UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI

Şcoala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

Decizie nr. 876 din 08-07-2022

REZUMAT TEZĂ DE DOCTORAT

Ing. Alexandru-Dan BOITAN

STUDII PRIVIND SECURITATEA INFORMAȚIILOR
- ANALIZĂ DIN PERSPECTIVA VULNERABILITĂȚILOR TEMPEST

RESEARCH ON INFORMATION SECURITY
- ANALYSIS FROM THE TEMPEST VULNERABILITY PERSPECTIVE

COMISIA DE DOCTORAT

Prof. Dr. Ing. Mihai CIUC Universitatea Politehnica din Bucureşti	Preşedinte
Prof. Dr. Ing. Simona HALUNGA Universitatea Politehnica din Bucureşti	Conducător de doctorat
Prof. dr. ing. Corina NAFORNIȚĂ Universitatea Politehnica din Timișoara	Referent
Prof. dr. ing. Ioan NICOLAESCU Academia Tehnică Militară din București	Referent
Prof. Dr. Ing. Ion MARGHESCU Universitatea Politehnica din Bucureşti	Referent

BUCUREŞTI 2022

Cuprins

Capitolul 1

Introducere

1.1 Prezentarea domeniului tezei de doctorat

În prezent dispozitivele electronice sunt utilizate pe scară largă pentru procesarea informațiilor, iar acest lucru se aplică nu numai dispozitivelor individuale, ci și sistemelor mai complexe, care pot fi utilizate în scopuri personale, în cadrul societăților sau companiilor comerciale sau chiar pentru aplicații militare. Este mai puțin cunoscut faptul că, prin recepționarea anumitor emisii electromagnetice generate de comunicațiile analogice sau digitale și prin aplicarea tehnicilor de prelucrare a semnalelor, este posibilă refacerea parțială sau totală a informațiilor transmise de comunicația vizată. Aceste aspecte sunt studiate de domeniul TEMPEST, al cărui obiect principal este tocmai protecția informațiilor sensibile împotriva acestor tipuri de atacuri. Acea parte a radiației electromagnetice care poate dezvălui informații se numește emanație sau emisie compromițătoare (CE – Compromising Emanation) în domeniul TEMPEST. Emisiile compromițătoare sunt definite ca fiind semnale neintenționate purtătoare de informații care, dacă sunt interceptate și analizate, pot dezvălui informațiile transmise, primite, manipulate sau prelucrate în alt mod de orice echipament de procesare a informațiilor.

Standardizarea acestui domeniu s-a extins atât în alianța NATO (standarde SDIP) [1] cât și la nivel UE (standarde IASG) [2] și orice țară membră, NATO sau UE, trebuie să respecte cerințele acestor standarde atunci când manipulează informații clasificate “secrete de stat” prin intermediul echipamentelor electrice, electronice sau optoelectronice. Standardele includ reguli de evaluare a nivelului de protecție oferit de spațiul fizic (mediu/zona securizat/ă) în care va funcționa echipamentul (SDIP-28 la nivel NATO şi IASG 7-02 la nivel UE), nivelul de protecție oferit de echipament (SDIP-27 la nivel NATO şi IASG 7-03 la nivel UE), precum și reguli și principii care trebuie implementate la instalarea acestuia (SDIP-29 la nivel NATO şi IASG 7-01 la nivel UE).

Rezultatele prezentate în această lucrare sunt obținute prin efectuarea unor măsurători specializate de laborator, specifice domeniului TEMPEST.

1.2 Scopul tezei de doctorat

Scopul acestei lucrări este în primul rând de conștientizare a publicului larg cu privire la existența vulnerabilităților TEMPEST care pot pune în pericol confidențialitatea informațiilor procesate prin intermediul echipamentelor electronice.

În al doilea rând, s-a dorit prezentarea metodelor posibile de protecție TEMPEST care ne pot proteja de amenințările de securitate prezentate în această lucrare și s-a avut în vedere de asemenea, și aspectul financiar al aplicării acestor metode de protecție.

Nu în ultimul rând, prin elaborarea acestei lucrări s-a dorit obținerea unui material consistent și sustenabil din punct de vedere tehnic care poate fi inclus, parțial sau total, în standardele TEMPEST existente la nivel național, NATO sau UE.

1.3 Conținutul tezei de doctorat

Această lucrare este structurată în 6 capitole. În capitolul 2 este tratată problema vulnerabilităților TEMPEST generate de comunicațiile USB.

În capitolul 3 vor fi analizate două fonturi de securizare TEMPEST care pot fi utilizate pentru asigurarea protecției informațiilor sensibile în cazul prelucrării acestora în format text. Fonturile analizate au obținut protecția Oficiului polonez de modele sub forma desenului industrial nr. 24487 (2018) și a brevetului nr. 231691 (2019).

În capitolul 4 vor fi analizate vulnerabilitățile de securitate datorate utilizării videoproiectoarelor. Va fi analizată și eficiența fonturilor de securizare TEMPEST în cazul utilizării unei palete cât mai largi de culori pentru text și fundal dar și prezentarea metodei culorilor care poate fi utilizată atât pentru minimizarea radiațiilor compromițătoare generate de echipamentul vizat cât și ca metodă de evaluare TEMPEST a echipamentelor în cazul analizării semnalului video de afișare.

În cadrul capitolului 5 vor fi prezentate principalele metode consacrate de protecție TEMPEST dar și metode inovative. Vor fi prezentate succint și rezultatele măsurătorilor de evaluare a eficacității de ecranare a tuturor soluțiilor prezentate în cadrul acestui capitol. În acest capitol vor fi prezentate și rezultatele unui studiu privind propagarea prin conducție a perturbațiilor compromițătoare pe linia de alimentare electrică la distanțe considerabile precum și, metode de protecție care pot fi utilizate împotriva acestei vulnerabilități electromagnetice.

În capitolul 6 vor fi prezentate concluziile acestei lucrări dar și sinteza rezultatelor prezentate în cadrul fiecărui capitol al lucrării. Capitolul 6 cuprinde de asemenea, sinteza contribuțiilor originale care vizează în primul rând metodele inovatoare de protecție TEMPEST. Acest capitol include de asemenea, lista articolelor publicate pe toată perioada stagiului doctoral, rezultatele prezentate în cinci dintre acestea fiind incluse parțial în această lucrare.

Capitolul 2

Emisiile compromițătoare generate de dispozitivele USB

Universal Serial Bus (USB) a devenit nelipsită în implementarea echipamentelor IT&C și de aici derivă importanța cercetărilor privind vulnerabilitățile de securitate ale acestei magistrale de date.

2.1. Standardizarea comunicației USB

În această secțiune au fost prezentate toate versiunile de standardizare existente ale magistralei USB precum și principalele specificații tehnice ale acestora.

2.2. Interfața USB

În cadrul acestei secțiuni s-a prezentat configurația pinilor (pinout) pentru toate interfețele USB existente în prezent.

2.3. Funcționarea comunicației USB

În această secțiune au fost prezentate principiile funcționale precum și, beneficiile utilizării acestei magistrale de date.

2.4. Controlere USB

În această secțiune au fost prezentate toate controlerele USB existente în implementările prezente.

2.5. Tipuri de transferuri USB

În această secțiune au fost prezentate cele 4 tipuri de transferuri USB, funcționarea și specificațiile acestora conform standardelor USB în vigoare.

2.6. Inițializarea dispozitivelor USB

Atunci când un dispozitiv USB este conectat pentru prima dată la magistrala USB este inițiat procesul de enumerare USB prin care se realizează schimbul de informații între dispozitiv și gazdă în vederea identificării particularităților dispozitivului USB.

2.7. Specificaţii electrice

În această secțiune a fost făcută o sinteză a informațiilor extrase din standardele USB care stabilesc specificațiile generale ale magistralei în funcție de versiune și care vor fi utilizate în secțiunile următoare pentru analiza radiațiilor compromițătoare (CE) generate de comunicația USB.

2.7.1. Codarea datelor USB

În această secțiune s-a prezentat codarea NRZI (*Non Return to Zero Inverted* – schema inversata de codare fără întoarcere la zero) precum și criteriul de *completare cu biți (bit-stuffing)* utilizate de această comunicație de date. Au fost prezentate de asemenea, tensiunile electrice existente pe linia de date USB.

2.7.2. Durata bitului USB

În această secțiune au fost sintetizate informațiile referitoare la perioada de bit USB corespunzător versiunilor 1.0, 1.1 și 2.0.

2.7.3. Timpii de creștere și descreștere a unui bit USB

S-a prezentat duratele pantelor de creștere și descreștere a unui bit USB corespunzător versiunilor 1.0, 1.1 și 2.0.

2.7.4. Stările de semnalizare USB

În această secțiune au fost prezentate stările de semnalizare utilizate de comunicația USB 1.0, 1.1 și 2.0.

2.8. Câmpurile pachetelor USB

Au fost prezentate principalele câmpuri care se regăsesc în cadrul pachetelor USB corespunzător versiunilor 1.0, 1.1 și 2.0.

