively measure the injection results: (1) the injection success rate is calculated by N_r/N, where N_r is the number of correctly recognized by

TABLE II
EXPERIMENT DEVICES, CATEGORY, SYSTEMS, AND RESULTS. WE EVALUATE MAGBACKDOOR FROM INJECTION SUCCESS RATE, PESQ, AND STOI IN AN OFFICE ENVIRONMENT WITH A BACKGROUND NOISE OF 30DB SPL.

Num.	Category	Devices	Manufacturer	OS/Ver.	VCS	Injection Success Rate(%)	PESQ	STOI
1	Smartphone	Pixel 4	Google	Android 10	Google	96.25	3.95	0.65
2	Smartphone	Honor 50	Huawei	Android 11	Celia	96.56	4.21	0.74
3	Smartphone	Mate 20Pro	Huawei	HarmonyOS 2.0	Celia	97.81	4.03	0.71
4	Smartphone	MI 5s Plus	Xiaomi	Android 6	Xiaoai	98.43	4.05	0.73
5	Smartphone	MI 10	Xiaomi	Android 12	Xiaoai	98.12	3.96	0.66
6	Smartphone	Galaxy S10+	Sumsung	Android 9	Bixby	96.87	4.07	0.63
7	Smartphone	iPhone 6s	Apple	iOS 14.8	Siri	97.18	3.88	0.65
8	Smartphone	iPhone 11	Apple	iOS 15.4	Siri	94.06	3.74	0.68
9	Tablet	iPad	Apple	iOS 15.4	Siri	94.68	3.75	0.59
10	Tablet	iPad Pro	Apple	iOS 14.1	Siri	95.00	3.85	0.69
11	Laptop	Surface Go 2	Microsoft	Windows 10	Cortana	91.56	3.94	0.61
12	Laptop	ThinkPad T490	Lenovo	Windows 10	Cortana	93.43	3.64	0.53
13	Laptop	Xiaoxin 15	Lenovo	Windows 11	Cortana	91.25	3.84	0.52
14	Laptop	MacBook Pro	Apple	MacOS 12.3	Siri	93.75	3.97	0.72
15	Speaker	HomePod mini	Apple	N/A	Siri	91.37	N/A	N/A
16	Speaker	MI Smart Speaker	Xiaomi	N/A	Xiaoai	92.12	N/A	N/A
17	Speaker	TmallGenie	AliGenie	N/A	TmallGenie	90.62	N/A	N/A



(a) MI 5s Plus: What time is it? (b) Galaxy S10+: Turn on Bluetooth.

Fig. 15. The comparison of injected signals received by devices (second row, red) and corresponding original audio (first row, blue).

VCSs in devices and N is the number of injection magnetic attacks; (2) the perceptual evaluation of speech quality (PESQ) [36] is an objective metric to assess the quality of received audio from victim microphones in devices. The PESQ ranges from -0.5 to 4.5, with higher scores indicating better quality; (3) the short-time objective intelligibility (STOI) [37] is an objective metric to assess the intelligibility of received audio from victim microphones in devices. The STOI ranges from 0 to 1, with higher scores indicating better intelligibility.

C. Overall Performance

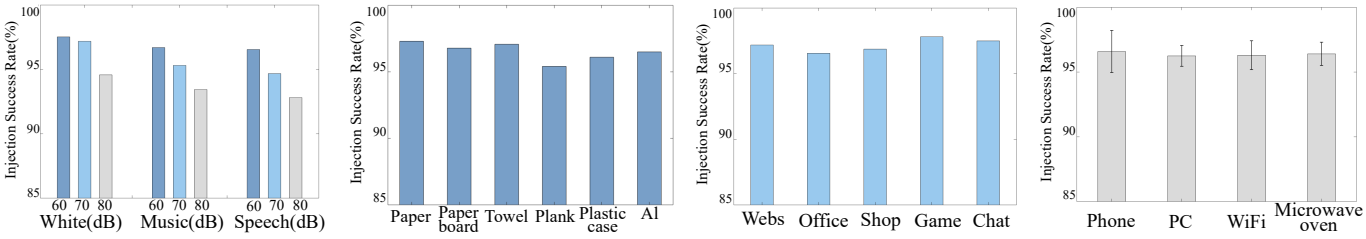
We evaluate the overall performance of MagBackdoor on four mainstream VCS-based electronic devices, including smartphones, speakers, tablets, and laptops. Concretely, a total of 16 mobile phones, two tablets, four computers, and three smart speakers are targets for the magnetic injection attack. The default distance between the MagBackdoor and the victim device is 25 mm. We repeat magnetic injection attacks 80 times per command on each device and measure the injection success rate, PESQ, and STOI. The summary of detailed attack results of MagBackdoor is reported in Table II and Appendix E. According to the results, MagBackdoor achieves an average injection success rate of 95.39%. Notably, MagBackdoor has the best performance in attacking smartphones among all devices, and has the worst performance in smart speakers. This is because smart speakers require a more powerful magnetic field to penetrate the large-size built-in stereo speakers. The injected signal received by the built-in microphones of victim devices and the corresponding audio are presented in Figure 15. It is observed that the injected signal is remarkably similar to the original ones. Moreover, the high PESQ and STOI of injected signals also demonstrate that the injected audio triggered by MagBackdoor is a human-like sound with high quality and intelligibility.

