4-18-1-PB

Data · January 2016

3 authors, including:

Lopes Esteves José
French Network and Information Security Ag…
27 PUBLICATIONS **35** CITATIONS
SEE PROFILE

Chaouki Kasmi
French Network and Information Security Ag…
58 PUBLICATIONS **70** CITATIONS
SEE PROFILE

Air-gap Limitations and Bypass Techniques: "Command and Control" using Smart Electromagnetic Interferences

Chaouki Kasmi, José Lopes Esteves and Philippe Valembois
Wireless Security Lab
French Network and Information Security Agency - ANSSI
51 boulevard de La Tour Maubourg, 75007 Paris, France
{name.familyname}@ssi.gouv.fr

This paper was presented at Botconf 2015, Paris, 2-4 December 2015, www.botconf.eu
It is published in the Journal on Cybercrime \& Digital Investigations by CECyF, https://journal.cecyf.fr/ojs

***Abstract*—Air gaps are generally considered to be a very efficient information security protection. However, this technique also showed limitations, involving finding covert channels for bridging the air gap. Interestingly, recent publications have pointed out that a smart use of the intentional electromagnetic interferences introduced new threats for information security. In this paper, an innovative way for remotely communicating with a malware already installed on a computer by involving the induced perturbations is discussed leading to the design of a new air gap bridging covert channel.**

Keywords—Control and Command; Air-gap; Electromagnetics;

I. INTRODUCTION

Information security has become a hot topic since the publication of important security flaws in critical infrastructures such as military facilities and country vital resources providers. In order to prevent information leakage, one of the organizational methodologies is the air-gap mitigation techniques which have been applied for a long time. The main aim of air-gap is to provide a physical isolation between secured and unsecured networks.

Recent studies have been dealing with bypass of air-gaps by creating communication links between the trusted environment and the unsecured world. Some researches were dedicated to the use of hardware characteristics of electronic devices to set-up mono- or bi-directional communication interfaces between physically isolated computers which are already infected by a malware. These techniques allow for bypassing air-gaps. Thus, air-gap techniques might give a false feeling of security to users and network security officers.

In addition, the susceptibility of electronic devices is investigated in order to define adequate protections to harden sensitive facilities against electromagnetic attacks. Recently, it has been proposed to rely on operating system logs of computers and the internal sensors in order to precisely characterize how computers react when exposed to electromagnetic perturbations. It has been observed that some communication links between the enclosed sensors and computer processor unit (CPU) can be disrupted which generates sensor reading errors. In this study, we propose to demonstrate how such electromagnetic vulnerability can become an information security issue.

The paper is organized as follows: first, in Section II, a depiction of the air-gap principle and its limitations are proposed. An exhaustive review of the published techniques dealing with the bypass of air-gaps is proposed. Then, in Section III, the technical details dealing with IEMI effects classification and characterization are recalled. Focusing on one of the induced effects, a command and control system involving smart electromagnetic interferences is detailed. Finally, in Section IV a set of counter-measures is recalled.

II. AIR-GAP PRINCIPLE AND LIMITATIONS

A. Principle

Most critical infrastructures, organizations and companies have to compose with several information systems (IS) with different levels of trust. In order to communicate with external entities and access public information, there is a need for Internet connectivity. Besides, internal IS are in place, both for internal organizational processes and operational processes. The permeability between trusted and untrusted IS introduces high security risks and several security practices can be applied in order to mitigate this attack vector, such as firewalls, diodes, sanitization devices or air gaps.

The air gap is a security measure which consists in isolating physically sensitive IS from untrusted ones. Usually, the isolation is achieved by avoiding networking links between the trusted and untrusted IS, so that there is no explicit communication interface that can be used to exchange data. In what follows, the untrusted IS is considered to be under control of the attacker. It can be either an IS that has been previously compromised and that the attacker has access to or the attackers IS.

However, many studies have shown that only disabling networking links is not enough to truly guarantee a complete isolation of sensitive IS. In the following sections, the attacker profile and challenges are discussed and a review of air gap bridging techniques is proposed.

