Cyber-Attacks Based in Electromagnetic Effects

M. B. Perotoni, R. M. Barreto and S. K. Manfrin

Abstract— **This article covers eavesdropping on computer and auxiliary data communication equipment by means of hardware, namely unintended electromagnetic emanations. The physical basis that underlies the process is covered, alongside with a canonical electromagnetic simulation. Some known cases of these exploits are covered, and real world examples of a leaking coaxial cable and a shielding conductive sheet are measured in the laboratory, with results relate to the data protection and its implications. The measured shielding effectiveness of the sheet proved to comply with usual Tempest requirements.**

Keywords— **Shielding, Electromagnetic Compatibility (EMC), Information Security.**

I. INTRODUCTION

SECURE communication is a theme that concerns almost everyone who uses emails, makes phone calls or even browses news on Internet on a regular basis. The confidentiality of these mundane activities, almost taken for granted in the beginning of the Internet era, is a foregone recall. Back then, the only concern for the majority of ordinary users was credit card passwords theft, when shopping online – nowadays much more sophisticated schemes are being used to steal and decode information, not only from individual hackers, but also by official government agencies. Emails, phone calls, history of the visited pages– all these data can be gathered and analyzed by third parties elsewhere, making daunting the confidential exchange of information.

Though these eavesdropping activities are usually related to software (Trojan horses, back door exploits, suspicious emails hiding executables, etc), the existing hardware and infrastructure also provides information windows from where data can be stolen. These infrastructure and hardware exploits, so far, require more sophisticated means to be implemented, therefore are not accessible to delinquent teenagers living next door. Though harder to implement, due to the both higher technical expertise required and more expensive pieces of equipment necessary, they are at the same time harder to detect and to prevent, partially due to the fact they are yet unbeknownst to most people and corporation IT sectors. These complicated requirements make cyber-attacks based on hardware and infrastructure more focused on corporate targets, rather than ordinary internet users. Usually they focus on valuable information theft (IP, intellectual property), kept in confidentiality due to the relevant financial or industrial impact, for instance.

This article deals with some ways by which attacks based on infrastructure and hardware are implemented, and the solutions that can be employed to prevent it. Naturally most information is kept disclosed from the public literature; therefore much of it cannot be checked or tested. The field is still on its development, with many tools yet to be widespread. Regardless, the means to implement such attacks are already available in the market.

II. PHYSICAL BACKGROUND

Any data or signal that is carried by a guided medium (for instance a wire, cable or PCB – Printed Circuit Board- trace) acts as source of unintended electromagnetic emission.

Though a single wire can be seen as self-contained element that is used to transport an electric current between two points, it also operates as a radiator (antenna). Electromagnetic (EM) waves arise whenever there are accelerated charges [1,2], according to the Larmor Formula [3] . As Fig. 1 shows, an infinite wire is not radiating, but if it is made finite (by truncating one of its ends), radiation arises, due to the fact that the carrier velocities drop abruptly to zero at the finite end. By the same token, a change of direction on the wire results on acceleration as well (since acceleration is a vector quantity) – the more acute the angle the more efficient is the radiation, as Fig. 1 illustrates. The rationale for implementing a cyber-attack based on this effect is that the radiated signal bears a relevant resemblance with the original signal, therefore by remotely capturing this EM wave one is able to reconstruct the original data.

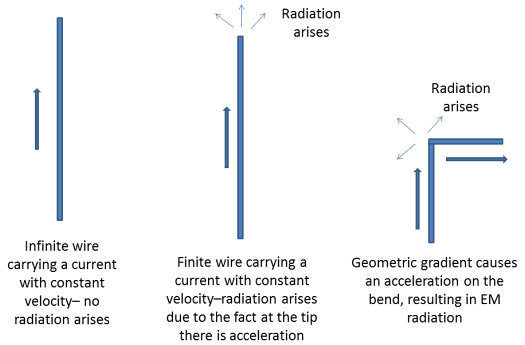
Radiation arises
Radiation arises
Infinite wire carrying a current with constant velocity– no radiation arises
Finite wire carrying a current with constant velocity–radiation arises due to the fact at the tip there is acceleration
Geometric gradient causes an acceleration on the bend, resulting in EM radiation

Figure 1. Pictorial examples of radiation arising from accelerated charges.

M. B. Perotoni, UFABC, Santo André, SP, Brasil, marcelo.perotoni@ufabc.edu.br
R. M. Barreto, QEMC Consulting, Rio de Janeiro, RJ, Brasil, roberto.menna@qemc.com.br
S. K. Manfrin, UFABC, Santo André, SP, Brasil, stilante.manfrin@ufabc.edu.br

Real world circuitry and equipment are more complicated than the straight wires from Fig. 1. Fig. 2 depicts EM simulations carried on with CST MICROWAVE STUDIO® [4], a 3D field solver which here employed its TLM (Transmission Line Method). It consists on a simple trace printed on PCB (FR-4 material, 1 mm thick, dielectric constant 4.9), excited by a generator and terminated with a 50 Ω load. Two scenarios were evaluated: the bare PCB and with the Plexiglas (chosen only for the sake of similarity with common used materials) enclosure.

