System Design & Assessment Note

SDAN 48

Remote and Silent Voice Command Injection on a Smartphone through Conducted IEMI

Threats of Smart IEMI for Information Security

José Lopes Esteves and Chaouki Kasmi

Wireless Security Lab
French Network and Information Security Agency - ANSSI

April 2018

***Abstract*—** Many papers dealing with the effects of electromagnetic attacks against critical electronics have been made publicly available. Recently, it has been demonstrated that a smart use of electromagnetic interference allows for injecting voice commands remotely through connected headsets by a front-door coupling phenomena. In this paper, we investigate the possibility of injecting voice commands on modern smartphones through a conducted propagation path exploiting the so-called back-door coupling. As an outcome, we introduce an innovative silent voice command injection technique on modern smartphones connected either to the power network or to a computer through the USB cable. This research is the continuity of the work related to radiated (front-door coupling) voice command injection technique published in 2015.

Table of Contents

I. CONTEXT

In parallel with classical research on the Electromagnetic Compatibility (EMC) of electronic devices [1-3], the information security community has been working for many years on the use of electromagnetic (EM) vulnerabilities (related to the EMC issues) in order to extract secret keys [4] from or to induce faults [5] on cryptographic algorithms running on hardware security modules. In general, preliminary experiments are focusing on the characterization of the devices with specific software controlling each elementary part of the device under test. The effects of EM pulses induced on electronic devices and integrated circuits are used to find the location of the targeted algorithm hardware blocks in order to exploit the EM susceptibility in a fault injection attack.

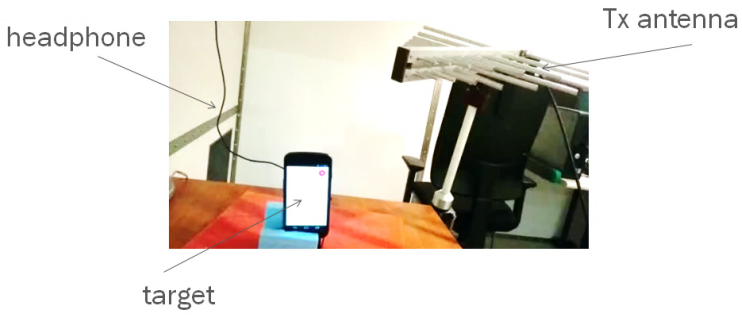

Fig. 1. Remote voice command injection on targeted device with connected headphones based on front-door coupling [6].

Furthermore, researchers have been working on exploiting the EM susceptibility for gaining access to physically isolated systems [7]. Because of their criticality, these systems are generally physically isolated from the outside world (principle of the "air-gap" mostly applied in military infrastructures). Based on the correlation of the effects on the target with the parasitic field amplitudes, it was shown that the observed temperature reading was disturbed and the recorded data was controlled by the attacker. A covert-channel [7] was designed in order to by-pass the physical isolation leading to a control and command channel for malicious software installed on the targeted computer by injecting the parasitic signal in the power network.

More recently, it has been demonstrated [6] that voice commands could be injected into smartphones by a front-door coupling phenomena involving the connected headphones acting as a receiving antenna (scenario represented in Fig. 1). Following the experimental set-up proposed in [6], an original scenario was imagined considering that a parasitic signal in the power network could reach charging smartphones and propagate to their audio front-end. Interesting results [8-9] confirming the good conducted propagation properties of the low power network have been published. Taking into account the EM susceptibility of the connected devices [1-3] and their power chargers [10], the purpose of this study is to investigate the possibility of triggering and executing voice commands on smartphones while they are charging through a back-door coupling of conducted smart intentional EM interference (IEMI).

The work[1] carried out in the paper has been applied to the Samsung Galaxy Nexus, running Android 4.3 with Google Now v.1.3. large, and its genuine Samsung USB charger. This was imposed as the main aim of this study if to compare the previous attack scenario presented in [6] and the potential exploitability of crosstalk for conducted Smart IEMI. All the material presented in this study can be straightforwardly applied to any other device. The paper is organized as follows: in Section II, the common voice command interpreters and their security features are summarized. In Section III, the conducted voice command injection technique is described and tested. In Section IV, the considered attack scenarios are discussed. A comparison between the back-door and front-door coupling-based attacks is proposed.

[1] The findings related to the targets of this study were reported to the smartphone manufacturer, Samsung, and the operating system editor, Google, through a responsible disclosure process. The public release of this work was not objected by Samsung and Google.

II. Voice Command Interface

1. Definition

The voice command interface (VCI) is a hands free user interface which allows interacting vocally with an electronic device as schematized in Fig. 2. This kind of user interaction feature is getting deployed into a wide variety of devices such as smartphones, smartwatches, desktop computers or automotive computers and is likely to become a very popular way to control electronic devices by naturally questioning or commanding them out loud. VCI is already supported by the main mobile operating systems and each editor developed his own solution: Apple features *Siri* [11], Google developed *Google Voice Search* [12], which is included in *Google Now* and Microsoft proposes *Cortana* [13]. Some third party editors which integrate their own layer over Android also have their own VCI engine, like Samsung with *S-Voice* [14].

