POLITEHNICA UNIVERSITY OF BUCHAREST

PhD School of Electronics, Telecommunications and Information Technology

Decision No 876 dated 08-07-2022

PHD THESIS ABSTRACT

Eng. Alexandru-Dan BOITAN

STUDII PRIVIND SECURITATEA INFORMAȚIILOR
- ANALIZĂ DIN PERSPECTIVA VULNERABILITĂȚILOR TEMPEST

RESEARCH ON INFORMATION SECURITY
- ANALYSIS FROM THE TEMPEST VULNERABILITY PERSPECTIVE

PhD Commission

Professor PhD Eng. Mihai CIUC Politehnica University of Bucharest	Chairman
Professor PhD Eng. Simona HALUNGA Politehnica University of Bucharest	PhD coordinator
Professor PhD Eng. Corina NAFORNIȚĂ Politehnica University of Timișoara	Reviewer
Professor PhD Eng. Ioan NICOLAESCU Technical Military Academy "Ferdinand I"	Reviewer
Professor PhD Eng. Ion MARGHESCU Politehnica University of Bucharest	Reviewer

BUCHAREST 2022

_____

Table of contents

Chapter 1

Introduction

1.1 Presentation of the PhD thesis domain

Electronic devices are now widely used for information processing, and this applies not only to individual devices, but also to more complex systems that can be used for personal purposes, in commercial companies or businesses, or even for military applications. It is less known that, by receiving certain electromagnetic emissions generated by analogue or digital communications and applying signal processing techniques, it is possible to partially or totally restore the information transmitted by the targeted communication.

These issues are studied by the TEMPEST domain, whose main focus is precisely the protection of sensitive information against these types of attacks. That part of the electromagnetic radiation that can reveal information is called Compromising Emanation (CE) in the TEMPEST domain. Compromising emissions are defined as unintentional information-bearing signals which if eavesdropped and analysed may reveal information transmitted, received, manipulated or otherwise processed by any information processing equipment.

Standardisation in this area has expanded both within the NATO alliance (SDIP standards) [1] and at EU level (IASG standards) [2] and any member country, NATO or EU, must comply with the requirements of these standards when handling classified information through electrical, electronic or optoelectronic equipment. TEMPEST standards include rules for assessing the level of protection provided by the physical space (secure environment/area) in which the equipment will operate (SDIP-28 at NATO level and IASG 7-02 at EU level), the level of protection provided by the equipment (SDIP-27 at NATO level and IASG 7-03 at EU level), as well as rules and principles to be implemented during its installation (SDIP-29 at NATO level and IASG 7-01 at EU level).

The results presented in this paper are obtained by performing specialized TEMPEST laboratory measurements.

1.2 The purpose of the PhD thesis

The purpose of this paper is primarily to raise awareness among the general public about the existence of TEMPEST vulnerabilities that may jeopardize the confidentiality of information processed through electronic equipment.

In the second place, it was intended to present the possible TEMPEST protection methods that can protect us from the security threats presented in this paper and also to consider the financial aspect of applying these protection methods.

Last but not least, the aim of this work was to obtain a consistent and technically sustainable material that can be included, partially or totally, in existing TEMPEST standards at national, NATO or EU level.

1.3 The content of the PhD thesis

This paper is structured in 6 chapters. Chapter 2 deals with TEMPEST vulnerabilities generated by USB communications.

In chapter 3 will be analysed two TEMPEST security fonts which can be used to ensure the protection of sensitive information when processing it in text format. The analysed fonts have obtained protection from the Polish Design Office in the form of industrial design No. 24487 (2018) and patent No. 231691 (2019).

Security vulnerabilities due to the use of video projectors will be analysed in Chapter 4. The effectiveness of TEMPEST security fonts in using with a wide range of colours as possible for text and background will also be analysed, as well as presenting the colour method which can be used both to minimise compromising radiation from the targeted equipment and as a method for TEMPEST evaluation of equipment when analysing the display video signal.

Chapter 5 will present the traditional TEMPEST protection methods as well as innovative methods. The results of measurements evaluating the shielding effectiveness of all solutions presented in this chapter will also be briefly presented. This chapter also presents the results of a study on the propagation of compromising disturbances through conduction on the power line at considerable distances and the protection methods that can be used against this electromagnetic vulnerability.

Chapter 6 will present the conclusions of this work and a summary of the results presented in each chapter of the paper. Chapter 6 also includes the synthesis of original contributions that focus primarily on innovative TEMPEST protection methods. This chapter also includes the list of articles published during the whole PhD research period. The results presented in five of these articles are partially included in this paper..

Chapter 2

Compromising emanations generated by USB devices

The Universal Serial Bus (USB) has become a common feature of IT&C equipment implementations and therefore it is important to investigate the security vulnerabilities of this data bus.

2.1. Standardisation of USB communication

All existing standardisation versions of the USB bus and their main technical specifications have been presented in this section.

2.2. The USB interface

The pin configuration (pinout) for all currently existing USB interfaces has been presented in this section.

2.3. The USB communication performance

The functional principles as well as the benefits of using this data bus have been presented in this section.

2.4. USB controllers

All existing USB controllers in the present implementations have been presented in this section.

2.5. USB transfers

This section presents the 4 types of USB transfers, their operation and specifications, according to the current USB standards.

2.6. USB device initialization

When a USB device is connected to the USB bus for the first time, the USB enumeration process is initiated, whereby information is exchanged between the device and the host in order to identify the particularities of the USB device.

2.7. Electrical specifications

A summary of the information extracted from the USB standards has been made in this section which set out the general bus specifications by version and which will be used in the following sections for the analysis of the compromising emanations (CE) generated by USB communication.

2.7.1. USB data coding

The NRZI (Non Return to Zero Inverted) coding and the bit-stuffing mechanism used by this data communication was presented in this section. The electrical voltages on the USB data line were also presented.

2.7.2. USB bit period

This section summarizes the USB bit period information corresponding to versions 1.0, 1.1 and 2.0.

2.7.3. Rise and fall times of a USB bit

The rise times and fall times of a USB bit corresponding to versions 1.0, 1.1 and 2.0 were presented.

2.7.4. USB signalling states

The signalling states used by USB 1.0, 1.1 and 2.0 communication have been presented in this section.

2.8. USB packet fields

The main fields of USB packets corresponding to versions 1.0, 1.1 and 2.0 were presented.

2.9. USB resilience and TEMPEST protection

The main functional advantages of this data bus have been presented in this section, on the basis of which it is considered to be reliable and resistant to interference. Some of the results presented in Section 2.10 have been published in [3].

2.10. USB keyboard

This section presents the results published in 15 reference articles that addressed the security vulnerabilities of these peripherals (PS/2, USB and Wireless keyboards) due to their compromising emissions.

2.10.1. The measurement setup

The research was carried out in a specialised TEMPEST laboratory consisting of two adjacent shielded enclosures. One of them is semi-anechoic, being lined with radio-absorbent material on the walls but not on the floor. In the research developed in the present work an Rohde & Schwarz (R&S) AM524 active antenna system [5] and a TEMPEST R&S FSET22 receiver [6] were used. The FSET22 receiver's RBW filter can reach a maximum bandwidth of up to 500 MHz, which is the maximum possible for a test receiver on the market today. The equipment under test (EUT) is the USB keyboard that was connected to a shielded computer (or TEMPEST) installed under normal working conditions. The use of the shielded computer (which provides the highest level of TEMPEST protection) is mandatory for TEMPEST testing of peripherals as the emissions from this equipment (which is considered auxiliary) must be lower than the TEMPEST limit against which the peripheral is tested. Both the positioning of the EUT on the test table and the positioning of the antennas used and their spacing from the EUT (distance of 1 meter) was performed according to the military electromagnetic compatibility standards MIL STD 461G [4]. Since TEMPEST standards are classified, the information cannot be disclosed and therefore the configuration specified in this military EMC standard will be taken as the reference, which presents the closest configuration of all EMC standards. During the author's TEMPEST evaluation activities (18 years), no USB keyboards were encountered using USB 2.0 bus-specific transfer speeds. Thus, the examples illustrated in this paper will be limited to CE signals generated by USB 1.0 and 1.1 keyboards.

