System Design & Assessment Note

Note 44

November 2014

Automation of the Immunity testing of COTS computers by the instrumentation of the internal sensors and involving the operating system logs – Technical report

C. Kasmi, J. Lopes-Esteves, M. Renard

French Network and Information Security Agency, 75 007 Paris, France

*chaouki.kasmi@ssi.gouv.fr

Abstract—Many studies were devoted to the analysis and the classification of effects induced by intentional electromagnetic interferences induced on COTS computers. This study focuses on the monitoring of the internal resources of these devices in order to obtain an in-depth analysis of the induced perturbations. The generalization of a monitoring tool and its deployment in a large IT network are the key contributions of this research.

Table of contents

List of figures

List of tables

1. Introduction: needs for susceptibility testing improvement

Many tests have demonstrated that the electronic systems are susceptible [1] to High Power Electromagnetic sources (HPEM). Since the trend in society is to integrate more and more electronic devices in critical infrastructures, it is of fundamental interest to estimate their susceptibility to attacks. For these reasons, several European funded projects are dealing with the vulnerability of critical infrastructures (e.g. STRUCTURES [2], HiPOW [3]) and transportation information systems (e.g. SECRET [4]). One of the challenges in those studies is to estimate and classify the effects of intentional electromagnetic interferences (IEMI) induced on electronic devices [5-16]. The existing classification method [17] of effects induced by intentional electromagnetic interference allows to estimate a set of events during and after the exposure. Hoad et al. [13] have shown that a complex matrix (recalled in Table 1) can be built for estimating the state of failure of a device under tests.

Table 1: Analysis of effects induced by IEMI during and after parasitic exposure [13]

Effect	During Exposure to EM Stress	After Exposure to EM Stress
No Effect	No Effect	No Effect
Monitor upset	Blanking or interference	Returns to normal function
Mouse pointer deflection	Influence position	Returns to normal function
Program closure	Pop up menus, program closures, programs moved or deleted	Desktop function may be altered, missing or moved icons
Network crash	The network throughput drops to zero	The network can be restored from a remote terminal
Crash with self restart	The computer stops processing and latches	The computer starts processing again or a soft reset (Ctrl-Alt-Del) is required
Shutdown with self restart	The computer switches off, and attempts to restart without manual intervention	Once EM stress removed the computer restarts normally. During restart operating system detects abnormal shutdown, several files may be affected
'Blue Screen'	An exception error occurs resulting in the customary 'blue screen' error message	The system, generally, can be re-booted without persistent effect
Crash with manual restart	The computer stops processing and latches	During restart the operating system detects abnormal shutdown, several files may be affected
Shutdown with manual restart	The computer shuts down or switches off spontaneously	The computer remains non-functional. During restart operating system detects abnormal shutdown. Several files may be affected
Network shutdown	The network throughput drops to zero	The network cannot be restored from a remote terminal. Manual restart of the network switch is required to re-initiate network
Peripheral Component Damage	The computer or network may crash or shutdown	Investigation reveals permanent damage to a peripheral component i.e. monitor, keyboard, mouse, hub etc.
Functional Damage	The computer or network may crash or shutdown	During restart the computer reports a failure to find the operating system. Re-installation of the operating system cures the fault (expected minimum outage 2 hours)
Physical Damage	The computer may crash or shutdown	During restart the Computer either fails to boot or a critical device such as the hard disk malfunctions (expected minimum outage 1 day)

In practical experiments, we would like to be able to detect and correlate the effects induced by Intentional Electromagnetic Interferences (IEMI) with hardware and software faults that can be recorded on the EUT. Already applied in the car industry in immunity testing, it has been shown

that the effects of HPEM on the CAN-Bus network can be estimated [12]. The hardware and the software internal resources of these automotive electronic devices cannot be monitored due to a restriction of these resources to manufacturers only. However, estimating the effects during exposure requires the possibility for the operator to monitor the electronic device components health status which is impossible for his safety. Moreover, short temporary failures may have disappeared at the time the operator is allowed to enter the experiment facility.

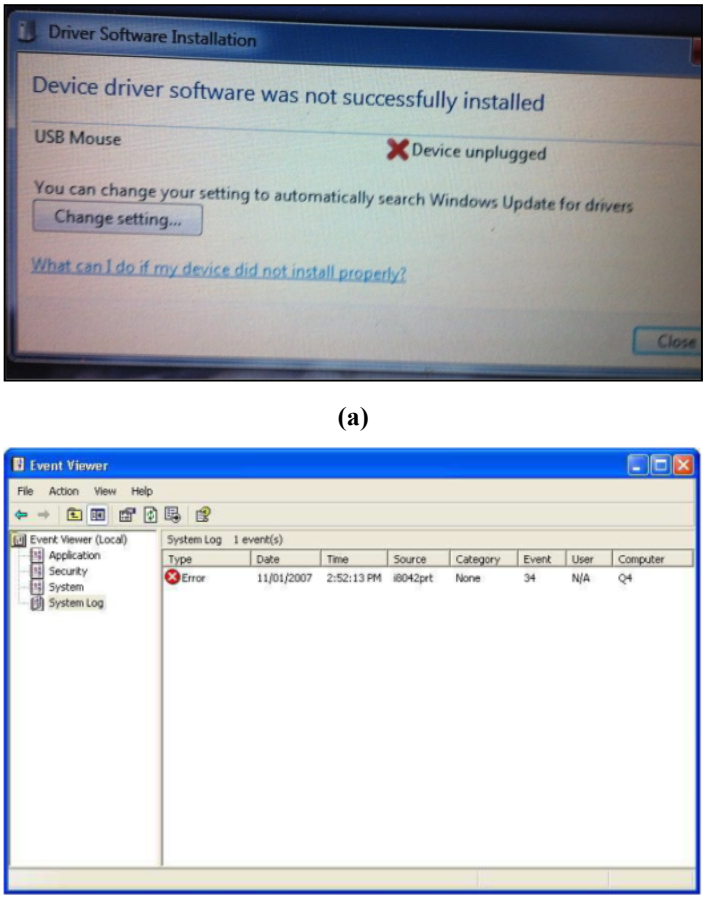


Fig. 1: Error messages of USB faults provided by the operating system : (a) Windows Vista (b) Windows XP [13])

More and more accurate information about the *CPU* (*load, temperature* and *integrity)*, the internal *Memories (integrity)* and the *Software crashes (operating system, firmware* and *drivers)* can be obtained using documented commands provided by electronic system manufacturers, as shown Fig. 1. By recording in real time this information, we are able to record and to analyze the perturbations induced by HPEM parasitic fields on the EUT in a finer grain and to trace the malfunctions from the hardware to the software level. More recently, experimental tests [18] were conducted in South-Korea in order to have a clue on the effects induced by HPEM attacks against an infrastructure, as depicted in Fig. 2 [18], containing an IT network.

