# Vulnerabilities of Remote Command Injection: IMEI Threats on Information Security on Modern Smartphones

**V. Uma Sankari[1] G. Elayaroja[2]**
[1,2]Department of Computer Science & Engineering
[1,2]CK College of Engineering & Technolgy, Cuddalore, India

*Abstract*— in cryptography, electromagnetic attacks are side-channel attacks preformed by measuring the electromagnetic radiation emitted from a device and performing signal analysis on it. Many papers dealing with the analysis of electromagnetic attacks against critical electronic devices have been. In this paper, we exploit the principle of front-door coupling on smart phones headphone cables with specific electromagnetic waveforms. Front door coupling is the possible disturbance to an aircraft system as received by the antenna of the system and mainly in the frequency band used by the system. It is also the responsibility of the certification applicant to demonstrate that the installed system does not interfere with the other aircraft system. We present a smart use of intentional electromagnetic interference, resulting in finer impacts on an information system than a classical denial of service effect. As an outcome, we introduce a new silent remote voice command injection technique on modern smart phones to secure the information.

***Keywords:*** Electronic warfare, information security, intentional electromagnetic interference

## I. INTRODUCTION

Directed energy radio-frequency weapons have been widely investigated for military applications aiming to either disturb or damage electronic devices. The main challenge, namely the generation of high amounts of energy, slowly evolved to the design of complex and efficient waveforms to decrease the required electromagnetic (EM) field intensity. The recent advances in the area of software-defined radio and the appearance of efficient low-cost amplifiers allow the design of flexible and reconfigurable radio frequency (RF) pulse sources for a relatively low budget (about 2000 €). As a result, risk management procedures need to be updated assigning a higher probability to threats related to RF pulses.

Electromagnetic compatibility (EMC) and electromagnetic interference (EMI) threats have been studied by EMC experts in order to enhance the survivability of electronic devices and communication networks exposed to intentional electromag- netic interferences (IEMI) [1]–[4]. In addition, information se- curity scientists have shown a high interest in fault injection on crypto systems [5]–[6] for secret keys extractions using EM pulses. Both communities have in common their need for char- acterizing the effects of EM perturbations at the system level.

Recently, a fine-grain classification of the effects of IEMI has been proposed [4] in which it was shown that the emitted sig- nal envelop was induced and could be recorded on a sound card without connecting a microphone. Complementary experi- ments [7] have confirmed the high susceptibility of sound cards,on desktop computers and smartphones, either by back-door or front-door coupling [2].

The possibility of inducing parasitic signals on the audio front-end of voice command capable devices could raise critical security impacts. This would require the possibility of generating specific waveforms for inducing a signal processed by the target as a legitimate signal. Interestingly, for accessing FM radio on smartphones (in the 80–108 MHz frequency band which is part of the Very High Frequency band—VHF for short) pro- viding this service, it is necessary to plug the headphone to the device as it acts as an FM radio receiving antenna. This component, considered as a front-door coupling interface [2], could propagate the induced signal to the input audio interface voice command. The first theoretical study has been proposed in [8], showing the possibility of signal induction in the differential lines of Ethernet but protocols information was not involved. The key contribution of this study is the design of a new attack vector on information systems by a smart use of IEMI resulting in a remote and silent voice command injection technique (even for the user of the targeted device).

The paper is organized as follows: in Section II, some back- ground information about the main deployed voice command interpreters is given. In Section III, the voice command injec- tion technique is described. In Section IV, a security analysis covering the considered attack scenarios and the related coun- termeasures are finally proposed.

## II. VOICE COMMANDS ON SMARTPHONES

Voice command is a feature that allows a hand-free use of an electronic device. This user interface (UI) has evolved during the past ten years to become a reliable and efficient way to interact with an information system. Thus, it is being widely deployed by operating system editors and electronic device manufactur- ers, and is sooner or later going to be one of the most commonly used interfaces, along with the touch screens. This interface is already available on smart phones, desktop computers, cars, smart watches, and is currently being deployed in wearable devices and other "smart objects" of the internet of things. This section provides an overview of the main voice command interpreters. Some insight is given on their software architecture and hardware requirements. Then, a brief summary of previous security related work on the voice command interface is given.

