UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Samo Maček

FIZIČNI NAPADI IN NEŽELENO ODTEKANJE PODATKOV PO STRANSKIH KANALIH

MAGISTRSKO DELO

Ljubljana, 2011

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št.: 119-MAG-ISO/2011
Datum: 19. 09. 2011

Samo MAČEK, univ. dipl. inž. el.

L j u b l j a n a

Fakulteta za računalništvo in informatiko Univerze v Ljubljani izdaja naslednjo magistrsko nalogo

Naslov naloge: **Fizični napadi in neželeno odtekanje podatkov po stranskih kanalih**

Physical attacks and unwanted data leaks through covert channels

Tematika naloge:
Vplivi na okolico, ki so stranski pojav uporabe informacijske in komunikacijske opreme, so lahko neposredno povezani z obravnavanimi podatki. Preko elektromagnetnega sevanja in drugih t. i. stranskih kanalov lahko podatki odtekajo v nenadzorovana območja. Pri tem smo izpostavljeni tveganju, ki ga predstavlja prestrezanje podatkov in posledično rekonstrukcija vsebine. Za zavarovanje tajnih podatkov, katerih razkritje bi lahko ogrozilo nacionalne interese države, zato zakonodaja predpisuje stroge zahteve glede neželenih emisij, kar naj bi preprečilo možnost njihove zlorabe. Ti protiukrepi so izvedeni na različnih nivojih, njihova implementacija pa je zahtevna.
V sklopu magistrske naloge podajte pregled tveganj, ki smo jim pri uporabi informacijske tehnologije izpostavljeni na fizični plasti – odtekanje podatkov po stranskih kanalih, TEMPEST napadi, sevanja in druge neželene emisije pri prenosu in obdelavi podatkov. Na primeru tipkovnice praktično preverite možnosti prestrezanja sevanih podatkov in navedite možne protiukrepe za zavarovanje. V praksi tudi preverite možnost aktivnega oddajanja podatkov prek elektromagnetnega sevanja in izvedite test napada. Ugotovitve glede tveganj prestrezanja neželenih emisij obravnavajte tako z vidika opreme, ki je namenjena običajni osebni in poslovni uporabi, kot tudi z vidika opreme, ki je namenjena obravnavi tajnih podatkov. Ugotovitve in rezultate kritično ovrednotite in komentirajte dejansko izpostavljenost fizičnim napadom v različnih okoliščinah uporabe računalniške opreme.

Mentorica:
M. Ciglarič
doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:
prof. dr. Nikolaj Zimic

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Samo Maček

FIZIČNI NAPADI IN NEŽELENO ODTEKANJE PODATKOV PO STRANSKIH KANALIH

MAGISTRSKO DELO

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana, 2011

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št.: 119-MAG-ISO/2011
Datum: 19. 09. 2011

Samo MAČEK, univ. dipl. inž. el.

L j u b l j a n a

Fakulteta za računalništvo in informatiko Univerze v Ljubljani izdaja naslednjo magistrsko nalogo

Naslov naloge: **Fizični napadi in neželeno odtekanje podatkov po stranskih kanalih**

Physical attacks and unwanted data leaks through covert channels

Tematika naloge:
Vplivi na okolico, ki so stranski pojav uporabe informacijske in komunikacijske opreme, so lahko neposredno povezani z obravnavanimi podatki. Preko elektromagnetnega sevanja in drugih t. i. stranskih kanalov lahko podatki odtekajo v nenadzorovana območja. Pri tem smo izpostavljeni tveganju, ki ga predstavlja prestrezanje podatkov in posledično rekonstrukcija vsebine. Za zavarovanje tajnih podatkov, katerih razkritje bi lahko ogrozilo nacionalne interese države, zato zakonodaja predpisuje stroge zahteve glede neželenih emisij, kar naj bi preprečilo možnost njihove zlorabe. Ti protiukrepi so izvedeni na različnih nivojih, njihova implementacija pa je zahtevna.
V sklopu magistrske naloge podajte pregled tveganj, ki smo jim pri uporabi informacijske tehnologije izpostavljeni na fizični plasti – odtekanje podatkov po stranskih kanalih, TEMPEST napadi, sevanja in druge neželene emisije pri prenosu in obdelavi podatkov. Na primeru tipkovnice praktično preverite možnosti prestrezanja sevanih podatkov in navedite možne protiukrepe za zavarovanje. V praksi tudi preverite možnost aktivnega oddajanja podatkov prek elektromagnetnega sevanja in izvedite test napada. Ugotovitve glede tveganj prestrezanja neželenih emisij obravnavajte tako z vidika opreme, ki je namenjena običajni osebni in poslovni uporabi, kot tudi z vidika opreme, ki je namenjena obravnavi tajnih podatkov. Ugotovitve in rezultate kritično ovrednotite in komentirajte dejansko izpostavljenost fizičnim napadom v različnih okoliščinah uporabe računalniške opreme.

