Autonomous Electromagnetic Attacks Detection considering a COTS Computer as a Multi-Sensor System

Chaouki Kasmi[*1], Jose Lopes-Esteves[1] and Mathieu Renard[2]*

[1]Wireless Security Lab, French Network and Information Security Agency – ANSSI,
[2]Hardware and Software Security Lab, French Network and Information Security Agency – ANSSI,
75 007 Paris, France,
*corresponding author: chaouki.kasmi@ssi.gouv.fr

Abstract

Many studies were devoted to the analysis and the detection of electromagnetic attacks against critical electronic systems at the system or the component levels. As far as we know, the effects induced by such threats are classified depending only on the working status of devices following an illumination. Nevertheless, the possible study of the preliminary symptoms of these effects has not been investigated. In this study, we propose to monitor a set of internal sensors that can be derived for the detection of electromagnetic attacks. We demonstrate the possibility for a COTS computer to detect abnormal activity due to electromagnetic attacks by using its own resources as sensors.

1. Introduction

The protection of critical systems against high power electromagnetic (HPEM) attacks has become an intensive challenge for the electromagnetic compatibility (EMC) community. Many tests have shown that electronic systems are vulnerable [1-3] to HPEM-attacks. Until now the existing solutions have relied on the integration of expensive external protective devices. Due to their cost, risk management procedures tend to accept the loss of widely deployed electronic systems due to electromagnetic (EM) attacks. In case of physical damages, the electronic system is simply replaced without wondering about a potential attack.

In this study, it will be argued that most computers are enclosing a wide variety of physical and logical sensors that can be used to detect HPEM-attacks. Several communication interfaces can be used to collect data about the surrounding electromagnetic environment [4] (e.g. WI-FI card, Power Line Communication transceivers (PLC)). Moreover the degradation of the electronic device performances (e.g. temperature, processors load, and memories read/write errors) can be gathered. It will be shown that the target itself can be naturally seen as a multi-sensor system. It will be pointed out that the analysis of the collected information is useful for the detection of HPEM-attacks.

The paper is organized as follows: in Section 2, some of the possible observables and their related sensors are described. In Section 3, a set of sensors have been instrumented and their response to HPEM-attacks is analyzed.

2. Monitoring internal sensors for IEMI detections

Commercial Off-The-Shelf (COTS) computers possess several interfaces (e.g. peripheral interfaces, communication links) and internal sensors (e.g. temperature sensor) in order to provide regular usage features. But they can be used as sensors by the operating system to monitor abnormal activity due to HPEM-attacks. Some of those sensors provide information regarding the external environment of the computer and some give an insight on its internal state. A list of relevant available sensors will be given in this Section. Note that the variability of these observables results either from *first order* and *second order front-door* coupling (wireless communication interfaces) or *back-door* coupling [5].

2.1 External sensors: communication interfaces

The sensors providing information about the environment are essentially the interfaces that are in interaction with external entities: the communication interfaces. The activity of the wired network interfaces (Ethernet, PLC) is one piece

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

of evidence worth monitoring. Previous work [1-2] focused on the analysis of EM perturbation on networking equipment (routers, switches): it has been shown that such equipment's susceptibility to EM perturbations has an impact on the data link throughput. The information about network activity can be accessed in real time through system Application Programming Interfaces (APIs).

The wireless (e.g. 2G/3G modem, WI-FI card), acting as front-door coupling interfaces, can be used to measure and to monitor the noise floor, the signal to noise ratio of the surrounding electromagnetic environment. Furthermore, one can expect to observe effects on data links on those interfaces. Data transfer rates and transferred data integrity can be provide further insight. In our case, the different communication interfaces have been instrumented to access the noise floors (NF), the signal-to-noise ratios (SNR) and also the received power (RP) when available.

2.2 Internal sensors: hardware and software sources of evidence

Many parameters can also be monitored on the computer to provide information about its health status. Computer Processor Unit (CPU) load, motherboard sensors status, input-output and memory faults or software crashes are watched to detect any suspicious behavior that could be a symptom of a HPEM-attack.

More and more information about hardware state is made available at the operating system level. Modern computers enclose many hardware sensors which can be polled directly through low level communication buses (e.g. I2C, SPI) or through high level APIs accessible by the system (at kernel level, driver level...).