2.9. Rezilienţa USB și protecția TEMPEST

În această secțiune au fost prezentate principalele avantaje funcționale ale acestei magistrale de date în baza cărora este considerată ca fiind fiabilă și rezistentă la interferențe. O parte din rezultatele prezentate în secțiunea 2.10 au fost publicate în [3].

2.10. Tastatura USB

Au fost prezentate în această secțiune rezultatele publicate în 15 articole de referință care au tratat vulnerabilitățile de securitate ale acestor periferice (tastaturi PS/2, USB și Wireless) datorită emisiilor compromițătoare generate de acestea.

2.10.1. Configurația de măsură utilizată

Cercetările au fost efectuate într-un laborator specializat TEMPEST care constă din două incinte ecranate adiacente. Una dintre ele este semi-anecoică, fiind căptușită cu material radio-absorbant pe pereți dar nu și pe podea. În cercetarea dezvoltată în cadrul prezentei lucrări s-au folosit un sistem de antene active AM524 [5] și un receptor TEMPEST FSET22 [6], ambele produse de firma Rohde & Schwarz. Filtrul de captură (RBW) al receptorului FSET22 poate ajunge la o lărgime de bandă maximă de până la 500 MHz, care este maximul posibil pentru un receptor de test în acest moment pe piață. Echipamentul testat (EUT) este reprezentat de tastatura USB care a fost conectată la un calculator ecranat (sau TEMPEST), instalat în condiții normale de lucru. Folosirea calculatorului ecranat (care asigură cel mai ridicat nivel de protecție TEMPEST) este obligatorie în cazul testării TEMPEST a perifericelor întrucât emisiile generate de acest echipament (care este considerat auxiliar) trebuie să aibă un nivel inferior celui impus de limita TEMPEST față de care este verificat echipamentul periferic. Atât poziționarea EUT pe masa de testare cât și poziționarea antenelor utilizate și spațierea acestora față de EUT (distanța de 1 metru) s-a realizat conform standardelor militare de compatibilitate electromagnetică MIL STD 461G [4]. Deoarece standardele TEMPEST sunt clasificate, informațiile nu pot fi dezvăluite și în consecință va fi considerată drept referință configurația specificată în aceste standarde CEM militare care prezintă cea mai apropiată configurație dintre toate standardele de compatibilitate electromagnetica (CEM). Pe tot parcursul activităților de evaluare TEMPEST ale autorului (18 ani) nu au fost întâlnite tastaturi USB care să utilizeze viteze de transfer specifice magistralei USB 2.0. Astfel, exemplele ilustrate în această lucrare se vor limita la semnalele CE generate de tastaturile USB 1.0 și 1.1.

2.10.2. Comunicația tastaturilor USB 1.0

În prima parte a acestei secțiuni a fost analizat semnalul de ceas care este transmis pe magistrala USB 1.0. Radiația CE constă din emisii electromagnetice generate la nivelul tranzițiilor semnalului electric. Practic, un bit de date generează 2 emisii distincte, una corespunzătoare frontului crescător al bitului de date și respectiv cealaltă corespunzătoare frontului descrescător. În a doua parte a acestei secțiuni a fost analizat pachetul de date transmis pe magistrală la acționarea unei taste. Corespunzător tastaturilor USB 1.0 au fost prezentate și analizate radiațiile CE ale tastelor ‚q', ‚p', ‚c', ‚k', ‚1' și ‚1 numlock' situat pe tastatura numerică. De exemplu, radiația CE generată de acționarea tastei ‚q' este ilustrată în figura 2.19.

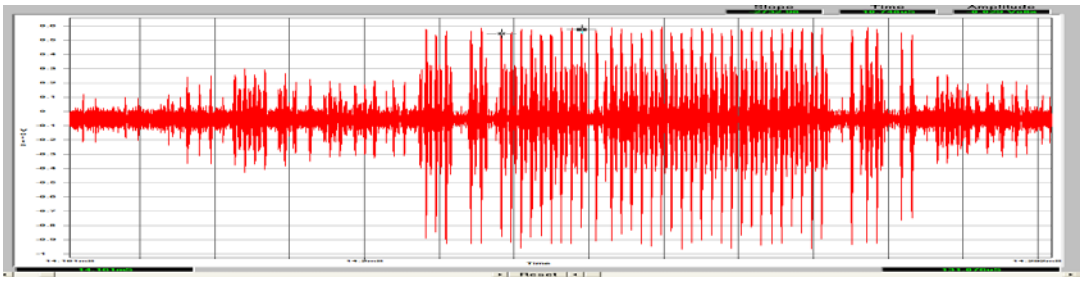


Figura 2.19 *Radiația CE corespunzătoare acționării tastei 'q'*

2.10.3. Comunicația tastaturilor USB 1.1

În prima parte a acestei secțiuni a fost analizat semnalul de ceas care este transmis pe magistrala USB 1.1 și ulterior pachetul de date transmis la acționarea unei taste. Au fost prezentate rezultatele obținute, similar cu secțiunea 2.10.2. De exemplu, radiația CE generată de acționarea tastei 'c' este ilustrat în figura 2.40.

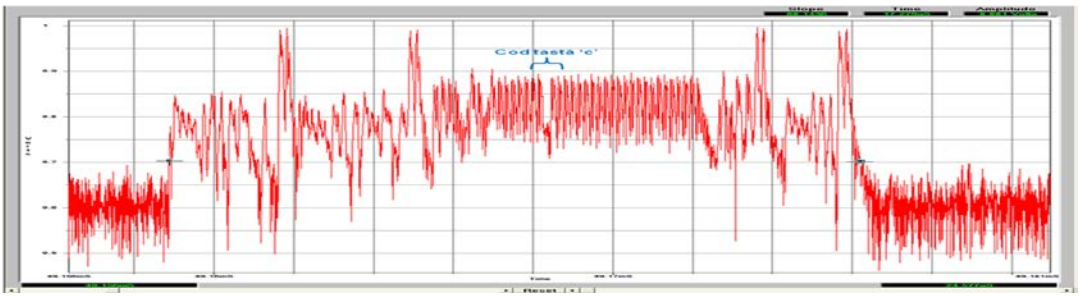


Figura 2.40 *Radiația CE recepționată corespunzător acționării tastei ,c'*

Au fost prezentate rezultate similare corespunzător tastelor ,p', ,q', ,m', ,k', ,j', ,1' și ,1 numlock'situat pe tastatura numerică. Au fost alese și taste comune între cele două versiuni pentru a facilita comparația. Verificarea informațiilor extrase din radiațiile CE generate de acționările tastelor ilustrate în cadrul secțiunilor 2.10.2 și 2.10.3 s-a realizat prin comparația cu informațiile extrase din standardele USB dar și cu semnalele electrice transferate pe magistrala USB, captate cu osciloscopul prin sondare galvanică.

2.11. Dispozitivele USB de stocare date

În această secțiune au fost prezentate rezultatele prezentate în 8 publicații care au tratat vulnerabilitățile de securitate ale acestui tip de transfer USB datorită emisiilor compromițătoare generate de acestea. O parte din rezultatele prezentate în secțiunea 2.11 au fost publicate în [7].

2.11.1. Configurația de măsură utilizată

Testele au fost efectuate în același laborator TEMPEST descris în cadrul secțiunii 2.10.1 precum și echipamente de măsură prezentate în această secțiune.

2.11.2. Comparație între CEM și TEMPEST

Au fost prezentate rezultatele testului comparativ între specificațiile CEM și TEMPEST, care au arătat că este posibil ca echipamentele electronice să treacă testele de conformitate CEM, dar nu și testele efectuate în conformitate cu procedurile TEMPEST.

2.11.3. Dispozitivele ecranate și neecranate

În această secțiune au fost prezentate comparativ radiațiile CE generate de un stick USB neecranat față de cele generate de unul ecranat în gama de frecvențe 420-520 MHz. Ca urmare a rezultatelor obținute, a fost recomandă utilizarea dispozitivelor USB ecranate pentru stocarea sau transportul informațiilor sensibile.

2.11.4. Emisiile compromițătoare generate de magistrala USB

Pentru analiza TEMPEST a comunicației USB în cazul transferurilor în masă sau în blocuri mari de date (transferuri bulk), s-au generat fișiere de date prin multiplicarea succesivă a unor secvențe hexazecimale predefinite: "FFFF00", "3F" și "FF".

2.11.4.1. Ceasul magistralei USB

În cadrul acestei secțiuni a fost analizat semnalul de ceas care este transmis pe magistrala USB 1.1 și 2.0, similar cu secțiunile 2.10.2 și 2.10.3.

2.11.4.2. Pachetul de date USB 1.1 în cazul transferurilor de tip bulk

S-a ilustrat radiația CE generată de pachetele de date transmise pe magistrala USB 1.1. De exemplu, corespunzător șablonului "3F", semnalul electric și radiația CE generată de acesta sunt ilustrate în figurile 2.70 și 2.71.