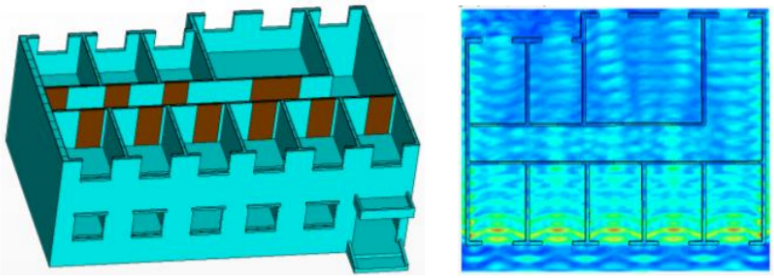


Fig. 2: Simulation of the EM waves propagation in a building [18]

In order to analyze a potential failure of the involved computers, a handmade test was conducted on each of those devices. Nevertheless, the last approach is known to be time-consuming. Moreover, monitoring temporary failures recovered by the operating system running on COTS IT systems requires a real-time recording of faults induced during tests. In the following study, we focus on a COTS computer, later called equipment under test (EUT) to show that more clear-cut details can be obtained thanks to operating system logs. The possibility of monitoring a large IT infrastructure in order to classify more precisely the effects induced in a realistic environment is also discussed.

In the following study, pulse radar signals having the characteristics, provided in Table 2, were used.

Table 2: Characteristic of the pulse radar signal used for the tests

Parameters	Range
E-field	250 – 300 V/m
CW frequency	100 MHz – 20 GHz
Modulation	100 % - AM / 50% - duty cycle
Repetition rate	1 Hz – 10 MHz

The paper is organized as follows: first, in Section 2, after presenting the common aspects of computer architecture, the analysis of hardware and software faults induced by HPEM sources will be presented. Section 3 provides the information gathered from communication interfaces. Finally, the design of a distributed solution suitable for monitoring and testing large IT network infrastructures against IEMI will be proposed.

2. Hardware and Software Faults

COTS computer manufacturers make more and more information about the condition of the equipment available to the operating system and to the users. As a result, modern computers contain many hardware sensors that can be polled directly by low-level communication buses (e.g. I2C) or via high level application interfaces (APIs) accessed by the system (e.g. kernel, drivers). For example, information about the temperature of the processor and the hard drive can be accessed by the operating system to manage the speed of the fans.

Modern motherboards also retrieve information about the voltage levels of some components. Most modern operating systems provide several programming interfaces and tools to collect information on software and hardware. The abnormal behavior of software computer equipment caused by electromagnetic interference sources has been reported [16] and analyzed in detail. It has been concluded that "system events" logs are a good source of information to verify the critical malfunctions in hardware and software, as well as the probable cause of system reboots or shutdowns. We propose hereafter to recall the main results of this study.

2.1 Computer general architecture

The way an operating system interacts with the hardware components (internal sensors, peripherals) can be described as a multilayer architecture, shown in Fig. 3. To summarize, a typical modern computer contains a set of hardware components among which microprocessors, memory devices, internal communication buses, sensors and controller devices. Some of them are directly controlled and polled by the microprocessor. Other more autonomous hardware components send interrupt signals to the microprocessor (CPU) to indicate they have information to share. The interrupt is then relayed to the operating system's kernel through a software interrupt. The hand is given to the device drivers which implement the communication protocol adapted to the device. The device drivers act as an intermediate layer between the kernel and user space upper layers and the physical device. Thus, when an application needs to interact with a device, it is done through the device driver.

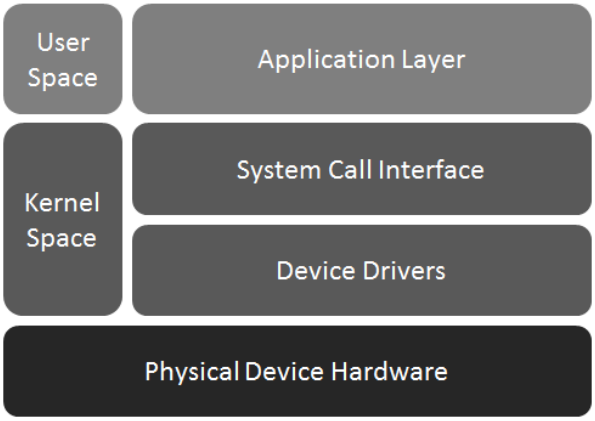


Fig. 3: General architecture of a Computer [16]

Information messages about the hardware devices usually show up in the system log files via device drivers. For example, the activity of the USB root hub controller is logged and errors on the link layer or the application layer are visible. PS/2 controllers also report activity and generate errors in the system log files. The equipment under test (EUT) in what follows is an Intel Pentium IV computer with a Debian 7.4 Linux operating system.

2.2 Peripheral interfaces testing

Information about internal hardware buses is generally not available to the operating system. Nevertheless, some communication links between peripheral devices can be monitored and the integrity of data transferred can be checked. In order to observe the symptoms of an HPEM attack on the peripheral interfaces, many tests were performed. It was demonstrated [14] that the signal integrity and the data rate of digital communication systems can be highly deteriorated by spurious electromagnetic fields. It is therefore interesting to monitor the errors on peripheral

interfaces. The EUT was instrumented at the operating system level to detect the presence of errors from two of the most widely deployed peripheral interfaces (USB and PS/2) during parasitic electromagnetic exposure through log analysis.