D. Robustness Analysis

1) Impact of Location: We quantify the impact of victim devices' position on the effectiveness of MagBackdoor, in relation to various attack distance and off-axis angles. In this experiment, we choose Mi 5s Plus and iPhone 6 as the attack target and compute the results.

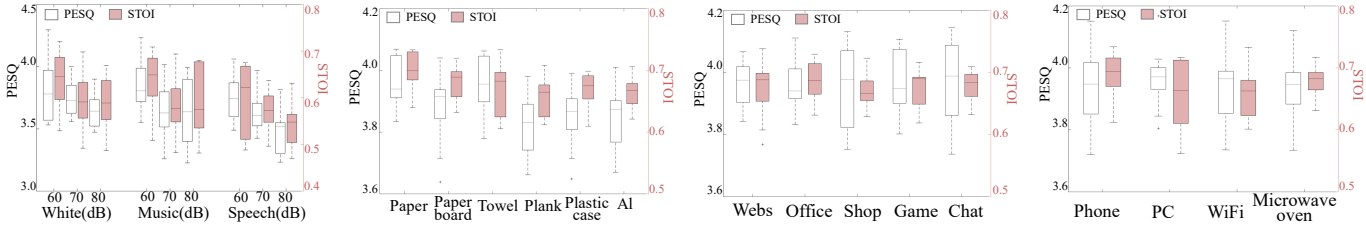
Orientation. According to the attack result presented in Figure 18, our system has a relatively omnidirectional attack range. When the attack angle to the device varies from -60° to 60° within 30mm, the injection success rate maintains above 95%. The MagBackdoor has a wide-range attacking angle, facilitating a convenient magnetic attack in practice.

Distance. The injection success rate remains above 80% within a distance of 55 mm, while gradually decreasing with increasing distance. This is because the energy of emitted magnetic fields tends to decay, especially for the limited power supply of our attacking prototype. Since our attack setup is compact enough to hide in unnoticed corners, such a limited attack distance is acceptable. For instance, MagBackdoor can be hidden in the charging socket or on the back of the table, always ready to attack the device.



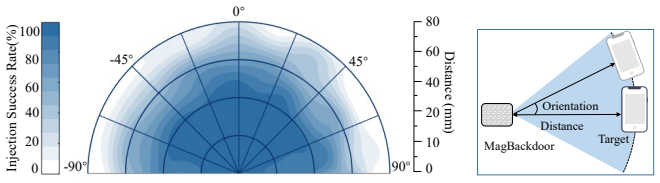
(a) Impact of noise. (b) Impact of occlusion. (c) Impact of application. (d) Impact of electromagnetic leakage.

Fig. 16. The injection success rate of MagBackdoor under various conditions.



(a) Impact of noise. (b) Impact of occlusion. (c) Impact of application. (d) Impact of electromagnetic leakage.

Fig. 17. The PESQ and STOI of MagBackdoor under various conditions.



(a) Attack Scenario. (b) An illustration of location evaluation.

Fig. 18. Performance under different locations.

2) Impact of Ambient Noise: During the magnetic injection attack, the ambient noise may affect the results of MagBackdoor. However, as MagBackdoor induces acoustic signals inside the device, MagBackdoor should be competent in noisy environments. To investigate it, we carry out a set of attack experiments under background noise with different sound pressure level (SPL) settings. The iPhone 6s and MI 5s are selected as target devices. A loudspeaker generates noise at a distance of 10 cm from the device. The sources of background noise are white noise, music, chatting, and traffic noise, respectively. The attacking results in Figure 16(a) and 17(a) reveal that the performance of MagBackdoor under 60dB of interfering noise is basically consistent with that of under low noise. Although with loud interfering noise like 80dB can degrade MagBackdoor, the injection success rate still maintains above 92% with PESQ of 3.57 and STOI of 0.56, meaning the anti-noise property of MagBackdoor.

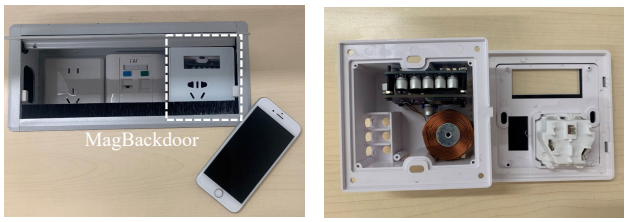
3) Impact of Occlusion: We evaluate the penetrability of MagBackdoor when the attacking setup is hidden by some occlusions and the target device is non-line-of-sight. The occlusion includes paper, a paperboard, a towel, a plank, a plastic case, and an aluminum alloy plate, blocking the device from the attack setup. Their thicknesses are 0.1mm, 3mm, 5mm, 8mm, 2.5mm, and 2.8mm, respectively. As shown in Figure 16(b), the average injection success rates under different occlusion are 97.30%, 96.79%, 97.08%, 95.41%, 96.10%, and 96.5%, respectively. There is a slight drop of only 2% in injection success rate, a difference of within 0.3 in PESQ, and within 0.1 in STOI when occluded by a plank, demonstrating the significant penetrability of MagBackdoor.