2.10.2. USB 1.0 keyboard communication

In the first part of this section the clock signal that is transmitted on the USB 1.0 bus was analysed. CE radiation consists of electromagnetic emissions generated at the level of electrical signal transitions. Basically, a data bit generates 2 distinct emissions, one corresponding to the rising edge of the data bit and the other corresponding to the falling edge. In the second part of this section, the data packet transmitted on the bus when a key is pressed was analysed. Corresponding to the USB 1.0 keyboards, the CE radiation of the 'q', 'p', 'c', 'k', '1' and '1 numlock' keys located on the numeric keypad were presented and analysed. For example, the CE radiation generated by pressing the 'q' key is illustrated in Figure 2.19.

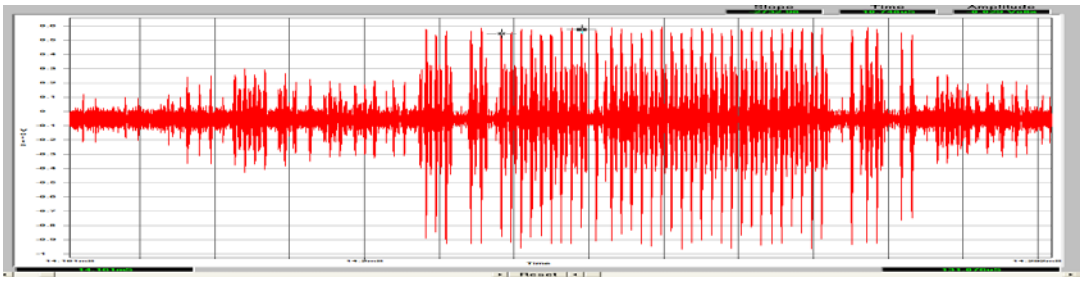


Figure 2.19 *CE radiation corresponding to the pressing of the 'q' key*

2.10.3. USB 1.1 keyboard communication

In the first part of this section the clock signal that is transmitted on the USB 1.1 bus and secondly the data packet that is transmitted when a key is pressed was analysed. The results obtained were presented, similar to section 2.10.2. For example, the CE radiation generated by pressing key 'c' is illustrated in Figure 2.40.

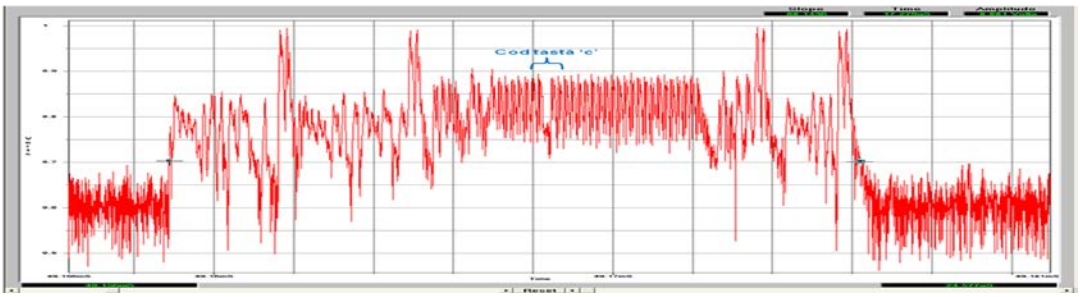


Figura 2.40 *CE radiation received while pressing the 'c' key*

Similar results were shown for the keys 'p', 'q', 'm', 'k', 'j', '1' and '1 numlock' located on the numeric keypad. Common keys between the two versions were also chosen to facilitate comparison. Verification of the information extracted from the CE radiation generated by the keystrokes illustrated in sections 2.10.2 and 2.10.3 was carried out by comparison with the information extracted from the USB standards but also with the electrical signals transferred on the USB bus, captured with the galvanic probing oscilloscope.

2.11. USB data storage devices

In this section, the results presented in 8 publications that investigated the security vulnerabilities of this type of USB transfer due to the compromising emissions generated by them were presented. Some of the results presented in section 2.11 were published in [7].

2.11.1. Measurement setup

The tests were carried out in the same TEMPEST laboratory described in section 2.10.1 and the measurement equipment described in the same section was used.

2.11.2. Comparison between the EMC and TEMPEST domain

Comparative test results between EMC and TEMPEST specifications were presented, which showed that it is possible for electronic equipment to pass EMC compliance tests, but not tests performed according to TEMPEST procedures.

2.11.3. Screened and unscreened devices

In this section the CE radiation generated by an unshielded USB stick was compared to that generated by a shielded one in the frequency range 420-520 MHz. As a result of the results obtained, it was recommended to use shielded USB devices for storing or storing sensitive information.

2.11.4. Compromising emissions from the USB bus

For TEMPEST analysis of USB communication in the case of mass or bulk transfers, data files were generated by sequentially multiplying predefined hexadecimal sequences: "FFFF00", "3F" and "FF".

2.11.4.1. USB bus clock

In this section the clock signal that is transmitted on the USB 1.1 and 2.0 bus was analysed, similar to sections 2.10.2 and 2.10.3.

2.11.4.2. USB 1.1 data packet for bulk transfers

The CE radiation generated by the data packets transmitted on the USB 1.1 bus has been illustrated. For example, corresponding to pattern "3F", the electrical signal and the CE radiation generated by it are illustrated in Figures 2.70 and 2.71.

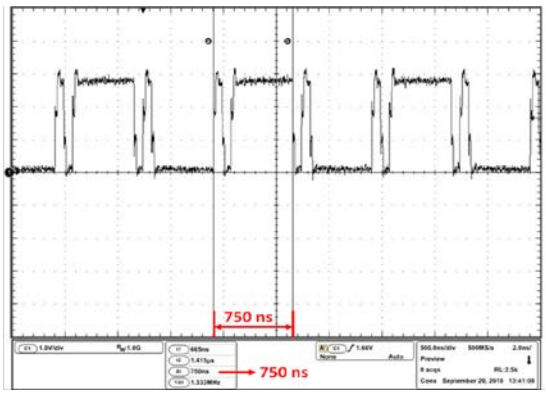


Figure 2.70 *Pattern "3F" (HEX), electrical domain (T_{CE} =750 ns)*

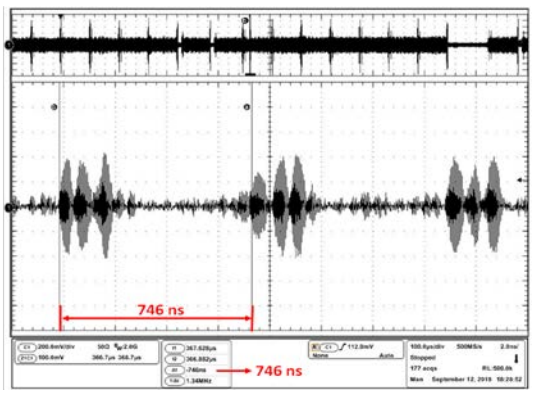


Figure 2.71 *CE radiation corresponding to pattern "3F" (HEX) - TCE =746 ns*

Both the CE radiation generated by the specified USB transfer and the electrical signal that is the source of the CE radiation have been illustrated to verify the accuracy of the received CE signals.

2.11.4.3. Defining the digital pattern

In this section the waveform of the CE radiation corresponding to the digital pattern (hexadecimal sequence) "3F" has been justified. The CE radiation generated by the hexadecimal pattern "3F" has been illustrated in Figure 2.71.

2.11.4.4. USB 2.0 data packet for bulk transfers

In this section the possibility of receiving the CE radiation generated by the data packets transmitted on the USB 2.0 bus when transferring the test files described in section 2.11.4.2 has been checked. For example, the electrical signal and the CE radiation generated by it have been illustrated in Figures 2.73 and 2.74 for the pattern "FF".