The scope of commands and actions available through the VCI are heavily dependent on the VCI solution itself, the operating system and even the device model. These actions can be classified in three categories: communication (phone calls, text messages, social media, email...), information (web browsing) and local interaction (applications launch, settings edition, authentication...). Furthermore, some editors are releasing application programming interfaces (APIs) in order to allow third party application developers to include voice interaction in their products, which widens the scope of possible actions through VCI. As for an example, Paypal recently enabled the possibility to achieve mobile payments only by voice commands via *Siri* [15].

Fig. 2. Voice command interfaces and the related available actions.

2. Access control to the VCI

The scope of commands available through the VCI is very wide and in constant expansion. Some of these commands can be considered as critical regarding the security of the device (e.g. settings edition, authentication) or the privacy of the user (e.g. access to the contacts through communication services). It is thus important to analyze the mechanisms in place in order to mitigate the risks related to an unauthorized access to the VCI by an attacker. In [6], the security implications of an unauthorized use of the VCI are summarized. Several attack scenarios have been proposed ranging from overpaid telephony services abuse to advanced exploitation scenarios allowing compromising the device.

In order to evaluate the exploitability of the aforementioned scenarios, two factors are decisive: the activation of the voice command interpreter and the authentication of the user. Again, these factors vary depending on the VCI solution, the operating system, the device model and the settings, but some main trends can be identified. The VCI activation can be either explicitly triggered by the user (by launching the interpreter manually), always on in a post-authentication environment (or when the device is charging) or always on even when the device is locked. As shown in Fig 3, *Siri* (a) and *Google Voice Search* (b) can be configured to be active pre-authentication when the device is charging.

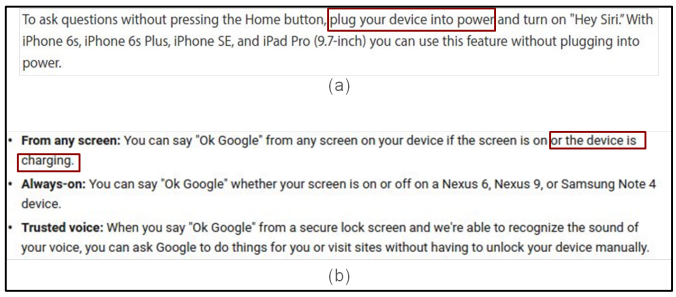

Fig. 3. Activation settings for VCIs on iOS [11] (a) and Android [12] (b).

Some editors restricted the commands available pre-authentication by forcing the authentication for using the most critical ones (e.g. placing a phone call). As the authentication through the touch screen tends to limit the interest of a VCI, a voice authentication on the keyword is available for unlocking the devices and using critical commands. Unfortunately, the granularity of these settings is still too coarse for a user to finely tune the security level she wants for the VCI.

3. Related work

The voice command interface has been subject to very few security analyses. Mostly, some proofs of concept have been published about using *Siri* to bypass the lock screen PIN code authentication in order to gain access, most of the times restricted, to other functionalities on the device [16]. Focusing on the network service, security researchers performed a complete reverse engineering of the early versions of *Siri*'s protocol and provided a framework to include *Siri* voice interpretation capabilities inside any web application [17]. However, they did not further investigate the possibility to exploit this vector to compromise the device. The privacy aspects of *Siri* have also been discussed after Apple announced they share the voice samples collected by the remote interpreter service to third parties [18]. Concerning *Google Voice Search*, an application with no specific permission on an Android device has been shown to be able to activate the voice interpreter and send commands through the phone's speaker, as stated in [19]. However, the main limitation of this work 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 out loud. This same idea has been further investigated in [20]. After a detailed analysis of the speech analysis process, the voice signal characteristics necessary for a correct interpretation have been identified. A voice mangling algorithm has been designed in order to modify legitimate voice commands so that they become unintelligible for a human while still containing enough spectral content to be correctly interpreted by speech recognition engines. This approach has then been improved resulting in an unnoticeable inclusion of mangled voice commands into video files [21].

In [6], an interesting way of sending the voice commands to the target device has been introduced. Instead of using acoustic "spoken" signals, the authors proposed to induce a parasitic audio electric signal at the input stage of the audio front end. To this end, the target needs to have wired headphones plugged in. The headphones' wire acting as an antenna for 80 MHz to 108 MHz radio signals, they are prone to a front-door coupling of radio signals in this frequency range. It has been demonstrated that a carrier radio signal modulated by the baseband voice command signal is well received by the headphones' cable and demodulated by the nonlinear components [6, 22, 23] of the audio input stage, resulting in a silent and remote voice command injection through radiated IEMI. However, the headphone requirement and the minimum power required for the attack to succeed are important limitations. The present study relies on the same key concepts while using a different injection technique, namely smart conducted IEMI, to overcome those limitations.

III. CONDUCTED PROPAGATION PATH AND CROSSTALK

This section provides an overview of the different experiments which have been performed in order to analyze the susceptibility of the audio front-end of target smartphones to conducted IEMI injected into the power wires of a USB charging cable.

1. Hypothesis

On modern smartphones, the charging USB connector and the microphone integrated circuit (IC) are co-localized (shown Fig. 4) for the Galaxy Nexus (further architectures show the colocation of the USB/Lighting port with the mic IC [27-29]). The possibility of a back-door coupling between the USB connector circuitry, which is the entry point of the parasitic signal on the phone's printed circuit board (PCB), and the audio front-end input circuitry (coupling target) was investigated. Two

phenomena could lead to a successful propagation of the EMI to the targeted microphone IC: a re-radiation of the interference from the USB circuitry bypassing the physical isolation by parasitic coupling (crosstalk) or the possible sharing of the Vcc and GND networks on the PCB.