4) Impact of Running Application: In addition to outside influence, we also study the performance of MagBackdoor when the target device is running different application programs like word processors or web browsers. In this experiment, iPhone 6s, MI 10, and MI 5s Plus are still chosen as the target. These devices are set to run diverse types of applications, i.e., webs, Office, games, and chatting software. From Figure 16(c) and 17(c), the balanced and significant attacking performance indicates that the running application of devices has an ignorable impact on the effectiveness of MagBackdoor.

5) Impact of Electromagnetic Leakage: In real-world scenes, the victim device is always surrounded by other electronic products. These electronic products involuntarily leak electromagnetic radiation. To investigate the impact of electromagnetic leakages, we place different electronic products such as a smartphone, a desktop computer, a WiFi router, and a microwave oven at the distance of 4 cm from the victim device. All electronic products are turned on and running during the magnetic injection attack. As shown in Figure 16(d) and 17(d), the injection rate ranges from 95% to 98.2% among various electromagnetic leakage, PESQ fluctuates between 3.72 and 4.17, and STOI fluctuates between 0.56 and 0.73. The results verify the robustness of MagBackdoor to the common electromagnetic leakage.

E. Real-world Experiment

Unlike the above experiments in a stationary laboratory, in this experiment, we study the effectiveness of MagBackdoor in real-world scenarios. We modify a commercial charging socket and embed the attack setup into it, as shown in Figure 19. The experiments are conducted in an open meeting room filled with 30-70dB noise, where the target smartphone is near the modified socket.



(a) Attack scenario. (b) Inside the charging socket.

Fig. 19. MagBackdoor in a charging socket.

The attacker remotely activates the MagBackdoor with Bluetooth and performs 20 times magnetic injection on MI 5s Plus, Mi 10, iPhone 6s, and iPad Pro, respectively, to calculate the average attacking result. The average injection success rate is 96.25% with the average PESQ of 3.96 and average STOI of 0.683. Most malicious voice commands can be successfully injected into the victim device with the aid of modulated magnetic fields. It demonstrates the significant injection ability of MagBackdoor.

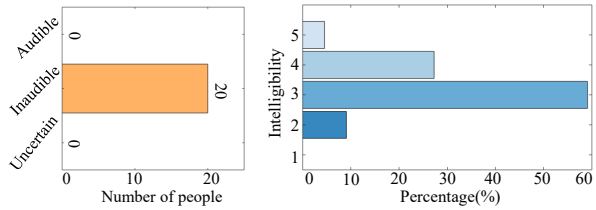
F. Experiment under voice authentication

It is observed that voice authentication is disabled by default at the time of receiving voice input for smart speakers and some mid-to-low-end phones (e.g., Mi 5s Plus, Redmi Note7). Nevertheless, for most smartphones, it is required for users to utter wake-up words three times for voice authentication. We investigate the feasibility of magnetic injection attacks when target smartphones are pre-trained by their owners' voices. Three smartphones, i.e., iPhone 6s, iPhone 12, and Galaxy S20+, are pre-trained by three users (2 females and 1 male), respectively, to ask for voice tasks 40 times as voice authentication. We use online TTS API to produce commands with different male and female voices and then load these commands into MagBackdoor to attack three smartphones. The injection success rate is 25% for iPhone 6s, 18% for iPhone 12, and 16% for Galaxy S20+, respectively. We find that compared with the baseline in Table II, the injection success rate sharply declines. Still, voice assistants may mistake other people's voices for their owners, especially for high-volume female voices. This is because the threshold of voice authentication is not strict for the need of fast response. Especially when users rarely call their voice assistants, the corresponding threshold is relatively loose.

G. Human Study

In this section, we conduct two human studies to prove that from human perception, the attacking process of MagBackdoor is inaudible, and the injected signal is intelligible. The two human studies are described as follows. Note that the audio source of study 1 and study 2 differs, that is, study 1: ambient sound around victim devices, study 2: injected audio in victim devices. (Our research is approved by the IRB: anonymous university.)

- *Study 1: Audible or Inaudible.* Study 1 is to test whether the attacking process is inaudible, where participants sit close to the victim device within 5cm and are asked to try their best to hear something during the attacking procedure. They are informed in advance that an acoustic injection is happening. We recruit 20 participants (6 females and 14 males) to assess the inaudibility of MagBackdoor. They are both native English and Chinese speakers aged from 20 to 31 years old. After five attack trials, the participant is asked whether he/she can distinguish something and to choose an option: whether MagBackdoor is inaudible (The options include audible, inaudible, and uncertain).
- *Study 2: Clear or Noisy.* The successful injection attack among various devices indicates that built-in speech-to-text algorithms of machines can recognize injected signals via MagBackdoor, demonstrating the intelligibility of the machine. Still, it is vital to prove that humans can understand injected commands, i.e., human intelligibility. Study 2 is to test the intelligibility of injected results from human hearing, where participants are asked to assess the quality and content of injected audio that we have extract from victim devices. We ask the 20 participants to listen to eight injected voice commands and then the original audio. They rate the score on injected audio on a scale from 1 to 5, 5 meaning that the intelligibility of the injected audio is equal to its original, 1 meaning that the injected audio cannot be distinguishable to their ears, just like static noise.



(a) Study 1: Audible or Inaudible. (b) Study 2: Clear or Noisy.