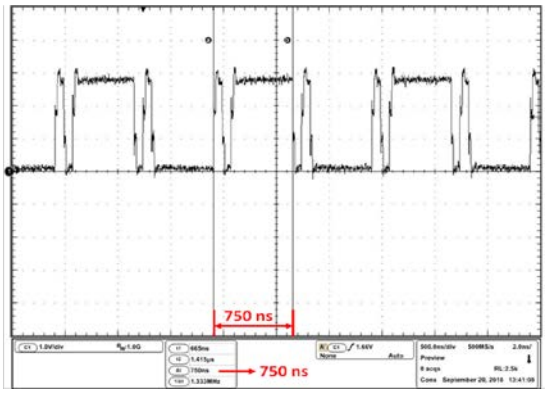


Figura 2.70 *Șablon „3F” (HEX), domeniul electric (T_{CE} =750 ns)*

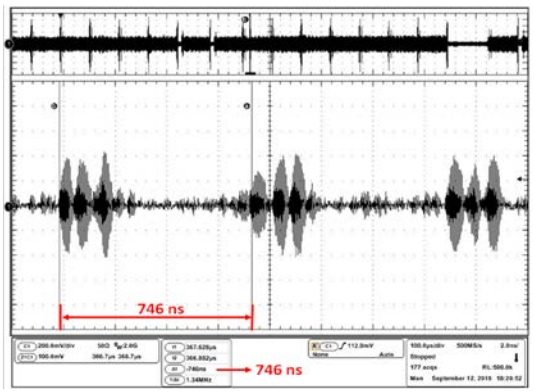


Figura 2.71 *Radiația CE corespunzătoare șablonului „3F” (HEX) (T_{CE} =746 ns)*

Au fost ilustrate atât radiația CE generată de transferul USB specificat, cât și semnalul electric care este sursa radiației CE pentru a verifica acuratețea semnalelor CE recepționate.

2.11.4.3. Definirea șablonului digital

În această secțiune a fost justificată forma de undă a radiației CE corespunzătoare șablonului digital (succesiunea hexazecimală) „3F". Radiația CE generată de șablonul hexazecimal „3F" a fost ilustrată în figura 2.71.

2.11.4.4. Pachetul de date pentru USB 2.0 în cazul transferurilor de tip bulk

În această secțiune a fost verificată posibilitatea recepției radiației CE generată de pachetele de date transmise pe magistrala USB 2.0 atunci când este realizat transferul fișierelor de test descrise în cadrul secțiunii 2.11.4.2. De exemplu, corespunzător șablonului "FF" au fost ilustrate semnalul electric și radiația CE generată de acesta în figurile 2.73 și 2.74.

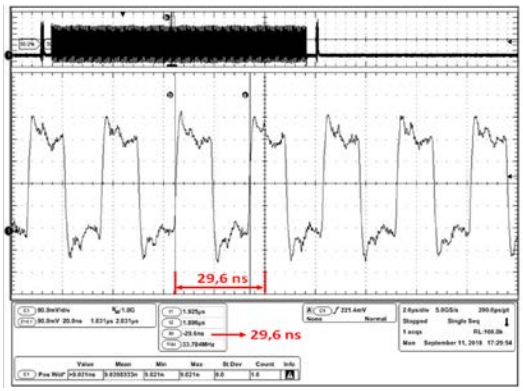


Figura 2.73 *Șablon „FF" (HEX), domeniul electric (T_{CE} =29.6 ns)*

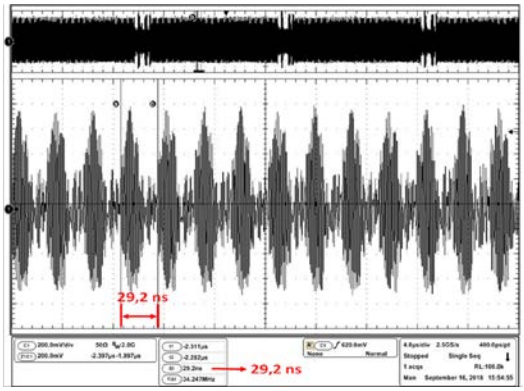


Figura 2.74 *Radiația CE corespunzătoare șablonului „FF" (HEX), (T_{CE} =29.2 ns)*

2.11.4.5. Calitatea semnalului CE în raport cu lățimea filtrului de captură

În această secțiune s-a prezentat influența lărgimii de bandă a filtrului de captură (RBW-ului) a receptorului utilizat în recepția corectă a radiației CE, care va permite în acest fel decelarea informațiilor la nivel de bit. Dacă este aleasă o valoare inferioară a RBW, radiația CE va fi recepționată în continuare dar nu va fi posibilă recuperarea integrală a informațiilor. Studiul a fost realizat pentru comunicația USB 1.1 și rezultatele au fost extrapolate și pentru comunicația USB 2.0.

Capitolul 3

Semnalul video

3.1. Semnalul video de afișare

Semnalul video de afișare este semnalul video generat de placa video a unui calculator personal care este transferat prin interfețe video dedicate către un dispozitiv de afișare. În această introducere au fost prezentate semnalele analogice de afișare video: video compozit, S-Video, video component.

3.2. Interfața VGA

În această secțiune a fost prezentată interfața VGA precum și, configurația pinilor (pinout) și semnalele transmise pe această interfață video analogică.

3.3. Interfața DVI

În această secțiune au fost prezentate toate interfețele existente pentru semnalul de afișare DVI (Digital Visual Interface), configurația pinilor (pinout), structura semnalelor TMDS (Transition Minimized Differential Signaling), codarea utilizată precum și vitezele de transfer ale acestei interfețe de afișare video.

3.4. Interfața HDMI

Au fost prezentate principalele specificații tehnice ale tuturor versiunilor de standardizare HDMI (High-Definition Multimedia Interface) dar și interfețele fizice existente și configurația pinilor.

3.5. Interfața DisplayPort

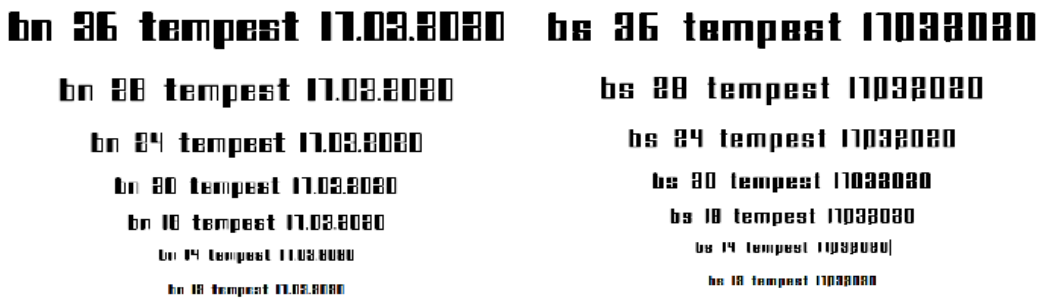
DisplayPort (DP) este singura interfață video care utilizează pachetizarea fluxului de date. Au fost prezentate principalele specificații tehnice ale tuturor versiunilor de standardizare DP, interfețele fizice utilizate și configurația pinilor.

3.6. Semnalul video de afișare din perspectiva domeniului TEMPEST

În această secțiune au fost prezentate rezultatele sintetice a peste 30 de publicații în care au fost tratate vulnerabilitățile de securitate ale interfețelor video de afișare (VGA, DVI, HDMI și DP) datorate emisiilor compromițătoare generate de acestea. Rezultatele cercetărilor prezentate în acest capitol au fost publicate în [8].

3.7. Modelarea surselor CE

În această secțiune a fost analizată eficacitatea modelării surselor de emisii compromițătoare (CE) care limitează eficacitatea infiltrării electromagnetice. Acest lucru se poate realiza prin folosirea unor fonturi de calculator specializate care au fost concepute tocmai pentru a îndeplini acest obiectiv și care sunt numite și fonturi de securizare TEMPEST. Fonturile de securizare utilizate sunt illustrate în figura 3.1.



(a) *(b)*

Figura 3.1 *Caracterele fonturilor securizate:*
(a) font securizat asimetric, (b) font securizat simetric

Fonturile securizate prezentate au obținut protecția Oficiului Polonez de modele și patentare sub forma desenului industrial nr. 24487 și a brevetului nr. 231691 și reprezintă o metodă inovativă și în continuă evoluție care poate sprijini protecția informațiilor procesate în format text.