2.2.1 Serial peripheral interfaces: PS/2

For monitoring the PS/2 interface symptoms, the Linux kernel logs are well suited. When the EUT is illuminated by HPEM sources, several errors show that the signal on the PS/2 cable is disturbed. Fig. 4 lists some of the most frequent log entries related to the PS/2 interface [19]. These error logs reported by the PS/2 controller suggest that the EM stimulus either creates or modifies some of the PS/2 data traffic [14].

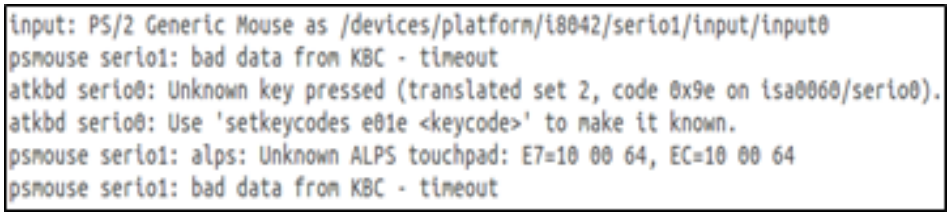


Fig. 4: Errors induced on the peripheral interfaces (USB and PS/2) [16]

The message “bad data from KBC” means that the PS/2 controller received malformed data. So does the line containing “Unknown ALPS touchpad”, showing that the device identifier of the mouse was modified during the transmission. Moreover, the log entries about the “atkbd” are very interesting. Indeed, they show that the EM stimuli induced PS/2 packets which are interpreted as invalid keyboard key codes. All these errors have been explained in [16] as a result of EM coupling on the PS/2 cables, on one or both (data or clock) lines.

2.2.2 Serial peripheral interfaces: USB

In order to observe the symptoms of an HPEM-attack on the USB interface, many different tests were performed. The results presented hereby were obtained by checking the USB errors notified by the USB root host controller through the USB driver at the kernel level; therefore the kernel logs were watched.

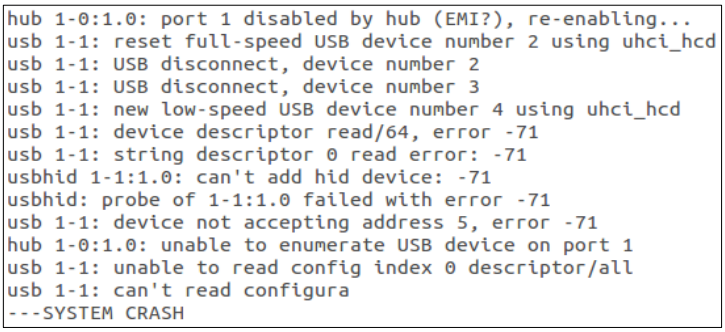


Fig. 5: Errors induced on the USB interface (truncated) [16]

The USB interface was very responsive to the EM perturbations. An extract of the kernel logs concerning USB is shown in Fig. 5. The main symptom is a repetition of device disconnections, resets and re-enumerations. It can also be pointed out that several read errors appear during parasitic illumination. These symptoms have been explained in detail in [16] as the result of the induction of special USB physical layer symbols (SE0 and SE1) [20], thus interrupting the

regular communication and inserting "*End of Packet*" or forbidden symbols in the middle of regular packets. This explains why the root hub indicates that there is a possible EMI phenomenon.

2.2.3 Summary of the effects

The different symptoms observed on the PS/2 and USB interfaces could be caused by a damaged cable or a problem with the controllers. The main effects appear synchronously on both interfaces when the burst repetition rate is very close to the PS/2 and USB 1.1 data rates while the CW frequency allows better parasitic signal coupling which depends on the hardware interfaces of the EUT.

Table 3: Encountered effects on peripherals interfaces [21]

interface	symptom
PS/2	corrupted data received
	unknown key code received
	modified device identifier received
	random valid packet injection
USB	device disabled by the HUB
	device disconnected
	corrupted descriptors received
	disconnect/reconnect/enumeration sequences

A summary of the detected effects induced on the PS/2 and USB interfaces is proposed in Table 3.

2.3 Temperature sensors monitoring

Two temperature sensors are available on the EUT. The motherboard encloses a temperature sensor which can be accessed by polling a Super I/O chip on the ISA bus. The hard drive encloses a local temperature sensor which can be polled directly using the S.M.A.R.T. protocol. The test results, depicted in Fig. 6, show that the CPU temperature sensor is highly reactive to HPEM. The reported temperature is subject to very fast and intense variations (shown in Fig. 6) which are very unlikely in a normal use case.

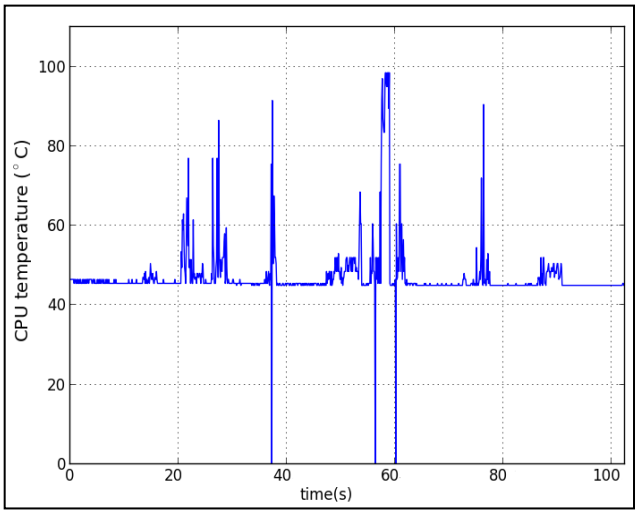


Fig. 6 : Evolution of the measured temperature under parasitic EM exposure [21]

As expected, these variations occur when the EUT is under EM illumination. As soon as the excitation is stopped the temperature provided by the sensor decreases to the value of 45 °C. This demonstrates that the parasitic currents and voltages on the link between the sensor and the CPU were introducing wrong values.