### *A. Hardware Voice Input Interfaces on Smartphones*

Most modern smartphones provide mainly two voice input interfaces: The built-in microphone and the headphones microphone. Generally, these interfaces are enabled alternatively, depending on the presence of microphone capable headphones (detected by the impedances on the 4-pin connector). The voice input interfaces are connected to a digital signal processor unit (DSP) stage which digitizes and low-pass filters the voice signal and forwards it to the application processor.

 

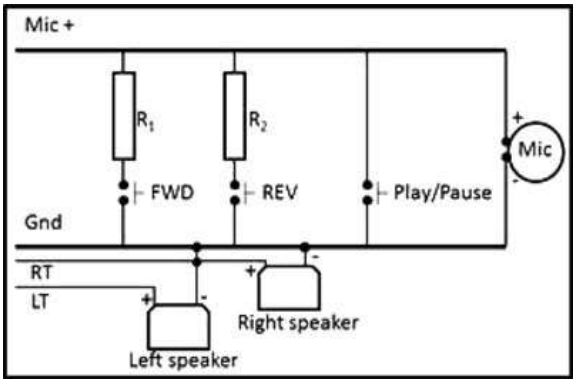


Fig. 1: Schematic of the hardware of headphones and the related interfaces

The headphones LT and RT audio outputs can also be used as an input antenna for FM radio signals in FM capable phones. Furthermore, microphone capable headphones provide a phys- ical button interface (see Fig. 1). A button press changes the impedance of the microphone line, which is detected by the phone.

### B. Software Services and Features

As voice command becomes more reliable and popular, it has been integrated to most of the recent desktop, mobile, and embedded operating systems. Some of the available interpreters are listed below:

1) Samsung [9]: Samsung voice control system is called S-Voice. It is a vendor software layer that is natively included in the Android core.
2) Apple [10]: Two services provide a voice command interface, namely Voice Control and Siri. On the latest versions of iOS, Siri completely replaced Voice Control.
3) Google [11]: Google Voice Search is the original voice command interface and was merged to Google Now since Android Jelly Bean.
4) Microsoft [12]: Cortana is the newly available voice command interface which replaced Speech [13].

Along with a wide deployment of this UI, Editors and Manufacturers seem to be in a testing phase where new usages emerge and where users get attracted by this new way of interaction. Consequently, they tend to allow control of more and more features through the voice interface. These features can be classified in three main categories:

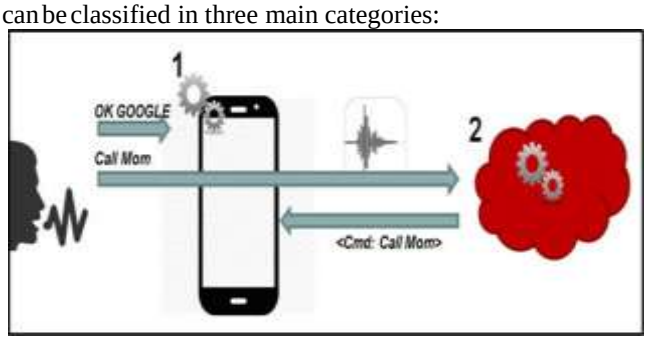


Fig. 2: Two-step procedure for audio signal processing for command execution.

1) Internet services: Web search, web browsing, sending emails, posting messages to social media.
2) Telephony services: Placing phone calls, sending text messages, resolving contact numbers from names.
3) Local services: Setting alarms up, creating calendar events, reminders, launching applications, changing the device's settings.

### C. Voice Command Interface Activation

In order to be able to use the voice command interface, the voice interpreter has to be activated. To simplify the user experience and to encourage the use of this interface, the voice interpreter tends to be always activated and running in the back- ground, waiting for the user to pronounce a keyword (e.g., "OK Google," "Hey Siri"). Low consumption allows for keeping the voice command interpreter running as a service in the operat- ing system. This last function raises another question about the risk introduced by such service for the privacy of users. When the voice command interpreter is not enabled permanently, it is generally activated by launching the aforementioned software applications or by a long hardware button press. The hardware button can generally be a button on the handset or a button from the remote command of the headset (e.g., referenced as the Play/Pause button in Fig. 1).

### D. Voice Command Process

The processing of the voice command is based on a two-step procedure, as represented in Fig. 2. The first keyword is recorded and processed on the smartphone. Once the voice interface is launched, the user asks for a defined command. The audio file is recorded and sent to the remote server of the service provider. The uploaded audio file is processed and the detected command is sent back from the provider servers to the mobile and is finally executed.