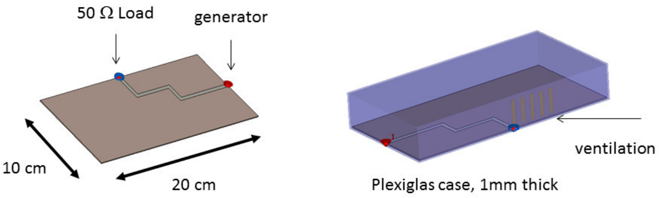

Figure 2. Simulated models to evaluate the radiation from a copper trace (bare board and with a case).

The system shown in Fig. 2 was excited with a rectangular pulse in the generator end (Fig. 3). Fig. 3 shows additionally the electric field captured at 3 meters from the board (the curves had their amplitudes normalized to ease the visualization).

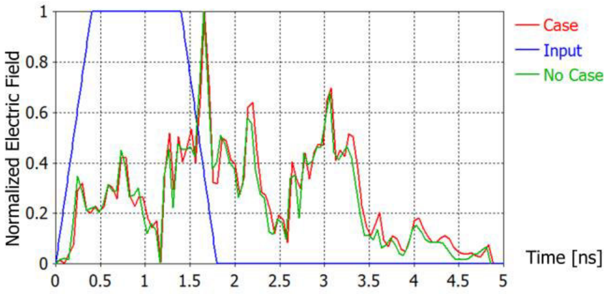

Figure 3. Normalized time response of the input signal on the trace (blue curve) and the electric fields measured at 3 meters distance from the equipment under test – for both scenarios.

Some conclusions can be drawn from the numerical simulations presented in Fig. 2:

- There is no significant difference whether a plastic case is used or not; their maximum amplitudes differ only 12% in the worst case. That means, the plastic case does not provide a relevant attenuation to the radiated signal. Other materials could be used, for instance plastic mixed with Carbon Black, which presents higher attenuation for electromagnetic waves [5];
- near field coupling effects (and consequently radiation) increase with the frequency, therefore signals with shorter rise times and higher repetition rates (which are generally associated with high data rates) are more prone to radiate and get captured elsewhere. It can be seen on the fields computed at 3 meters from the system; both in time (Fig.3) and frequency (Fig 4) domains;
- the comparison between the original and radiated signals power spectrums is shown in Fig. 4. It can be seen that the original signal has energy spread up to 2 GHz (limit where the power fell by approximately 40 dB). And the resemblance among the spectra is larger as the frequency increases – lower frequencies are poorly radiated, therefore the information is lost. However a remote pulse reconstruction based on the captured electric field could be implemented using filters (as a first order analysis a kind of low pass filter) to compensate for the channel frequency response.

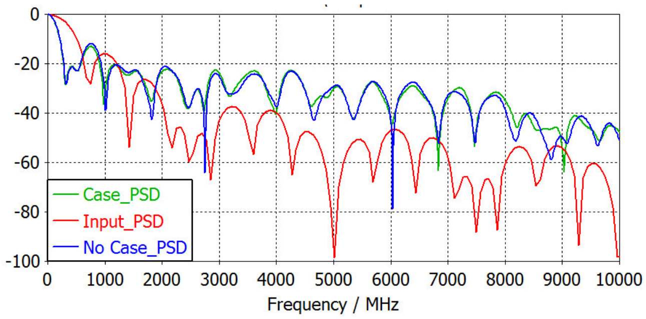

Figure 4. Power spectrum densities (PSD's) of the input and radiated signals.

III. A BRIEF INTRODUCTION TO ATTACKS

This section covers some known examples where attacks are performed exploring infra-structure fragilities. It is not an exhaustive list, but it pinpoints some typical examples where these physical fragilities can be explored.

A. Laser Bouncing on Windows

If a meeting is taking place in some closed space, the sound waves resonate and propagate inside the area. Upon hitting the windows, the same sound waves make the glass structure vibrate, similarly to loudspeakers. Though these mechanical vibration on the glass presents very low amplitudes, if a laser bounces the window its amplitude will be modulated with the same time pattern as the one from the conversation (as Fig. 5 shows). A receiver located outside needs only to demodulated the backscattered beam to recover the information. Since lasers can be made invisible, the technique is almost impossible to be detected.

A simple way to avoid this technique is the use of curtains, possible made of heavy cloth, as to damp the acoustic waves before they hit the window. This technique was allegedly used to discover first the new Popes name, Francis, back in 2013.

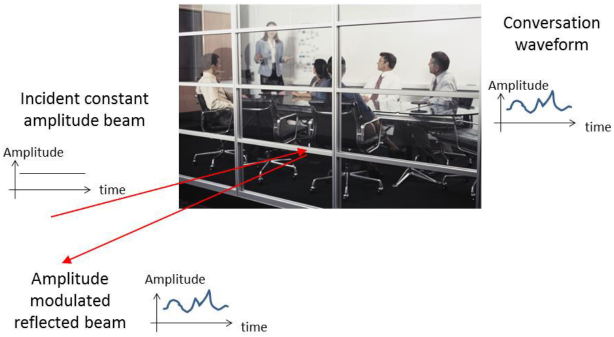
Conversation waveform
Amplitude
time
Incident constant amplitude beam
Amplitude
time
Amplitude modulated reflected beam
Amplitude
time

Figure 5. An incident constant amplitude laser beam is modulated as it backscatters the glass window.