B. (In-) Security challenges

In order to circumvent the security function achieved by an air gap, an attacker wants to find ways to establish a communication between a computer from the trusted air gapped IS and a computer from the untrusted IS. Furthermore, this supposes that the attacker is able to run software on both sides of the air gap which will try to exchange data. To achieve that, the attacker is facing the following challenges:

1) *How to place a malware on the targeted trusted computer:* the initial infection of the target is the main prerequisite for this attack to work. Although, this paper focuses

on the design of a covert communication channel assuming the infection phase has already succeeded, the main lines of information system infections are briefly recalled hereafter. The exchanges between the trusted IS and external entities are supposed to be rare and controlled. However, several threats can be considered as a compromise vector. First, the malware can be spread by a software or hardware modification of the target in the supply chain [1, 2]. This could be done by compromising the suppliers IS or by intercepting and modifying the devices before they are delivered to the final user. Secondly, the malware can be introduced intentionally or unintentionally by an authorized employee, through an infected flash drive for example. Finally, the update procedures can also be considered as a weak point that can be exploited in order to compromise the target, by either adding a malicious payload in the update package itself or by infecting the transport medium.

2) *How to communicate with the malware:* once the preliminary infection phase is performed and depending on the context and his motivations, the attacker may need to set up a communication channel. A channel to send data to the target will mainly be a command and control channel, to send commands, new payloads to execute and to trigger the execution or the interruption of a task. A channel to receive data from the target will generally be used as a feedback vector to retrieve the internal state of the malware or as a data exfiltration channel. Some of the techniques that can be used in order to exchange data with the target isolated system are discussed in the next section.

C. Review of air gap bypass techniques

In this section it is assumed that the preliminary infection phase has succeeded. Both air gapped computers run a malicious process which will, among other malicious actions, try to establish one or several communication channels between the trusted IS and the untrusted IS. The techniques that can be used to achieve this mainly consist in exploiting the available built-in wireless communication interfaces or in setting up a covert channel using the internal resources of the targeted device either as a transmitter or as a receiver.

In order to set up a communication channel, the malware running on the target can try to get access to the built-in communication interfaces the target encloses. It will first check the presence of such interfaces, e.g. Wi-Fi, Bluetooth or GSM adapters. If one of these interfaces is present and can be enabled by the malware, an attacker could set-up a fake base-station or routers to start communicating with the malware or to act as a bridge between the target and other compromised IS. Nevertheless, in sensitive environments, the wireless interfaces or at least the drivers (not recommended) are generally removed. Thus, it is necessary to explore alternative methods to set-up a communication channel, by exploiting a single bidirectional covert channel or by combining two unidirectional channels resulting in a so called hybrid covert channel [3]. A covert channel is generally defined as a computer security attack that creates a capability to transfer information between two entities that are not allowed to communicate by using channels that are neither intended for information transfer nor subjected to access control rules [4]. In what follows, a review of some previous work that can result in a covert channel allowing to bridge air gaps is proposed.

Removable peripherals that are generally used along with computers can sometimes be inadvertently used as a data storage platform. They generally enclose microcontrollers and memory chips that can be accessed directly by the host system. Mice, keyboards (with USB report descriptors) [5] and even screens or video projectors (with DDC and MCCS) [6, 7] possess memory units that can be modified by the host for configuration purposes. Switching peripherals such as KVM switches have been widely investigated and it has been proven that most of them provide ways to exchange data between two connected hosts [8]. Thus, even if they are not intended to provide a communication channel, they can become a good bidirectional half-duplex covert channel. This statement can be generalized to any electronic device that is simultaneously or alternatively connected to both of the air gapped computers.

Using sound as a physical communication vector has also been proposed, either by a direct use of a sound card with a microphone and speakers or via noisy internal components. Google has recently released a Google Chrome plugin called Google Tone that emits DTMF modulated sounds in order to share data between two computers. In this case, the system is not conceived as stealthy because the chosen frequencies and modulations can be heard by the human ear [9]. However, it is a good example of bidirectional covert channel. Stealth can be achieved by using other modulations [10] or frequencies (ultrasonic signals), as it has previously been proposed in [11].