3.7.1. Configurația de măsură utilizată

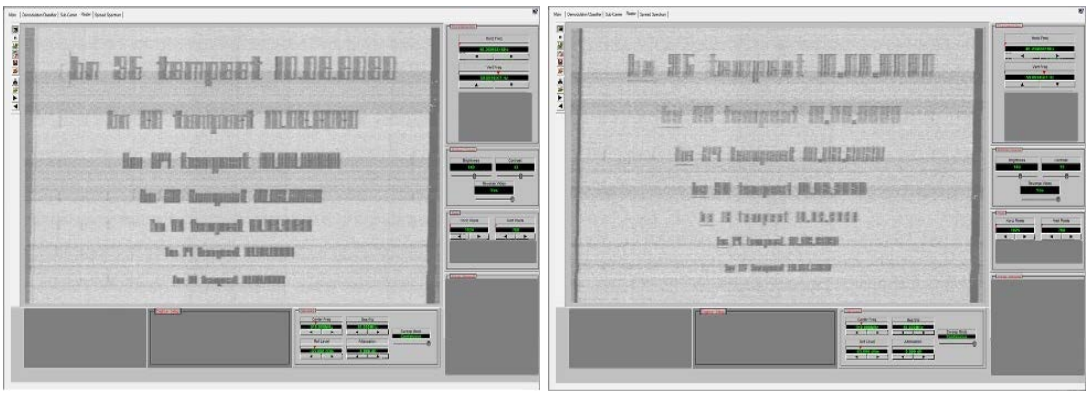
Testele au fost efectuate cu un laptop Fujitsu Siemens, model Lifebook C110 și echipamente de măsură utilizate au fost prezentate în cadrul secțiunii 2.10.1.

3.7.1. Parametrii semnalului video de afișare

În această secțiune uu fost prezentați în detaliu parametrii semnalului video de afișare corespunzători calculatorului portabil utilizat în cadrul testelor, conform standardului VESA DMT v1.3.

3.7.2. Rezultatele măsurătorilor efectuate

S-au efectuat teste specifice pentru standardul de afișare VGA care este încă foarte popular în sistemele clasificate. Verificarea eficacității fonturilor securizate prin analiza vizuală a fost efectuată în două medii de măsurare distincte: o cameră anecoică a laboratorului MCI (Institutului Militar de Comunicații) din Polonia și o cameră semianecoică a STS (Serviciului de Telecomunicații Speciale) din România. Fiecare laborator a utilizat un receptor de măsurare TEMPEST diferit. Acest aspect a reprezentat tocmai scopul evaluării comparative a noilor fonturi în procesarea securizată a informațiilor în format text. În această secțiune au fost prezentate rezultatele obținute de laboratorul TEMPEST din cadrul STS, prin utilizarea a două receptoare TEMPEST, FSET22 și FSWT26, care au confirmat eficiența noii metode propuse. În figurile 3.5 (a) și (b) sunt prezentate rezultatele testelor sub formă de imagini reproduse din recepția emisiilor compromițătoare generate de EUT, corespunzător utilizării fonturilor securizat asimetric și asimetric.

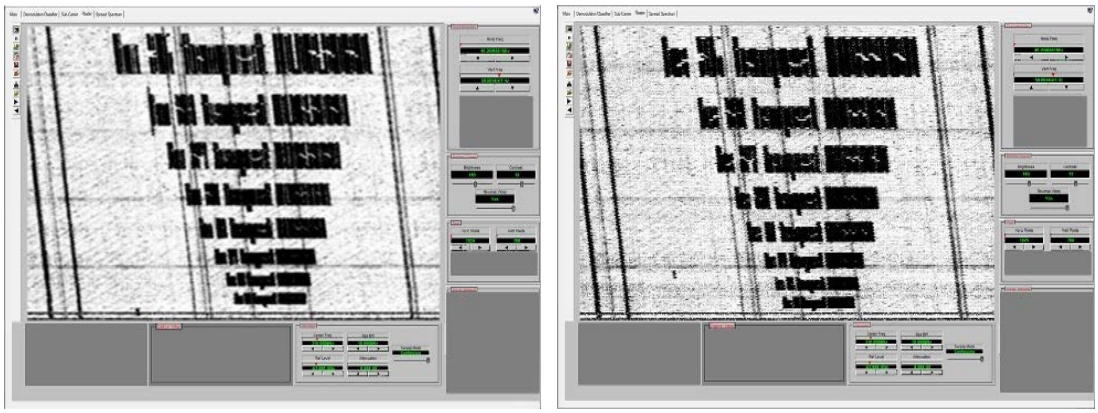


(a) *(b)*

Figura 3.5 *Imagine refacută cu receptor FSET22 pentru afișare cu font: securizat asimetric(a) și securizat simetric (b)*

Receptorul FSWT26 este cel mai recent model de receptor TEMPEST lansat pe piață de către compania germană Rohde&Schwarz. Acest echipament vine cu modulul raster încorporat. Eficiența fonturilor securizate a fost comparată cu cea a fonturilor tradiționale, Arial și Times New Roman, pentru diverse dimensiuni ale acestora: 72, 36, 28, 24, 20, 18, 14 și 12. În fiecare caz, au fost detectate emisii compromițătoare, care au fost înregistrate și rasterizate (refăcute). În cadrul testelor au fost utilizate atât litere majuscule cât și minuscule, cifre arabe, scris normal și îngroșat (bold) dar și introducerea spațiilor libere între caracterele alfanumerice scrise cu fonturi securizate asimetrice și simetrice pentru o mai bună inteligibilitate a informațiilor cuprinse în cadrul imaginilor rasterizate.

Rezultatele prezentate în figura 3.5 au fost obținute pentru frecvența de recepție de 910 MHz, aleasă favorabil pentru a evita zgomotul electromagnetic generat de alimentatorul electric al laptop-ului folosit în cadrul testelor efectuate. În figura 3.20 sunt ilustrate refacerile video corespunzătoare fonturlor securizate (asimetri și simetric) realizate pe frecvența de 310 MHz.



(a) *(b)*

Figura 3.20 *Font de dimensiune 36, frecvența de recepție 310 MHz: (a) font securizat asimetric, (b) font securizat simetric*

În figurile 3.20(a) și 3.20(b) pot fi observate linii verticale și orizontale care apar suplimentar în fundal în raport cu imaginile ilustrate în figurile 3.5(a) și (b). Acestea se datorează zgomotului electromagnetic existent pe frecvența de recepție dar care nu se datorează semnalului video de afișare care a fost analizat în acest capitol ci „zgomotului" electromagnetic existent pe frecvența de recepție respectivă.

Testele de conformitate TEMPEST nu se rezumă doar la emisiile radiate de EUT și sunt efectuate de asemenea și pentru emisiile conduse ale acestuia. Pentru evaluarea emisiilor conduse pe linia de alimentare a EUT s-a folosit un traductor TEMP 8400, fabricat de firma Schwarzbeck.

În figura 3.23 sunt illustrate refacerile video realizate pentru fonturile securizate (simetric și asimetric) prin recepția perturbațiilor CE propagate pe linia de alimentare.

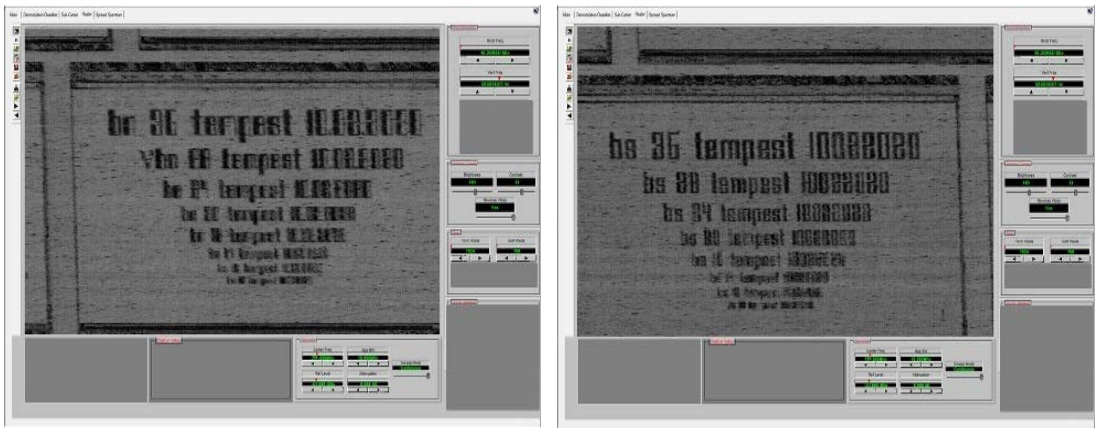


Figura 3.23 *Font de dimensiune 36, frecvența de recepție 204 MHz, emisii conduse: (a) font securizat asimetric, (b) font securizat simetric*

Ca urmare a rezultatelor obținute, considerăm că utilizarea acestor fonturi securizate poate fi introdusă ca una dintre contramăsurile oficiale TEMPEST precizate în documentele clasificate NATO și UE, care reglementează activitățile implicate în acest domeniu tehnic și care reprezintă măsuri naționale de securitate pentru echipamentele IT&C cu utilizare specifică domeniului și care trebuie implementate de fiecare stat membru NATO și UE.

Capitolul 4

Metoda culorilor

În această primă parte a capitolului sunt prezentate principalele tehnologii utilizate în producția videoproiectoarelor: DLP (Digital Light Processing), LCD (Liquid Crystal Display) și LCoS (Liquid Crystal on Silicon). Au fost prezentate de asemenea, și principalele evoluții tehnologice a acestor echipamente.