B. *Electronic Bugs*

The use of electronic bugs is known since the beginning of the electronic era. They basically have the ambient sound modulating a carrier which in turn is wirelessly transmitted. They might be hidden in telephone sets, portraits, small gifts received by the subject etc. Since electronics became more and more advanced and present in everyday gadgets, so does increase the possibilities to tap conversations. Nowadays it is virtually impossible to guarantee that a conversation is kept secret, since electronics can be even implanted inside human bodies [6,7].

Though in the past conversations carry a lot of relevant information, nowadays access to data stored in computers or transmitted by email is much richer – it can convey blueprints of industrial projects, strategic or financial decisions. Therefore the use of electronic bugs became less important in the arsenal of the contemporary espionage.

Electronic bugs can be traced and located by searching for their wireless signal (carrier). Since the signal amplitude becomes stronger closer to the bug, a directional antenna plugged into a tuned field strength meter can help find them. Other alternative is the use of jamming, where a high amplitude broadband noise source overpowers eventual hidden transmitters in an area. It is the principle behind Mobile phone jammers, commercially available.

C. *Hardware with hidden exploits*

Microprocessors are present in almost any mass consumer equipment. Currently, due to their lower production prices, most of the commercial microelectronics manufactures are based in Asia, whereas the design is still partially kept on Western countries [8,9]. Their small sizes and high complexity make almost impossible to get them checked after the purchase, so the consumers and final users have to rely on their internal content. Indeed they are nice targets to be used as a vector to steal information by means of Trojans and Backdoors implemented inside them [10]. One documented case is presented by a group from Cambridge [11] which found backdoors in a commercial FPGA (field-programmable gate array) chip specifically targeted for military and industrial applications. Ironically, the chip manufacturer states that "*low power flash devices are unique in being reprogrammable and having inherent resistance to both invasive and noninvasive attacks on valuable IP*" [12].

The use of counterfeit chips is hard to be repressed, due to their large volume and small sizes. In 2010 two men were caught with 13,000 fake chips imported from China, having common brand names on it (like Intel, AMD and National Instruments) [8]. One of the purchasers of such batch was the US Navy.

The New York Times reported that during an Israeli air raid on Syrian nuclear laboratories their anti-aircraft defenses were temporarily disabled by a "kill-switch" feature that had been surreptitiously introduced by Israeli intelligence [13].

Given the extreme sensitivity that microprocessors impose into the data security realm, chip design and manufacture is considered a national security issue for critical applications. Brazil has its own secure microprocessor designed and produced so that it can be used in highly secure and critical applications, like defense, financial transactions and also powering the electronic voting machines [14,15]. Naturally, the complete design of a microprocessor is a costly and long endeavor, which demands continuous investment and a highly specialized workforce, not easily achieved by any country.

D. *Infrastructure and Data Center exploits (TEMPEST)*

As stated before, any current circulating in a conductor generates magnetic fields. Though common Kirchhoff laws do not cover electromagnetic emanations [16], there is always an electromagnetic wave associated with time-varying electric currents (accelerated charges produce electromagnetic radiation). Therefore the information encoded in an electric current running in wires or printed circuits is not fully guided and contained by the medium, it is also free to propagate as a wave. That means that normal wires, cables and printed circuit traces can also be seen as antennas, normally ineffective but still radiating part of the energy. By gathering this emanation it might be possible to reconstruct the original data content.

In order to illustrate the leaking problem, Fig. 6 shows the measurement setup (inside an anechoic chamber) of 1.2 m long standard RG-58 cable, terminated with a matched 50 Ω as to avoid reflections and stationary waves. The cable was excited by a signal generator (from 20 MHz to 1 GHz), with 10 dBm power, and a broadband antenna captures the leaked electric field at a distance of 2.7 m. Fig. 7 shows the received power for two scenarios: with both ends grounded (connection between the shield to the ground plane) and floating. It can be seen that the simple act of connecting the metallic shields from both cable ends to the ground plane helps reduce the emissions in most frequencies across the band.

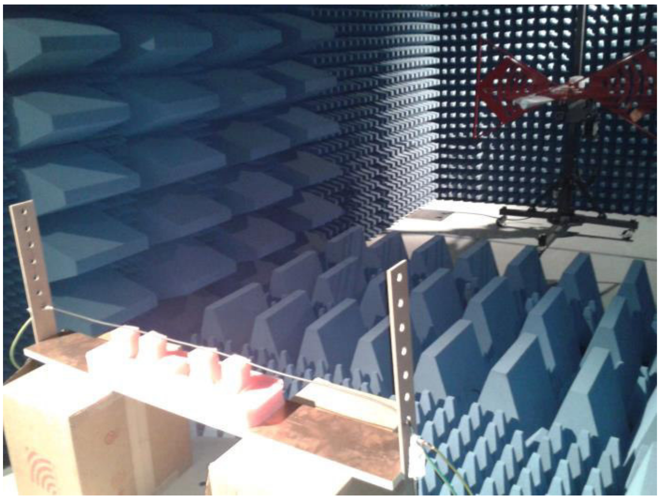

Figure 6. RG 58 over a ground plane, matched. The electric field that leaks from it is captured at distance, with a broadband antenna.