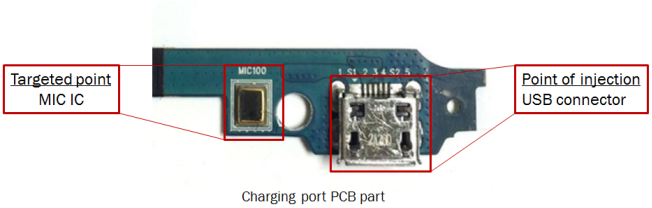

Fig. 4. Charging port PCB of a Samsung Galaxy Nexus.

As discussed in [6], the induced signal should be demodulated by the filters and the nonlinear components of the audio front-end, resulting in an envelope detection of the modulated parasitic signal. Furthermore, the pre-amplification components of the microphone integrated circuit could also be responsible for the demodulation. This point would be worth to further investigation in order to determine if digital output microphones are vulnerable to these phenomena.
In order to validate this hypothesis, several parameters had to be determined. First, it has been necessary to identify the frequencies for which the target is most susceptible to EM coupling. This has been achieved thanks to a so-called off-line[2] characterization. Then, a set of experiments, defined as on-line characterization[3], has been performed in order to analyze the propagation of the parasitic signal from different injection points on the power network to the audio front end in the target. The propagation chain has been considered as a black box, and the signal received on the audio front-end has been recorded and analyzed. The generated signal was an amplitude modulated sweep in 0.01 – 20 kHz (covering the audio frequency band) with a carrier frequency in 1 MHz – 1 GHz. A magnetic injection probe was placed on the power network and the targeted device.

2. Off-line Characterization

Interestingly, multiple studies [24-25] related to the characterization of power socket chargers and devices have pointed out the variability of the input impedance of electric and electronic devices. The set-up [24] schematized in Fig. 5 has been applied in the same way to analyze the transmission of the signal strength reaching the audio input stage of the smartphone. It is worth to mention that off-line and on-line impedances are likely to be similar as it was shown in [24-26] for these power chargers.

Off-line testing allowed for characterizing the impact of the elements of the propagation path on the injected signal. Several chargers and USB cables have been tested and their frequency responses have been analyzed. The work carried out in this study focuses on the possible exploitation of back-door coupling of EM waves in the information security domain.

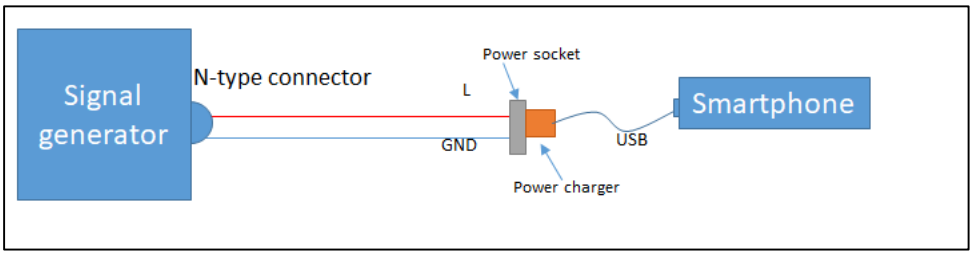

Fig. 5. Characterization procedure of the injection path

Tests have been decomposed as preliminary experiments to uncover the possibility of inducing an audio signal by connecting the power charger directly to a 2 wire adapter as shown Figure 5. This offline analysis is the basis for the analysis of a potential exploitability.

[2] Off-line characterization refers in this paper to a direct connection of the device under test to the signal generator through a dedicated adaptor. The device is connected but not powered by the power network.
[3] On-line characterization refers to a connection of the device under test to power supply either through a USB connection to a computer or through the power socket.

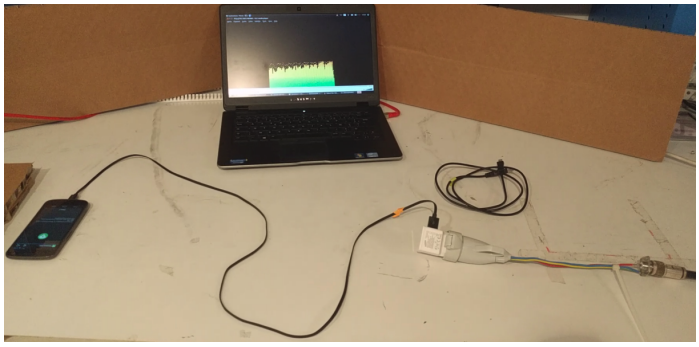

Fig. 6. Experimental set-up for the characterization of devices offline.

For offline testing, the parasitic signal was injected directly into the power charger using a custom made power socket connected to a source. With this configuration, the elements on the signal propagation path are limited to the charger and the USB charging cable. Furthermore, as these are not connected to the power network, only the injected signal propagates towards the target, with no additional noise due to the power network or the loads connected to it. A comparison of charger [24] has been carried out showing that above 100 MHz they behave in a very similar way. Thus, the study was considering that the chargers has a negligible effect on the transmission. Moreover, the adapter has been considered as an extension of the power network and it potential effect on the conducted propagation has been considered negligible.