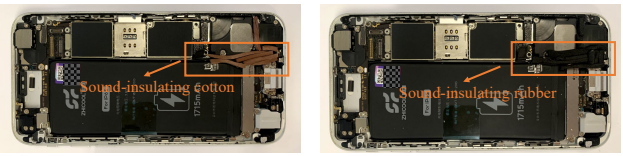
Fig. 20. Results of human studies.

The results of two human studies among 20 participants are shown in Figure 20. For study 1, all participants after experiencing the magnetic attack choose the inaudible option, and regard MagBackdoor as an inaudible attack, indicating the stealthiness of MagBackdoor. This is because the volume of induced audio via MagBackdoor is too low to propagate outside the device. For study 2 which inspects the intelligibility of injected signals, 59.1% of participants score the injected signal as 3, illustrating that they consider the injected audio a little noisy but are still able to distinguish audio content. Based on the percentage of people who score 4 and 5, 31.8% of participants believe the injected signal is similar to the original audio. With the injected signal similar to the genuine voice command, MagBackdoor can act as a ghost call to launch voice phishing fraud by means of sending voicemail.

VIII. Countermeasure

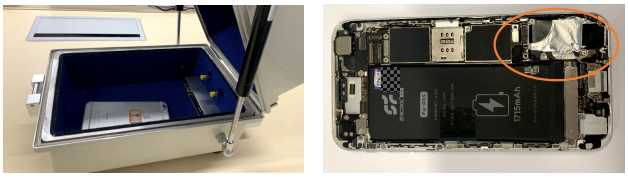
Our study has shown the threat of magnetic attacks on commercial electronic devices. To mitigate the threat, we propose possible countermeasures from two perspectives.

Sound blocking. The root cause of magnetic injection attack is that the loudspeaker is physically close to the microphone in the hardware circuit of audio systems. Redesigning the arrangement of loudspeakers and microphones is an effective method, ensuring their distance far enough away from each other. Additionally, it is possible to block out sound propagation from loudspeakers to microphones by putting a sound-deadening barrier [38] between them. However, note that extending distances or placing barriers inevitably costs more and takes up larger volume. To investigate the sound blocking against MagBackdoor, we conduct experiments in Figure 21 to test the defense capability of sound-insulating cotton and rubber wrapping the built-in loudspeakers. After magnetic injection 30 times, the injection rates for sound-insulating cotton and sound-insulating rubber are 87% and 70%, respectively. It is indicated that the sound-insulating material can partly suppress the sound injection from nearby loudspeakers.



(a) Sound-insulating cotton. (b) Sound-insulating rubber.
Fig. 21. The setup of sounding blocking against MagBackdoor.

Electromagnetic shielding. In addition to sound blocking, manufacturers may cover built-in loudspeakers with the aid of electromagnetic shielding like a Faraday cage [39], protecting them from external magnetic interferences. Instead of covering the entire audio system with electromagnetic shielding, using magnetic elements to shelter mini-components of interior circuits has low costs and can protect against electromagnetic intrusion. For instance, manufacturers can install ferrite beads [40] inside amplifiers or connectors in audio systems, which can filter out electromagnetic noises. Although these hardware-based modifications could attenuate the impact of MagBackdoor, fine-grained hardware redesign and optimization will be required. As shown in Figure 22, we conduct two experiments: 1) The iPhone 6s is placed inside a professional Faraday cage ($20cm \times 16cm \times 16cm$); 2) The loudspeaker of the iPhone 6s is tightly wrapped by tinfoil. The attacker makes every effort to use MagBackdoor to inject malicious magnetic signals from diverse ranges and angles. However, every attempt to attack iPhone 6s inside the Faraday cage fails. The Faraday cage can block out external magnetic signals transmitted from MagBackdoor. It is noted that electronic devices in the Faraday cage also cannot receive communication signals, e.g., WiFi, 4G, and 5G. Conversely, the magnetic signal via MagBackdoor can still successfully inject into iPhone 6s whose loudspeaker is wrapped in tinfoil. This experiment proves that a thin layer of tin foil does not completely block magnetic radiation.



(a) Professional Faraday cage. (b) iPhone 6s inside the cage.
Fig. 22. The setup of electromagnetic shielding against MagBackdoor.

IX. Discussion

A. Limitation

When a varying magnetic field from MagBackdoor covers the target device like a smartphone, intrinsically, the injected audio depends on the rate of change of magnetic flux. If the target device has any movement change or vibration deviation, the corresponding magnetic flux will change, possibly failing to achieve the desired final attack effect. To maximize the effect of attacks, it is best for MagBackdoor to aim at stationary targets. Also, the attacking distance of MagBackdoor is limited (no exceeding 8 cm), thus the attacking setup needs to be close to the target. However, the size of the MagBackdoor prototype is compact enough that an attacker can hide inside a common power socket and be unnoticeable in various scenes, e.g., meeting rooms, cafes, and lounges. Through the modified power socket, the attacker can opportunistically trigger the voice assistants of devices charging at the socket. When users lock their smartphones, MagBackdoor can inject malicious commands into locked smartphones, but smartphones (e.g., iPhone) cannot be triggered to execute tasks without users unlocking action. However, some locked android phones (e.g., OPPO) still can execute simple commands like open Bluetooth or WiFi, leading to potential risks.