4.1. Videoproiectoarele LCD

În această secțiune au fost prezentate detaliile funcționale ale videoproiectoarelor realizate în această tehnologie.

4.2. Parametrii semnalului video de afișare

Echipamentul supus testării (EUT) a fost un videoproiector EPSON, model EH-TW650. În această secțiune au fost prezentați parametrii semnalului video de afișare, similar cu secțiunea 3.7.2.

4.3. Configurația de măsură utilizată

Testele au fost efectuate în același laborator TEMPEST, descris în cadrul secțiunii 2.10.1, prin utilizarea echipamentelor de măsură prezentate de asemenea, în cadrul aceleiași secțiuni.

4.4. Metoda culorilor

Scopul testelor și analizelor care au fost prezentate în acest capitol: vulnerabilitățile de securitate ale echipamentelor de videoproiecție, propunerea și argumentarea utilizării unor fonturi securizate de calculator pentru a contracara procesul de infiltrare electromagnetică, prezentarea metodei culorilor utilizate ca soluție de protecție electromagnetică a informațiilor grafice prelucrate, prezentarea metodei culorilor ca metodă de testare în cadrul testelor specializate de evaluare a emisiilor compromițătoare conform standardelor TEMPEST.

4.5. Măsurarea parametrilor de timp

În această secțiune au fost ilustrate rezultate experimentale care confirmă parametrii semnalului video de afișare, prezentați în cadrul secțiunii 4.2, prin utilizarea unor semnale de test selectate avantajos în vederea îndeplinirii acestui obiectiv. În figura 4.11 sunt prezentate 2 exemple de imagini de test utilizate.

a) b)

Figura 4.11 *Linii orizontale egale, culori RGB (a) și CMY (b) pe fundal alb*

Măsurarea parametrilor de timp ai semnalului video de afișare se poate face și direct cu receptorul TEMPEST, așa cum este ilustrat în figurile 4.7 și 4.8.

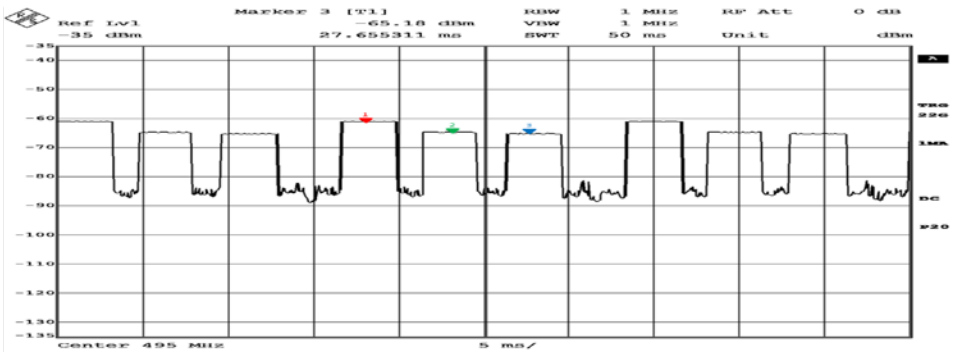


Figura 4.1 *Emisiile CE vizualizate în domeniul timp (span 0), frecvență recepție 495 MHz: marker 1 – linie orizontală în culoarea roșu, marker 2 – linie în culoarea verde, marker 3 – linie în culoarea albastru, fundal - culoare negru*

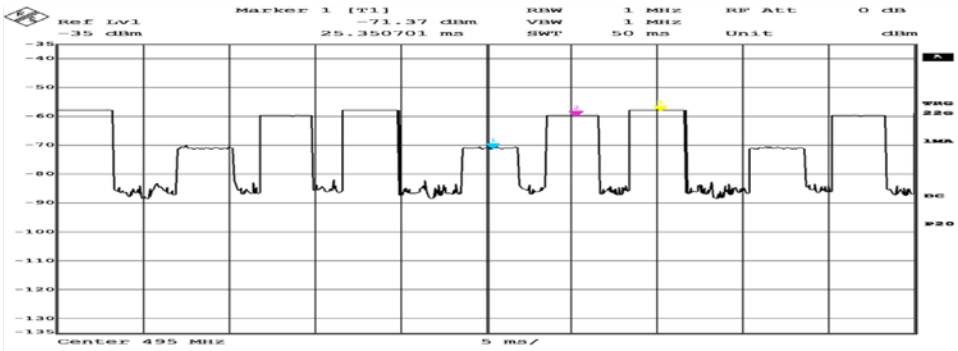


Figura4.9 *Emisiile CE vizualizate în domeniul timp (span 0), frecvență recepție 495 MHz: marker 1 – culoare cyan, marker 2 – culoare magenta, marker 3 – culoare yellow, fundal - culoare neagru*

În figurile 4.7 și 4.8 pot fi observate nivelurile diferențiate ale amplitudinilor semnalului înregistrate corespunzător celor trei culori utilizate.

Rezultatele cercetărilor prezentate în acest capitol au fost publicate în [9].

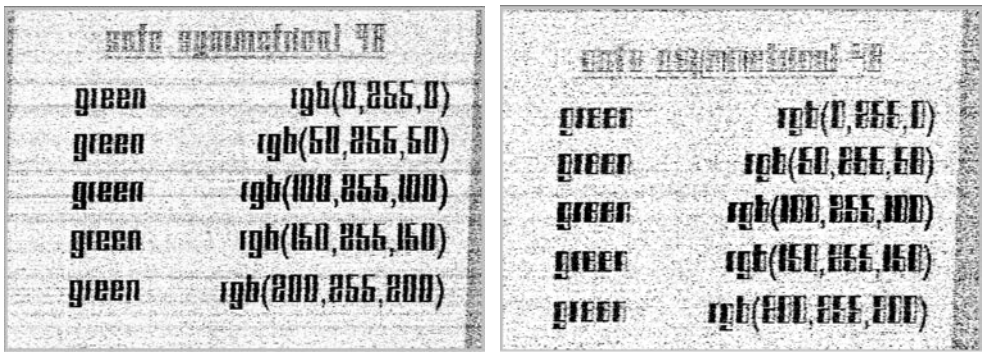
4.6. Alegerea corespunzătoare a RBW-ului

În această secțiune s-a prezentat influența lărgimii de bandă a filtrului de captură (RBW-ului) a receptorului utilizat în recepția corectă a semnalelor de test utilizate în cadrul testelor realizate, așa cum s-a procedat și în cazul radiației CE generate de comunicația USB în cadrul secțiunii 2.11.4.5.

4.7. Evaluarea fonturilor securizate

În această secțiune au fost realizate măsurători corespunzător mesajelor de test afișate în culorile primare (roșu, verde și albastru) ale modului de culoare RGB dar și în nuanțe de culoare ale acestora, pe fundal alb și negru, astfel: nuanțe de gri pe fundal alb - Negru (0,0,0), (50,50,50), (100,100,100), (150,150,150) și (200,200,200), nuanțe de roșu pe fundal alb și negru - roșu (255,0,0), (255,50,50), (255,100,100), (255,150,150) și (255,200,200), nuanțe de verde pe fundal alb și negru - verde (0,255,0), (50,255,50), (100,255,100), (150,255,150) și (200,255,200), nuanțe de albastru pe fundal alb și negru - albastru (0,0,255), (50,50,255), (100,100,255), (150,150,255) și (200,200,255), nuanțe de gri pe fundal negru - alb (255,255,255), (200,200,200), (150,150,150), (100,100,100) și (50,50,50).

La afișarea imaginilor de test corespunzătoare culorii verde au fost refăcute imaginile ilustrate în figura 4.21 prin recepția radiației CE generate de videoproiectorul testat.