The most common hardware information that can be accessed by the operating system is the CPU temperature and the Hard Disk Drive (HDD) temperature. They are used to trigger the fan when the EUT overheats. The fans' activity can also be monitored. Modern motherboards allow to retrieve information about voltage levels of CPU, motherboard... There exists several proprietary and open source software projects for accessing this information such as *lm-sensors*, *mcelog* (Linux/Unix systems) and Open Hardware Monitor (MS Windows systems).

Abnormal software behavior of an IT equipment perturbed by EM sources has already been reported [3] but the effects had not been precisely analyzed at the system level. Most modern operating systems provide several APIs and tools for gathering a lot of information about both software and hardware. The CPU load is a good reference indicator about the system's activity. System logs are a good source for checking for hardware disruptions, peripherals' malfunction and critical software anomalies, which usually trigger kernel errors. They are also useful for determining whereas the cause of a reboot or shutdown was intentional (at the system's or the user's initiative) or consecutive to a perturbation.

Peripherals also report information to the system through drivers that end into the system logs. USB root hub activity is logged and errors on the link layer or the application layer are accessible. PS/2 controllers also report activity and errors through the system logs. Moreover, network interfaces generally log link layer errors. Information about internal hardware buses is not commonly available to the system. Nevertheless, communication links to storage devices (HDD, peripherals) can be monitored and the integrity of the data transferred can be verified.

3. Sensors response analysis

Electromagnetic sources can be used to disrupt or to induce physical damages to electronic systems. The data collected from the sensors is analysed in real time or stored, either locally or remotely. In this section, it will be demonstrated that the sources of evidence introduced in the previous section provide information closely related to whereas the EUT is under HPEM-attack or not.

3.1 Wireless activity monitoring

Wireless communication interfaces provide a good way to monitor the RF spectrum activity (in their respective bands). To illustrate this point, the example of using a 2G/3G interface (iCON 225) to detect abnormal RF activity (in this case 2G/3G jamming) is presented. Generally, the software application provided with the 2G/3G modem returns to users messages indicating that the communication link is lost. Nevertheless, the reason of the signal loss is not available.

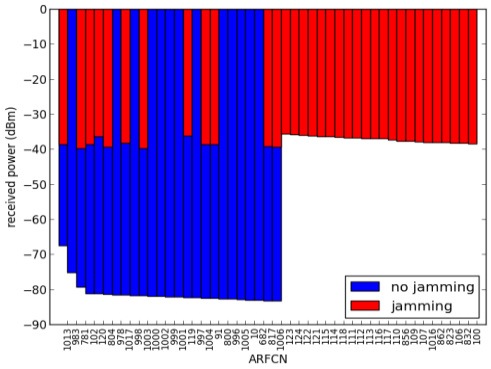
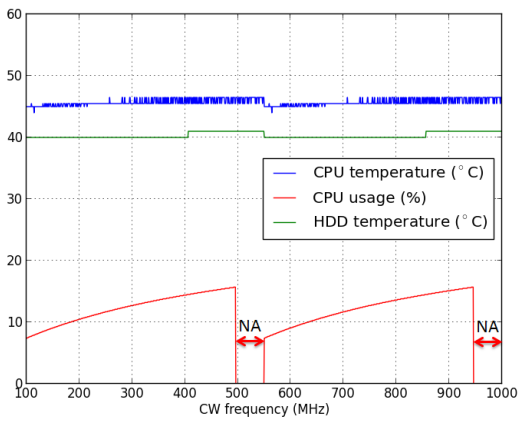


Figure 1: Received power (RP) on the 2G/3G modem with the jammer turned ON and OFF

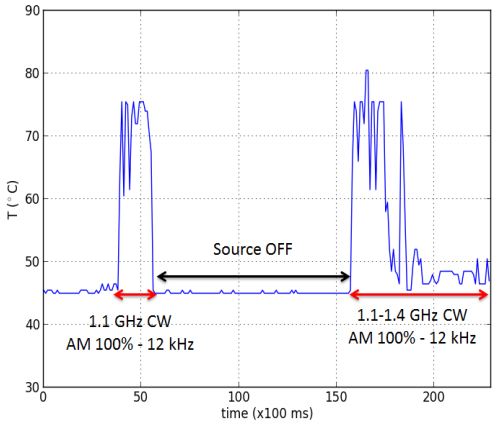
As the electromagnetic environment is monitored in real-time and the signal strength analyzed at the receiver RF front-end, the reason of a disconnection can be deduced. The 2G/3G modem allows to measure the received power for 200 channels (ARFCN) however for graph readability only 50 channels are depicted in Fig. 1. Under jamming condition, the 2G/3G modem has shown a signal loss message. By analyzing the received power, the jamming can be detected. This method has also been applied to the other communication interfaces such as PLC, WI-FI, Bluetooth interfaces. As a result, we are able to detect abnormal activity due to electromagnetic attacks with information gathered from these interfaces.