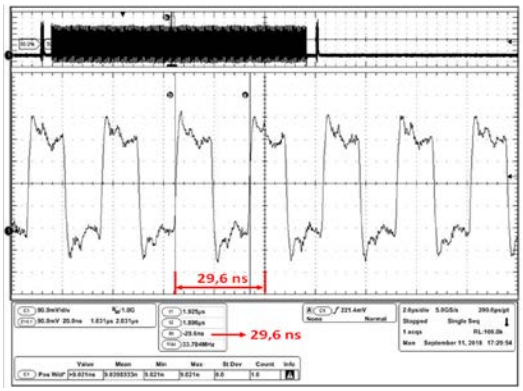


Figure 2.73 *Pattern "FF" (HEX), electrical domain (T_{CE} =29.6 ns)*

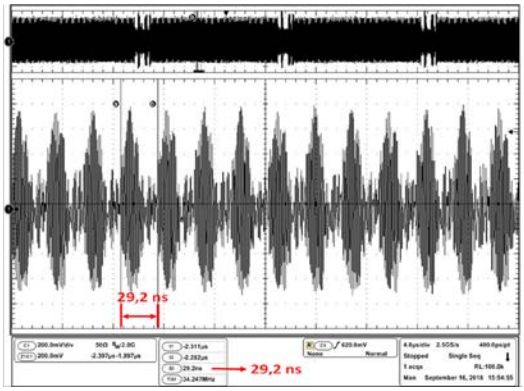


Figure 2.74 *CE radiation corresponding to pattern "FF" (HEX)- T_{CE} =29.2 ns*

2.11.4.5. CE signal quality versus capture filter bandwidth

In this section, the influence of the receiver's resolution bandwidth (RBW) on the accurate reception of the CE radiation has been presented, which will allow the bit-level information to be decoded. If a lower RBW value is chosen, the CE radiation will still be received but it will not be possible to recover the full information. The study was performed for USB 1.1 communication and the results were extrapolated to USB 2.0 communication

Chapter 3

Video signal

3.1. Video display signal

The display video signal is the video signal generated by the video card of a personal computer that is transferred through dedicated video interfaces to a display device. In this introduction the analogue video display signals have been presented: composite video, S-Video, component video.

3.2. VGA interface

In this section the VGA interface was presented as well as the pin configuration (pinout) and the signals transmitted on this analog video interface.

3.3. DVI interface

The existing DVI (Digital Visual Interface) display signal interfaces, pin configuration (pinout), TMDS (Transition Minimized Differential Signaling) signal structure, coding used as well as the transfer speeds of this video display interface have been presented in this section.

3.4. HDMI interface

The main technical specifications of all HDMI (High-Definition Multimedia Interface) standardisation versions were presented, as well as the existing physical interfaces and pin configuration.

3.5. DisplayPort interface

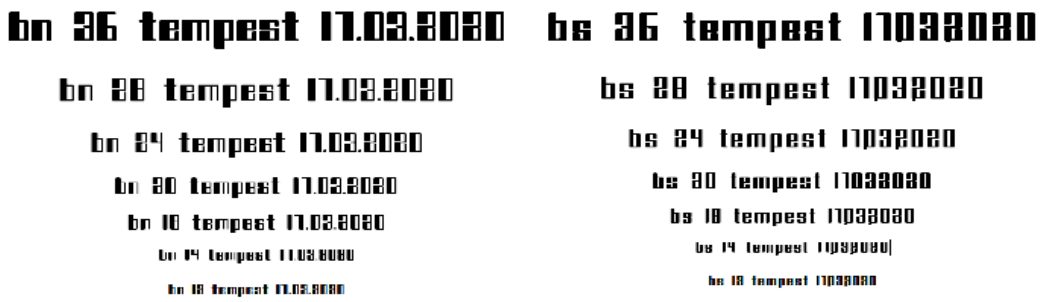
DisplayPort (DP) is the only video interface that uses data stream packetisation. The main technical specifications of all DP standardisation versions, the physical interfaces used and the pin configuration have been presented.

3.6. Display video signal from TEMPEST domain perspective

In this section, the summary results of more than 30 publications have been presented, which have focused on security vulnerabilities of video display interfaces (VGA, DVI, HDMI and DP) due to compromising emissions generated by them. The results of the research presented in this chapter have been published in [8].

3.7. The modelling of CE sources

In this section, the effectiveness of modeling compromising emission sources (CE) that limit the effectiveness of electromagnetic infiltration was analyzed. This can be achieved by using specialised computer fonts that have been designed precisely to achieve this objective and are also called TEMPEST security fonts. The security fonts used are illustrated in Figure 3.1.



(a) *(b)*

Figure 3.1 *Secure font characters:*
(a) asymmetric secure font, (b) symmetric secure font

The presented TEMPEST secure fonts are protected by the Polish Patent and Design Office under Industrial Design No. 24487 and Patent No. 231691 and represent an innovative and evolving method that can support the protection of processed information in text format.

3.7.1. Measurement setup

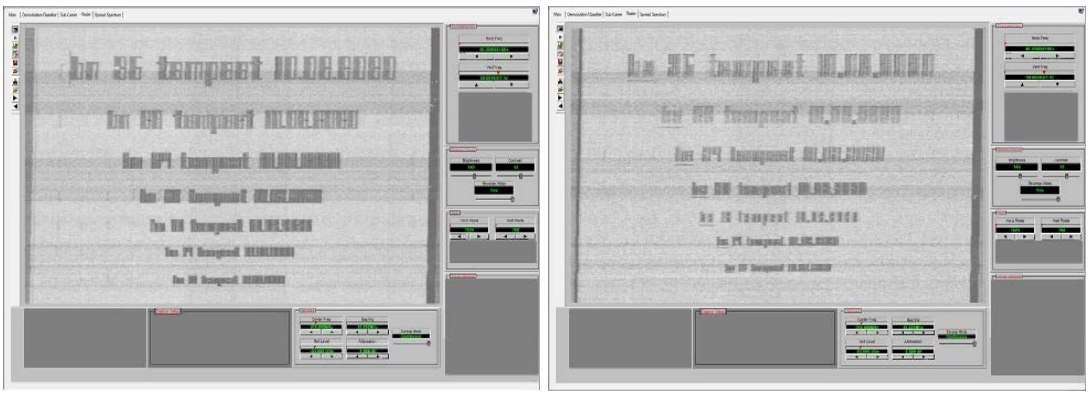
The tests were carried out with a Fujitsu Siemens laptop, model Lifebook C110 and the measurement equipment used was presented in section 2.10.1.

3.7.1. Parametrii semnalului video de afișare

In this section, the display video signal parameters for the laptop used in the tests have been detailed according to the VESA DMT v1.3 standard.

3.7.2. Measurement results

Specific tests have been performed for the VGA display standard which is still very popular in classified systems. Verification of the effectiveness of secure fonts by visual analysis was carried out in two separate measuring environments: an anechoic chamber of the MCI (Military Communications Institute) laboratory in Poland and a semi-anechoic chamber of the STS (Special Telecommunications Service) in Romania. Each laboratory used a different TEMPEST receiver. This was precisely the purpose of the comparative evaluation of new fonts in secure text information processing. In this section, the results obtained by the TEMPEST STS laboratory, using two TEMPEST receivers, FSET22 and FSWT26, were presented, confirming the efficiency of the proposed new method. Figures 3.5 (a) and (b) show the test results in the form of reproduced images of the reception of compromising emissions generated by EUT, corresponding to the use of asymmetric and asymmetrically secured fonts.

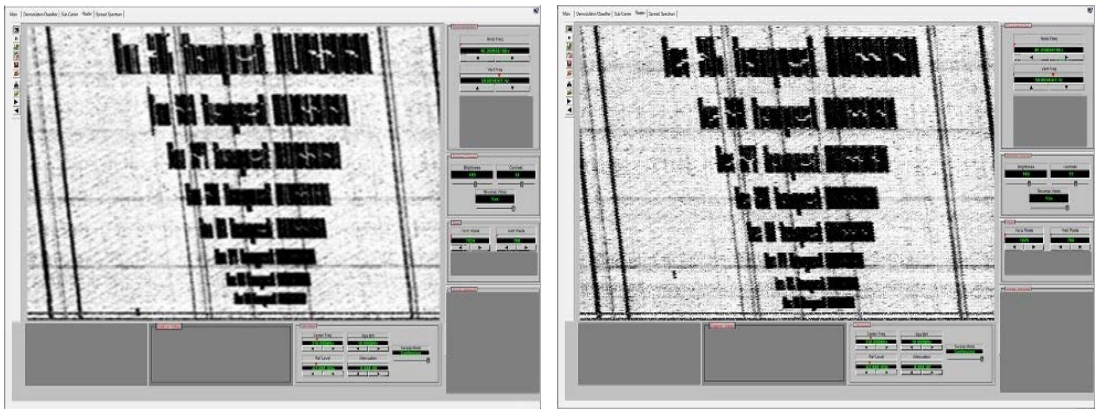


(a) *(b)*

Figure 3.5 *Image restored with FSET22 receiver for display with font: asymmetrically secured (a) and symmetrically secured (b)*

The FSWT26 receiver is the latest TEMPEST receiver model released on the market by the Rohde&Schwarz Company. This equipment comes with built-in raster module. The efficiency of secure fonts has been compared with that of traditional fonts, Arial and Times New Roman, for various font sizes: 72, 36, 28, 24, 20, 18, 14 and 12. In each case, compromising emissions were detected, recorded and rasterised (restored). Both upper and lower case letters, Arabic numerals, normal and bold type were used in the tests, as well as the introduction of free spaces between alphanumeric characters written in asymmetric and symmetric secure fonts for better intelligibility of the information contained in the rasterised images.