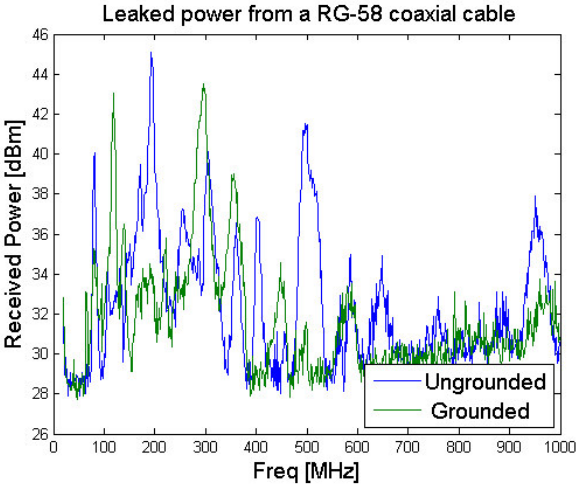

Figure 7. Received power on the antenna, for two different cases: with and without connection to the ground plane.

TEMPEST is a codename established by the US Department of Defense (DoD) Agency in 1974 to address eavesdropping based on leaking emanations, unintentional radio or electrical signals [17]. The code stands for "Telecommunication and Electronic Material Protected from Emanating Spurious Transmission".

Cathode ray tubes (CRT's) were once commonplace as computer screens. They operate based on an electron beam made to sweep a phosphor-based screen. The electron beam is deflected, focused and directed by means of high voltages and magnets (yokes). In order to synchronize transmission and reception, the frequencies by which the beam was made sweep the screen was fixed (15.734 kHz for TV). Since there were high amplitudes involved in the accelerated beam voltage (typically 20 kV), proportional high fields were also generated. By means of decoding these fields (both at fundamental or harmonics) it was possible to reconstruct, at distance, the same image seen on the eavesdropped TV set (as shows Fig. 8). Van Eck [18] in 1985 published a comprehensive and seminal paper on such apparatus, where with a directional antenna, a TV receiver and tuned circuits housed in a van he was able to gather and reconstruct signals from a nearby TV set located inside a building. Modern similar techniques were also applied to normal flat screen monitors, based on the same principle of focusing on the fixed frequency synchronization signals [19]. Common contemporary monitors have adopted the raster scan method, where each line is swept at a time. Therefore the picked signal should be the analog RGB information, not the digital complex image transmitted from the graphic board to the monitor – an approach that required only a broadband scanner and a dipole antenna to reconstruct the image generated by a video signal.

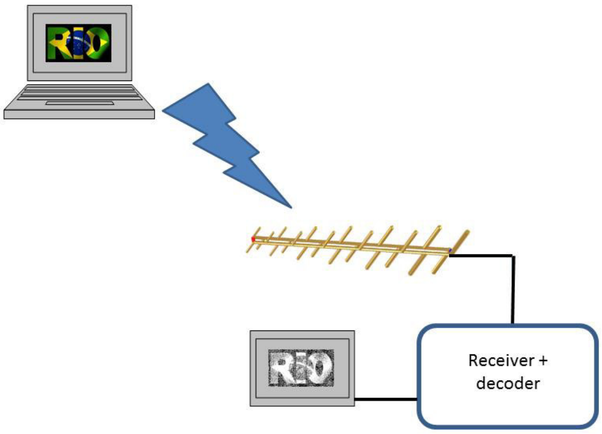

Figure 8. Basic elements to decode the leaked information from the monitor.

In addition to monitors, keyboards can also have their keys stroke remotely detected, since to each one is assigned a different code [21]. One found countermeasure consists on assigning each key a code defined by a cryptographic routine [22].

One more sophisticated way to countermeasure the information gathered through the monitor electromagnetic leakage is jamming. In [23] a circuit was enclosed in a box connected to a laptop by the USB port. It receives tracing information from the monitor RGB signals and adds jamming signal in frequencies where the emanation occurs. The artificially polluted signal is then back-fed into the laptop as a common mode voltage, and it turns out radiated by the laptop with the same mechanism as the normal information, making the eavesdropping harder.

Since most equipment is fed by AC mains, the connection to power chords is a viable vehicle to where information can be extracted. In this case, the information is not radiated, but conducted [16]. Power analysis is the name given to techniques that try to guess cryptographic keys by statistically observing power magnitude fluctuations from the target computer [24]. Magnitude fluctuations can be analyzed both in single and in differential mode, the latter conveying much richer information about the binary transitions inside the CPU [25].

The standard measure to tackle unintended leaked emissions from data equipment is shielding [26]. Operating similarly to Faraday cages, a metallic enclosure will block radiation from sources within its volume. Though simple in concept, enclosing a complete data center in a metallic box is a daunting task. Even a single computer is hard to be completely enclosed in a metallic case, since it requires cabling inlets and ventilation holes. Therefore the shielding has to be used in a smart way, in such a way it provides an adequate shielding to the fields. The shielding the metallic layer provides prevents electric fields from propagating, but low frequency magnetic fields are still allowed to go through.