It has also been reported that the BadBIOS malware was using ultrasounds to bridge air gaps [12]. The exploitation of the acoustic emanations due to internal components activity can also be used as a unidirectional covert channel to exfiltrate data. It has been shown in [13] that electronic components can produce an acoustic emanation that is correlated to the operations processed. Mechanical waves can also be captured by using vibration aware sensors such as gyroscopes embedded in modern smartphones and tablets. In [14] a smartphone's gyroscope is used to eavesdrop on voice conversations. Thus it is straightforward that this can easily be used as a unidirectional or bidirectional (depending on the targeted device's capabilities) air gap bridging covert channel.
Some electronic devices also produce a radio frequency (RF) signal that is related to the software activity, enabling the exploitation of this characteristic to set up a unidirectional covert channel. In [15], the RF radiation of video cables (VGA, DVI, HDMI) is precisely controlled by a malware in order to produce a FM modulated signal which can be intercepted from several meters away from the target. The proposed proof of concept involves an FM receiving smartphone as the untrusted compromised IS to which the data is exfiltrated. Some internal components or wires can also be used as an antenna to send modulated data over the air. It has been proposed in [16] to use the offhook switch wire of compromised IP phones as an antenna to radiate RF signals and thus create a unidirectional covert channel for data exfiltration.

The physical characteristics of the environment of the target can also be an interesting physical layer vector for transporting

data both from or to the target. Data transmission using light is a well-known technique (optical fiber, Li-Fi). For data exfiltration, the target can modulate a signal on light sources it controls, such as the video display or the many LEDs that are available on both the computer and its peripherals (e.g. keyboard). If smart light sources (e.g. network controlled smart light bulbs) can be controlled by one of the compromised entities, they can also be used as a communication channel. On the other side, a light sensor or a video camera can be used to receive the signals. It is proposed in [17] to use the room's temperature to communicate. In the proposed scenario, the attacker can control the air conditioning and heating system of the room the target is. Exploiting that, it has been demonstrated that the target computer can then monitor the temperature reported by its internal sensors and retrieve the data, resulting in a very low bandwidth covert channel.

In the next section, an alternative approach based on a smart use of IEMI and resulting in a unidirectional air gap bridging covert channel is proposed.

III. DESIGN AND EXPLOITATION OF A COMMAND AND CONTROL SYSTEM

Many studies have been devoted to the analysis and the classification of failures induced by parasitic field on information systems. One of the main contributions is related to the hardening of electronic devices to improve the resilience of critical infrastructures and systems to intentional electromagnetic interferences (IEMI). Electromagnetic compatibility (EMC) and interference (EMI) communities have been working on parasitic coupling to and emanations from electronic devices considering threats such as electromagnetic perturbations. In addition, military research and information security communities have shown that EMC is a non-negligible threat for the confidentiality (related to TEMPEST and side-channels) as well as for the resilience and the integrity (related to IEMI) of electronic systems and processed information [18-21].

In recently published studies, it has been shown that DRAM design flaws could lead in privilege elevation on COTS computers due to bit-flip on the memory [22]. It can be pointed out that memory errors due to EMC were known by microelectronic designers for a long time. More recently, the use of specific signals to get access remotely to modern smartphones has been demonstrated [23]. These proof-of-concepts show that electromagnetic compatibility and electromagnetic interference threats could be considered by the information security community as TEMPEST already is.

During the last two years, we have been working on the classification of effects induced by IEMI on COTS computers from an information security perspective [24]. In fact, the operating system logs and the internal sensors of computers were monitored and processed in real-time during parasitic exposure. Some perturbations induced between the temperature sensor and the CPU were interestingly directly correlated to the parasitic field [24]. Electromagnetic fields induce parasitic currents and voltages on electronic devices. Abnormal behavior of electronic devices in such circumstances is directly related to its susceptibility as defined by EMC. During our experiments, the communication between the analogue temperature sensor and the CPU was responsive to the electromagnetic waves. In this research, we propose to involve IEMI as a command and control system for an installed malware on a targeted computer through sensors responsive to IEMI.