Among other tests, we tried to estimate the waveform allowing maximizing the dynamic between the real temperature and the fake one, as depicted in Fig. 7. It is important to mention that as soon as temperature increases, the CPU is increasing the fan speed and if the temperature reaches the critical temperature values the computer is stopped.

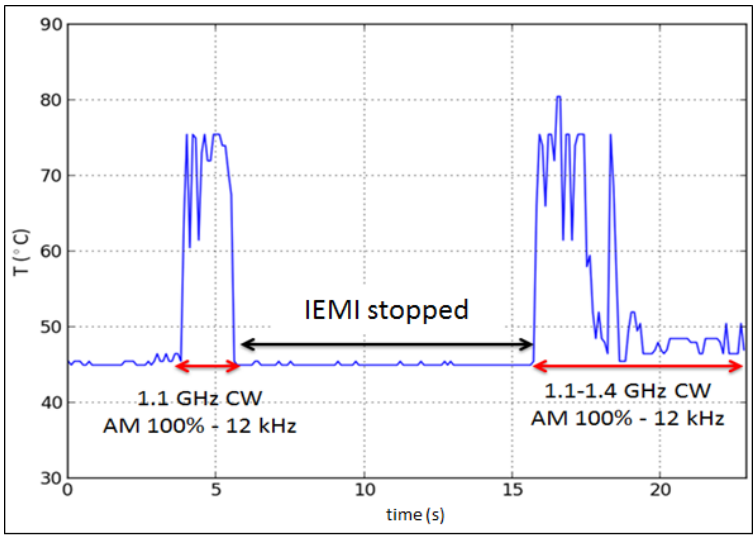


Fig. 7 : Estimation of the resonating frequency of the temperature sensor for EM coupling maximization

2.4 Sound card

Spurious voltages and currents can also be induced in motherboard components and in the sound card in particular. Digital audio recording works by recording, or sampling, an analog audio signal at regular intervals of time. During experimental tests, we detected the coupling of parasitic signals on the computer sound card components.

The analog-to-digital converter measures and stores each sample as a numerical value that represents the audio amplitude at that particular moment. Converting the amplitude of each sample to a binary number is called quantization. The number of bits used for quantization is referred to as bit depth. The quality of a digital audio recording heavily depends on two factors: the sample rate and the sample format or bit depth. Features of the specification include: a sample rate in the range of 6 – 192 kHz with a sample resolution between 8 – 32 bits.

Although the audio receivers are designed primarily for the 20 – 20,000 Hz range of human hearing, modern sound cards support 44.1 kHz (CD), 48 kHz and 88.2 kHz, or 96 kHz sampling rates. Sampling rates higher than 50 kHz to 60 kHz cannot supply more usable information for human listeners but may be interesting when using a sound card as a sensor.

The noise floor on the sound card was measured without connecting any sound-to-electrical signal transducer (e.g. microphone). The spectrogram representation (later called waterfall) of the measured signal is given on Fig. 8. The observed signal results from the electromagnetic direct coupling into the computer sound card.

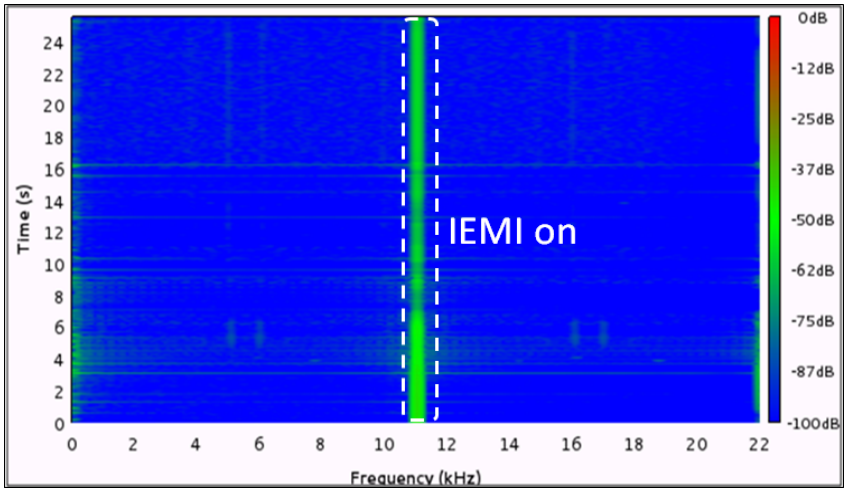


Fig. 8 : Evolution of the noise floor under parasitic EM exposure [21]

3. Network Communication Interfaces

The network communication interfaces are, just like the peripherals interfaces, open entry points allowing a both electrical and logical interaction between the EUT and external entities. While wired interfaces can be prone to interferences coupling to the cables by parasitic fields, the wireless communication interfaces provide raw data about the external electromagnetic environment. However, accessing this information may require some modifications in the network card firmware (depending on the chipset manufacturer).

3.1 Wireless Interfaces

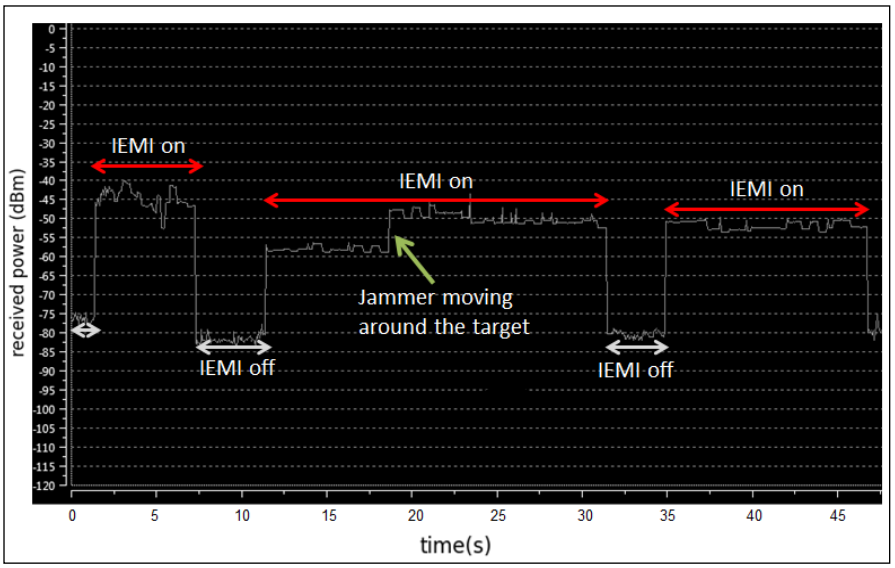
The wireless communication interfaces (e.g. 2G/3G modem card, WI-FI), acting as interfaces for direct coupling, can be exploited [9] to measure and monitor the noise floor (NF) and the signal-to-noise ratio (SNR) of the EUT electromagnetic environment (summarized in Table 4).

