URSI AP-RASC 2019, New Delhi, India, 09 - 15 March 2019

Analysis of Soft-Faults induced by IEMI in Elementary Functions and Complex Electronics

J. Lopes Esteves [(1)], C. Kasmi* [(2)], and E. Cottais[(1)]
(1) Wireless Security Lab, ANSSI, France
(2) Mobile and Telecom Lab, Darkmatter LLC, UAE

Abstract

Many papers were devoted to the detection and analysis of effects induced by intentional electromagnetic interference on electronic devices. Most of studies have shown the possibility of analyzing failures when devices are exposed to specific electromagnetic waves. In this paper, we propose to instrument the operating system of multiple devices to gather and process in real-time software failures to detect and classify effects induced during parasitic exposure. A replication of elementary functions has been performed to characterize the point of failures of a complex system.

1. Introduction

In the context of Electromagnetic Security, risks management impose the characterization of electromagnetic leakage against potential compromising emanations [1] and the susceptibility to intentional electromagnetic interferences (IEMI) [2] in order to have the information security requirements fulfilled (namely the confidentiality, integrity and availability of data and the infrastructure). Many studies have been devoted to the detection and the analysis of effects induced by IEMI. Complementary techniques [3-4] have been proposed either monitoring the electromagnetic environment [3] or accessing software failures [4]. This study refers to the second technique where the operating system is fully instrumented to detect any software failure due to cascaded and propagated effects. Understanding the appearance of a software failure when the device is exposed to a specific waveform could lead to the understanding of how the induced currents/voltages could affect the state of the electronic device either from front-door or back-door coupling [5]. It is worth to mention that depending on the type of signals, the devices can be remotely shutdown and the devices would still provide the evidence of software failures. An additional outcome of this work is to provide the evaluators an idea of what could be obtained during a forensic activity. In this study, we propose a description of the application of a system-centric approach to elementary functions of complex electronics which have been instrumented in order to gather the evidences of effects.

The paper is organized as follow: in Section 2, a description of the system-centric approach is proposed. In Section 3, the test setup to expose devices under test is described. In Section 4, the detected effects based on the system-centric approach applied to elementary functions and the entire system. Finally, in Section 5, conclusions drawn from the experiments are given.

2. System-centric Approach

Electric and electronic devices can be decomposed as a set of software modules (e.g. operating system, drivers), hardware components (e.g. sensors) and wired and/or wireless network interfaces. Understanding the way these parts interact is highly valuable as it could provide a deep understanding of the malfunctions of the targets when they are exposed to electromagnetic waves.

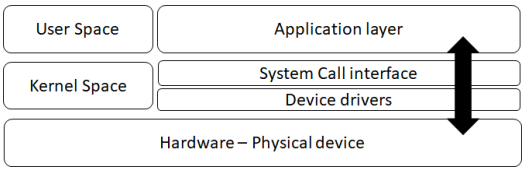

Fig. 1. Generic System description highlighting the decomposition of the hardware and software parts.

These parts, when affected, can be classified as front-door coupling interfaces and back-door coupling interfaces. A set of observables can be listed on a generic basis, potentially providing the capability to a health monitoring agent to gather from the software level any hardware, communication and software failure.

A modern electronic device, as schematized in Fig. 1, contains a set of hardware components among which microprocessors or microcontrollers, memory devices, sensors and controller devices, connected through internal communication buses. Some of these components are controlled and polled by the main controller. More autonomous components send interrupt signals to the main controller to indicate they have information to report. The interrupt is then relayed to the operating system's kernel through a software interrupt. The device drivers will then proceed as an intermediate layer between the kernel and the user space upper layers and the physical device. Interestingly, when an application needs to interact with a device, it is done through the device driver. This opens a variety of exploitable software failures if IEMI attacks could create unexpected hardware

behaviors. As for example data parsers, which have not been hardened to take into account out of bounds values reported by sensors, could lead to a crash of the driver.

3. Description of the Testbed

In order to detect and to characterize the effects induced by IEMI, it is necessary to synchronize the variations of waveform's parameters with the detection software running on the tested device. For that particular reason and to have a maximum flexibility, the source is composed of a software defined radio and a power amplifier. Table I lists a set of RF pulse parameters used to stimulate the targets.