Theoretically, a magnetic field can penetrate arbitrary materials whose penetration depth varies on the permeability of media and the frequency of excitation current [41]. However, considering a particular case where a metal block is placed around the target device, the metal block may be able to produce eddy currents under varying magnetic fields transmitting from MagBackdoor. The induced eddy currents inside the metal block will activate a magnetic field that opposes the change in the malicious magnetic field. Thus, the magnetic field inside the target device is a superposition of two magnetic fields, i.e., from the metal block and MagBackdoor, therefore counteracting parts of malicious magnetic fields. When the number of metal blocks is increased, the interference effect on the magnetic attack will be reinforced. Additionally, high temperature [42] and corrosive liquid (e.g., water) [43] can degauss the magnetism of the MagBackdoor setup, neutralizing magnetic attacks.

B. Future work

Potential Improvement. The MagBackdoor is charged by only the power supply with 12V and 1A , which satisfies the attacker's demand for portability but greatly limits the range of attack. It can be foreseeable that by increasing the power of supply and the number of connected electromagnets, the attacking range can be extended from centimeter to even

meter long distances. Considering the selected electromagnet of MagBackdoor, parts of magnetic fields generated by a cylinder electromagnet remain inside rather than scattered outside for injection. With the help of electromagnetic simulation software like COMSOL and Ansys [15], it is achievable to remodel the shape of the electromagnet, to enhance external magnetic distributions. Furthermore, to further mask the sound from built-in loudspeakers, MagBackdoor can re-modulate the current signal into 20kHz, using the DolphinAttack [7] mechanism to emit ultrasound to attack the target.

Other targets available for magnetic attacks. This paper illustrates the magnetic attack on the audio system in virtue of the magnetic mechanism of loudspeakers. Inspired by this, the attacker can perform magnetic attacks on other magnetism electronic components such as dynamic microphones [44] and transformers [45]. Dynamic microphones have an acoustic-electro structure opposite to loudspeakers. That is, a sound wave hits the diaphragm of dynamic microphones and the attached voice coil ensuingly vibrates, generating the electrical signal by electromagnetic induction. By performing MagBackdoor on dynamic microphones, injecting arbitrary audio into them is the same as intrusion on loudspeakers. (2) A transformer is an electrical component that consists of two windings on the same magnetic path, working on basic principles of electromagnetic induction for transferring electrical energy from one circuit to another circuit. It is widely employed in circuits for varying purposes, e.g., to protect the low-voltage devices and to communicate over long distances. By applying the external varying magnetic fields on it, the transferred voltage is destabilized, which can cause damage to power supplies or communication networks.

X. Related Work

Injection work on VCSs. Most existing injection work on VCSs can be categorized as: audible attack and inaudible attack. *(1) Audible Attack:* Earlier studies have shown the vulnerability of VCSs when facing mimic attacks [46] and replay attacks [47]. Compared with those noticeable attacks, a more prevalent trend is to add artificial perturbation crafted from adversarial learning into broadcasting music [8]–[10], [48], [49]. Based on the analysis of interpretation errors in VCSs, the combination of phonemes with similar sounds to wake-up words is likely to provoke the misclassification of VCSs [50]. Differing from the above audible attacks, MagBackdoor is more covert since its crafted audio is confined to the victim device's interior. *(2) Inaudible Attack:* Backdoor [6] and DolphinAttack [7] first point out the non-linearity of microphones, whereby microphones can hear the modulated hidden commands on high-frequency ultrasound. SurfingAttack [51] and Capspeaker [52] present an ultrasound injection attack through different transmission media (i.e., solid) or sound sources (i.e., capacitor), respectively. Compared with ultrasonic attacks, MagBackdoor has high penetrability and omnidirectivity. In terms of the quality of injected voice commands, ultrasound leverages the frequency non-linearity of microphones, which gives more frequency distortion to injection results than MagBackdoor that controls built-in loudspeakers to emit audio. Except for ultrasonic attacks, researchers prove that microphone analog circuits are vulnerable to electromagnetic interference [13], [53], [54] and laser [14]. Currently, Wang et al. [14] alter the charging cable to compromise the voice assistant of devices via a power line side-channel. In this study, MagBackdoor poses a new backdoor in the audio system and a new magnetic injection attack for voice commands.

Work on magnetic security. Extensive efforts have been devoted to exploring side-channel attacks and security applications based on magnetism. Some researchers have focused on magnetic covert channels [55]–[57], where an insider exfiltrates sensitive information from an air-gapped computer by controlling the magnetic field emanating from the CPU core's workload. Additionally, Biedermann et al. [58] propose a magnetic side-channel attack on hard drives, employing the magnetic sensor of smartphones to fingerprint the operation of hard drives. Some researchers reveal that magnetic fluctuations caused by furniture in indoor environments render indoor localization practicable [59], bringing about the underlying indoor privacy leakage. Chen et al. [46] implement the idea of detecting the magnetic field emitted from the loudspeaker to defend against the machine-based voice impersonation attack. Some works [60], [61] on magnetic gestural authentication are designed to withstand shoulder surfing attacks. Unlike the conventional work on utilizing magnetic channels, this paper focuses more on the threat of magnetic injections and poses a new magnetic attack prototype.