The results shown in Figure 3.5 were achieved for the 910 MHz reception frequency, chosen favourably to avoid electromagnetic noise generated by the laptop power supply used in the tests. Figure 3.20 shows the video recoveries corresponding to the secured fonts (asymmetrical and symmetrical) performed on the 310 MHz reception frequency.



(a) *(b)*

Figure 3.20 *Font size 36, receiving frequency 310 MHz: (a) asymmetric secure font, (b) symmetric secure font*

In Figures 3.20(a) and 3.20(b) we can see vertical and horizontal lines appearing additionally in the background compared to the images shown in Figures 3.5(a) and (b). These are due to electromagnetic noise existing on the receiving frequency but which is not caused by the display video signal which has been analysed in this chapter but by the electromagnetic "noise" existing on the respective receiving frequency.

TEMPEST compliance testing is not limited to EUT radiated emissions and is also carried out for EUT conducted emissions. A TEMP 8400 transducer was used, manufactured by Schwarzbeck Company. Figure 3.23 illustrates the video restoration performed for secured fonts (symmetrical and asymmetrical) by receiving the CE disturbances propagated on the power line.

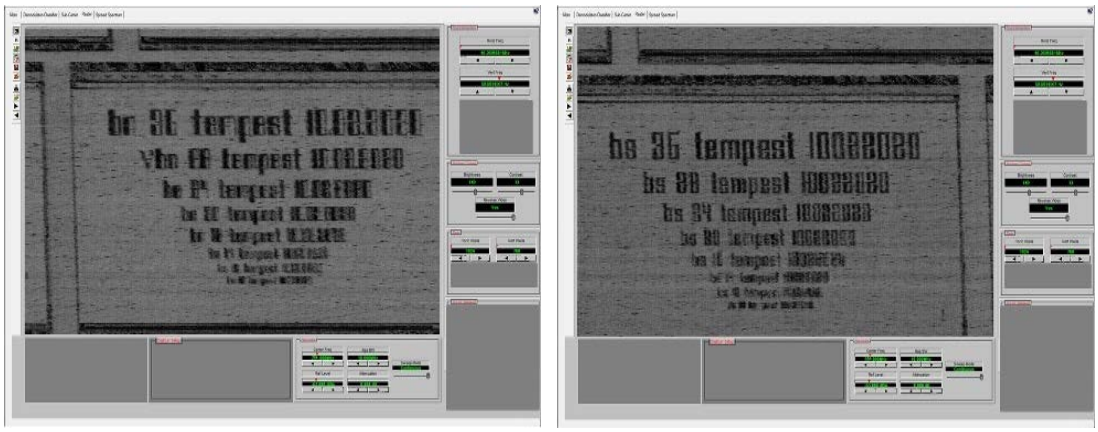


Figure 3.23 *Font size 36, 204 MHz receive frequency, conducted emissions: (a) asymmetric secure font, (b) symmetric secure font*

Based on the results obtained, we consider that the use of these secure fonts can be introduced as one of the official TEMPEST countermeasures that should be specified in the NATO and EU classified documents, which regulate the activities involved in this technical field and which represent national security measures for all IT&C equipment with classified use and which could be implemented by each NATO and EU member state.

Chapter 4

The colour method

In this first part of the chapter the main technologies used in the production of video projectors are presented: DLP (Digital Light Processing), LCD (Liquid Crystal Display) and LCoS (Liquid Crystal on Silicon). The main technological developments of these devices have also been presented.

4.1. LCD projectors

In this section we have presented the functional details of projectors manufactured in this technology.

4.2. Video display signal parameters

The equipment under test (EUT) was an EPSON video projector, model EH-TW650. In this section the parameters of the video display signal were presented, similar to section 3.7.2.

4.3. Measurement setup

The tests were carried out in the same TEMPEST laboratory described in section 2.10.1, using the measurement equipment also described in the same section.

4.4. The colour method

The purpose of the tests and analyses that have been presented in this chapter: security vulnerabilities of video projection equipment, proposing and argumentation of the use of computer-secured fonts to counteract the electromagnetic infiltration process, presentation of the colour method used as a solution for electromagnetic protection of processed graphical information, presentation of the colour method as a test method in specialized tests for evaluating compromising emissions according to TEMPEST standards.

4.5. Time parameters measurement

In this section, experimental results that confirm the display video signal parameters presented in Section 4.2 have been illustrated using conveniently test signals to meet this objective. Figure 4.11 shows 2 examples of test images that were used.

a) b)

Figure 4.11 *Equal horizontal lines, RGB (a) and CMY (b) colours on white background*

Measurement of the time parameters of the display video signal can also be performed directly with the TEMPEST receiver, as shown in Figures 4.7 and 4.8.

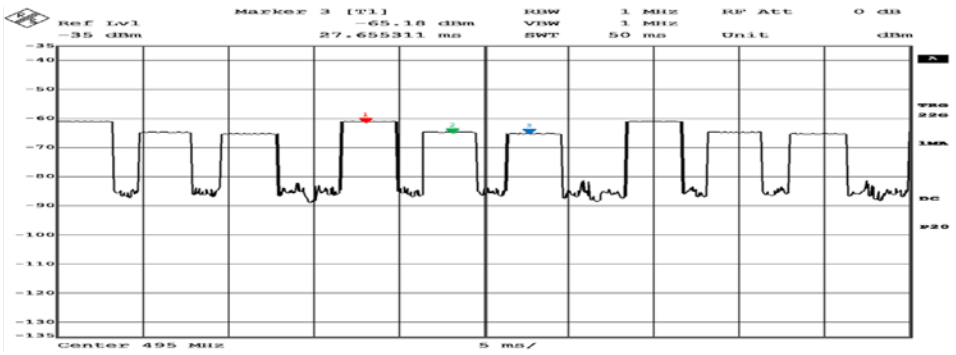


Figura 4.1 *CE emissions displayed in time domain (span 0 mode), reception frequency 495 MHz: marker 1 - horizontal line in red colour, marker 2 - horizontal line in green colour, marker 3 - horizontal line in blue colour, background - black*

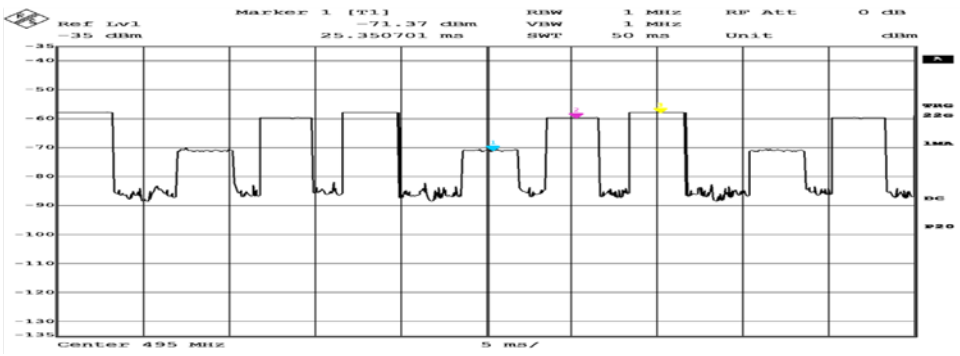


Figure4.9 *CE emissions displayed in time domain (span 0 mode), reception frequency 495 MHz: marker 1 - cyan colour, marker 2 - magenta colour, marker 3 - yellow colour, background - black colour*

In Figures 4.7 and 4.8 the different levels of the recorded signal amplitudes corresponding to the three colours used can be observed.

The results of the research presented in this chapter have been published in [9].