The received audio signal was recorded on the target and streamed through a Wi-Fi connection to a monitoring computer. This setup allowed studying different test cases to characterize the propagation of the parasitic signal both offline (setup disconnected from the power network) and online (setup connected to the power network, along with other devices).

3. Identification of the resonant frequencies

The identification of the carrier frequencies providing a high coupling of the parasitic signal could be empirically achieved by monitoring the amplitude of multiple modulation signal sweeps in the recorded audio signal. To this end, for each tested carrier frequency, a 1 s sweep has been repeated during 7 seconds and the induced demodulated signal on the audio front-end has been recorded. In Fig. 7, the recorded signal for carrier frequencies of 242 MHz and 243 MHz is shown.

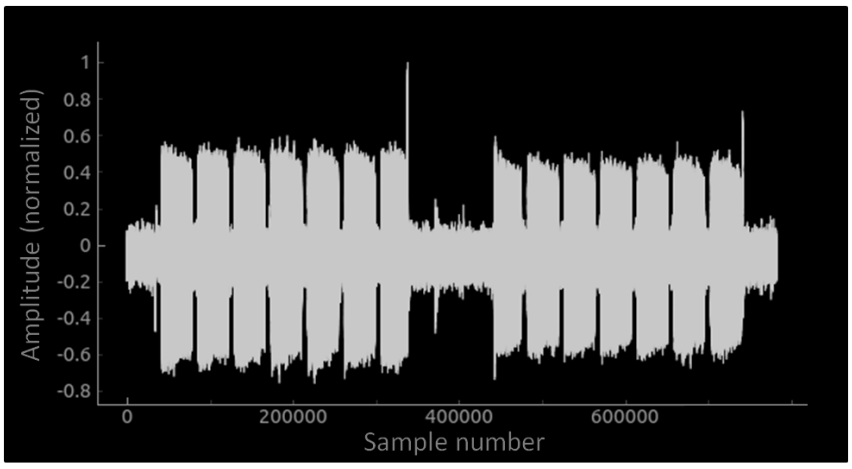

Fig. 7. Time domain representation of the induced audio signal recorded on the target, one 7 sweeps sequence per carrier frequency in 242 MHz – 243 MHz (sample rate: 44100 Hz).

For each frequency, the seven sweeps are easily distinguishable, along with the microphone noise floor. The peaks at each end of the sweep series are due to the signal generator turning on and off. The spacing between each sweep reflects the bandwidth of the audio front-end. Indeed, audio frequencies above 17 kHz are rejected. The decomposed transfer function is depicted Fig. 8, the successive parts on the propagation path are highlighted. The mismatch between each part of the propagation channel is out of scope of this study as we consider the resulting overall propagation chain.

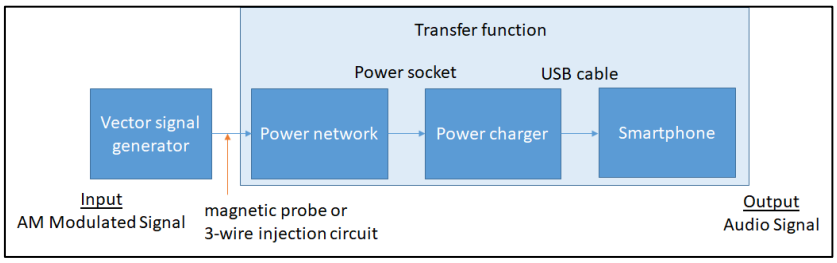

Fig. 8. Transfer function measurement of the conducted propagation when devices are connected to the low power network. The injection is made either with a magnetic injection probe or a 3-wire adaptor.

Fig. 9 represents the transfer function (TF) normalized amplitude computed by:

$$|\mathrm{TF}(f_\mathrm{m})|_{fc} = \left| \frac{V_{out}(f_m)}{V_{input}((f_m)} \right|_{fc}$$

where $V_{input}(f_m)$ is the modulating signal amplitude at 10 kHz at the external signal generator and $V_{output}(f_m)$ is the signal amplitude induced at the audio input recorded by the software application.

The estimated TF Fig. 9 has been obtained relatively to the carrier frequencies in the range 200 MHz – 250 MHz with 1 MHz steps modulated with the f_m = 10 kHz signal. It appears that in this frequency band, the strongest induced signal corresponds to carrier frequencies f_m around 231 MHz.

As we can't deduce the quality of the audio signal from the estimated transfer function magnitude, the next step will be to submit voice command at the detected resonating frequency to check the possibility of inducing real voice commands through conducted injection in later experiments.