XI. Conclusion

This study investigates a security issue caused by loudspeakers of audio systems, leaving backdoor to voice command injection into VCSs. We propose a novel injection attack called MagBackdoor, aiming at loudspeakers inside victim devices, which emits magnetic fields modulated by commands to manipulate the sound production of loudspeakers. Through comprehensive experiments and theoretical analysis, the working mechanism of external magnetic fields on loudspeakers is thoroughly disclosed, providing guidance on magnetic injection attacks. To mount magnetic attacks stealthily, we self-design a MagBackdoor prototype based on the integrated circuit system to achieve refined injected signals with high power, which can be concealed inside charging sockets.

XII. Acknowledgments

This paper is partially supported by the National Key R&D Program of China (2020AAA0107700), National Natural Science Foundation of China (62032021, 61772236, 61972348, 62172359, and 62102354), Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (2018R01005), Fundamental Research Funds for the Central Universities (2021FZZX001-27).

REFERENCES

[1] W. Zhang, P. N. Samarasinghe, H. Chen, and T. D. Abhayapala, "Surround by sound: A review of spatial audio recording and reproduction," *Applied Sciences*, vol. 7, no. 5, p. 532, 2017.

[2] M. C. Hans and M. T. Smith, "Interacting with audio streams for entertainment and communication," in *Proceedings of the eleventh ACM international conference on Multimedia*, 2003, pp. 539–545.

[3] Apple, "Apple siri," 2022, https://www.apple.com/siri/.

[4] Google, "Google assistant," 2022, https://assistant.google.com/.

[5] Amazon, "Amazon alexa," 2022, https://developer.amazon.com/en-US/alexa.

[6] N. Roy, H. Hassanieh, and R. Roy Choudhury, "Backdoor: Making microphones hear inaudible sounds," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, 2017.

[7] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017.

[8] L. Schönherr, K. Kohls, S. Zeiler, T. Holz, and D. Kolossa, "Adversarial attacks against automatic speech recognition systems via psychoacoustic hiding," in *26th Annual Network and Distributed System Security Symposium, NDSS*, 2019.

[9] 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 *27th USENIX security symposium (USENIX security 18)*, 2018.

[10] T. Du, S. Ji, J. Li, Q. Gu, T. Wang, and R. Beyah, "Sirenattack: Generating adversarial audio for end-to-end acoustic systems," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020.

[11] J. Krautkrämer and H. Krautkrämer, *Ultrasonic testing of materials*. Springer Science & Business Media, 2013.

[12] N. Roy, S. Shen, H. Hassanieh, and R. R. Choudhury, "Inaudible voice commands: The {Long-Range} attack and defense," in *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, 2018, pp. 547–560.

[13] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021.

[14] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands:{Laser-Based} audio injection attacks on {Voice-Controllable} systems," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[15] D. M. Buede and W. D. Miller, "The engineering design of systems: models and methods," 2016.

[16] Android, "Keep your data private and secure," 2022, https://www.android.com/safety/.

[17] Apple, "App store review guidelines," 2022, https://developer.apple.com/app-store/review/guidelines/.

[18] W. K. Panofsky and M. Phillips, *Classical electricity and magnetism*. Courier Corporation, 2005.

[19] S. P. Thompson, *The electromagnet and electromagnetic mechanism*. E. & FN Spon, 1891.

[20] R. Mikail, "Fundamentals of electric motors and transformers," *Bangladesh University of Engineering and Technology, Dhaka, Short Course*, pp. 984–32, 1803.

[21] F. T. Ulaby, E. Michielssen, and U. Ravaioli, *Fundamentals of applied electromagnetics*. Pearson Upper Saddle River, NJ, 2015, vol. 7.

[22] J. Borwick, *Loudspeaker and headphone handbook*. CRC Press, 2012.

[23] J. Weigold, T. Brosnihan, J. Bergeron, and X. Zhang, "A mems condenser microphone for consumer applications," in *19th IEEE International Conference on Micro Electro Mechanical Systems*, 2006, pp. 86–89.

[24] B. McCarthy, *Sound systems: design and optimization: modern techniques and tools for sound system design and alignment*. Routledge, 2012.

[25] C. Multiphysics, "Introduction to comsol multiphysics®," *COMSOL Multiphysics, Burlington, MA, accessed Feb*, vol. 9, no. 2018, p. 32, 1998.

[26] Deegoo-FPV, "Tpa3116d2 dual channel audio stereo amp high power digital subwoofer power amplifier board," 2022, https://www.amazon.com/Amplifier-TPA3116D2-Subwoofer-Solicitation-Speakers/dp/B08GYQTTXF.

[27] Arduino, "Arduino uno & genuino uno," 2022, https://www.arduino.cc/en/main/arduinoBoardUno.

[28] W. M. Saslow, "Chapter 11 - how electric currents make magnetic fields: The biot– savart law and ampère's law," in *Electricity, Magnetism, and Light*, W. M. Saslow, Ed. San Diego: Academic Press, 2002, pp. 460–504.

[29] E. P. Furlani, *Permanent magnet and electromechanical devices: materials, analysis, and applications*. Academic press, 2001.

[30] M. Electronics, "Delixi sound level meter," 2022, https://www.cn-delixi.com/.

[31] K.-C. Wang and Y.-H. Tasi, "Voice activity detection algorithm with low signal-to-noise ratios based on spectrum entropy," in *Second International Symposium on Universal Communication*, 2008, pp. 423–428.