The data rate and the data integrity can also be monitored. Several wireless communication interfaces were instrumented to access the NF, the s SNR and the R_XP. One of the main threats on wireless communication systems is denial-of-service (DoS) attacks using jammers [4].

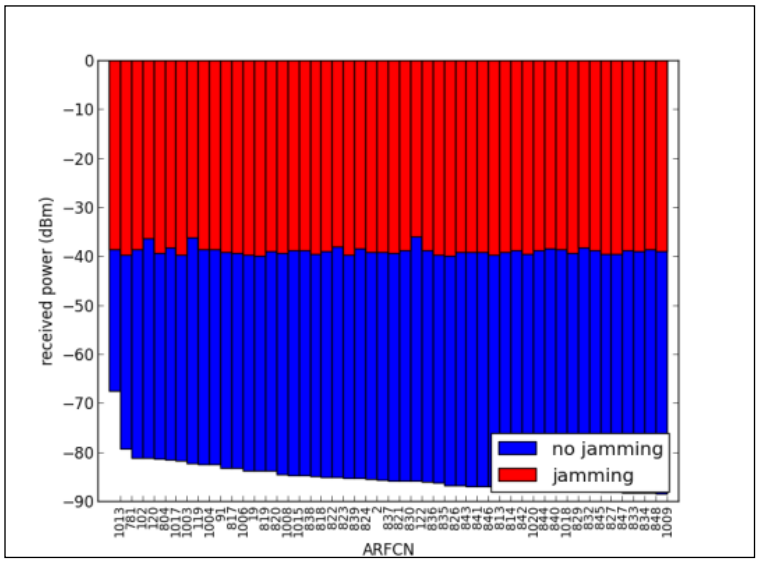
Table 4 : Communication interfaces available on a computer

	interface	information available
communication interfaces	2G/3G, NFC, Bluetooth, WI-FI card	noise floor, signal-to-noise ratio, bit-error-rate, R_X power

It is therefore important to be able to detect such attacks. It is shown in Figs. 9 that the instrumentation of wireless interfaces allows detecting jamming attacks against 2G and 3G interfaces.



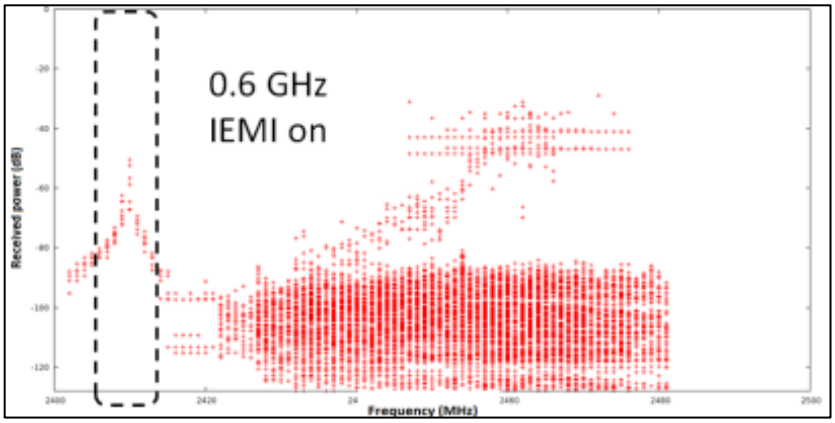
(a)



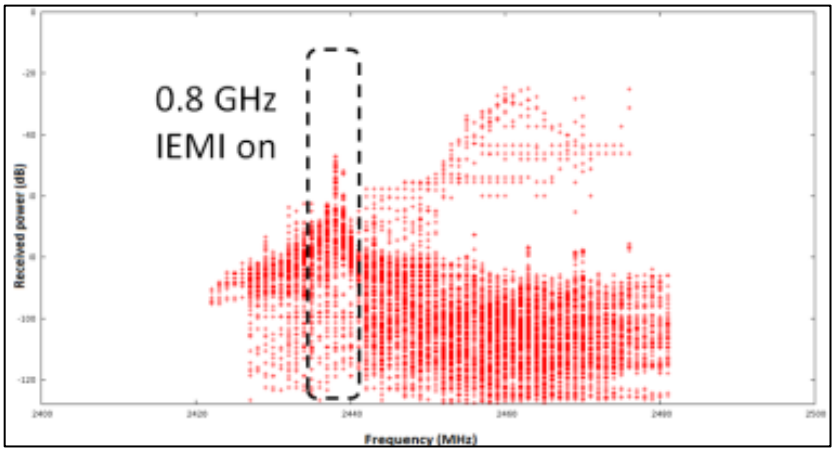
(b)

Fig. 9 : Received power by a 2G/3G modem enforced in a 3G mode (a) and enforced in a 2G mode (b) under normal and jamming conditions [21]

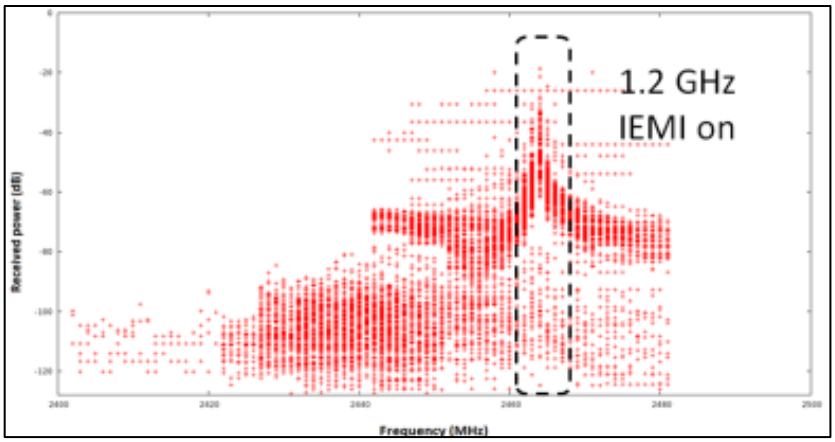
Furthermore, other attacks on wireless links involving the emission of a malicious signal that is stronger than the legit one could be easily identified using this technique. Other wireless interfaces have been tested [21] and it has been shown that the correlation of suspicious behavior simultaneously from several interfaces leads to an accurate detection mechanism.