A. *Principle hypothesis*

The main hypothesis considered in this study is as follows: if the temperature reading error is correlated to the field amplitude it should be possible to co mmunicate through a specifically crafted signal to generate and induce temperature reading errors related to the transmitted data.

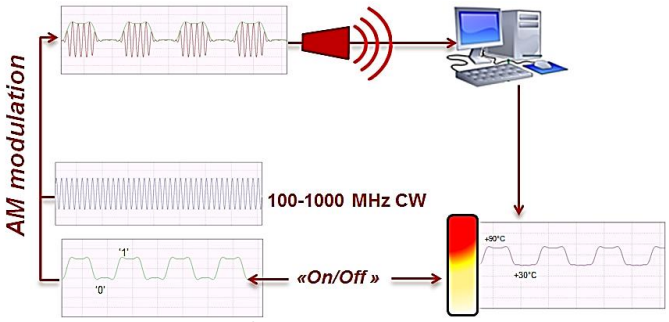

Figure 1: Simulation of the bit-transmission hypothesis using GNURadio [25].

A first simulation was performed using the GNURadio companion [25] signal processing software. A continuous wave is modulated with 2 level of amplitudes (AM for short): a low and a high level where the low level '0' is simulated with a null amplitude (source off) and a high level '1' is simulated with the maximal amplitude (source on).

The temperature sensor reaction itself was simulated as having a normal activity which consists in reading the real temperature T_{real} and reading a wrong temperature T_{pert} when the source is turned on. As it can be observed in Fig. 1, the amplitude modulation of a continuous wave allows to perform an inline coding of data through the temperature sensor reading activity. The next step is to test the temperature sensor and to experimentally evaluate the possibility of exploiting the reading errors thanks to parasitic electromagnetic field and using this phenomenon as a covert communication channel.

B. *Preleminary experiments*

For a validation purpose, we set-up the configuration depicted in Figs. 2 and 4. The tested computer was placed in a shielded room, namely a Faraday cage, in order to prevent any disturbances induced by the experiments in the public electromagnetic environment. A monitoring computer, placed outside the shielded room, was connected to the computer under test to have a direct access to the temperature reading error through a fiber optic link.

The signal generator used in the experiment is the software-defined radio Ettus USRP 1. A power amplifier was used in order to achieve field amplitudes higher than the susceptibility level of the communication bus between the temperature sensor and the motherboard CPU. Continuous waves (CW) in the 0.1-1 GHz frequency band were tested to get the optimal frequency

for improving the coupling efficiency. Results are summarized in Table I.

Frequencies above 1 GHz, which could also provide interesting results, have been tested. In the 1 GHz – 2 GHz frequency band, it has been observed that the targeted computers often shutdown when illuminated with parasitic fields. Thus, this working frequency band was not further investigated. Moreover, it is important to mention that the attenuation of the signal amplitude increases with this parameter for a given distance between the source and the target.

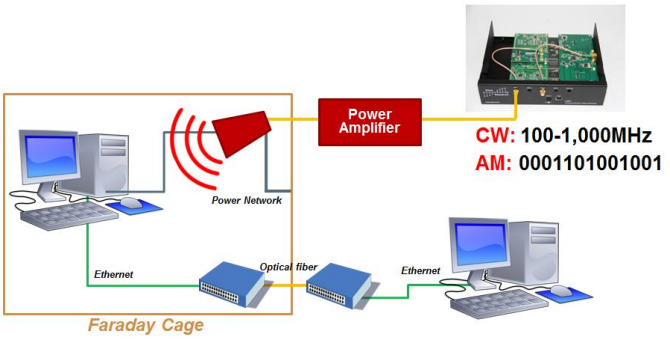

Figure 2: Experimental set-up for the radiated case.