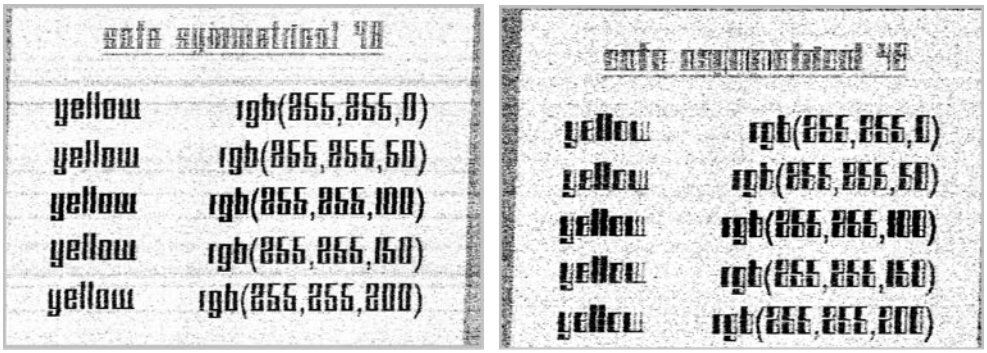


a) b)

Figura 4.21 *Imagine reconstruită corespunzător: font securizat simetric în nuanțe de verde* ***(a),*** *font securizat asimetric în nuanțe de verde* ***(b)****- fundal alb*

Modul de culoare CMY este, de asemenea, un mod de afișare foarte frecvent utilizat, folosit implicit la dispozitivele de imprimare, care folosește combinația de culori turcoaz (cyan), roșu-purpuriu (magenta) și galben (yellow). Astfel, s-au realizat și teste corespunzătoare acestor culori pentru a verifica eficiența procesului de

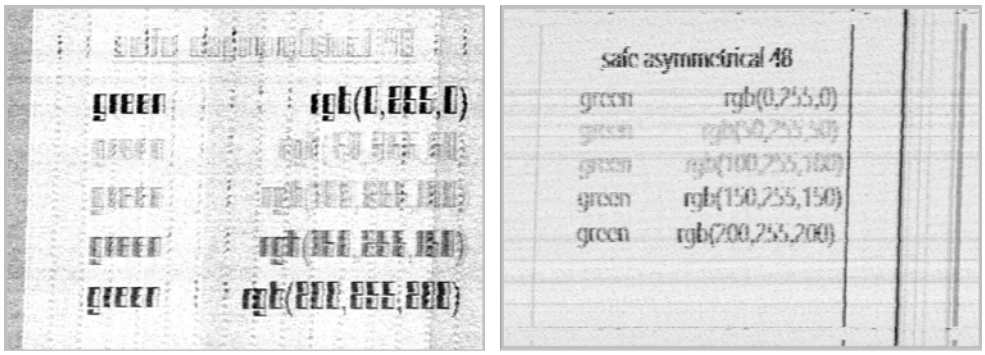
infiltrare electromagnetică pentru o plajă cât mai extinsă de culori posibile dar și pentru identificarea combinațiilor favorabile. În figura 4.27 sunt ilustrate 2 exemple în acest sens, corespunzator culorii galben. Caracterele sunt inteligibile deși sunt afișate pe un fundal alb.



a) b)

Figura 4.27 *Imagine reconstruită corespunzător: font securizat simetric în nuanțe de galben* ***(a),*** *font securizat asimetric în nuanțe de galben* ***(b)****- fundal alb*

Pentru a exprima mai bine complexitatea radiațiilor CE și influența utilizării unei palete cât mai largi de culori, au fost realizate teste pe trei frecvențe de recepție: 495 MHz, 520 MHz și 851 MHz. Rezultatele prezentate în figurile 4.21 și 4.22 au fost obținute prin recepția CE pe prima frecvență de test. În figura 4.28 sunt ilustrate două exemple pentru ultimele două frecvențe de recepție, corespunzător culorii verde și fontului asimetric și care au fost ilustrate în cadrul tezei în figurile 4.30 (b) și 4.32 (c).



a) b)

Figura 4.28 *Imagine reconstruită pe baza emisiei CE recepționate pe frecvența de 520 MHz (a) și 851 MHz (2), font securizat asimetric, dimensiune 48fundal alb*

O analiză atentă a rezultatelor obținute în urma examinării videoproiectorului ca sursă de emisii nedorite arată că metoda culorilor nu este întotdeauna eficientă pentru perechile de culori selectate. Acest lucru se datorează complexității sursei de radiații, adică a videoproiectorului. O pereche de culori selectate în mod corespunzător poate reduce nivelul emisiilor măsurate la o frecvență, în timp ce la o altă frecvență nivelul măsurat al aceleiași emisii poate rămâne neschimbat. Prin urmare, metoda culorilor poate reduce numărul de incidențe ale emisiilor nedorite.

Capitolul 5

Metode de protecție TEMPEST

În prima parte a acestui capitol au fost prezentate atât metode consacrate de protecție TEMPEST cât și metode inovative care asigură nivelul necesar de protecție cu implicarea unor costuri minime de implementare sau care prezintă avantaje operaționale evidente. Metodele consacrate sunt reprezentate de utilizarea echipamentelor protejate TEMPEST, utilizarea incintelor ecranate și utilizarea modelului zonal. Rezultatele cercetărilor prezentate în acest capitol au fost publicate în [10].

Echipamentele protejate TEMPEST care oferă cel mai ridicat nivel de protecție TEMPEST pot fi instalate în cele mai vulnerabile obiective. Acestea sunt echipamente comerciale asupra cărora s-au aplicat măsuri suplimentare de ecranare care au fost detaliate în cadrul capitolului. Fabricarea echipamentelor protejate TEMPEST trebuie să se facă sub un control atent al calității pentru a se asigura că unitățile realizate pe linia de producție sunt construite exact la fel ca cele care au fost testate în etapa de prototip și din acest motiv, companiile producătoare de echipamente protejate TEMPEST trebuie să primească acreditare pentru a putea comercializa astfel de produse.

Ca primă metodă inovativă de protecție TEMPEST, au fost prezentate rack-urile și corturile ecranate. Acestea pot fi utilizate cu succes ca alternativă a echipamentelor protejate TEMPEST. Au fost prezentate produse de acest tip, evaluate pe toată perioada stagiului doctoral: produse realizate de 3 firme producătoare de rack-uri (compania Eurotempest și 2 companii naționale acreditate la nivel NATO și UE) și 2 produse realizate de firme producătoare de corturi (firma Holland Shielding Systems BV și Soliani EMC SRL). Au fost prezentate atât avantajele cât și dezavantajele fiecărei categorii de produse precum și opțiunile tehnice și constructive care pot fi solicitate la achiziționarea acestora. A fost precizat nivelul minim de atenuare oferit de produsele testate.

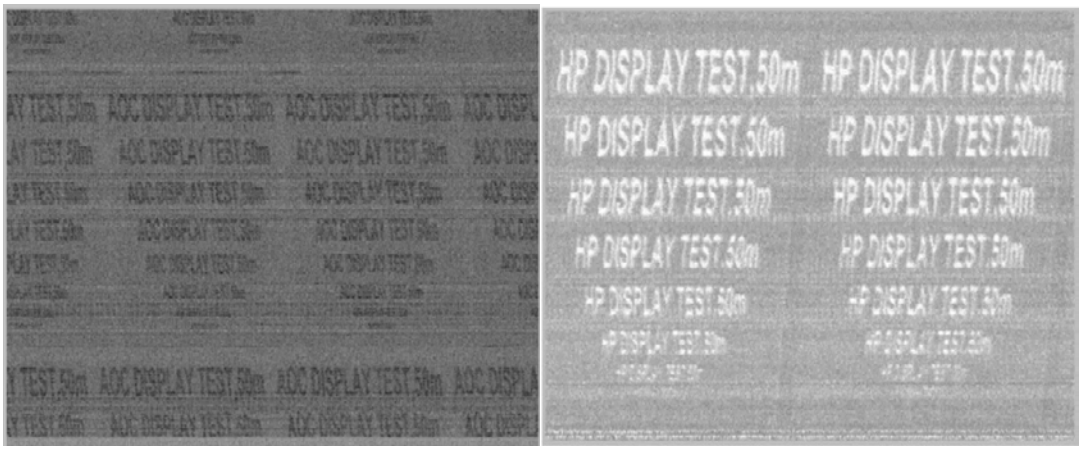
Din categoria metodelor consacrate face parte și ecranarea spațiilor în care se intenționează operaționalizarea sistemelor informatice și de comunicații care vor manipula informații sensibile. Ecranarea spațiilor fizice poate fi realizată la nivelul unei camere sau chiar la nivelul unei clădiri și de regulă se utilizează o anvelopă din tablă de cupru pentru atingerea acestui obiectiv dar și ecranarea tuturor străpungerilor ecranului: puncte/uși de acces, alimentare electrică, ventilație, țevi refrigerent sau gaz, fluxuri de comunicații de date, etc. Au fost prezentate atât avantajele cât și

dezavantajele acestei metode de protecție TEMPEST, în special în cazul ecranării clădirilor. În general, în cazul unui spațiu obișnuit de birou, peretele care cuprinde fereastra este cel mai vulnerabil din punct de vedere al protecției TEMPEST. Acest lucru se datorează faptului că fereastra prezintă în general valori foarte scăzute de atenuare electromagnetică.

Ca și metode inovative de ecranare a spațiilor fizice au fost prezentate perdele și draperii de ecranare a ferestrelor și folii de ecranare a ferestrelor. De asemenea a fost prezentată și soluția aplicării de vopsele de ecranare electromagnetică care poate fi utilizată cu succes la ecranarea pereților. Au fost prezentate mai multe produse testate de autor pe toată perioada stagiului doctoral care pot fi utilizate cu succes la confecționarea perdelelor și draperiilor de ecranare și care se regăsesc în portofoliul a două firme specializate: Holland Shielding Systems BV și Amradield. Au fost prezentate și aspecte privind confecționarea și montarea acestor produse. Din categoria foliilor de ecranare a fost prezentat un singur produs din portofoliul firmei Holland Shielding Systems BV. De asemenea, tot un singur produs a fost prezentat și din categoria vopselelor de ecranare, din portofoliul „Safe Solutions". În cazul vopselei de ecranare, s-au aplicat în total 5 straturi de vopsea și s-a evaluat eficacitatea de ecranare după fiecare strat nou aplicat. A fost precizat nivelul minim de atenuare oferit de produsele testate. Evaluarea eficacității de ecranare a materialele inovative de ecranare prezentate în acest capitol a fost realizată în mediu de laborator, prin utilizarea unei incinte ecranate de mici dimensiuni. A fost prezentată configurația de măsură dar și aspectele tehnice care trebuie avute în vedere pentru minimizarea erorilor care pot fi înregistrate la efectuarea acestor măsurători.