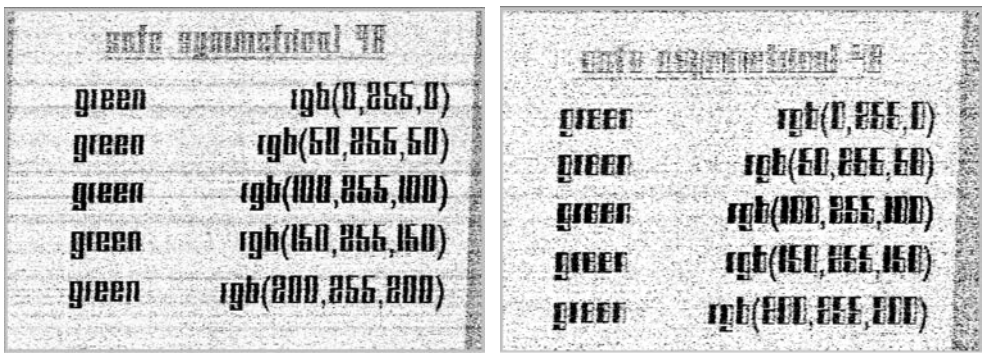
4.6. Choosing the most suitable RBW

In this section the influence of the RBW bandwidth of the receiver used on the accurate reception of the test signals used in the tests was presented, as was also presented for the CE radiation generated by USB communication in section 2.11.4.5.

4.7. Secure fonts assessment

In this section measurements were performed corresponding to the test messages displayed in the primary colours (red, green and blue) of the RGB colour mode but also in their colour shades on a white and black background, as follows: Grey shades on white background - Black (0,0,0), (50,50,50), (100,100,100), (150,150,150) and (200,200,200), Red shades on black and white background - Red (255,0,0), (255,50,50), (255,100,100), (255,150,150) and (255,200,200), Green shades on black and white background - Green (0,255,0), (50, 255,50), (100,255,100), (150,255,150) and (200,255,200), shades of blue on white and black background - blue (0,0,255), (50,50,255), (100,100,255), (150,150,255) and (200,200,255), shades of grey on black background - white (255,255,255), (200,200,200), (150,150,150), (100,100,100) and (50,50,50).

When the green test images were displayed, the images shown in Figure 4.21 were reproduced by receiving the CE radiation generated by the video projector under test.

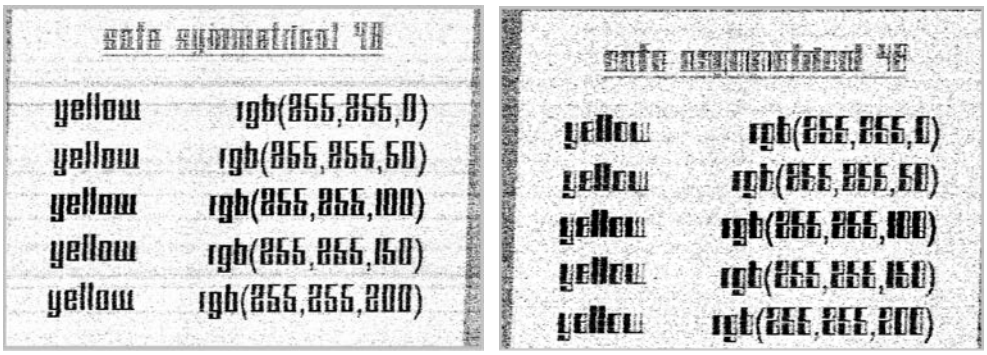


a) b)

Figure 4.21 *Reconstructed images according to: symmetrically secured font in shades of green (a), asymmetrically secured font in shades of green (b) - white background*

The CMY colour mode is also a widely used display mode, used by default in printing devices, which uses the combination of turquoise (cyan), red-purple (magenta) and yellow (yellow) colours. Thus, tests have also been carried out on these colours to examine the efficiency of the electromagnetic infiltration process for the

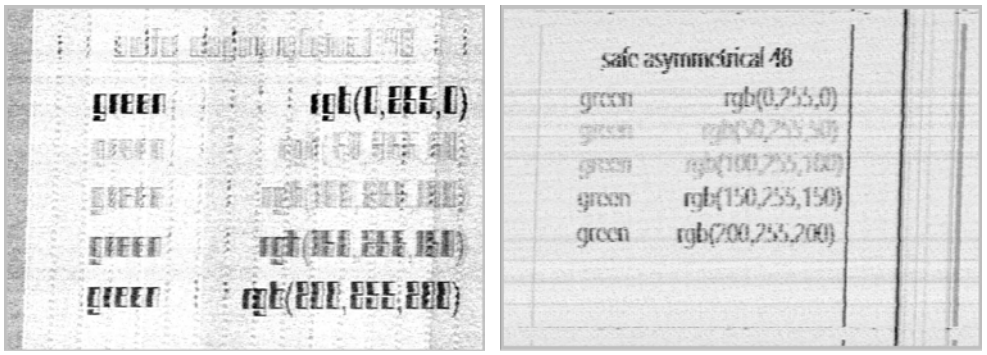
most extensive range of possible colours and to identify favourable combinations. Figure 4.27 shows 2 examples, corresponding to yellow colour. Characters are legible although displayed on a white background.



a) b)

Figure 4.27 *Reconstructed image: symmetrical yellow secure font (a), asymmetrical yellow secure font (b) - white background*

In order to express more clearly the complexity of the CE radiation and the influence of using wide colour palettes, tests were carried out on three receiving frequencies: 495 MHz, 520 MHz and 851 MHz. Figure 4.28 shows two examples for the last two reception frequencies, corresponding to the green colour and the asymmetric font, which were illustrated in the PhD thesis in Figures 4.30 (b) and 4.32 (c).



a) b)

Figure 4.28 *Reconstructed image based on CE emission received on 520 MHz (a) and 851 MHz (2) frequencies, asymmetrically secured font, size 48 and white background*

A careful analysis of the results obtained from examining the projector as a source of unwanted emissions shows that the colour method is not always effective for selected colour combinations. This is caused by the complexity of the radiation source, i.e. the projector. A properly selected colour combination for text and background may reduce the measured emission level at some frequencies, while at other frequencies the measured level of the same emission may remain unchanged. The colour method can therefore reduce the number of incidences of unwanted emissions.

Chapter 5

TEMPEST protection methods

In the first part of this chapter, both traditional TEMPEST protection methods and innovative methods that provide the necessary level of protection with minimal implementation costs or with clear operational advantages have been presented. The traditional methods are the use of TEMPEST protected equipment, the use of shielded enclosures and the use of the zonal model. The results of the research presented in this chapter have been published in [10].

TEMPEST protected equipment offering the highest level of TEMPEST protection can be installed in the most vulnerable locations. These are commercial equipment on which additional shielding measures have been applied and these technological modifications have been detailed within the chapter. The manufacture of TEMPEST protected equipment must be done under careful quality control to ensure that the units made on the production line are built exactly like those that have been tested at the prototype stage and for this reason, companies manufacturing TEMPEST protected equipment must receive accreditation in order to commercialise such products.

As the first innovative method of TEMPEST protection, shielded racks and tents were presented. These can be successfully used as an alternative to TEMPEST protected equipment. Products of this type were presented and evaluated during the PhD research period: products made by 3 companies producing racks (Eurotempest and 2 Romanian companies accredited at NATO and EU level) and 2 products made by companies producing tents (Holland Shielding Systems BV and Soliani EMC SRL). The advantages and disadvantages of each product category were presented as well as the technical and design options that can be requested when purchasing these products. The minimum level of attenuation offered by the products tested was specified.