The induction of an electric signal to the motherboard printed circuit board (PCB) resulting from an electromagnetic signal is called a back-door coupling [19] as the PCB is not designed to receive electromagnetic waves as opposed to antennas (defined as front-door coupling interfaces [19]). Moreover, the induced parasitic currents and voltages on the PCB can result from direct field to PCB coupling in the case of a radiated emission or from the propagation of electromagnetic waves along the cable networks (e.g. power lines or Ethernet cables). In order to have a clue on an efficient way to induce temperature reading errors on the computer, we tested the following configurations:

1) *Radiation case*: an emission antenna was placed inside the shielded room as shown in Fig. 2. It was observed that in this case the readings errors reach more than 60°C of dynamic range. In a real environment, the electromagnetic field topology around the target is directly related to the facility configuration in which computers are installed. In order to have a clue on the effects of random configurations of the electromagnetic field topology, the experiment was recently performed in a reverberation chamber [26]. It has been pointed out that the susceptibility of the communication bus is so high that the field topology has little impact on the possibility of inducing perturbations. Nevertheless, the reading errors dynamic for a full generation of the field topologies at low level is between +5°C and +60° above the real temperature which is clearly enough for bit modulation.

Table I: Temperature reading errors versus minimal required mean field strength and collateral effects

CW frequency (MHz)	Temperature reading error (°C)	Mean field strength required (V/m)	Additional effects
200	+5	35	no
	+25	81	Fan speed increases
300	+5	23	no
	+15	33	Fan speed increases Network interface down
	+25	65	Computer reboots
600	+5	31	no
	+25	50	Fan speed increases

In order to get access to the minimum field strength, a field probe was placed in several locations around the computer. The minimum mean field strength required to induce temperature reading errors is about 30 V/m (close to the limit field strength for the human safety).

In order to have a clue on the range between the targeted computer and the source for a given emitted signal power, the basic free-space propagation formula was used. In order to reach the target for a given distance, the mean powers required have been computed for a 7 dBi gain log-periodic antenna: the power required at 5 meters is 200 W and 3,100 W at 20 meters. Note that the use of higher gain antennas leads to the reduction of the required power. Nevertheless, the required signal powers are in good agreement with existing high power sources which could be used [27]. Furthermore, keeping the use of the software defined radio and a power amplifier, the form factor of the system can be deduced as represented in Fig. 3.

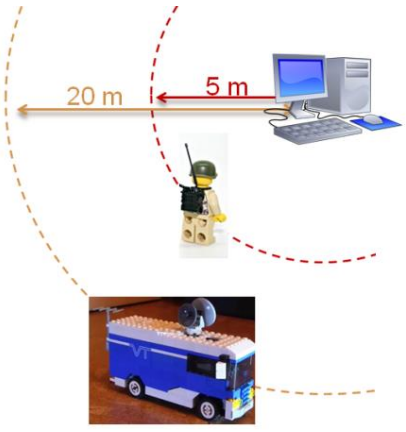

Figure 3: Risk analysis, range versus required emission power

In order to better evaluate the field attenuation in practical scenarios, tests should be performed on a real infrastructure [21] or simulation should be performed with 3D electromagnetic computation software or using more complex propagation equations.

2) *Conducted case:* an injection probe connected to a small power network is used as represented in Fig. 4. The dynamic of

the reading errors is between +5°C and +50°C above the real temperature which is again clearly enough for bit modulation. Considering the possibility of generating low frequency signals modulated in amplitude and the low attenuation of the conducted propagation of electromagnetic waves along the power network cables, it allows for enhancing the range between the source and the targeted computer.

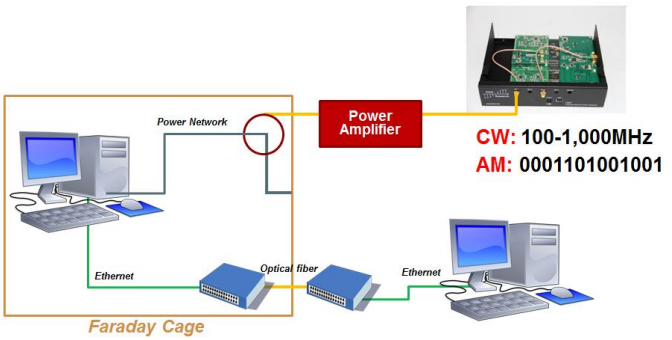

Figure 4: Experimental set-up for the conducted case

Nevertheless, the type and number of electronic devices connected to the power network have been shown to be a significant parameter as the quality of the conducted propagation of electromagnetic interferences along the power network is highly susceptible to this parameter. In order to evaluate the real feasibility of inducing system perturbations by direct signal injection, a large power network would be necessary. In this study, only the radiated case will be considered.