În partea a doua a capitolului au fost prezentate rezultatele unui studiu realizat în premieră pentru evaluarea atenuării perturbațiilor electromagnetice compromițătoare la distanțe considerabile, care se propagă condus pe linia de alimentare a echipamentelor electronice. Din perspectiva domeniului TEMPEST, cea mai mare vulnerabilitate de scurgere a informațiilor este atribuită semnalului video de afișare. În acest sens, au fost utilizate 2 monitoare de calculator, marca AOC și HP, precum și, un traductor electromagnetic de tip Line Impedance Stabilization Network (LISN), LISN TEMP 8400. Pentru propagarea la distanțele de 1, 10 și 50 metri au fost utilizate cabluri electrice prelungitoare cu această dimensiune, interpuse între cablul de alimentare al monitoarelor și echipamentul TEMP 8400. Detecția semnalului compromițător s-a realizat pentru monitorul AOC (Admiral Overseas Corporation) pe frecvența de 484 MHz în timp ce pentru monitorul HP (Hewlett-Packard), pe frecvența de 274 MHz. Măsurătorile au fost efectuate într-un spațiu de birouri, deoarece propagarea la distanțe mari nu poate fi testată într-un laborator specializat TEMPEST care nu are dimensiuni atât de generoase, de ordinul zecilor de metri.

Au fost realizate măsurători de evaluare a rapoartelor semnal pe zgomot (SNR – Signal to Noise Ratio) și s-a ilustrat de asemenea, posibilitatea refacerii imaginii (rasterizării) la aceste distanțe. Refacerea semnalului video la distanța de 50 metri, prin recepția perturbației CE propagate pe linia de alimentare a EUT, este ilustrată pentru monitorul AOC în figura 5.6(a) și pentru monitorul HP în figura 5.6(b).



(a) (b)

Figura 5.6 *Refacerea de imagine la distanța de 50 metri: (a) – monitor AOC și (b) – monitor HP*

Dacă în cazul emisiilor compromițătoare (CE) care se propagă radiat, distanțarea ne oferă protecție considerabilă, în cazul CE care se propagă condus (pe linia de alimentare electrică de exemplu) acest aspect nu mai este valabil sau poate fi considerat infim, așa cum a rezultat și din cercetarea noastră. Au fost prezentate contramăsuri, atât procedurale cât și tehnice, pentru a reduce sau chiar elimina aceste amenințări, pe baza rezultatelor și a analizei raportului semnal pe zgomot înregistrate pe parcursul cercetării noastre.

O măsură posibilă de protecție împotriva perturbațiilor compromițătoare care se pot propaga pe linia de alimentare electrică a EUT și care implică costuri reduse este aplicarea mărgelelor sau inelelor de ferită (ferrite beads/ferrite rings) care sunt construite și sub forma de clemă, fiind ușor de aplicat pe cablul de alimentare sau de date al echipamentului electronic vizat. Au fost prezentate rezultatele testelor realizate prin aplicarea inelelor de ferită pe cablul de alimentare a unui monitor. Au fost utilizate două tipuri de ferite, TDK SEIWA și FAIR-RITE VO. Prin aplicarea feritelor la un singur capăt al cablului de alimentare s-a înregistrat o atenuare de aproximativ 2dB în timp ce prin aplicarea inelelor de ferită la ambele capete ale cablului de alimentare, s-a obținut o atenuare de aproximativ 4 dB.

S-au efectuat teste și pentru comunicația USB analizată în capitolul 2, în gama de frecvență 375 MHz – 1 GHz. În acest sens, s-a conectat un stick ecranat la portul USB al unui calculator portabil care a funcționat pe toată perioada testelor cu alimentarea furnizată de la acumulator. Între stick-ul USB și portul calculatorului s-a interpus un cablu prelungitor USB, cu lungimea de 1 metru. Au fost prezentate rezultatele testelor realizate prin aplicarea inelelor de ferită pe cablul USB, la fiecare capăt al acestuia. Au fost utilizate două tipuri de ferite, FAIR-RITE VO și Wurth Elektronik. Radiația CE a fost eliminată atunci când feritele au fost aplicate la capătul situat spre EUT (stick USB).

Capitolul 6

Concluzii

În această lucrare au fost prezentate rezultatele obținute în urma realizării unor cercetări inovative în domeniul TEMPEST, specifice activității de evaluare TEMPEST a echipamentelor, în vederea identificării vulnerabilităților de securitate a acestora la emisiile electromagnetice compromițătoare (protecția EMSEC) generate de comunicația USB și semnalul video de afișare.

Deoarece oamenilor li se cere în ultima vreme să fie cât mai deschiși în ceea ce privește programul de lucru, s-a ajuns să lucrăm la calculator în interes de serviciu nu numai la birou ci și acasă, în mașină sau chiar în aer liber, în parcuri sau la locul de joacă al copiilor. Acest aspect a fost și mai accentuat în ultimii 3 ani datorită apariției pandemiei COVID-19 în lume și din cauza restricțiilor impuse pentru limitarea răspândirii virusului SARS-COV-2. Acest lucru poate fi eficient din punct de vedere al flexibilității și al optimizării timpului de lucru, dar implică și vulnerabilități semnificative în ceea ce privește securitatea informațiilor vehiculate.

Având în vedere aceste aspecte, au fost prezentate în cadrul prezentei lucrări atât metodele consacrate de protecție TEMPEST dar și metode alternative care au fost identificate pe parcursul stagiului doctoral și care au fost testate și aplicate cu succes în acest domeniu de activitate. În orice domeniu tehnic, standardele pot fi îmbunătățite pe baza publicațiilor și cercetărilor din domeniu și cu suportul întregii comunități științifice. Prin sintagma “metode alternative” trebuie să înțelegem că metodele respective nu sunt menționate în prezent de standardele în vigoare dar acest aspect nu implică faptul că nu sunt soluții viabile și eficiente pentru contracararea vulnerabilităților de securitate semnalate și considerăm că vor putea fi încorporate în viitor în standardele care reglementează domeniul TEMPEST.

6.1. Rezultate obținute

În capitolul 2 al acestei lucrări sunt ilustrate în premieră posibilitățile de recuperare la nivel de bit a informațiilor transmise pe magistrala USB, atât pentru perifericele de tip tastatură cât și pentru dispozitivele USB de stocare date, precum și, măsurile de protecție posibile care pot fi aplicate cu costuri reduse. Exemplele au vizat tastaturile USB care utilizează versiunile 1.0 și 1.1 ale acestei comunicații de date și transferurilor USB în masă sau în blocuri mari de date (transferuri bulk), corespunzător versiunilor 1.1 și 2.0, care sunt specifice conectării la un calculator

personal (gazdă USB) a oricărui mediu de stocare USB. Verificarea informațiilor extrase din radiațiile CE recepționate s-a realizat prin comparația cu informațiile extrase din standardele USB dar și cu semnalele electrice transferate pe magistrala USB, captate cu osciloscopul prin sondare galvanică.

Toate rezultatele prezentate în cadrul capitolelor 2, 3 și 4 au fost obținute în urma testelor efectuate într-un laborator specializat TEMPEST prin utilizarea echipamentelor de măsură dedicate acestui domeniu, care posedă specificațiile tehnice necesare utilizării lor în cadrul testelor de laborator impuse de standardele în vigoare din domeniul TEMPEST.

În capitolul 3 sunt prezentate rezultatele cercetărilor efectuate pentru verificarea eficacității protecției informațiilor afișate în format text prin utilizarea unor fonturi de securizare TEMPEST care au obținut protecția Oficiului Polonez de modele și patentare sub forma desenului industrial nr. 24487 și a brevetului nr. 231691 precum și, vulnerabilitățile de securitate ale echipamentelor de afișare ale echipamentelor IT&C. Fonturile securizate prezentate reprezintă o metodă inovativă și în continuă evoluție care poate sprijini protecția informațiilor procesate în format text dar ca în orice domeniu tehnic, eficacitatea soluțiilor propuse trebuie să fie supusă verificării inter-laboratoare. Eficiența fonturilor securizate a fost comparată cu cea a fonturilor tradiționale, Arial și Times New Roman, pentru diverse dimensiuni ale acestora. În cadrul testelor au fost utilizate atât litere majuscule cât și minuscule, cifre arabe, scris normal și îngroșat (bold) dar și introducerea spațiilor libere între caracterele alfanumerice scrise cu fonturi securizate asimetrice și simetrice pentru o mai bună inteligibilitate a informațiilor cuprinse în cadrul imaginilor rasterizate.