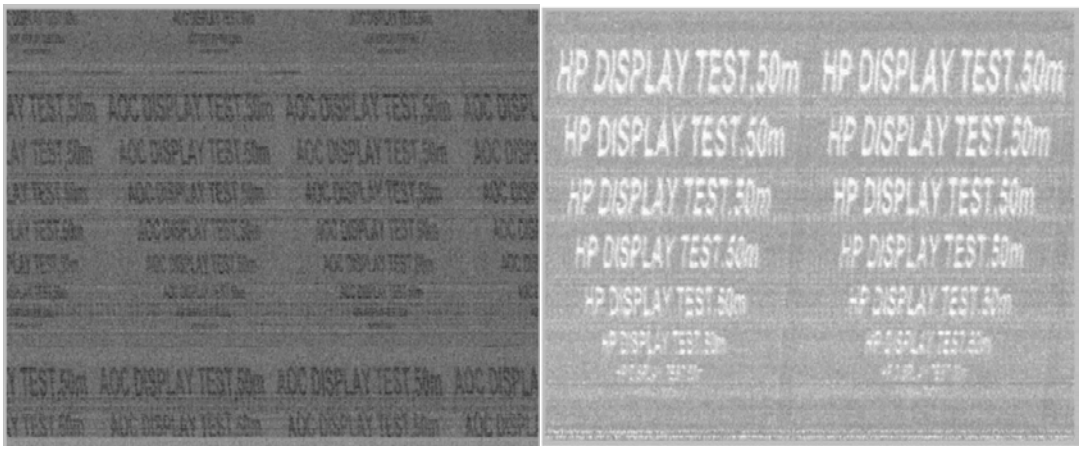
Shielding of facilities where it is intended to operate information and communication systems that will handle sensitive information is also part of the traditional methods. Shielding of physical spaces can be done at room level or even at building level and usually a copper sheet envelope is used to achieve this objective as well as shielding of all screen penetrations: access points/outlets, power supply, ventilation, cooling or gas pipes, data communication flows, etc.

The advantages and disadvantages of this TEMPEST protection method were presented, in particular in the case of shielding buildings. In general, in a typical office space, the wall which incorporates the window is the most vulnerable in terms of TEMPEST protection. This is mainly because the window generally provides very low values of electromagnetic attenuation.

Innovative methods of shielding the physical spaces included window screening curtains/drapes and window screening films were presented. The application of electromagnetic shielding paints that can be successfully used to shield walls was also presented. Several products tested by the author during the PhD period that can be successfully used for curtain and drape shielding and that are in the portfolio of two specialised companies, Holland Shielding Systems BV and Amradield, were presented. Aspects of the manufacture and assembly of these products were also presented. One product from the Holland Shielding Systems BV portfolio was presented from the category of shielding films. One product was also presented from the category of shielding paints from the "Safe Solutions" portfolio. In the case of the shielding paint, a total of 5 layers of paint were applied and the shielding effectiveness was evaluated after each new layer was applied. The minimum level of attenuation provided by the products tested was specified. Evaluation of the shielding effectiveness of the innovative shielding materials presented in this chapter was carried out in a laboratory environment using a small shielded enclosure. The measurement setup was presented as well as the technical aspects to be taken into account in order to minimise the errors that can be encountered when performing these measurements.

The second part of the chapter presented the results of a pioneering study to assess the attenuation of compromising electromagnetic disturbances at considerable distances, propagating on the power line of electronic equipment. From a TEMPEST domain perspective, the greatest vulnerability to information leakage is attributed to the display video signal. Two monitors manufactured by AOC and HP were used for this test, as well as a Line Impedance Stabilization Network (LISN) electromagnetic transducer, LISN TEMP 8400. For propagation at distances of 1, 10 and 50 metres, extension cables of this size were used, interposed between the power cable of the monitors and the TEMP 8400 transducer. The detection of the compromising signal was carried out for the AOC (Admiral Overseas Corporation) monitor at 484 MHz frequency while for the HP (Hewlett-Packard) monitor at 274 MHz. The measurements were carried out in an office space enviroment, as propagation over long distances cannot be tested in a specialised TEMPEST laboratory which is not so generously sized, in the order of tens of metres..

Measurements were carried out to evaluate the Signal to Noise Ratio (SNR) and also to illustrate the possibility of image restoration (rasterisation) at these distances. The video signal recovery at a distance of 50 metres, by receiving the CE disturbance propagated on the EUT power line, is illustrated for the AOC monitor in Figure 5.6(a) and for the HP monitor in Figure 5.6(b).



(a) (b)

Figure 5.6 *Image recovery at a distance of 50 meters: (a) - AOC monitor and (b) - HP monitor*

While in the case of radiating compromising emanations (CE), the separation distance offers considerable protection, in the case of conducted CE (e.g. on the power line), this is no longer the case or can be considered to be very small, as our research has shown. Countermeasures, both procedural and technical, have been presented to reduce or even eliminate these threats, based on the results and analysis of the signal-to-noise ratio recorded during our research.

A possible low-cost measure to protect against compromising disturbances that may propagate on the power supply line of the EUT is the application of ferrite beads/ferrite rings, which are also constructed in the form of a clamp and are therefore easy to apply to the power or data cable of the electronic equipment targeted. The results of tests carried out by applying ferrite rings to the power cable of a monitor were presented. Two types of ferrite were used, TDK SEIWA and FAIR-RITE VO. Applying ferrites rings to one end of the power cable resulted in an attenuation of about 2 dB while applying ferrite rings to both ends of the power cable resulted in an attenuation of about 4 dB.

Tests were also performed for the USB communication analysed in Chapter 2, in the frequency range 375 MHz - 1 GHz. For this purpose, a shielded USB stick was connected to the USB port of a laptop computer and operated throughout the tests with battery power supply. A one metre long USB extension cable was inserted between the USB stick and the computer port. The results of the tests carried out by applying ferrite rings to the USB cable at each end were presented. Two types of ferrite were used, FAIR-RITE VO and Wurth Elektronik. CE radiation was eliminated when the ferrite ring was applied to the end facing the EUT (USB stick).

Chapter 6

Conclusions

This paper presented the results of innovative TEMPEST research specific to the TEMPEST evaluation of IT&C equipment to identify their security vulnerabilities due to compromising electromagnetic emissions (EMSEC protection) generated by USB communication and display video signals.

As people are nowadays asked to be as open as possible in terms of working hours, we end up working on the computer for work purposes not only in the office space but also at home, in the car or even outdoors in parks or at the children's playground. This has become even more accentuated in the last 3 years due to the emergence of the COVID-19 pandemic in the world and the restrictions imposed to limit the spread of the SARS-COV-2 virus. This can be effective in terms of flexibility and optimisation of working time, but also involves significant vulnerabilities in terms of the security of the information processed.

Taking these aspects into consideration, both traditional TEMPEST protection methods and alternative methods that have been identified during the doctoral studies period and that have been successfully tested and applied in this area of expertise have been presented in this paper. In any technical domain, standards can be improved based on publications and research in the field and with the support of the whole scientific community. By "alternative methods" it should be understood that these methods are not currently mentioned in the standards in force but this does not imply that they are not feasible and effective solutions to counteract the security vulnerabilities reported in this paper and we believe that they could be incorporated in the future in the standards that govern the TEMPEST domain.

6.1. The achieved results

In Chapter 2 of this paper, the possibilities of bit-level recovery of information transmitted over the USB bus for both keyboard peripherals and USB data storage devices are illustrated for the first time, as well as possible protection measures that can be applied at low cost. The examples illustrated focused on USB keyboards using versions USB 1.0 and 1.1 and USB bulk transfers, corresponding to versions 1.1 and 2.0, which are designed for connection to a personal computer (USB host) of any USB storage medium. Verification of the information extracted from the received CE radiations was performed by checking against the information extracted from the USB

standards but also against the electrical signals transferred on the USB bus, acquired with the oscilloscope by galvanic probing.

All the results presented in chapters 2, 3 and 4 have been obtained from tests carried out in a specialised TEMPEST laboratory using dedicated TEMPEST measuring equipment, which has the technical specifications required for use in laboratory tests according to the current TEMPEST standards.

Chapter 3 presents the results of research carried out to verify the effectiveness of the protection of information displayed in text format by using TEMPEST security fonts that have obtained the protection of the Polish Patent and Design Office in the form of Industrial Design No. 24487 and Patent No. 231691 as well as the security vulnerabilities of IT&C display equipment. The secure fonts presented in this paper represent an innovative and evolving method that can support the protection of text-processed information, but as in any technical field, the effectiveness of the proposed solutions must be subject to inter-laboratory verification. The effectiveness of secure fonts has been compared with that of traditional fonts, Arial and Times New Roman, for various font sizes. In the tests performed, both upper and lower case letters, Arabic numerals, normal and bold writing were used, as well as the introduction of free spaces between alphanumeric characters written in asymmetrical and symmetrical secure fonts for better intelligibility of the information contained within the raster images.

Following the results obtained, we consider that the use of these secure fonts can be introduced as one of the official TEMPEST countermeasures specified in the NATO and EU classified documents governing the activities involved in this technical field.