C. *Channel coding and data transmission*

It was shown in the experiments that the main hypothesis is validated experimentally. Based on the possibility of inducing reading errors on the temperature sensor we created a proof of concept receiver. In order to set-up a mono-directional communication link between the computer under test and the source, a basic malware was implemented which monitors the temperature level provided by the sensor chip enclosed in the computer of the trusted IS. It is assumed that the communication link between the trusted IS computer and the untrusted IS computer could be designed by one of the techniques summarized in Section 2.

Considering that a high level of emitted signals introduces temperature reading errors and that the temperature is decreasing instantaneously when the source is stopped, the continuous wave signal is modulated using a 2-ASK scheme. A 0-symbol means that no RF field is emitted and a 1-symbol means that a RF field is radiated.

As the time needed to query sensors isn't constant, the sampling of temperature has some jitter. To immunize the decoder against de-synchronization, we use a Manchester coding method. Manchester coding makes clock recovery easier because there is a transition for each bit transmitted. The clock must have a frequency twice higher than the bit-rate and the bit sequence is *XORed* with the clock sequence. As a consequence, the clock is included in the signal with the data.
In order to start the recording and the decoding of the sent commands, we encapsulate the data with a preamble. The chosen preamble is a Barker [28] sequence of 7 bits, like in the Bluetooth [29] protocol, prepended by a 0 bit which gives the bit sequence "01110010". The Barker sequence has good auto-correlation properties and thus facilitates the detection of starting packets. Then, we append the size of the data payload to let the decoder determine when to end the sampling. The frame composition is shown in Fig. 5.

Offset in bits	0	8	16	N*8+16
Content	Preamble	Size (N)	Data	

Figure 5: Format of the frame before Manchester coding

The demodulation consists in monitoring continuously the temperature reported by the sensors. The results are then continuously averaged. When the measured temperature is higher than 1.05 times the average, we consider it as a logical high. Otherwise it is a logical low. An example frame received by monitoring the temperature is shown in Fig. 6. Each level is then mapped to a symbol 0 (low) or 1 (high). Then, we simply need to monitor the symbol changes to correct the timing and recover the bits transmitted. The sampling rate needed to correctly decode the bits is four times the bit-rate: twice to isolate each symbol (according to Nyquist-Shannon sampling theorem) and twice to decode Manchester and get bit sequence.

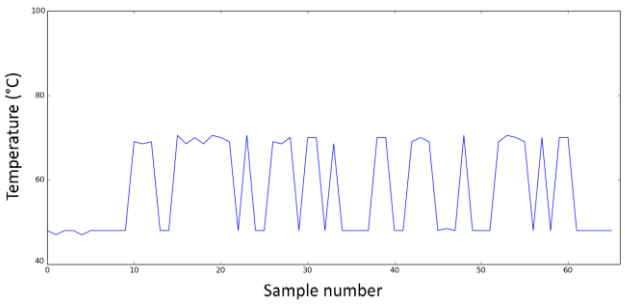

Figure 6: Received signal by monitoring the temperature

As soon as it detects a modulated IEMI with the defined mask of bits, it parses it and executes the payload transmitted by the attacker as a Linux shell command. An example of a signal recorded by reading the temperature is represented in Fig. 6. The bit-rate is related to the hardware time constraint for accessing the temperature sensor measurement. A value is obtained each 100 ms and we used 4 measures for one bit in order to prevent decoding errors. Based on the last considerations, it has been observed experimentally that the bit-rate can reach 2.5 bits/s which is sufficient to communicate with the malware as well as to update it. The optimization of the transmission rate has not been further explored in this research.

IV. COUNTER-MEASURES

As pointed out in Section II, using air gaps to physically isolate sensitive IS from untrusted IS is a good security practice. However, like any other security defense technique, air gaps have limitations and can be bypassed, depending on the context and the considered attacker profile. Indeed, under certain circumstances, it has been shown that air gaps can be bridged in several ways, mostly consisting in a malware infection of both sides of the air gap followed by the exploitation of one or several covert communication channels. In this section, a discussion about some countermeasures and good practices is

proposed. As can be expected, the countermeasures aim to prevent the malware infection and the establishment of covert channels.