The voice and speech recognition is generally performed on a remote server, except for the keyword. This means that voice command cannot be used without internet connectivity through Wi-Fi or mobile network.

### E. Security Related Work

Since it is widespread, the voice command interface has been subject to security analyses and security related controversies.

Historically, the first solution that has been widely deployed and enabled by default was Siri. Several researchers and journalists published warnings on the possibility offered by Siri to bypass the lock screen PIN code authentication to gain access to other functionalities on the device [14]. On the network service side, security researchers performed a complete reverse engineering of the remote command interpretation protocol and provided a framework to remotely use Siri voice interpretation capabilities from any web application [15]. However, they did not further in- vestigate the possibility to exploit this vector to compromise the device. The privacy aspects of Siri have also been discussed af- ter Apple announced that they share the voice samples collected by the remote interpreter service to the third party [16].

Concerning Google Voice Search, it has been proven that a malicious application with no specific permission on an Android device was able to activate the voice interpreter and send com- mands through the phones speaker [17]. The commands were simple sound files that could be downloaded by the malicious application. However, the main limitation of this paper is the use of the speaker to send the commands,

 

which is not silent and can be easily detected by the victim. An interesting local attack vector to overcome this limitation could be the exploitation of the software sound mixer to provide the malicious command to the software audio input pipe without playing it outloud.

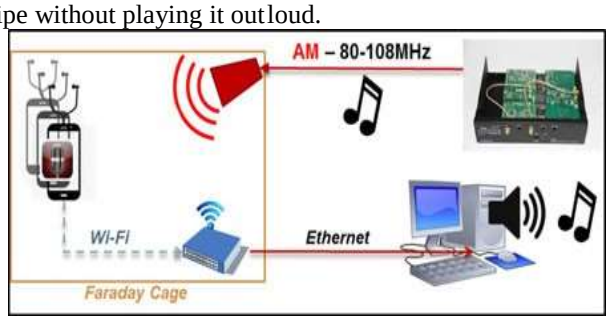


Fig. 3: Experimental test setup

## III. COMMAND INJECTION WITH SMART IEMI

In this section, the above concerns will be validated experimentally. For preliminary validation, it is necessary to check, for both smartphones with and without a FM radio-integrated cir- cuit, that the headphones provided by manufacturers are acting as efficient antennas. Considering the input filter of the audio interface, we checked the feasibility of voice signal injection. Finally, the successful result of a silent remote voice command injection will be discussed.

### *A. Preliminary Experiments and Simulations*

A first test setup has been designed which aimed to validate the following hypothesis. As the headphones act as a FM antenna, it should be possible to use them as a front door coupling interface for voice command injection. To achieve this verification, the experimental setup (see Fig. 3) consisted of placing the phones, with headphones plugged in and randomly positioned, in a Faraday cage with a wireless access point relaying the IP traffic to a computer outside the cage via optical fiber. Addi- tionally, a three-axis E-field probe was also installed next to the target so that we were able to link the trigger of the voice com- mand controller and the required minimal field level. A Wi-Fi link was set up in order to provide an access to the providers servers simulating a normal use of the smartphones.

On the phones, an application which records sound from the microphone was installed. This application streamed the recorded sound on the network in real time to the computer, which could store and play the received sound samples. For voice emission, we used a software defined radio combined with a 50 W amplifier. In complement to these experiments, we simulated the emission and reception stages in a software signal processing framework to check the quality of the induced voice signal and to confirm that the envelop recovery by the audio input stage. Fig. 4 is a schematic of the emitted and induced signals. In fact, it has been observed that the induced signal recorded by the application installed on the target and streamed to the monitoring computer was slightly distorted.

Based on the preliminary simulations and experiments, we considered the two following scenarios.

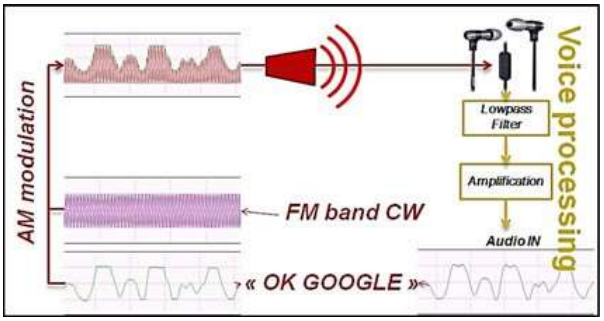


Fig. 4: Schematic of the emitted AM modulated signal and the induced signal envelop at the audio input interface of the smartphone.