Chapter 4 presents and analyses the security vulnerabilities of the video display signal due to CE radiation according to the colours used, which is recognised in the scientific community as the colour method. This method represents the most comprehensive approach from the perspective of TEMPEST equipment evaluation and can also be used successfully to protect displayed information. These security vulnerabilities primarily concern IT&C equipment that is used in video presentations and in particular video projectors. Measurements were performed corresponding to the test messages displayed in the primary colours (red, green and blue) of the RGB colour mode but also in their colour shades on a black and white background. A similar approach was used for the CMYK (cyan, magenta, yellow, black) colour mode.

Chapter 5 presents methods of protection against reported TEMPEST vulnerabilities (use of TEMPEST protected equipment, shielded racks and tents) as well as innovative methods of electromagnetic shielding of windows (curtains, drapes and shielding foils) and walls of a physical space (shielding paint) where such equipment can be safely installed. It was presented for the first time the possibility of restoring information displayed at considerable distances (50 meters) by receiving electromagnetic disturbances generated by IT&C equipment that propagate on their power line and TEMPEST protection methods that can counteract this phenomenon. The tests were carried out this time in an office space and involved two display

devices (computer monitors) which were powered sequentially via 1 metre, 10 metre and 50 metre electrical extension cords. Countermeasures to protect against these phenomena were presented, including the financial aspects of applying these TEMPEST countermeasures.

We can conclude that the TEMPEST phenomenon is complex and that methods of protection against CE radiation and disturbances are expensive. If CE protection is required, a TEMPEST security officer will be able to provide customised technical expertise, depending on the equipment, location and classification level of the information.

6.2. Original contributions

The original contributions contained in this paper are the result of research and studies carried out during the whole doctoral research period and can be summarised as follows:

1. Study on electromagnetic vulnerability imposed by the use of USB keyboards;
2. The presentation for the first time of the possibility of clearly identifying USB 1.0 and 1.1 keys operated from these indispensable peripherals for IT&C equipment through the ability to recover USB key codes at bit level from the reception and analysis of compromising radiation generated by this equipment as well as the presentation of the detection and analysis parameters necessary to achieve this objective;
3. Study on electromagnetic vulnerability imposed by the use of USB storage devices;
4. The presentation for the first time of the possibility of bit-level recovery of USB 1.1 and 2.0 data transferred in large blocks of data on this universal serial communication bus by detecting and analysing the compromising radiation generated by these data transfers and to present the detection and analysis parameters required to achieve this objective;
5. Carry out a comparative study between EMC domain-specific measurements and TEMPEST domain measurements;
6. Electromagnetic security effectiveness verification of shielded data storage devices;
7. Study on the influence of parameters used in the detection and analysis of compromising emissions;
8. Checking the EMSEC effectiveness when using secure fonts which is an innovative TEMPEST protection method and makes it difficult or even impossible to recover text information displayed by IT&C equipment using specific electromagnetic intrusion methods;
9. Checking the EMSEC effectiveness of TEMPEST security fonts and the use of colours when displaying text information;
10. Introduction of the colour method as a TEMPEST protection method involving the use of different colour combinations for font and background in order to

minimise the signal-to-noise ratios of compromising emissions from IT&C equipment when displaying information in text format;

11. Introduction of the colour method as a equipment TEMPEST evaluation method involving the use of different colour combinations for font and background in order to maximise signal-to-noise ratios of compromising emissions from IT&C equipment when displaying information in text format;
12. Presentation of traditional TEMPEST protection methods including the use of TEMPEST protected equipment, the RED/ BLACK principle and the use of small and large shielded enclosures;
13. Conducting a study on the use of shielding curtains and drapes as an innovative TEMPEST protection measure that can be applied as a method of electromagnetic shielding of windows and verification of the shielding effectiveness of different materials used for this purpose;
14. Conducting a study on the use of shielding foils as an innovative TEMPEST protection measure that can be applied to windows as well as display devices and verifying the shielding effectiveness of such a material;
15. Conducting a study on the use of shielding paints as an innovative TEMPEST protection measure that can be applied to shield rooms or even buildings in order to increase the level of TEMPEST protection offered by physical spaces and present the shielding effectiveness of such a material;
16. Performing a research on the use of TEMPEST racks as an alternative measure for the use of TEMPEST protected equipment and verify the shielding effectiveness of such products;
17. Performing a research on the use of shielded tents as an innovative TEMPEST protection measure that can be used as an alternative to the use of TEMPEST racks, in which both advantages and disadvantages of the application of this method were presented, as well as the testing of the shielding effectiveness of these products;
18. Presentation for the first time of the results of a study on the propagation of compromising emissions along power lines at considerable distances: 1 metre, 10 metres and 50 metres;
19. Presentation of the results of a study on the capability of ferrite filters to reduce or even eliminate electromagnetic emissions that are generated by IT&C equipment and can propagate along power or data lines.

6.3. List of original publications

During the doctoral research period, seven journal articles were published, of which two as first author, and fifteen conference papers, of which four as first author. The results of articles [R4] and [C1] are partially inserted in Chapter 2, the results of article [R2] will be partially found in Chapter 3 and the results of article [R5] have been used in Chapter 4. Also, results obtained and partially published in the article

[R6] have been inserted in Chapter 5 but there are also results inserted in Chapter 5 that have not yet been published.

Journal papers

[R1] V. Butnariu, B. Trip, A. Macovei, G Rosu, A. Boitan, S. Halunga, Power line compromising emanations analysis, Annals of the University of Craiova, Electrical Engineering Series, vol. 48, Corpus ID: 195655228, 2018.

[R2] I. Kubiak, A. Boitan, S. Halunga, Assessing the Security of TEMPEST Fonts against Electromagnetic Eavesdropping by Using Different Specialized Receivers. Applied Sciences. 2020, 10, 2828, https://doi.org/10.3390/app10082828. (**ISI, Q2, IF: 2,679, WOS:000533352100192**)

[R3] X. Rognean, Georgiana Rosu, Alexandru Boitan, Bogdan Trip, Vlad Butnariu, Chaouki Kasmi, Lars Ole Fichte, Octavian Baltag, "Study of Compromising Emissions of PS/2 Keyboards by Correlative Methods", Revue Roumaine des Sciences Techniques-Serie Electrotechnique et Energetique, Vol. 65, 1-2, pp. 15–20, Bucharest, 2020, Corpus ID 220683897. (**ISI, Q4, IF: 0,443, WOS:000552052900024**)

[R4] Boitan A., Halunga S., Bîndar V., "Compromising Electromagnetic Emanations of USB Mass Storage Devices", 7th Annual Workshop of the CTIF-SEE at AIT, Athens, *Wireless Personal Communications* (2020), p. 1-26, https://doi.org/10.1007/s11277-020-07329-8. (**ISI, Q3, IF:1.671,WOS:000528336100007**)

[R5] A. Boitan, I. Kubiak, S. Halunga, A. Przybysz, A. Stańczak, Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process, Multidisciplinary Digital Publishing Institute, Symmetry 2020, 12(11), 1908; https://doi.org/10.3390/sym12111908. (**ISI, Q2, IF: 2,713, WOS:000593717100001**)

[R6] Bogdan Trip, Vlad Butnariu, Mădălin Vizitiu, Alexandru Boitan, Simona Halunga, Analysis of Compromising Video Disturbances through Power Line, Sensors 2022, 22(1), 267; State-of-the-Art Sensors Technology in Romania 2021, https://doi.org/10.3390/s22010267. (**ISI, Q1, IF: 3.576, WOS:000752818700001**)

[R7] G. Rosu, V. Velicu, A. Boitan, G. Mihai, L. Tuta, O. Baltag, On the electromagnetic shielding properties of carbon fiber materials, Electrical Engineering & Electromechanics,2022, Pages 38-43, DOI: https://doi.org/10.20998/2074-272X.2022.1.05. (**ISI, IF: 1,148, WOS:000768687300012**)

Conference papers

[C1] A. Boitan, R. Bărtușică, S. Halunga, M. Popescu, I. Ionuță, Compromising Electromagnetic Emanations of Wired USB Keyboards, International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2017, Bucharest, pp. 39-44, DOI: 10.1007/978-3-319-92213-3_6, 2017. (**ISI, WOS:000481658200006**)