The first main class of countermeasures concerns the malware infection. Thus, the classical technical and organizational good practices to prevent and detect malware shall be applied. Ideally, the sensitive isolated IS shall not have interactions directly or indirectly with untrusted IS. It is also possible to use sanitization machines for legitimate data transit and inspection, but with data exchange comes risk. This class of measures has been widely investigated during the last twenty years and many reference guides and tools are available for further information.

The second class of countermeasures aims to increase the difficulty to establish a covert communication channel. Depending on the physical phenomenon the communication relies on, several countermeasures allowing prevention or detection can be considered. First, in order to reduce the attack surface, the unnecessary built-in communication interfaces shall be physically removed from the devices from the sensitive isolated IS. For radio frequency communications, using TEMPEST proof devices for sensitive IS can be a good start. These devices are generally better shielded and are supposed to guarantee that the electromagnetic emanations of their components cannot be intercepted from beyond a certain distance. Placing sensitive equipment in shielded racks or even better in Faraday cages can also prevent electromagnetic exchanges with an outsider [30]. To avoid conducted diffusion of the electromagnetic activity, filters can be placed in the power network to contain the spurious signals. The detection of covert channels using radio frequencies is a big challenge. Generally, a continuous monitoring of the radio spectrum is needed, along with artificial intelligence algorithms to identify discrepancies in the spectrum.

For covert channels involving IEMI, a detection solution based on the built-in sensors of the devices has recently been proposed [24, 31]. It consists in a continuous monitoring of the sensors (e.g. voltage, temperature and fan speed) and operating system logs and applying detection heuristics to detect abnormal electromagnetic activity around the target device. Part of this solution could also be used for the detection of the attacks based on sensor measurement variations, such as the room temperature modulation.

For communications relying on light and sound, it is possible to combine a good physical isolation and organizational processes. Devices belonging to the sensitive IS shall be placed in specific rooms, ideally without windows and with good phonic isolation properties. For preventing the reception of data through these channels, the corresponding hardware sensors shall be removed: video camera, sound card, microphone, IrDA interface…

V. CONCLUSION

Air gap is a technique that is commonly used for isolating trusted information systems from untrusted ones. Unfortunately, the security brought up by such a technique is generally overestimated. It has been shown that air-gaps limits can be overcome by a malware infection of the air gapped IS and by setting up covert communication channels between the trusted IS and the untrusted ones.

In this paper, a summary of known techniques to bypass air gaps was presented. A new method has been proposed relying on the use of intentional electromagnetic sources and exploiting the sensitivity to parasitic electromagnetic field of some built-in sensors in commercial-off-the-shelf computers. It has been shown that this technique opens a new way to set up a unidirectional covert communication channel between an attacker and a compromised air gapped computer, leading to an interesting way to command and control a malware installed on the air-gapped device.

In order to prevent the preliminary infection, several common techniques can be used like applying the state of the art of information security best practices. Technical and organizational countermeasures have been provided in order to prevent the communication link establishment. The need for additional monitoring systems has been highlighted in order to detect abnormal physical layer activities due to covert channel exploitation.

Finally, this study shows the main limitations of the air gap for information security. Covert channels are generally hard to detect and their prevention involves heavy physical and organizational measures. Additionally, the security brought up by air gaps can easily be circumvented if the technical and organizational best practices are not correctly applied. The huge constraints air gaps imply for the users in their day to day work can lead to small deceptive behaviors from legitimate users, who often assume that the isolation will be enough to support their deception. This shows that besides the technical and organizational measures that should be enforced for an air gap to be efficient, the education of the users is also mandatory to fully benefit from the security brought by air gaps.

REFERENCES

[1] NIST, National Supply Chain Risk Management Practices for Federal Information Systems, 2014.

[2] CERT-UK, Cyber-security risks in the supply chain, 2015.

[3] H. Okhravi, S. Bak, S. T. King, “Design, Implementation and Evaluation of Covert Channel Attacks”, IEEE International Conference on Technologies for Homeland Security, 2010.