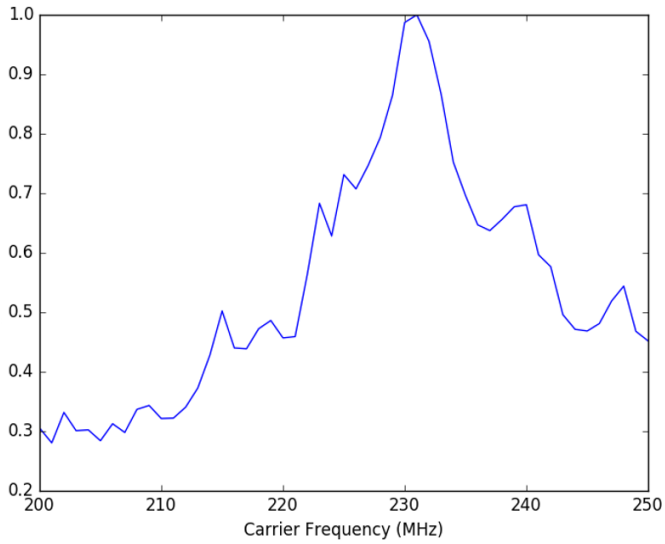

Fig. 9. Transfer function amplitude (normalized) of the signal received on the target for carrier frequencies f_c between 200 MHz and 250 MHz and a modulation frequency f_m = 10kHz.

4. On-line Characterization

For online testing, the set-up was modified by connecting the targeted devices to the power network. Two techniques of injection have been tested: with a commercial injection probe, and with a custom coupler made with capacitors, resistors and a high-frequency transformer. The injection probe allowed for placing the injection point between the power source and the target (injection points i4-i2). The coupler was used to act as a malicious peripheral sharing the power network with the target (injection points i1-i3). Again, the frequency response has been analyzed to detect a possible filtering introduced by the propagation path composed of the injection hardware, the power network (e.g. cable network and connected appliances)

and the EMC filter of the power charger. Based on these experiments, it has been shown that it was possible to induce a parasitic signal on the target audio front-end by injecting the interferences through the power network.

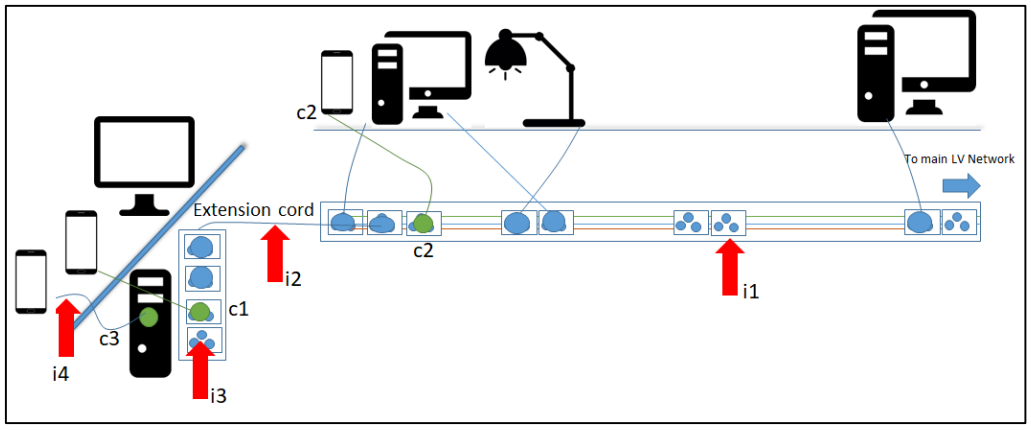

Fig. 10. Power network considered during the experimental characterization of the audio injection – i1 i2 i3 i4 are injection point and c1 c2 c3 are the connection point of the smartphone.

The aim was to connect the smartphone to the power network, to the USB port of a computer injecting the signal through a magnetic probe or RLC circuit. As the attacker will not have any information about the targeted power network, we assume that they are frequencies that will better propagate the signal to the targeted device audio input. Thus, the power network in this study has been chosen to reflect a classical TT power network with a set of devices connected as shown Figure 10. Experiments have been carried out as shown Fig. 11.

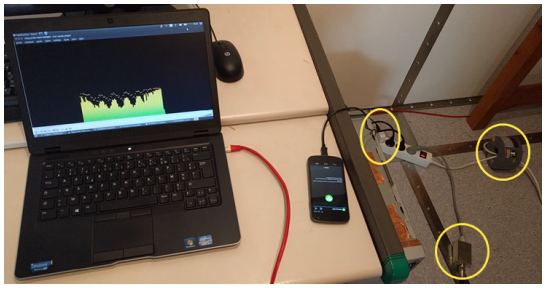

Fig. 11. Experimental set-up for the characterization of devices online. The yellow circles highlight the USB charger (left), the injection probe (center right) and the custom coupler (bottom right).

The frequency responses of online and offline experiments are given in Fig. 12. In the online setup, the 50 Hz component of the power network and its harmonics are added to the injected signal along with additional noise. The injected signal is also slightly more attenuated than in the offline case. This can be either due to the coupling circuit to the power network or by connected devices that may absorb part of the induced energy as shown in [24-26].

While a study of the effect of adding or removing connected appliances has been considered out-of-scope of study the preliminary analysis has shown to be efficient for defining the frequency of injection when the device is connected to the power network as shown Fig. 8 and Fig. 11. This means that the preliminary analysis provides a valuable input to define the source parameters for the exploitability of the attack path.