[32] B. Corporation, "Bk3266," 2022, http://www.bekencorp.com/index/goods/detail/cid/27.html.

[33] NXP, "Tda8932b," 2022, https://www.nxp.com/products/audio-and-radio/audio-amplifiers/home-audio-amplifiers/class-d-audio-amplifier:TDA8932B.

[34] L. ELECTRONICS, "Ch224k," 2022, https://www.lcsc.com/product-detail/USB-ICs_WCH-Jiangsu-Qin-Heng-CH224K_C970725.html.

[35] Google, "Text-to-speech," 2022, https://cloud.google.com/text-to-speech?hl=zh-cn.

[36] A. W. Rix, J. G. Beerends, M. P. Hollier, and A. P. Hekstra, "Perceptual evaluation of speech quality (pesq)-a new method for speech quality assessment of telephone networks and codecs," in *IEEE international conference on acoustics, speech, and signal processing. Proceedings (Cat. No. 01CH37221)*, vol. 2, 2001, pp. 749–752.

[37] C. H. Taal, R. C. Hendriks, R. Heusdens, and J. Jensen, "A short-time objective intelligibility measure for time-frequency weighted noisy speech," in *IEEE international conference on acoustics, speech and signal processing*, 2010, pp. 4214–4217.

[38] M. E. Tull and J. H. Freis, "Sound-deadening device," *The Journal of the Acoustical Society of America*, vol. 73, no. 5, pp. 1886–1886, 1983.

[39] S. J. Chapman, D. P. Hewett, and L. N. Trefethen, "Mathematics of the faraday cage," *Siam Review*, vol. 57, no. 3, pp. 398–417, 2015.

[40] S. Saario, D. Thiel, S. O'Keefe, and J. W. Lu, "Analysis of ferrite beads for rf isolation on straight wire conductors," *Electronics Letters*, vol. 33, no. 16, pp. 1359–1360, 1997.

[41] D. Jiles, *Introduction to magnetism and magnetic materials*. CRC press, 2015.

[42] C. Jian, L. Ma, W. Yang, Q. Huang, J. Xu, H. Zhai, and G. Cao, "Influence of high temperature degaussing on lifting capacity of linear motor reciprocating pump," in *Journal of Physics: Conference Series*, vol. 2109, no. 1. IOP Publishing, 2021, p. 012009.

[43] T. Minowa, M. Yoshikawa, and M. Honshima, "Improvement of the corrosion resistance on nd-fe-b magnet with nickel plating," *IEEE Transactions on Magnetics*, vol. 25, no. 5, pp. 3776–3778, 1989.

[44] W. Jones and L. Giles, "A moving coil microphone for high quality sound reproduction," *Journal of the Society of Motion Picture Engineers*, vol. 17, no. 6, pp. 977–993, 1931.

[45] S. V. Kulkarni and S. Khaparde, *Transformer engineering*. Marcel Dekker New York, 2004.

[46] S. Chen, K. Ren, S. Piao, C. Wang, Q. Wang, J. Weng, L. Su, and A. Mohaisen, "You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2017.

[47] S. Wang, J. Cao, X. He, K. Sun, and Q. Li, "When the differences in frequency domain are compensated: Understanding and defeating modulated replay attacks on automatic speech recognition," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020.

[48] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, and W. Zhou, "Hidden voice commands," in *25th USENIX security symposium (USENIX security 16)*, 2016.

[49] H. Abdullah, W. Garcia, C. Peeters, P. Traynor, K. R. B. Butler, and J. Wilson, "Practical hidden voice attacks against speech and speaker recognition systems," in *26th Annual Network and Distributed System Security Symposium, NDSS*, 2019.

[50] Y. Chen, Y. Bai, R. Mitev, K. Wang, A.-R. Sadeghi, and W. Xu, "Fakewake: Understanding and mitigating fake wake-up words of voice

assistants," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021.
[51] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, "Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves," in *Network and Distributed Systems Security (NDSS) Symposium*, 2020.
[52] X. Ji, J. Zhang, S. Jiang, J. Li, and W. Xu, "Capspeaker: Injecting voices to microphones via capacitors," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021.
[53] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.
[54] Y. Tu, V. S. Tida, Z. Pan, and X. Hei, "Transduction shield: A low-complexity method to detect and correct the effects of emi injection attacks on sensors," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021.
[55] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2016, pp. 525–532.
[56] M. Guri, "Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields," *Future Generation Computer Systems*, vol. 115, pp. 115–125, 2021.
[57] M. Guri, B. Zadov, and Y. Elovici, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1190–1203, 2019.
[58] S. Biedermann, S. Katzenbeisser, and J. Szefer, "Hard drive side-channel attacks using smartphone magnetic field sensors," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 489–496.
[59] D. Vandermeulen, C. Vercauteren, M. Weyn, and D. Vandermeulen, "Indoor localization using a magnetic flux density map of a building," in *The Third International Conference on Ambient Computing, Applications, Services and Technologies*, 2013, pp. 42–49.
[60] A. Sahami Shirazi, P. Moghadam, H. Ketabdar, and A. Schmidt, "Assessing the vulnerability of magnetic gestural authentication to video-based shoulder surfing attacks," in *Proceedings of the sigchi conference on human factors in computing systems*, 2012, pp. 2045–2048.
[61] A. E. Ali and H. Ketabdar, "Investigating handedness in air signatures for magnetic 3d gestural user authentication," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, 2015, pp. 704–711.