(a)



(b)



(c)

Fig. 10 : Measured power with the Wi-Fi interface during parasitic exposure for the following jamming frequencies (CW frequencies of the burst): (a) 0.6 GHz, (b) 0.8 GHz and (c) 1.2 GHz

It is also important to point out that the use of HPEM signals with very high power allows stopping a wireless communication [21-22] due to low cost antennas used in COTS devices. In Figs. 10, it can be observed how we are able to detect the parasitic field on a Wi-Fi interface of the EUT.

3.2 Ethernet

Previous works [8, 10, 11] have focused on the analysis of IEMI effects on wired network equipment (e.g. routers, switches). It was shown that the sensitivity of the equipment to electromagnetic interference results in the reduction of data rate on the communication links. The susceptibility of the Ethernet interface at the physical layer against HPEM has already been demonstrated in several studies [11]. Fast decreases of the performance of wired communication interfaces (eg. Ethernet, Power Line Communications) can thus be considered as relevant evidence of effects induced by HPEM.

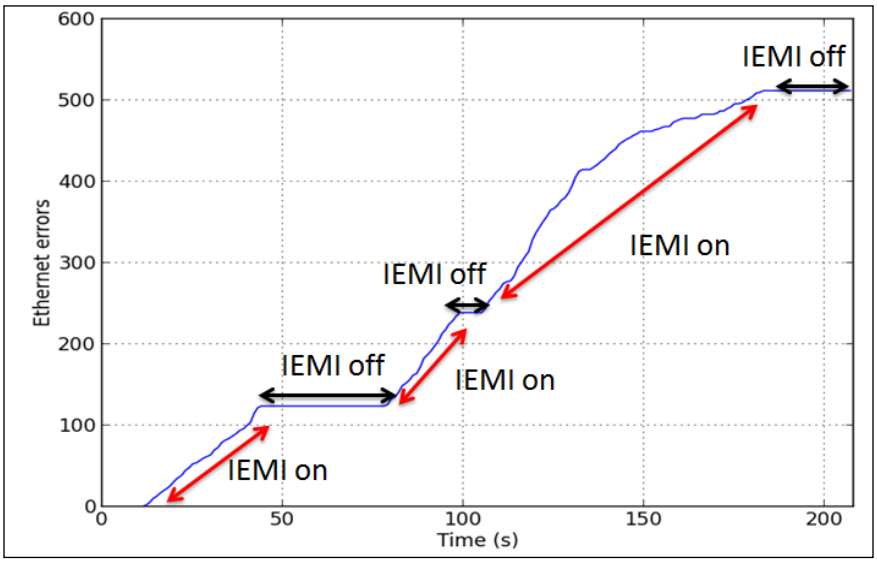


Fig. 11 : Evolution of errors reported on the Ethernet link during IEMI exposure [21]

For testing purposes, we used common network information tools to gather data about errors on the Ethernet interfaces during illumination. A continuous TCP/IP and UDP/IP traffic has been generated on the Ethernet link and the errors were analysed. The Ethernet protocol includes frame integrity checks (Frame Check Sequence) and a collision detection mechanism. Furthermore, encapsulated protocol payloads (e.g. TCP/IP ...) usually also provide integrity checks and error detection mechanisms. As the technology evolved, some Ethernet controllers perform verifications both on Ethernet frames and upper layer protocols payloads. However, the granularity of the errors reported to the operating system is usually limited to a count of errors and collisions.

Access to further information would require low level modifications at the driver, kernel or controller firmware layers. Thus, we first focused on the most commonly available information about the Ethernet interface errors. The results are shown in Fig. 11. The tests show that when the EUT is targeted by EM sources, the errors on the Ethernet link increase drastically. A link loss correlated with a health status monitor of subsidiary connected IT network equipment can indeed be considered as a clear indication of a perturbation.

4. Testing and monitoring a complex IT network

In order to overcome the complex challenges involved by testing and monitoring the effects of IEMI induced in a complex IT network, we propose a distributed software architecture performing the instrumentation of information sources and the analysis of the gathered data, thus providing a real time monitoring of the effects of IEMI exposure on a set of COTS computers. This architecture is composed of several software subsystems. The first subsystem is the *Symptom Observer Subsystem*, which gathers data from a set of sensors and is specific to the host machine hardware and software configuration.

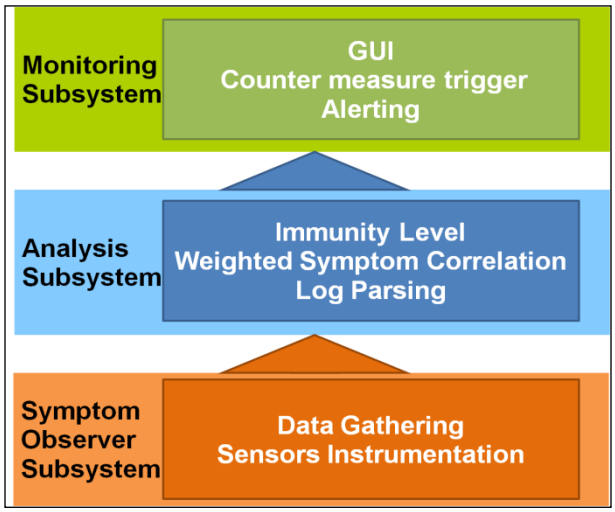


Fig. 12 : Software architecture of the detection system

The data is then processed by the *Analysis Subsystem*, which parses the logged data, correlates the symptoms and determines the immunity level of the EUT machine. The *Monitoring Subsystem* centralizes the data and handles the user interface. It gives an overview of the evolution of the immunity level and raises messages to the operator. The software architecture is depicted in Fig. 12. It provides a great flexibility and the possibility to deploy each subsystem both locally or distributed over a network.