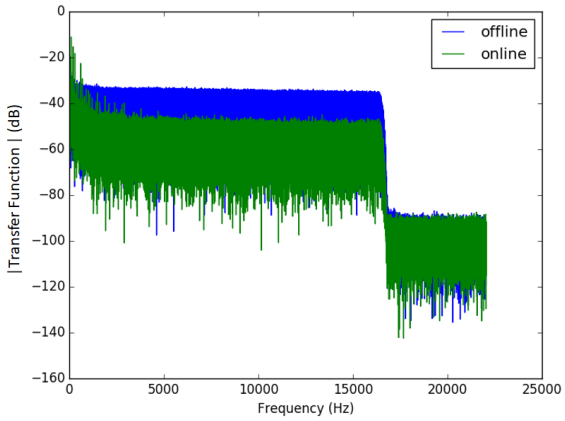

Fig. 12. Transfer function magnitude (normalized) of the signal received by the target for a 231 MHz carrier frequency modulated with one sweep between 1Hz and 23 kHz with charger 2 and cable 1 in offline and online test configurations.

IV. Exploitation for Voice Command Injection

The results obtained in the previous section provide information about the way the injected parasitic signal gets distorted by the different elements on the propagation path and demodulated by the input audio stage of the target. Interestingly, the resulting demodulated audio signal has been shown to be subject to a very low attenuation in the 100 Hz-17 kHz band. This means that a voice signal injected using the proposed technique should not suffer a high distortion and still possess the temporal and spectral characteristics necessary to be correctly interpreted by VCIs. In this section, several attack scenarios are proposed, exploiting the electromagnetic susceptibility of the targets to submit and execute unauthorized voice commands.

1. Remote Voice Command Injection Attack Scenarios

Once the possibility of inducing audio signal into a smartphone while it is charging has been demonstrated, it was necessary to validate that the quality and the level of the audio signal were high enough to get properly processed and interpreted by VCI engines. In order to perform these tests, the smartphones have been configured to have their VCI interpreters always on and connected to internet through a Wi-Fi router. Several test vectors containing the VCI activation keyword and a voice command have been injected. A test was considered successful when the commands have been correctly interpreted and executed by the target. To better match the reality, several configurations have been tested taking into account the main use cases for charging smartphones (Fig 13).

a. Scenario 1

Smartphones are charging through a USB charger connected to the power network: In this context, the devices are connected to the power network through a genuine power charger provided by the manufacturer. The point of injection of the parasitic signal is located somewhere in the power network behind the power socket. The electromagnetic waves have to by-pass the transformers and the EMC high-pass filters encountered in the propagation path.

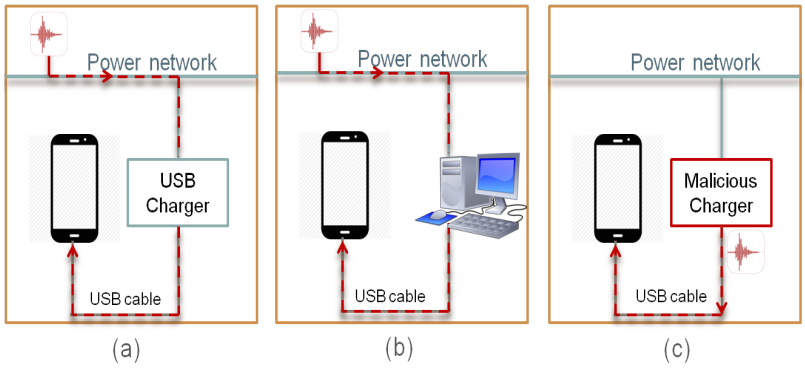

Fig. 13. Charging scenarios considered for the exploitation tests, (a) scenario 1, (b) scenario 2, (c) scenario 3.

b. Scenario 2

Smartphones are charging through the USB port of a computer connected to the power network: In this scenario, the devices are connected to the USB port of a desktop computer with a USB cable. The computer is connected to the low voltage power network. The point of injection of the parasitic signal is located somewhere in the power network behind the power socket. The electromagnetic waves have also to by-pass the transformers and the EMC high-pass filters of the computer's power unit along with those encountered in the propagation path. Moreover, the signal should be strong enough to couple into the targeted USB cable. In addition, the possibility of not disturbing the computer is a critical issue as a two-step attack could lead to the compromising of the computer through the USB interface.

c. Scenario 3

Smartphones are connected to a malicious USB power charger dock: This scenario is likely to be the most efficient as there are less filtering elements on the propagation path of the parasitic signal. Indeed, the point of injection is located within the charger directly on the output power signal of the USB charging cable. A modified USB charging device (or a portable power bank) is considered here, which is able to properly provide the power required by the target device (5 V – 5 A max. DC) and also to superimpose a malicious parasitic signal intended to exploit the VCI. The target device is thus directly exposed to the parasitic signal. To simulate this scenario during our experiments, an injection probe has been placed directly on the USB cable of the target device connected to the power network through a genuine USB charger.

2. Summary of tested scenarios and results

The presented scenarios have been validated by combining the point of injections (i1 to i4) and the point of connection (c1 to c3) as summarized in Table 1. Interestingly it has been observed that the experiments confirmed the possibility of injecting the voice commands on the targeted device for all combinations. The probability of success was close to 99 % - a success is defined as the voice command getting processed and executed by the voice command engine for each trial - for a set of 20 trials in each configuration. As the injection point shall be pertinent regarding the attack scenarios combinations have not been tested.

Table 1: Combinations of points of injection and points of connection regarding the possible attack scenarios for f_m = 231 MHz

		point of injection			
		i1	i2	i3	i4
point of connection	c1	A	A	B	X
	c2	A	A	B	X
	c3	A	A	B	C

Tested configurations with successful voice command injection and execution by the targeted device.
X Untested configurations as considered irrelevant for an attack scenario.