Filtering can also be used to reduce the emission levels [27]. By allowing the passage of only a limited frequency range, the detection of harmonics whose higher frequencies are more effectively radiated from cables and circuits can be made harder.

So in order to reduce the unintended radiation from data centers, the following procedures can be taken:

- use of metallic layers to block the EM waves generated by screens, keyboards and other elements;
- use of power chords with filters and shields;
- cables, connectors and jacks made with higher isolation rates.

An adequate protection of a data center demands a thorough analysis. To evaluate the performance of the shielding, there are three different levels of Tempest protection, according to the respective NATO regulation [28]; A, B and C, with decreasing levels of shielding from both conducted and emitted radiation. Solutions provided from industries refer to these aforementioned different levels as parameters.

E. HIRF (High Intensity Radiated Fields)

Historically, after the first nuclear detonation test in 1940 it was noticed that the monitoring electronic apparatuses based on semiconductors (then a brand new technology) were destroyed, not due to the blast, but because of the intense electromagnetic wave originated after the explosion [16], phenomena currently named HIRF. It aroused the interest on the unintended radiation effects on systems that may not properly operate. In 1978 the first open conference focused on the theme took place (named Nuclear EMP Meeting), as well as a publication followed on the subject [29]. Particularly electromagnetic effects due to nuclear explosions are treated by the acronym NEMP (Nuclear Electromagnetic Pulse), and nowadays, studies regarding it are carried out mainly based on simulations, considering that the last high altitude nuclear test detonations took place in 1963. Waveforms of typical pulses caused by NEMPs are known, some in the open literature, some to restricted applications [30], and they are similar to the ones used by lightning discharges, though with spectra reaching higher frequencies (NEMPs around 300 MHz whereas lightning reaching barely 10 MHz). The very first analytical waveform concerning a NEMP was proposed in 1963 by Bell Labs , whose rise time was 4.6 ns and maximum electric field amplitude of 50 kV/m [31], presented in Fig. 9.

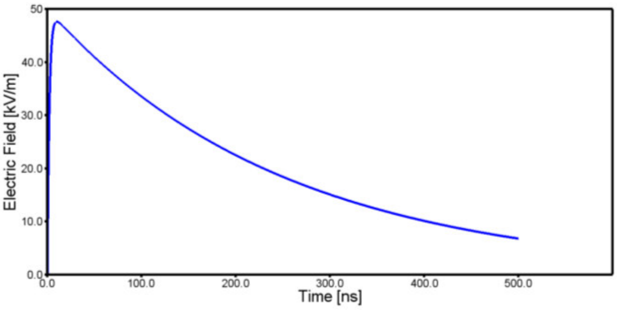

Figure 9. Analytical waveform of the Electric Field developed after a nuclear explosion in high altitude, according to Bell Labs [31].

Physically, the high amplitude electromagnetic fields generated by the nuclear blast propagate at the speed of light, and reach electronic circuitry and systems almost instantly. Induced voltages may eventually burn integrated circuits, effects that can even make planes in nearby areas crash due to lack of electronic flight control. The major defense against HEMP and HIRF is shielding and radiation hardening components, mainly integrated circuits. High impedance devices, such as CMOS, of widespread use due to their low cost and good performance in integrated circuits, are particularly sensitive to this incoming high amplitude electric fields, and should therefore go through a hardening process if they are intended to be made robust against NEMPs (for instance in missiles or jet planes supposed to fly over combat zones).

Though NEMPS and HIRFS are not meant to explicitly steal data and eavesdropping, they can block and turn inoperative large communication areas, including power distribution and transmission systems, causing havoc by destroying the existing infrastructure.

IV. SHIELDING CLOTH EVALUATION

The main counter measure against attacks based on Tempest or other similar emanation-based techniques is shielding. There has been considerable investigation in sheets and cloth operating as shielding materials, with carbon often used as a component, in the format of graphite [32], Carbon nanotubes and polymer composites [33] and also graphene-based sheets [34]. Copper wires inserted into a cloth made of Polypropylene and fiberglass is also used [35], also with evaporated silver and polypyrrole –both conductive – into a plastic fabric [36]. Shielding a room requires metallic sheets on the walls, floor and ceiling, with appropriate soldering and seaming, which is an expensive and complicated task that demands trained workforce and sophisticated instrumentation to certify its performance. An alternative is the shielding cloth or sheet – fabrics with metallic parts embedded, that provide an easily deployed and light weigh surface, able to be quickly deployed on normal and temporary spaces (such as field data centers).

A sample of such shielding cloth was investigated, from Soliani EMC s.r.l. [37]. It is a polyester sheet impregnated with metallic particles, such as Nickel, and does not present visually any difference to other types of clothing. The fabric was placed between two rectangular loop wire antennas, each with 17 cm length. Fig. 10 shows the antenna in front of the fabric and Fig. 11 the antenna measured reflection loss in dB (S11 parameter). This method is based on the IEEE Std. 299-1997, specifically aimed to Shielding Effectiveness Measurement of Enclosures[38].