*1) Permanent Activation:*

The voice control command has been activated by default by the user. This means that the voice command service starts as soon as a keyword is pronounced by the user. The experiments demonstrated that it is possible to trig- ger voice commands remotely by emitting an AM-modulated signal containing the keyword followed by some voice com- mands at 103 MHz (this frequency is given as an example as it is related to a specific model). The resulting electric signal induced in the microphone cable of the headphones is correctly interpreted by the voice command interface.

*2) User Activation:*

The voice command is not activated by default and a long hardware button press is required for launch- ing the service. In this case, we have worked on injecting a spe- cially crafted radio signal to trigger the activation of the voice command interpreter by emulating a headphones command but- ton press. It was shown that, thanks to a FM modulated signal at the same emitted frequency, we were able to launch the voice command service and to inject the voice command.

*3) Discussion:*

It was also observed that the minimal field required around the target was in the range of 25–30 V/m at 103 MHz, which is close to the limit accepted for human safety but higher than the required immunity level of the device (3 V/m). Thus, smartphones could be disturbed by the parasitic field. Nevertheless, no collateral effects have been encountered during our experiments. Moreover, depending on the cable arrangement and the cable length (between 1 and 1.20 m), it has been observed that the efficient frequency leading to command execution varies in the 80–108 MHz range.

## IV. SECURITY ANALYSIS

Being able to execute voice commands remotely on a system can be critical from an information security point of view. Fur- thermore, potentially all voice control capable systems can be vulnerable to this kind of attack. The attacker profile required for this attack can be considered as “proficient” (according to the Common Criteria), and involves publicly only available RF equipment. In this section, we provide a security analysis with the related countermeasures.

### *A. Attack Scenarios*

To understand the impact such an attack can have on a target, some attack scenarios have been studied considering public vulnerabilities and threats to mobile security.

 

1) Tracking: The attacker activates the wireless interfaces of the target for enabling mid-range tracking. As Wi-Fi and Bluetooth protocols involve several discovery phases, the device will send packets over the air containing a unique identifier (MAC address). An attacker able to receive the packets is also able to determine if a device is in range.
2) Audio spying: The attacker sends a voice command to place a phone call to his own eavesdropping phone, doing so he is able to listen to the targets surrounding environment;
3) Paid services: The attacker targets all the users in range and forces them to send a text message or place a call to a paid service.
4) Reputation and phishing: The attacker uses the communication features accessible by voice, text message, emails or social networks, to publish information that can be compromising for the reputation of the target user. This attack vector can also be exploited for launching phishing attacks.
5) Advanced compromising: The exploitation of the voice command interface is used as a first step to further compromise the device. The attacker can force the target to visit a malicious web page which exploits a vulnerability to compromise the targets operating system. As an example, one could think of installing a malicious application [18], or further exploiting vulnerabilities on the wireless interfaces.

### *B. Countermeasures*

In order to mitigate this attack vector, some countermeasures could be applied. Unfortunately, there is always a tradeoff between security and usability. We propose here a set of recommendations to users and manufacturers:

1) Hardware improvement: Some modifications on the audio front-end can be done in order to reduce the sensitivity of the input interface. A better shielding of the headphones cable would also contribute to this mitigation. This would force the attacker to reach higher EM field levels to achieve the attack.
2) User voice identification: Voice and speech recognition improvements can also be part of the solution. Indeed, better recognizing the voice of the legit user would force the attacker to forget the commands with the users voice signature.
3) Configuration settings: A better granularity in the user settings could be a great improvement: Letting the user choose his own keyword (already possible on most of devices but few users are doing so), disabling the voice interface by default, allowing the user to finely choose the authorized applications and actions via this interface, especially those accessible before the lock screen authentication process, would be interesting options.
4) Unusual EM activity detection: Recently, it has been shown that the many built-in sensors present in smartphones react to variations of the EM field nearby the device [19]. This characteristic could be used in order to monitor and detect any abnormal EM activity around the smartphone when a voice command is being processed, resulting in a rejection of the command when a suspicious Activity is detected.