The tested combinations summarized in Table 1 shall be interpreted as follows:

- A: the target device is connected to the power supply either directly (c1, c2) or through the USB port of the computer (c3). An attacker will place his injection probe or injection circuit to a power socket (i1 or i2).
- B: the attacker may have tampered the extension cord (i3) or a device connected to it. He will try to reach a target connected to the power network (c1, c2 or c3).
- C: the attacker has created and inserted a malicious USB circuit (i4). The target is connected to it (c3) providing a direct connection with attacker system. This can be performed through USB power banks available in public areas like airports.

V. SECURITY DISCUSSION AND COUNTERMEASURES

1. Injection techniques based on Smart IEMI – Attacker profile

The results given in what follows were obtained with a Samsung Galaxy Nexus, running Android 4.3 with Google Now v.1.3. large, and its genuine Samsung USB charger. To get commands properly interpreted by the VCI for all tested injection configurations (online or offline, coupler or injection probe), the required emitted power was nearly 500 mW at carrier frequencies close to the resonant frequencies identified in the previous experiments.

Furthermore, it was shown based on the scenarios considered in this study that the charging use case has a negligible effect on the possibility of inducing audio signals on the charging target via the power lines of the USB cable. A comparison between the radiated-based injection technique [6] and the present conducted-based injection technique is proposed in Table 2. The main limitations imposed by the radiated case could be overcome by involving the conducted propagation path and the exploitation of back-door coupling effects induced on the charging port PCB. It can be mentioned that the required power to successfully inject voice commands has been lowered to 500 mW for reaching targets at a distance higher than 10 meters (we reached 30 meters during experiments). The source size has been reduced to fit in a so-called malicious PLC-like modem and its power consumption can be directly provided by the targeted power network.

Table 2: Comparison of the radiated and the conducted based injection techniques

Characteristic	**Radiated case [6]**	**Conducted case**
Coupling mode	Front-door	Back-door
Propagation path	Air	Power lines
Pre-requisite	Headphones cable with microphone	Charging USB cable
Required power	40 W (2 m) 200 W (4 m)	0.5 W (> 10 m)
Source size	Backpack (SDR[1] + PC[2] + amplifier + battery + antenna)	PLC[3] coupler / Charger
Target type	Outdoor mobile	Indoor stationary

[1]SDR : Software Defined Radio.
[2]PC : Personal Computer.
[3]PLC : Power Line Communication.

2. Security analysis

This study illustrates a two-stage exploitation resulting in a stealth and unauthorized abuse of VCIs. The first stage takes advantage of the electrical and microelectronic design of the targets and their robustness against IEMI and results in an injection of malicious signals into their audio front-end input stage. This possibility emphasizes the fact that from an information security point of view, standard EMC and EMI practices provide limited protection. Indeed, their scope is limited to unintentional parasitic signals and do not take a malicious behavior of an attacker into account. For software security engineers, input interface filtering against malicious inputs is a common practice. Electronic devices destined to critical applications should enforce the same principles on their interfaces (analog, digital and power inputs) by properly filtering signals the closest to their operational frequency band, integrating EMI filters or designing low-level sub-domains mutually isolated on the PCB.

The second stage takes advantage of the access control for the voice interface. Since its widespread deployment, the VCI editors seem to have been focusing on its ease of use in order to identify potential usages and encourage its adoption by end-users and service providers. As a consequence, it can be foreseen that the number of critical actions achievable via VCIs will keep increasing. As discussed in Section II-C, several studies, have demonstrated that voice commands could be submitted and executed without the user noticing. Thus, in order to mitigate this vulnerability, VCI editors could consider several layers of countermeasures. Voice recognition for authenticating (or at least identifying) the user would force the attacker to forge or to acquire voice samples of the target user. Challenge-response confirmation protocols, such as audio captchas, would make it necessary for an attacker to intercept the challenge in order to forge a response signal. Allowing for a personalization of the keyword would also impose an information gathering step for an attacker and restrict the exploitation to a targeted attack. In order to both make the user more conscious of the risks and allow for tuning the impact of this vulnerability, editors should provide finer grain settings for choosing which actions and which applications should be available through VCI, and which should require an authentication. Finally, to further mitigate the risk for security unaware users, editors should set up secure default settings and inform the user of the risks when he opts for less secure settings.

VI. CONCLUSION

In this study, we presented a new technique for remote and silent voice command injection in a specific model of smartphones based on conducted propagation and back-door coupling phenomena. This technique is complementary to the existing one based on radiated propagation and front-door coupling and allows compromising different targets, from a longer range and with less emitted power. By characterizing different configurations of the propagation path, it was shown that a proper voice command injection is achievable with a reduced effect of the elements on the propagation path. Finally, this study highlights a potential attack vector on VCIs, demonstrating that a stealth unauthorized exploitation of this UI is possible, attracting the attention of both vendors and users on its criticality and emphasizing the need to secure it and to use it wisely. More EMC/EMI analysis are required in order to have a better understanding of the power network random configurations on the efficiency of the attack scenario. Moreover, as proposed in this study, the experimental set-up can be used to characterize other devices in order to check the exploitability of this attack path against other Smartphones.