Table 1: Parameters of RF pulses

Parameters	Range
E-field	5 – 300 V/m
CW frequency	100 MHz – 20 GHz
Modulation	100 % AM – 50 % duty cycle
Repetition rate	1 Hz – 10 MHz

A remote connection is used between the device under test and the health monitoring station outside the Faraday cage. The device under test is placed in the Faraday test volume at a far-field distance from the emission antenna. While a uniform field can't be demonstrated, the authors would like to point out that the goal is the instrumentation of the targets and the design of efficient techniques to detect effects induced by IEMI. Any other test chamber (e.g. anechoic chamber, mode-stirred chamber) could be used once the appropriate health-monitoring tools have been implemented.

4. Detection and Classification of Effects

Commercial off-the-shelf (COTS) IT devices such as computers are interesting targets as the access to software logs, embedded sensors and communication interfaces is relatively easy. Examples of detected effects are erroneous sensors values (hardware), driver crashes (software) and denial-of-service on Ethernet link (Communication).

In contrary, closed systems such as embedded systems require a pre-analysis step. Accessing the internals of such devices is generally prevented by security mechanisms introduced by manufacturers. Two complementary techniques could be applied to define observables: reproducing elementary functions with the same hardware components and understanding the way they react during the IEMI exposure or circumventing the security mechanisms to gain the execution of a health monitoring software. We propose hereafter a discussion regarding both techniques to understand how the sensors behave as a standalone function and inside a COTS UAV. In order to reach a deep understanding of effects induced on elementary functions, a testbed has been designed to understand the effects during parasitic exposure. Sensors are directly connected to an analog to digital converter (ADC) with a defined sample rate. The power supply applied is 3.3 V or 5 V and the sensors are placed in pull-up and pull-down circuits. It has been shown that the power supply has a non-negligible effect (susceptibility level is higher at 3 V) and that the pull-up and pull-down circuitry show that the boundaries of effects are larger for a pull-up circuit. The equivalent sensors in an UAV having exactly the same power supply and a main ADC controller working at the equivalent sample rate have been tested against parasitic exposures. It has been observed that the propagated effects within the flight-control can be retrieved. Based on a running health monitoring software, it was possible to observe specific malfunctions due to specific parts. Nevertheless, combined effects are still a challenge as the complexity of the target requires the combination of elementary functions. Valuable deductions have been made regarding induced effects related to a single point of entry at the software level (temperature rise, altitude increase).

5. Conclusion

In this paper, a system-centric approach has been proposed in order to detect and to characterize the effects induced by IEMI attacks. From the user point of view, it has been demonstrated that software failures due to parasitic exposure could be detected. Interestingly, in real-time and remotely the evaluator is able to access the effects at fine-grain level. During the presentation, the applied system-centric approach to multiple devices in different scenarios will be discussed highlighting its reproducibility for multiple configurations. Hardware configurations for elementary functions (e.g. temperature measurement) have been tested with standalone testbed and a complex system in order to understand if the electronic design and the choice of the power supply have a significant influence on the susceptibility level. One of the main outcomes is the possibility to emulate a coupled signal by removing the sensor on the complex device to simulate out of range values to detect a propagated effect within the system. From an information security perspective, these tests could lead to the hardening at the software level of the UAV.

7. References

1. M. Vuagnoux, S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards", USENIX Conference, Aug. 2009.
2. Q. Zhijun, P. Xuchao, H. Yong, C. Hong, S. Jie, Y. Cheng, "Damage of high power electromagnetic pulse to unmanned aerial vehicles," High Power Laser and Particle Beams, November 2017.
3. J. F. Dawson et al., "A Cost-Efficient System for Detecting an Intentional Electromagnetic Interference (IEMI) attack," 2014 International Symposium on Electromagnetic Compatibility, Gothenburg, 2014, pp. 1252-1256.
4. J. Lopes-Esteves, E. Cottais and C. Kasmi, "Software Instrumentation of an Unmanned Aerial Vehicle for HPEM Effects Detection," 2018 2nd URSI Atlantic Radio Science Meeting Gran Canaria, 2018, pp. 1-4.

5. 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, 2004.