## V. CONCLUSION

In this paper, we introduced a new technique for remote silent voice command injection in smartphones based on smart IEMI. The main contributions of this research are threefold: first, the reduction of the attacker costs for conceiving RF DEWs is illus- trated. Second, a smart use of IEMI, which is not only focused on denial of service attacks is enlightened. A security analysis has been performed and some possible countermeasures have been proposed. Finally, the use of the voice command interface as a remote and silent attack vector is demonstrated, attracting the attention of both vendors and users on its sensitivity and the need to secure it and to use it wisely.

## REFERENCES

[1] L. Palisek and L. Suchy, "High power microwave effects on computer networks," in Proc. EMC Europe 2011 York Conf., York, U.K., Sept. 26– 30, 2011, pp. 18–21..
[2] M. G. Bäckström and K. G. Lövstrand, "Susceptibility of electronic systems to high-power microwaves: Summary of test experience," IEEE Trans. Electromagn. Compat., vol. 46, no. 3, pp. 396–403, Aug. 2004.
[3] F. Sabath, "Classification of electromagnetic effects at system level," in Proc. Electromagn. Compat. EMC Europe Int. Symp. Conf., Hamburg, Germany, Sep. 8–12, 2008, pp. 1–5.
[4] C. Kasmi, J. Lopes-Esteves, N. Picard, and M. Renard, "Event logs gen- erated by an operating system running on a COTS computer during IEMI exposure," IEEE Trans. Electromagn. Compat., vol. 56, no. 6, pp. 1723–1726, Dec. 2014.
[5] Y. Hayashi, S. Gomisawa, and Y. Li, "Intentional electromagnetic inter- ference for fault analysis on AES block cipher IC," in Proc. Electromagn. Compat. Integr. Circuits, Nov. 6–9, 2011, pp. 235–240.
[6] T. Fuhr, E. Jaulmes, V. Lomne, and A. Thillard, "Fault Attacks on AES with faulty ciphertexts only," in Proc. Workshop Fault Diagnosis Tolerance Cryptography, Aug. 20–20 2013, pp. 108–118.
[7] K. B. Rasmussen, C. Castlluccia, T. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," pre- sented at the 16th ACM Conf. Computer Communication Security, Chicago, IL, USA, Nov. 9–13, 2009.
[8] A. Tatematsu, M. Rubinstein, F. Rachidi et al., "On the feasibility of low-power IEMI attacks on communication and control lines," presented at the 34th Progress Electromagn. Res. Symp., Stockholm, Sweden, Aug. 12–15, 2013.
[9] Samsung. (2014). How do I Use Samsung S-Voice. [Online]. Available: http://www.samsung.com/us/support/supportOwnersHowToGuidePopup.do?howto_guide_seq=7061&prd_ia_cd=N0000003&map_seq=54784
[10] Apple. (2015). Siri. [Online]. Available: https://www.apple.com/ios/siri/
[11] Google. (2015). Ok Google. [Online]. Available: https://support.google.com/websearch/answer/2940021?hl=en

 

[12] Microsoft. (2015). Meet Cortana. [Online]. Available: http://www.windowsphone.com/en-us/how-to/wp8/cortana/meet-cortana
[13] Microsoft. (2015). Speech. [Online]. Available: http://www.windowsphone.com/en-us/how-to/wp8/apps/use-speech-on-my-phone
[14] N. Gonzalez. (2014). Siri exploited again—how to bypass the lock screen in iOS 8. [Online]. Available: ios.wonderhowto.com
[15] Applidium. (2011). Cracking Siri. [Online]. Available: GitHub
[16] W. Wei. (2015). Apple admits Siri voice data is being shared with third parties. [Online]. Available: www.hackernews.com
[17] W. Diao, X. Liu, Z. Zhou, and K. Zhang, "Your voice assistant is mine: How to abuse speakers to steal information and control your phone," in Proc. 4th ACM Workshop Security Privacy Smartphones Mobile Devices, New York, USA, 2014, pp. 63–74.
[18] A. Moulu, Abusing Samsung KNOX to remotely install a malicious ap- plication, Quarkslab, 2014.
[19] C. Kasmi and J. Lopes Esteves, "Automated analysis of the effects induced by radio-frequency pulses on embedded systems for EMC functional safety," presented at the URSI Atlantic Radio Science Conf., Canarias Islands, Spain, 2015.

 