REFERENCES

[1] L. Palisek, L. Suchy, “High Power Microwave effects on computer networks,” EMC Europe 2011, vol., no., pp.18-21, 26-30 Sept. 2011.

[2] M. G. Bäckström, K. G. Lövstrand, “Susceptibility of electronic systems to high-power microwaves: Summary of test experience,” IEEE Trans. Electromagn. Compat., vol. 46, no. 3, pp. 2004.

[3] C. Kasmi, J. Lopes-Esteves, N. Picard et al., “Event Logs Generated by an Operating System Running on a COTS Computer During IEMI Exposure,” Electromagnetic Compatibility, IEEE Transactions on , vol.56, no.6, pp.1723,1726, Dec. 2014.

[4] Y. Hayashi, S. Gomisawa, Y. Li et al., “Intentional electromagnetic interference for fault analysis on AES block cipher IC,” Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 2011 8th Workshop on, vol., no., pp. 235,240, 6-9 Nov. 2011.

[5] T. Fuhr, E. Jaulmes, V. Lomne et al., “Fault Attacks on AES with Faulty Ciphertexts Only,” Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on , vol., no., pp.108,118, 20-20 Aug. 2013.

[6] C. Kasmi and J. Lopes Esteves, “IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones”, in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 6, pp. 1752-1755, Dec. 2015.

[7] C. Kasmi, J. Lopes Esteves, P. Valembois, “Air-gap Limitations and Bypass Techniques: “Command and Control” using Smart Electromagnetic Interferences”, Journal on Cybercrime and Digital Investigations, Vol. 1, No. 1, pp. 13-19, Dec. 2015.

[8] Y. V. Parfenov, L. N. Zdoukhov, W. A. Radasky et al., “Conducted IEMI threats for commercial buildings”, in IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 404-411, Aug. 2004.

[9] N. Mora, C. Kasmi, F. Rachidi, et al. “Modeling of the propagation along low voltage power networks for IEMI studies”, Electromagnetics in Advanced Applications (ICEAA), 2013 International Conference on, Torino, 2013, pp. 436-439.

[10] E. Savage, W. Radasky, M. Madrid, “IEMI AC Harmonic Vulnerability of Small External Power Supplies”, In Proc. of AMEREM 2014 Conference, no. 6, Albuquerque, New-Mexico, USA, 27 - 31 July. 2014.

[11] Apple, “Siri”. [Online]. Available: https://www.apple.com/ios/siri/, 2015.

[12] Google, “Ok Google”, [Online]. Available: https://support.google.com/websearch/answer/2940021?hl=en, 2015.

[13] Microsoft, “Meet Cortana”, [Online]. Available: http://www.windowsphone.com/en-us/how-to/wp8/cortana/meet-cortana, 2015.

[14] Samsung, “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, 2014.

[15] Paypal, “Hey, Siri! Sending & Receiveing Money with Paypal is now easier”, [Online]. Available: https://www.paypal.com/stories/us/hey-siri-sending-receiving-money-with-paypal-is-now-easier,10 Nov 2016.

[16] N.Gonzalez, “Siri exploited again – how to bypass the lock screen in iOS 8”, [Online]. Available: ios.wonderhowto.com, 2014.

[17] Applidium, “Cracking Siri”, [Online] Available: http://github.com/applidium/Cracking-Siri, 2011.

[18] W.Wei, “Apple admits Siri voice data is being shared with third parties”, [Online]. Available: www.hackernews.com, 2015.

[19] W.Diao, X.Liu, Z.Zhou, K.Zhang. 2014. “Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone”, In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM '14). ACM, New York, NY, USA, 63-74

[20] T. Vaidya, Y. Zhang, M. Sherr, C. Shields, “Cocaine Noodles: Exploiting the gap between Human and Machine Speech Recognition”, USENIX Workshop pn Offensive Technologies (WOOT), Aug. 2015

[21] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, W. Zhou, “Hidden Voice Commands”, 25th USENIX Security Symposium, Austin TX, Aug. 2016.

[22] F. Fiori, P.S. Crovetti, “Nonlinear Effects of Radio Frequency Interference in Operational Amplifiers”, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 49(3), 367-372, Mar. 2002.

[23] D.F. Kune, J. Backes, S.S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, W. Xu, “Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors”, Security and Privacy (SP), IEEE Symposium on, 145-159, 2013.

[24] C. Kasmi, Application de la topologie électromagnétique à la modélisation du réseau énergétique basse-tension: étude statistique des perturbations conduites, PhD thesis, 2013.

[25] N. Mora, Contribution to the Study of the Vulnerability of Critical Systems to Intentional Electromagnetic Interference (IEMI)”, PhD Thesis, 2016.

[26] N Mora, C Kasmi, F Rachidi, M Hélier, M Darces, “Modeling of the propagation along low voltage power networks for IEMI studies”, EPFL Technical report, 2013.

[27] http://www.chipworks.com/sites/default/files/Apple_iPhone_6s_A1688_Smartphone_Chipworks_Teardown_Report_BPT-1509-801_with_Commentary.pdf

[28] https://fr.ifixit.com/Teardown/Samsung+Galaxy+S8+Teardown/87136

[29] https://fr.ifixit.com/Teardown/Nexus+9+Teardown/31425