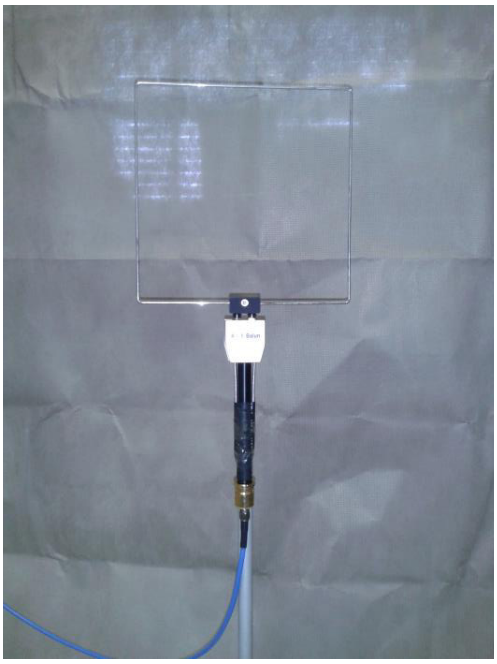

Figure 10. Quad Loop Antenna used to address the shielding effectiveness of the fabric, seen on the background.

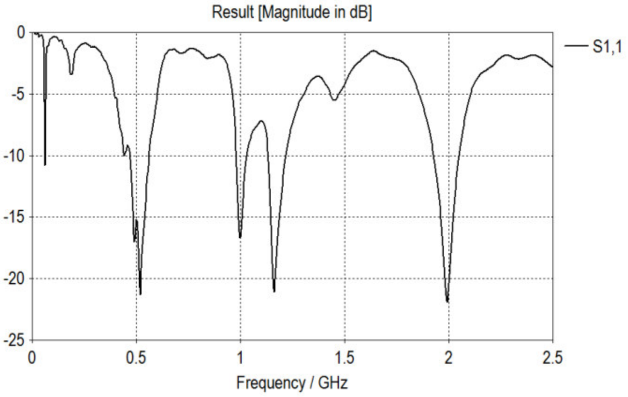

Figure 11. Quad Loop Antenna S11 measured response.

This specific antenna is chosen to investigate the cloth shielding around 500 MHz, which according to Fig. 11 is the resonant frequency of the antenna. The available sheet had its performance indicated for frequencies up to 1 GHz, therefore well within the antenna operating range.

The two similar quad loop antennas were placed 70 cm apart, and their transmission scattering parameter S21 (equivalent to the power transmission factor of both) was measured in two conditions: with and without a shielding sheet placed at mid distance, as Fig. 12 shows. The measurement was performed outside of an anechoic chamber, so there were reflections on the pieces of furniture, ceiling and further objects, and the covering was not perfect (due to the limited sample fabric width).

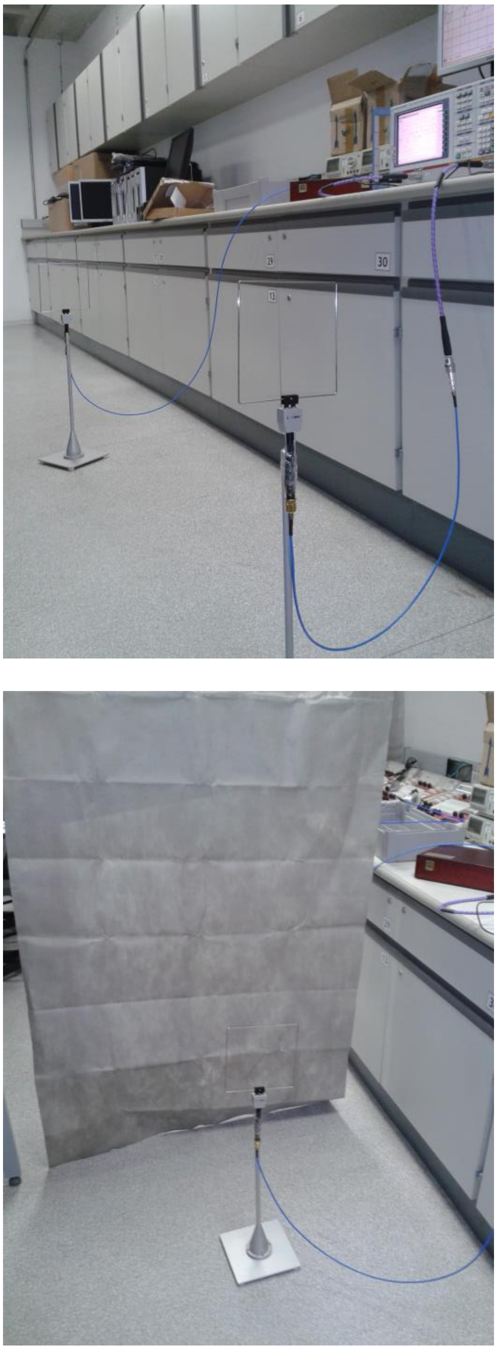

Figure 12. Two measured scenarios: (top) direct transmission and (bottom) with the conductive sheet.