[C2] M. Popescu, R. Bărtuşică, A. Boitan, I. Marcu, S. Halunga, Considerations on Estimating the Minimal Level of Attenuation in TEMPEST Filtering for IT

Equipments, International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2017, Bucharest, pp. 9–15, DOI: 10.1007/978-3-319-92213-3_2. (**ISI, WOS:000481658200002**)

[C3] R. Bărtușică, A. Boitan, S. Halunga, M. Popescu, V. Bindar, Security Risk: Detection of Compromising Emanations Radiated or Conducted by Display Units**,** International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2017, Bucharest, pp. 45–51, DOI: 10.1007/978-3-319-92213-3_7. (**ISI, WOS:000481658200007**)

[C4] R. Bărtușică, M. Popescu, A. Boitan, S. Halunga, Considerations for Emission Security Risks from the Perspective of Signal Processing Techniques, 2018 International Conference on Communications (COMM)**,** 14-16 June 2018**,** Bucharest, Romania, IEEE, pp. 535-538, Date Added to IEEE Xplore: 08 October 2018**,** DOI: 10.1109/ICComm.2018.8484832. (**ISI, WOS:00044952600010**)

[C5] A. Boitan, R. Bărtușică, M. Popescu, V. Bîndar, O. Fratu, Wireless Keyboards Communication Interception-The Balance Between Convenience and Security, 2018 International Conference on Communications (COMM), Bucharest, Romania, Pages 539-542, Publisher IEEE, DOI: 10.1109/ICComm.2018.8484812, 2018. (**ISI, WOS:000449526000102**)

[C6] A. Idita, G. Roşu, A. Boitan, V. Butnariu, B. Trip, O. Baltag, Study of shielding effectiveness on spurious emissions of information systems by means of metallic and carbon powder screens, 2018 International Conference on Applied and Theoretical Electricity (ICATE), 4-6 Oct. 2018, Craiova, Romania, IEEE, pp. 1-6, DOI: 10.1109/ICATE.2018.8551420. (**ISI, WOS:000487278600046**)

[C7] A. Macovei, V. Butnariu, A. Boitan, G. Rosu, B. Trip, and S. Halunga, Detection of Electromagnetic Emissions Transmitted on The Power Line Through Electrical Conduction, Proceedings of the International Conference on Applied and Theoretical Electricity (ICATE), Romania, Craiova, 4–6 October 2018, IEEE: Piscataway, NJ, USA, 2018, doi:10.1109. (**ISI, WOS:000487278600058**)

[C8] A. Boitan, S. Halunga, R. Bărtușică, V. Bîndar, Video signal recovery from the laser printer LCD display, Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies IX, 2018, International Society for Optics and Photonics, Volume 10977, Pages 1097726, doi:10.1117/12.2324759. (**ISI, WOS:000458717900077**)

[C9] B. Trip, V. Butnariu, A. Boitan, S. Halunga, V. Bîndar, Video Signal Recovery from the Smartphones Touchscreen LCD Display, FABULOUS 2019: Future Access Enablers for Ubiquitous and Intelligent Infrastructures, pp 89-95, DOI: 10.1007/978-3-030-23976-3_9. (**ISI, WOS:000552334400009**)

[C10] Boitan, A.; Bătușică, R.; Halunga, S.; Fratu, O. Electromagnetic Vulnerabilities of LCD Projectors. In Proceedings of the 6th Conference on the Engineering of Computer Based Systems, Bucharest, Romania, 2–3 September 2019; University Politechnica of Bucharest: Bucharest, Romania, 2019; pp. 1–6, doi:10.1145/3352700.3352722. (**ISI, WOS:000525376600022**)

[C11] V. Velicu, A. Boitan, V. Butnariu, B. Trip, M. I. Rebican, V. Ionita, Experimental Study of Radiated Compromising Emanations for Computer Monitors, 2019 6th International Symposium on Electrical and Electronics

Engineering (ISEEE), 2019, Pages 1-4, Publisher IEEE, DOI: 10.1109/ISEEE48094.2019.9136138 (**ISI, WOS:000614815800037**)

[C12] R Bărtuşică, A Boitan, O Fratu, M Mihai, Processing gain considerations on compromising emissions, Proc. SPIE 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, 2020, https://doi.org/10.1117/12.2571272. (**ISI, WOS:000641147900072**)

[C13] B Trip, V Butnariu, V Velicu, S Halunga, A Boitan, Analysis of the Compromising Audio Signal From the Emission Security Perspective, 2020 13th International Conference on Communications (COMM), 2020, Pages 363-366, Publisher IEEE, DOI: 10.1109/COMM48946.2020.9142022. (**ISI, WOS:000612723900064**)

[C14] Bogdan Trip, Vlad Butnariu, Valentin Velicu, Simona Halunga, Alexandru Boitan, "Analysis of PS/2 compromising emanations", Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, Volume 11718, Pages 1171823, Publisher International Society for Optics and Photonics, 31 December 2020, DOI: 10.1117/12.2571338. (**ISI, WOS:000641147900074**)

[C15] V. Velicu, V. Butnariu, B. Trip, A. Boitan, V. Ionita, Experimental study of shielding composite materials for protection of computer systems, 2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE), 2021, Pages 1-4, Publisher IEEE, DOI: 10.1109/ATEE52255.2021.9425176. (**ISI, WOS:000614815800037**)

6.4. Future development perspectives

We intend to publish the results of our research on RS232 serial communication and RJ-45 interface in the period immediately following the successful accomplishment of our PhD thesis. We will also take into account the publication of the detailed results of the measurements carried out to evaluate the shielding effectiveness of the shielded enclosures and shielding materials presented as TEMPEST protection alternatives in Chapter 5.

Bibliography

[1]. NATO Standard (2016) SDIP-27/2: NATO TEMPEST Requirements and Evaluation Procedures, (published March 2016 but not for public use, NATO CONFIDENTIAL), *NATO Military Committee Communication and Information Systems Security and Evaluation Agency* (SECAN).

[2]. EU Standard (2013) IASG 7–03: Information assurance security guidelines on EU TEMPEST requirements and evaluation procedures (published March 2016 but not for public use, EU CONFIDENTIAL). *General Secretariat of the Council of the European Union* (GSC).

[3]. A. Boitan, R. Bărtușică, S. Halunga, M. Popescu, I. Ionuță, Compromising Electromagnetic Emanations of Wired USB Keyboards, International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2017, Bucharest, pp. 39-44, DOI: 10.1007/978-3-319-92213-3_6, 2017

[4]. US Department of Defence, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, MIL-STD-461G, 11 December, 2015, https://govtribe.com/file/government-file/attachment-2-mil-std-461g-dot-pdf

[5]. Rohde&Schwarz AM524 active antenna system, https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/AM524_cat_2015_48-49.pdf, 2021

[6]. Rohde&Schwarz FSET22 receiver, https://docplayer.net/3509140-Test-receiver-r-s-fset7-r-s-fset22-rf-preselector-r-s-fset-z2-r-s-fset-z22-measurement-and-evaluation-of-compromising-emissions.html, 2021

[7]. A. Boitan, S. Halunga, V. Bîndar, Compromising Electromagnetic Emanations of USB Mass Storage Devices, 7th Annual Workshop of the CTIF-SEE at AIT, Athens, *Wireless Personal Communications*, 2020, p. 1-26, https://doi.org/10.1007/s11277-020-07329-8

[8]. I. Kubiak, A. Boitan, S. Halunga, Assessing the Security of TEMPEST Fonts against Electromagnetic Eavesdropping by Using Different Specialized Receivers, Applied Sciences, 2020, 10, 2828, https://doi.org/10.3390/app10082828.

[9]. Alexandru Boitan, Ireneusz Kubiak, Simona Halunga, Artur Przybysz, Andrzej Stańczak, Method of Colors and Secure Fonts Used for Source Shaping of Valuable Emissions from Projector in Electromagnetic Eavesdropping Process, Multidisciplinary Digital Publishing Institute, Symmetry 2020, 12(11), 1908, https://doi.org/10.3390/sym12111908.

[10]. Bogdan Trip, Vlad Butnariu, Mădălin Vizitiu, Alexandru Boitan, Simona Halunga, Analysis of Compromising Video Disturbances through Power Line, Sensors 2022, 22(1), 267; State-of-the-Art Sensors Technology in Romania 2021, https://doi.org/10.3390/s22010267.