APPENDIX

APPENDIX A
LOCATION OF SPEAKERS AND MICROPHONES IN SOME SMART DEVICES

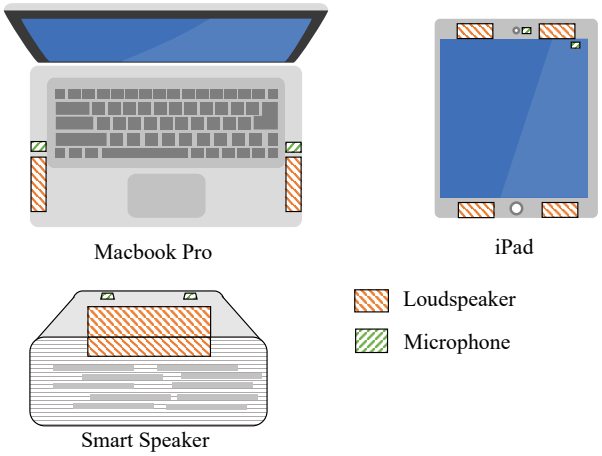


Fig. 23. The position distribution of loudspeakers and microphones.

APPENDIX B
FORMULA DERIVATION FOR PWM SIGNAL

As introduced in Section 6.2, the triangle wave is periodic with period $T_c = \frac{1}{f_c}$. Thus, for a specific t in $a(t)$, $\delta(t)$ can be regarded as a periodic function of $c(t)$. The $\delta(t)$ can be expanded into a Fourier series:

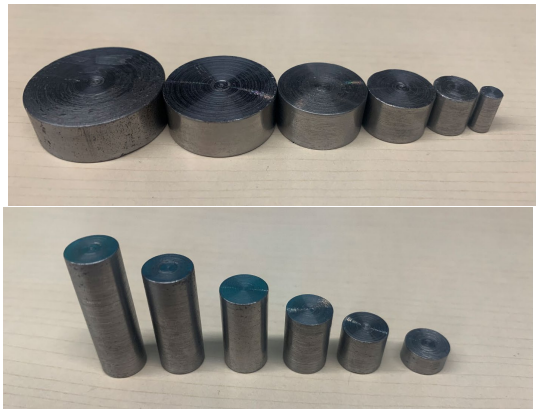
$$\delta(t) = \sum_{k=-\infty}^{+\infty} \tau_k(a(t)) e^{j2\pi k f_c t}, \tag{7}$$

where the Fourier series coefficients $\tau(t)$ can be calculated from:

$$\begin{aligned} \tau_k(a(t)) &= \frac{1}{T_c} \int_0^{T_c} \delta(t) e^{-j2\pi k f_c t} dt. \\ &= \frac{1}{T_c} \int_{\frac{T_c}{2} - \frac{a(t)T_c}{2}}^{\frac{T_c}{2} + \frac{a(t)T_c}{2}} e^{-j2\pi k f_c t} dt. \\ &= \frac{1}{\pi k} sin(\pi k a(t)) e^{-j\pi k}. \end{aligned} \tag{8}$$

By replacing $\tau_k(a(t))$ in Eq.7 with Eq.8, we can finally acquire the Eq.6.

APPENDIX C
DIFFERENT DIAMETER AND HEIGHT OF MAGNET



APPENDIX D
THE SELECTION OF VOICE COMMANDS

TABLE III
LIST OF MALICIOUS VOICE COMMANDS PRE-STORED IN MAGBACKDOOR, WAITING TO BE INJECTED INTO THE DEVICE.

The content of voice commands	
Open the door	Call my boss
Open Instagram	Set an alarm
Turn on Bluetooth	Purchase an iPad Pro
What time is it	What's forty four plus ninety three

APPENDIX E
REST RESULTS OF TABLE 2

TABLE IV
EXPERIMENT DEVICES, CATEGORY, SYSTEMS, AND RESULTS. WE EVALUATE MAGBACKDOOR FROM INJECTION SUCCESS RATE, PESQ, AND STOI IN AN OFFICE ENVIRONMENT WITH A BACKGROUND NOISE OF 30DB SPL.

Num.	Category	Devices	Manufacturer	OS/Ver.	VCS	Injection Success Rate(%)	PESQ	STOI
1	Smartphone	Mate 30Pro	Huawei	HarmonyOS 2.0	Celia	98.81	4.23	0.66
2	Smartphone	Mate P40	Huawei	HarmonyOS 2.0	Celia	95.63	4.03	0.67
3	Smartphone	Nova 7	Huawei	HarmonyOS 2.0	Celia	95.94	4.00	0.65
4	Smartphone	Find x20Pro	Oppo	Android 11	Breeno	95.62	3.98	0.54
5	Smartphone	Reno Pro	Oppo	Android 11	Breeno	95.93	3.89	0.58
6	Smartphone	Redmi K50	Xiaomi	Android 12	Xiaoai	97.81	4.14	0.67
7	Smartphone	Galaxy S20+	Sumsung	Android 10	Bixby	97.50	4.17	0.60
8	Smartphone	iPhone 12	Apple	iOS 14.8	Siri	96.25	3.72	0.65