[4] B. W. Lampson, “A Note on the Confinement Problem”, Communications of the ACM, pp 613-615, 1973.

[5] USB Implementers Forum, USB Device Class Definition for Human Interface Devices (HID), 2001.

[6] Video Electronics Standards Association, VESA Enhanced Display Data Channel Standard, 2004.

[7] Video Electronics Standards Association, VESA Monitor Control Command Set Standard Version 3, 2006.

[8] A. Davis, “HDMI – Hacking Displays Made Interesting”, BlackHat USA 2012.

[9] A. Kaufmann, B. Smus, “Tone: An experimental Chrome extension for instant sharing over audio”, Google Research Blog, 2015,

http://googleresearch.blogspot.fr/2015/05/tone-experimental-chrome-extension-for.html.

[10] S. J. O'Malley, K. K. R. Choo, "Bridging the Air Gap: Inaudible Data Exfiltration by Insiders", 20th Americas Conference on Information Systems, 2014.

[11] P. M. Ricordel, P. Capillon, Rump Session, Symposium sur la Sécurité des Technologies de l'Information et des Communications, 2014.

[12] D. Goodin, "Meet "badBIOS", the mysterious Mac and PC malware that jumps airgaps", Arstechnica, 2013, http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps.

[13] D. Genkin, A. Shamir, E. Tromer, "RSA Key Extraction via Low-Bandwith Acoustic Cryptanalysis", Advances in Cryptology – CRYPTO 2014.

[14] Y. Michalevsky, G. Nakibly, D. Boneh, "Gyrophone: Recognizing Speech from Gyroscope Signals", RSA Conference 2015, 2015.

[15] M. Guri, G. Kedma, A. Kachlon, Y. Elovici, "AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies", 9th IEEE International Conference on Malicious and Unwanted Software, 2014.

[16] A. Cui, M. Costello, "Hacking Cisco Phones", CCC conference 29C3, Hamburg, Germany, 2012.

[17] M. Guri, M. Monitz, Y. Mirski, Y. Elovici: "BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations", online: http://dblp.uni-trier.de/rec/bib/journals/corr/GuriMME15, 2015.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] M. Seaborn, with contributions by T. Dullien, "Exploiting the DRAM rowhammer bug to gain kernel privileges", online: http://googleprojectzero.blogspot.fr/2015/03/exploiting-dram-rowhammer-bug-to-gain.html, March 9, 2015.

[23] C. Kasmi, J. Lopes Esteves, "You don't hear me but your phone voice interface does", Hack In Paris 2015, Paris, France, 2015.

[24] C. Kasmi, J. Lopes Esteves, M. Renard, "Automation of the Immunity testing of COTS computers by the instrumentation of the internal sensors and involving the operating system logs – Technical report ", System Design and Assessment Note SDAN 044, November 2014.

[25] GNU Radio is a free & open-source software development toolkit, online: http://gnuradio.org/redmine/projects/gnuradio/wiki, 2015.

[26] V. Houchouas, C. Kasmi, J. Lopes Esteves, D. Coiffard, "Experimental comparison of mode-stirrer geometries for EMC", In Proc. of ASIAEM 2015, Jeju, South Korea, 2015.

[27] N. Mora, F. Vega, G. Lugrin, F. Rachidi, "Study and classification of Potential IEMI sources", System Design and Assessment Note SDAN 041, July 2014.

[28] R. H. Barker, "Group Synchronizing of Binary Digital Sequences". pp. 273–287, Communication Theory. London: Butterworth, 1953.

[29] Bluetooth SIG, Bluetooth Specification Version 4.0, 2010.

[30] Agence Nationale de la Sécurité des Systèmes d'Information, Instruction Interministérielle N°300 relative à la Protection contre les Signaux Compromettants, online : www.ssi.gouv.fr, 2014.

[31] C. Kasmi, J. Lopes Esteves, "Automated Analysis of the Effects induced by Radio-Frequency Pulses on Embedded Systems for EMC Functional Safety", URSI AT-RASC Conference, Spain, May 2015.