Fig. 13 shows the measured shielding effectiveness of the sheet, based on the difference of the S21 parameter for the two scenarios. It was considered the frequency range of the 300 MHz to 700 MHz, around the center resonant antenna frequency. Since the measurement covers a broad band, eventual emissions from a computer, for instance, are covered by the measurement. It can be seen that at the frequency where the antenna resonates the nominal attenuation is larger than 50 dB, a high value but yet insufficient to be used as protection against Tempest attacks – the usual assumed safe Shielding Effectiveness is 100 dB, according to the NSA-65-6 [39], value normally achieved only with large solid metal plates. The cloth provides, though, a quick and transportable way to offer protection to sites temporarily located in areas where a complete shielded room is not available or too costly.

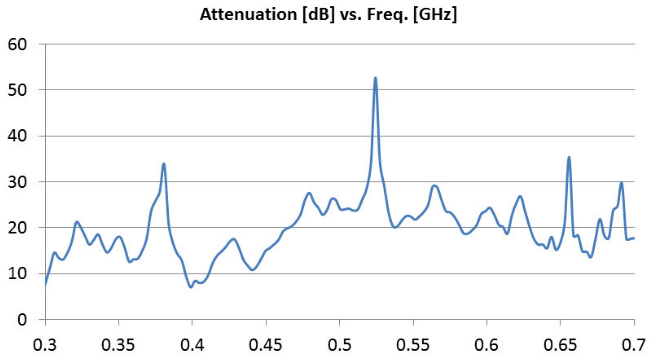

Figure 13. Measured attenuation of the conductive shielding sheet.

V. CONCLUSIONS

The article covered some formats of Cyber-Attacks based on hardware, mostly the ones that are based on eavesdropping taking advantage of unintended electromagnetic emanations from the data sources, as well as the effects caused by nuclear bombs detonation at high altitudes. A survey of some attacks are presented, alongside with simulations of measurements that show the basic nature and underlying principles involved. A sample of shielding sheet is measured and had its performance evaluated, which proved to provide a simple and light way to prevent this sort of attacks.

VI. ACKNOWLEDGEMENTS

The authors thank Mr. Maurizio Rizzati, from Soliani EMC, for kindly providing the sheet samples that were subjected to the measurement.

This article is included within the larger RENASIC Project, this one particularly named IT Critical Installation Security, and it has been conducted by Roberto M. Barreto, from QEMC, Engineering, Quality and Electromagnetic Compatibility Ltda, and Prof. Marcelo B. Perotoni.

REFERENCES

[1] Z. Popovic, B. D. Popovic, “Introductory Electromagnetics”,Ed. Prentice Hall, New Jersey, 2000.

[2] D. Halliday, R. Resnick, J. Walker, “Fundamentals of Physics”, Ed. Wiley, 9th Edition, 2010.

[3] J. D. Jackson, “Classical Electrodynamics”, Ed. John Wiley, 2nd Edition, New York, 1975.

[4] CST STUDIO SUITE EM simulation software, v.2015, www.cst.com.

[5] Q. H and M. S. Kim, “Electromagnetic Interference Shielding Properties of CO$_2$ Activated Carbon Black Filled Polymer Coating Materials”, Carbon Letters, Vol. 9, No.4, Dec. 2008, pp. 298-302.

[6] K. Y. Yazdandoost , R. Kohno, “Wireless Communications for Body Implanted Medical Device”, Proceedings of Asia-Pacific Microwave Conference 2007, pp.1-4.

[7] M. Balouchestani, K. Raahemifar , S. Krishnan, “Wireless Body Area Networks with Compressed Sensing Theory”, Proceedings of 20121 CME International Conference on Complex Medical Engineering, pp. 364-369.

[8] M. Bilzor, T. Huffmire, C. Irvine, T. Levin, “Security Checkers: Detecting processor malicious inclusions at runtime”, Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on, 2011.

[9] M. M. Farag, L. W. Lerner, C. D. Patterson,” Interacting with Hardware Trojans Over a Network”, 2012 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp.69-74.

[10] M. Tehranipoor, F. Koushanfar, “A survey on hardware Trojan taxonomy and detection”, IEEE Design and Test of Computers, 2010.

[11] S. Skorobogatov, C. Woods, “Breakthrough silicon scanning discovers backdoor in military chip”, Cryptographic Hardware and Embedded Systems – CHES 2012, Lecture Notes in Computer Science, Vol. 7428, 2012, pp. 23-40.

[12] Military ProASIC3/EL FPGA Fabric User’s Guide. Microsemi, 2011, http://www.actel.com/documents/Mil PA3 EL UG.pdf.

[13] J. Markoff. Old Trick Threatens Newest Weapons. New York Times, October 2009.

[14] R. Gallo, H.Kawakami and R. Dahab, “SCuP – Secure Cryptographic Microprocessor”, Proceedings of the XI Brazilian Symposium of Information Security and Computational Systems SBSEG 2011, 2011.

[15] R. Gallo et al, “T-DRE: a hardware trusted computing base for direct recording electronic vote machines”, Proceedings of the 26th Annual Computer Security Applications Conference, 2010, pp. 191-198.