4.1 Network considerations

This software architecture was designed in order to be able to adapt and optimize the deployment of the detection system according to two main factors, namely the processing load distribution between machines and the network topology. The processing load involved by the detection system can be easily balanced according to the characteristics and the available resources of the machines in the network. The monitored machines must run the Symptom Observer Subsystem at least. The Analysis Subsystem and the Monitoring Subsystem can then run on all machines or on some specifically chosen machines.

Besides load balancing, the software architecture of the detection system can be adapted to any network topology. In a centralized model, a specific machine can be in charge of the monitoring function while the other machines in the network run the Symptom Observation Subsystem. In a decentralized model, all the machines can be aware of all other machines' state. In this case, all the machines run the Symptom Observation Subsystem, the Analysis Subsystem and the Monitoring Subsystem. Some possible architectures are depicted in Fig. 13.

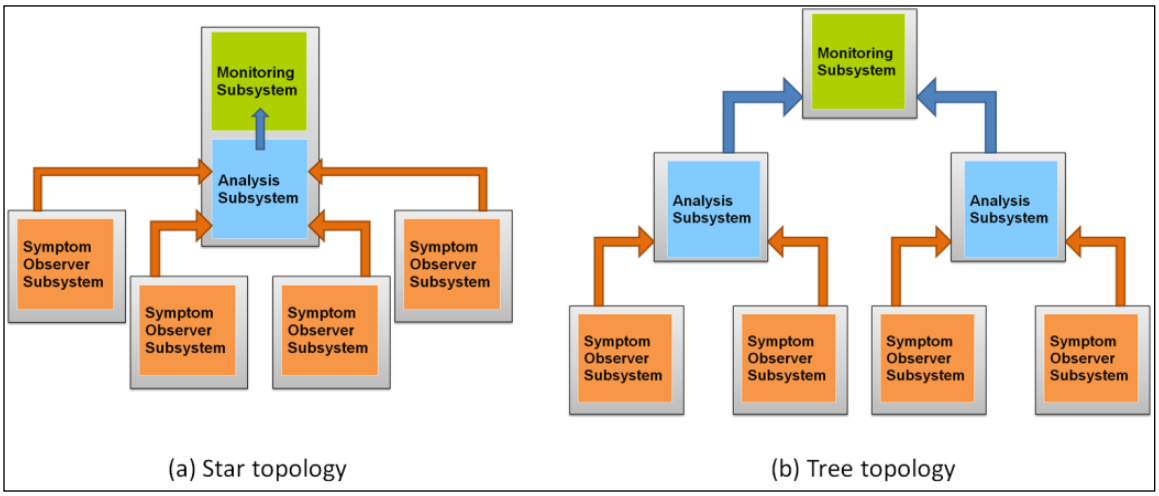


Fig. 13 : Schematized Star (a) and Tree (b) topologies of a distributed detector integrated in an IT network

For our proof of concept (POC), a centralized model with a star topology was preferred. The main reason is that in a centralized model, the monitoring machine can be placed in a secure room hardened against EM perturbations. This monitoring machine runs the *Analysis* and the *Monitoring Subsystems*, and the monitored machines only run the *Symptom Observation Subsystem* in order to reduce the processing load on these machines which are more prone to disruption caused by sources.

4.2 Symptom Observation Subsystem

The *Symptom Observation Subsystem* is the most machine specific part of the detection system. It is adapted to each machine's hardware and software characteristics. It is in charge of the instrumentation of the available sensors and the real time gathering of the symptoms for each sensor. The gathered data is then normalized and sent to one or more *Analysis Subsystems*. This was implemented in the POC by writing the normalized data in specific system log files and by using a remote log utility which handles the real time transmission of each log entry to remote *Analysis Subsystems*.

4.3 Analysis Subsystem

This subsystem is the entity in charge of the diagnostics. It analyses, for each logically connected machine, the incoming symptoms and deduces its immunity state. The symptoms are labeled with the originating machine identity (e.g. machine name, IP address) in complement to the timestamp. The *Analysis Subsystem* is a real time parsing module. It extracts the normalized data and applies a weight model to each symptom chosen accordingly to the reliability of the symptom. By correlating the weighted symptoms, the immunity status is computed and forwarded to the *Monitoring Subsystem*.

4.4 Monitoring Subsystem

The *Monitoring Subsystem* is the end user interface of the detection system. It is in charge of storing and displaying the monitored machines' immunity status received from the *Analysis Subsystems*. It is intended to be installed on security management machines to provide operator with spatial and temporal information about the immunity status of the machines on the network. When faults are detected, health status messages can be displayed to the operator. The interface we implemented is depicted in Fig. 14.

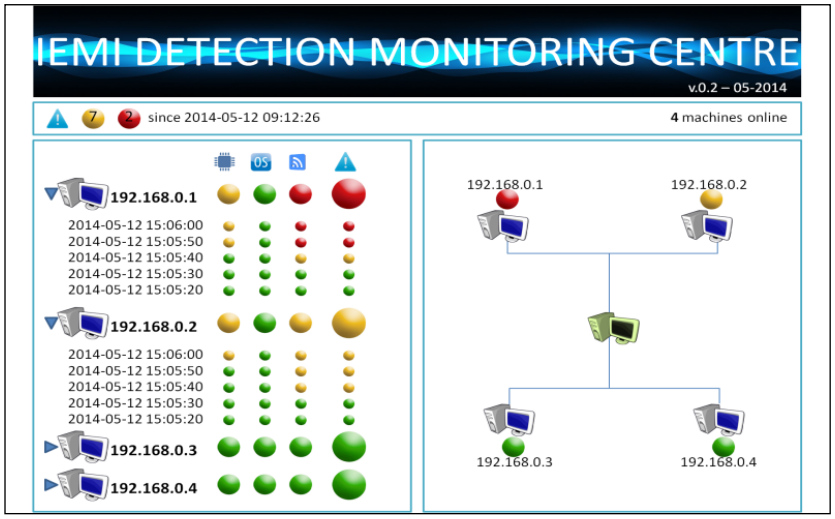


Fig. 14 : Monitoring interface of the HPEM detection system provided to the operator

The POC Monitoring Subsystem consists of a web server running PHP5 and a MySQL database. The Graphical User Interface (GUI) is a dynamic self-refreshing web page allowing the operator to have a simple and fast real time overview of the monitored machines.