Ca urmare a rezultatelor obținute, considerăm că utilizarea acestor fonturi securizate poate fi introdusă ca una dintre contramăsurile oficiale TEMPEST precizate în documentele clasificate NATO și UE, care reglementează activitățile implicate în acest domeniu tehnic.

În capitolul 4 sunt prezentate și analizate vulnerabilitățile de securitate ale semnalului video de afișare datorate radiațiilor CE, în funcție de culorile utilizate, care este recunoscută în comunitatea științifică de specialitate ca fiind metoda culorilor. Această metodă reprezintă cea mai cuprinzătoare abordare din perspectiva evaluării TEMPEST a echipamentelor și poate fi utilizată cu succes și la protecția informațiilor afișate. Aceste vulnerabilități de securitate vizează în primul rând echipamentele IT&C care sunt utilizate în cadrul prezentărilor video și în special a videoproiectoarelor. Au fost realizate măsurători corespunzător mesajelor de test afișate în culorile primare (roșu, verde și albastru) ale modului de culoare RGB dar și în nuanțe de culoare ale acestora, pe fundal alb și negru. S-a procedat similar și pentru modul de culoare CMYK (cyan, magenta, yellow, black).

În capitolul 5 sunt prezentate metode de protecție împotriva vulnerabilităților TEMPEST semnalate (utilizarea echipamentelor protejate TEMPEST, a rack-urilor și corturilor ecranate) dar și metode inovative de ecranare electromagnetică a ferestrelor (perdele, draperii și folii de ecranare) și a pereților unui spațiu fizic (vopsea de ecranare) în care pot fi instalate în siguranță asemenea echipamente. A fost prezentată în premieră posibilitatea refacerii informațiilor afișate la distanțe considerabile (50

metri) prin recepția perturbațiilor electromagnetice generate de echipamentele IT&C și care se propagă pe linia de alimentare a acestora precum și, metodele de protecție TEMPEST care pot contracara acest fenomen. Testele au fost efectuate de această dată într-un spațiu de birouri și au vizat două dispozitive de afișare (monitoare de calculator) care au fost alimentate succesiv prin intermediul unor prelungitoare electrice cu lungimi de 1 metru, 10 metri și 50 metri. Au fost prezentate contramăsuri de protecție împotriva acestor fenomene, inclusiv aspectele financiare ale aplicării contramăsurilor TEMPEST.

Putem concluziona că fenomenul TEMPEST este complex și că metodele de protecție împotriva radiațiilor și perturbațiilor CE sunt costisitoare. În cazul în care este necesară protecția împotriva CE, un ofițer de securitate TEMPEST va fi capabil să ofere expertiză tehnică personalizată, în funcție de echipament, locație și nivelul de clasificare a informațiilor.

6.2. Contribuții originale

Contribuțiile originale cuprinse în prezenta lucrare reprezintă rezultatul cercetărilor și studiilor efectuate pe toată perioada ciclului doctoral și pot fi sintetizate astfel:

1. Studiu privind vulnerabilitatea electromagnetică impusă de utilizarea tastaturilor USB;
2. Prezentarea în premieră a posibilității identificării fără echivoc a tastelor USB 1.0 și 1.1 acționate de la aceste periferice indispensabile pentru echipamentele IT&C prin capacitatea de recuperare a codurilor tastelor USB la nivel de bit din recepția și analiza radiațiilor compromițătoare generate de aceste echipamente precum și prezentarea parametrilor de detecție și analiză necesari îndeplinirii acestui obiectiv;
3. Studiu privind vulnerabilitatea electromagnetică impusă de utilizarea mediilor de stocare USB;
4. Prezentarea în premieră a posibilității recuperării la nivel de bit a datelor USB 1.1 și 2.0 transferate în blocuri mari de date pe această magistrală universală de comunicație serială prin recepția și analiza radiațiilor compromițătoare generate de aceste transferuri de date precum și prezentarea parametrilor de detecție și analiză necesari îndeplinirii acestui obiectiv;
5. Realizarea unui studiu comparativ între măsurătorile specifice domeniului CEM cu cele din domeniul TEMPEST;
6. Verificarea eficacității de asigurare a securității electromagnetice a dispozitivelor ecranate de stocare date;
7. Studiu privind influența parametrilor utilizați la detecția și analiza emisiilor compromițătoare;
8. Verificarea eficacității EMSEC în cazul utilizării fonturilor securizate care este o metodă inovativă de protecție TEMPEST și care îngreunează sau chiar face imposibilă recuperarea informațiilor text afișate de echipamentele IT&C prin utilizarea metodelor specifice de intruziune electromagnetică;

9. Verificarea eficacității EMSEC a fonturilor de securizare TEMPEST și în cazul utilizării culorilor la afișarea informațiilor text;
10. Introducerea metodei culorilor ca metodă de protecție TEMPEST care implică utilizarea diferitelor combinații cromatice pentru font și fundal cu scopul minimizării rapoartelor semnal pe zgomot a emisiilor compromițătoare generate de echipamentele IT&C la afișarea informațiilor în format text;
11. Introducerea metodei culorilor ca metodă de evaluare TEMPEST a echipamentelor care implică utilizarea diferitelor combinații cromatice pentru font și fundal cu scopul maximizării rapoartelor semnal pe zgomot a emisiilor compromițătoare generate de echipamentele IT&C la afișarea informațiilor în format text;
12. Prezentarea metodelor consacrate de protecție TEMPEST care includ utilizarea echipamentelor protejate TEMPEST, principiul RED/ BLACK și utilizarea incintelor ecranate de mici și mari dimensiuni;
13. Studiu privind utilizarea perdelelor și draperiilor de ecranare ca măsură inovativă de protecție TEMPEST care poate fi aplicată ca metodă de protecție electromagnetică a ferestrelor și verificarea eficacității de ecranare a diferitelor materiale utilizate în acest scop;
14. Studiu privind utilizarea foliilor de ecranare ca măsură inovativă de protecție TEMPEST care poate fi aplicată ferestrelor dar și dispozitivelor de afișare precum și verificarea eficacității de ecranare a unui material de acest fel;
15. Studiu privind utilizarea vopselelor de ecranare ca măsură inovativă de protecție TEMPEST care poate fi aplicată la ecranarea camerelor sau chiar a clădirilor în vederea creșterii nivelului de protecție TEMPEST oferit de spațiile fizice precum și prezentarea eficacității de ecranare a unui material de acest fel;
16. Studiu privind utilizarea rack-urilor TEMPEST ca măsură alternativă pentru utilizarea echipamentelor protejate TEMPEST și verificarea eficacității de ecranare a unor produse de acest fel;
17. Studiu privind utilizarea corturilor ecranate ca măsură inovativă de protecție TEMPEST care poate fi utilizată ca alternativă la utilizarea rack-urilor TEMPEST în care au fost prezentate atât avantajele cât și dezavantajele aplicării acestei metode precum și verificarea eficacității de ecranare a acestor produse;
18. Prezentarea în premieră a rezultatelor obținute în urma efectuării unui studiu privind propagarea emisiilor compromițătoare de-a lungul liniei de alimentare electrică la distanțe considerabile: 1 metru, 10 metri și 50 metri;
19. Prezentarea rezultatelor obținute în urma realizării unui studiu privind capacitatea filtrelor de ferită de a diminua sau chiar elimina emisiile electromagnetice care sunt generate de echipamentele IT&C și care se pot propaga de-a lungul liniilor de alimentare electrică sau a celor de date.

6.3. Lista lucrărilor originale

Pe toată perioada stagiului doctoral au fost publicate șapte articole de revistă dintre care două ca prim autor și cincisprezece articole de conferință dintre care patru ca prim autor. Rezultatele articolelor [R4] și [C1] sunt inserate parțial în cadrul capitolului 2, rezultatele articolului [R2] vor fi regăsite parțial în capitolul 3 și rezultatele articolului [R5] au fost utilizate în cadrul capitolului 4. De asemenea, în capitolul 5 au fost introduse rezultate obținute și publicate parțial în articolul [R6] dar există și rezultate inserate în capitolul 5 care nu au fost încă publicate.

Articole de revistă

[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**)

Articole de conferință

[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. Bărtuşică, 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. Perspective de dezvoltare ulterioară

Intenționăm ca în perioada imediat următoare finalizării tezei de doctorat să publicăm rezultatele cercetărilor realizate în cazul comunicației seriale RS232 precum și a celor realizate în cazul interfeței RJ-45. Vom avea în vedere și publicarea rezultatelor detaliate înregistrate în cazul măsurătorilor efectuate pentru evaluarea eficacității de ecranare a incintelor ecranate și a materialelor de ecranare prezentate ca soluții alternative de protecție TEMPEST în cadrul capitolului 5.

Bibliografie

[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.