[16] C. R. Paul, “Introduction to Electromagnetic Compatibility”, 2nd Edition, Ed.Wiley, 2006.

[17] A. Auddy and S. Sahy, “Tempest: Magnitude of threat and mitigation techniques”, Electromagnetic Interference & Compatibility, 2008. INCEMIC 2008. 10th International Conference on, 2008.

[18] W. van Eck: “Electromagnetic Radiation from Video DisplayUnits: An Eavesdropping Risk?”, Computers & Security, Vol. 4, pp. 269–286, 1985.

[19] C. Xiang and J. Xi, “A Method to Extract the Synchronous Characters in the Electromagnetic Information Leaked by a Computer”, 2011 4th International Congress on Image and Signal Processing.

[20] H. Sekiguchi and S. Seto, “Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Causing Information Leakage”, IEEE Transactions on Electromagnetic Compatibility, vol.55, No. 3, June 2013, pp. 547-554.

[21] M. Kinugawa, Y. Hayashi, T. Mizuki and H. Sone, “The effects of PS/2 keyboard setup on a conductive table on electromagnetic information leakages”, Proceedings of SICE Annual Conference, 2012, pp. 60-63.

[22] J. A. Ross and M. G. Kuhn, “Soft tempest – an opportunity for NATO”, Protecting NATO Information Systems in the 21st century (1999).

[23] Y. Suzuki and Y. Akyiama, “Jamming Technique to Prevent Information Leakage Caused by Unintentional Emissions of PC Video Signals”, 2010 IEEE International Symposium on Electromagnetic Compatibility (EMC), 2010, pp. 132-137.

[24] A. Arora, J. A. Ambrose, J. Peddersen and S. Parameswaran, “A Double-width Algorithmic Balancing to prevent Power Analysis Side Channel Attacks in AES”, 2013 IEEE Computer Society Annual Symposium on VLSI, pp. 76-83.

[25] P. Kocher, J. Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks”, Technical Report, 1998.

[26] S. Pennesi and S. Sebastiani, “Information security and emissions control”, 2005 International Symposium on Electromagnetic Compatibility, pp. 777-781.

[27] S. Sebastiani, “Characterization to a TEMPEST testing laboratory and methodology for control to compromising emanation”, 1998 IEEE International Symposium on Electromagnetic Compatibility, 1998, pp. 165-170.

[28] NATO SDIP-27 Standard.

[29] K. S .H .Lee, "EMP Interaction: Principles, Techniques and Reference Data", New York: Hemisphere, 1980.

[30] W. A. Radasky, "Review of unclassified HEMP calculations and analytic waveforms", NEM 1990 Record, p. 71.

[31] EMP Engineering and Design Principles, Bell Telephone Labs, Whippany, NJ, 1975.

[32] D. D. L. Chung, "Electromagnetic interference shielding effectiveness of carbon materials", Carbon, vol. 39, No. 2, 2001, 279-285.

[33] M.H. Al-Saleh and U. Sundararaj, "Electromagnetic interference shielding mechanisms of CNT/Polymer composites", Carbon, vol.47, No.7, 2009, pp.1738-1746.

[34] J. Liang et al, "Electromagnetic interference shielding of graphene/epoxy composites", Carbon, vol..47, No. 3, 2009, pp. 922-925.

[35] K. B. Cheng, S. Ramakrishna and K. C. Lee, "Electromagnetic Shielding effectiveness of copper/glass fiber knitted fabric reinforced polypropylene composites", Composites Part A: Applied Science and Manufacturing, vol. 31, No. 10, 2000, pp. 1039-1045.

[36] Y. K. Hong et al, "Electromagnetic interference shielding characteristics of fabric complexes coated with conductive polypyrrole and thermally evaporated Ag", Current Applied Physics, vol. 1, No. 6, 2001, pp. 439-442.

[37] Soliani EMC s.r.l., http://www.solianiemc.com/

[38] IEEE Std. 299-1997.

[39] MIL-HDBK-1195 Military Handbook Radio Frequency Shielded Enclosures, 1988.

Marcelo Bender Perotoni is from Porto Alegre, RS, Brazil. He holds an Electrical Engineer degree from UFRGS, Porto Alegre, 1995; a Masters (2001) and PhD (2005) degrees in Electrical Engineering, both from Escola Politécnica da USP, São Paulo, SP. He was visiting researcher at the Colorado University, Boulder , US, 2004 and a postdoc researcher at TEMF Institute, Darmstadt, Germany, 2006. He currently is Professor at UFABC, Santo André, SP, Brazil.

Roberto Menna Barreto holds an Electrical Enginner degree from IME, Rio de Janeiro, (1976), and a masters (1979) from Philips International Institute. He is currently General Manager of QEMC, located in Rio de Janeiro, focused on consulting and training in EMC-related areas. He is member of the "dB Society" and also " ssociation of Old Crows", both from US.

Stilante Koch Manfrin is from Santo André, SP, and holds an Electrical Engineering degree from FEI, São Bernardo do Campo (1990), a MsC (1995) and PhD (2003) degrees from USP São Carlos, both in Electrical Engineering. He currently is Professor at UFABC, Santo André, SP, Brazil.