5. Conclusion

In this paper, it has been shown that we are able to exploit the internal resources of COTS devices and their operating system to gather information about their health status during high power electromagnetic tests. An effective set of sensors has been identified and it has been shown that these sensors are sensitive to electromagnetic disturbances. Jamming attacks, which are considered more and more affordable, have also been considered. It has been demonstrated that the wireless interfaces provide standardized features which can be used for the detection of denial-of-service attacks. A software-based HPEM-attack detection agent has been designed by automating the instrumentation of identified sensors and properly correlating the observed symptoms. Its architecture was designed to easily allow a flexible deployment in a complex IT network. We show that this distributed agent network provides a novel way to monitor and record disturbances induced by HPEM, both temporally and spatially over a whole infrastructure. It overcomes the limitations of a local implementation and can be considered as a low cost, flexible, easily maintainable and deployable HPEM attack monitoring system for enhancing large scale HPEM tests.

6. References

[1] W. A. Radasky, C. E. Baum and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," Electromagnetic Compatibility, IEEE Transactions on , vol.46, no.3, pp.314,321, Aug. 2004.

[2] Project "STRUCTURES: Strategies for The impRovement of critical infrastrUCTUre Resilience to Electromagnetic attackS", European Research Project FP7, description available online: http://www.structures-project.eu/overview.

[3] Project "HiPOW: Protection of Critical Infrastructure against High Power Microwave Threat", European Research Project FP7, description available online: http://www.hipow-project.eu/hipow/project.

[4] Project "SECRET: SECurity of Railways against Electromagnetic aTtacks", European Research Project FP7, description available online: http://www.secret-project.eu/.

[5] R. Hoad, N. J. Carter, D. Herke et al., "Trends in EM susceptibility of IT equipment," Electromagnetic Compatibility, IEEE Transactions on, vol.46, no.3, pp.390-395, Aug. 2004.

[6] 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, 2004.

[7] L. Palisek, L. Suchy, "High Power Microwave effects on computer networks" Electromagnetic Compatibility (EMC EUROPE), 2011 International Symposium on, vol., no., pp.18-21, 26-30 Sept. 2011.

[8] F. Sabath, "Susceptibility Test on IT-Networks and their Components". In Proc. of URSI General Assembly 2008, Chicago, USA, Aug. 2008.

[9] W. A. Radasky, R. Hoad, "An overview of the impacts of three high power electromagnetic (HPEM) threats on Smart Grids," Electromagnetic Compatibility (EMC EUROPE), 2012 International Symposium on , vol., no., pp.1,6, 17-21 Sept. 2012.

[10] F. Sabath, B. Römer, "Susceptibility of IT-Networks to HPM and UWB Threats". In Proc. of European Electromagnetics Conf. (EUROEM), Lausanne, Switzerland, 2008.

[11] E. B. Savage, W. A. Radasky, K. S. Smith et al., "Susceptibility of Network Interface Cards to High-Level Conducted Pulses", In Proc. of European Electromagnetics Conf. (EUROEM), Lausanne, Switzerland, 2008

[12] J. Mirschberger, F. Sonnemann, J. Urban and R. H. Stark, "High-Power Electromagnetic effects on Distributed and Automotive CAN-bus systems", In Proc. of EUROEM 2012, pp. 85, July, 2012.

[13] R. Hoad, I. Sutherland, "The forensic utility of detecting disruptive electromagnetic interference". In Proc. of the 6th European Conference on Information Warfare & Security, pp.77-87, 2007.

[14] Y. V. Parfenov, W. A. Radasky, B. A. Titov, et al. "Some Features of the Pulse Electrical Disturbances Influence on Digital Devices Functioning". In Proc. of the URSI General Assembly, Beijing, China, Aug. 2014.

[15] J. Mirschberger, F. Sonnemann, J. Urban, et al., "High-Power Electromagnetic effects on Distributed and Automotive CAN-bus systems", In Proc. of European Electromagnetics Conf. (EUROEM), pp. 85, July, 2012.

[16] C. Kasmi, J. Lopes-Esteves, N. Picard, et al. "Event Logs Generated by an Operating System Running on a COTS Computer During HPEM Exposure, " Electromagnetic Compatibility, IEEE Transactions on , vol.PP, no.99, pp.1,4

[17] F. Sabath, “Classification of electromagnetic effects at system level”, Electromagnetic Compatibility - EMC Europe, 2008 International Symposium on , vol., no., pp.1,5, 8-12 Sept. 2008.
[18] J. S. Choi, J. Lee, J. Ryu, et al. “Evaluation of Effects of Electronic Equipments in Actual Environments”. In Proc. of AMEREM 2014, Albuquerque, USA, July, 2014.
[19] Chapweske, A., “The PS/2 mouse/keyboard protocol”, electronic file available: http://www.computer-engineering.org/ps2protocol/,2003.
[20] Universal Serial Bus Specifications, electronic file available: Revision 1.1, http://www.usb.org/developers/docs/, 1998.
[21] C. Kasmi, J. Lopes-Esteves, M. Renard, “Design of an IEMI-Attack detector involving the internal resources of a COTS Computer”. In Proc. of Future Security 2014 conference, Berlin, September 2014.
[22] M. Camp, J. Schmitz, M. Jung, Susceptibility of a Tetra Station to Electromagnetic Field Threats and Determination of Failure Effects, Electromagnetic Compatibility - EMC Europe, 2014 International Symposium on , vol., no., pp.1246,1251, 1-4 Sept. 2014.