3.2 Temperatures and CPU load

During a HPEM-attack, some internal symptoms to the EUT can be observed through the motherboard's sensors. Among other tests, a Continuous Wave source (CW) (100 MHz to 1GHz) with a 100 % Amplitude modulation pulsed at 12 kHz (50 % duty cycle) has been used to illuminate an Intel Pentium IV computer with a Debian 7.4 Linux operating system. During the tests, the temperature of the CPU, the temperature of the HDD and the CPU load were monitored.



(a)



(b)

Figure 2: Evolution of the CPU and HDD temperature (°C) and the CPU usage (%) in regards of the 100 % AM CW frequency (a) Variability of the measured CPU temperature due to the CW illumination between 1.1 and 1.4 GHz (b)

The results, depicted in Fig. 2a and Fig. 2b, show that the CPU temperature sensor is very susceptible to the EM stimuli. Depending on the nature of the perturbation, very fast increases of the reported temperature (shown in Fig. 2.b), which cannot occur in a regular usage of the EUT, were observed. The HDD temperature sensor reacts to EM stimuli but less drastically. The acquired value of the CPU load is also tied to the EM perturbations.

At some point, invalid values are retrieved (Not Available – NA in Fig. 2a), which clearly indicates low level software disruption due to the EM activity. It can be pointed out that the evolution of those three observables is tied. Thus one can deduce that those observables react synchronously to the same events. The specific behavior of each observable can be correlated to detect EM abnormal activity.

4. Conclusion

While reserved to the military community for a long time, high power electromagnetic attacks are getting more and more affordable and technically accessible. Most of the effort on detection of and protection against this kind of attacks has been focusing on using external devices. Instead, in this paper, we emphasize the possibility for an electronic device to detect abnormal activity due to HPEM-attacks by using its own resources as sensors. Available sensors have been identified. It has been shown that the selected sensors react to HPEM stimuli. Front-door coupling communication interfaces allow gathering information about the device's external environment (RF spectrum activity) and internal sensors enable the analysis of the device's health status, and watching symptoms. An electronic device is thus able to collect useful information which, properly correlated, could allow to reliably detect HPEM-attacks.

Furthermore, the sensors' activity can be real-time monitored and recorded. Alert messages are then provided to the user of the computer. Then, if a computer is physically damaged, a forensic analysis can be applied by extracting and analyzing the collected data in order to estimate if the computer has been hit by EM attacks.

In future works, the correlation and the characterization of many more observables' symptoms to different stimuli will be further investigated. During the presentation the test results of EM attacks against a monitored computer will be presented. It will be shown how the proposed method provides a low-cost built-in reliable way to detect and analyze HPEM-attacks and their effects on the target.

5. Acknowledgments

The authors would like to thank the French Network and Information Security Agency – ANSSI for its support.

6. References

1. Brauer, F.; Fahlbusch, S.; ter Haseborg, J.L.; Potthast, S., "Investigation of Hardening Measures for IT Equipment against Radiated and Conducted IEMI," Electromagnetic Compatibility, IEEE Transactions on, vol.54, no.5, pp.1055-1065, Oct. 2012.

2. Palisek, L.; Suchy, L., "High Power Microwave effects on computer networks," EMC Europe 2011 York, vol., no., pp.18-21, 26-30 Sept. 2011.

3. Hoad, R.; Carter, N.J.; Herke, D.; Watkins, S.P., "Trends in EM susceptibility of IT equipment," Electromagnetic Compatibility, IEEE Transactions on, vol.46, no.3, pp.390-395, Aug. 2004.

4. Betta, G.; Capriglione, D.; Miele, G.; Rossi, L., "Reliable Measurements of Wi-Fi Electromagnetic Pollution by Means of Traditional Spectrum Analyzers," Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC 2008. IEEE , vol., no., pp.206,211, 12-15 May 2008

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.