M e n t o r i c a :

M. Ciglarič

doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

D e k a n :

prof. dr. Nikolaj Zimic

I Z J A V A O A V T O R S T V U

magistrskega dela

Spodaj podpisani/-a _____Samo Maček_____,

z vpisno številko _____63010325_____,

sem avtor/-ica magistrskega dela z naslovom

__FIZIČNI NAPADI IN NEŽELENO ODTEKANJE PODATKOV PO STRANSKIH KANALIH___

_____

S svojim podpisom zagotavljam, da:

- sem magistrsko delo izdelal/-a samostojno pod vodstvom mentorja (naziv, ime in priimek)

  _____doc. dr. Mojca Ciglarič _____

  in somentorstvom (naziv, ime in priimek)

  _____

- so elektronska oblika magistrskega dela, naslova (slov., angl.), povzetka (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko magistrskega dela

- in soglašam z javno objavo elektronske oblike magistrskega dela v zbirki »Dela FRI«.

V Ljubljani, dne ___19. 9. 2011_____ Podpis avtorja/-ice: _____

Zahvala

Za pomoč in strokovne nasvete pri izdelavi naloge se zahvaljujem mentorici doc. dr. Mojci Ciglarič, za razumevanje in podporo pa Metki, Mateju, Roku, očetu in mami.

KAZALO

POVZETEK **1**

ABSTRACT **3**

1 UVOD **5**

1.1 MOTIVACIJA IN CILJI 6
1.2 STRUKTURA NALOGE 7

2 PREGLED PODROČJA **8**

3 VRSTE IN LASTNOSTI STRANSKIH KANALOV **12**

3.1 PRENOSNE POTI SIGNALA PREKO ELEKTRIČNIH LASTNOSTI 13
3.2 ELEKTROMAGNETNO SEVANJE 14
3.3 PARAZITNI SKLOPI MED PREVODNIKI 15
3.3.1 Sklop na podlagi skupne prevodnosti *16*
3.3.2 Kapacitivni sklop *16*
3.3.3 Induktivni sklop *18*
3.4 VRSTE SEVANJA 18
3.5 KONDUKTIVNE EMISIJE 20
3.6 EMISIJE PODATKOVNIH VODIL 20
3.7 DRUGI STRANSKI KANALI 23

4 STANDARDI IN PREDPISI **24**

4.1 VARNOST, KI JO ZAGOTAVLJAJO PREDPISI O ELEKTROMAGNETNI SKLADNOSTI 24
4.2 EM EMISIJE V ODVISNOSTI OD RAZVOJA TEHNOLOGIJE 28
4.3 PREDPISI S PODROČJA ZAŠČITE PRED PRESTREZANJEM PODATKOV 28

5 PRESTREZANJE PODATKOV PREKO STRANSKIH KANALOV **32**

5.1 PRESTREZANJE PODATKOV PREKO ELEKTRIČNIH LASTNOSTI 32
5.1.1 Pregled objavljenih primerov *33*
5.1.2 Prestrezanje podatkov pri uporabi tipkovnice *37*
5.1.3 Prestrezanje slike z zaslona *39*
5.1.4 Tiskalnik *42*
5.1.5 Pametne kartice *43*
5.1.6 Škodljiva koda *44*
5.1.7 Napadi »NONSTOP« *44*
5.2 PRESTREZANJE PODATKOV PREKO DRUGIH LASTNOSTI 45
5.2.1 Specifični zvočni učinki *45*
5.2.2 Optični napadi *46*

6 PRAKTIČNI PRIMERI IZVEDBE PRESTREZANJA PODATKOV **49**

6.1 REKONSTRUKCIJA PODATKOV 49
6.2 PRAKTIČEN PRESKUS PRESTREZANJA PODATKOV S TIPKOVNICE 50
6.3 VIRUS TEMPEST 61

7 VARNOSTNI PROTIUKREPI IN PRIPOROČILA **64**

7.1 SPLOŠNE METODE IN SREDSTVA ZA ZMANJŠEVANJE EM SEVANJA 64
7.2 PROTIUKREPI ZA PREPREČEVANJE PRESTREZANJA SLIKE Z ZASLONA 67
7.2.1 Programske metode *67*

7.2.2 Generatorji motenj *69*
7.3 UKREPI ZA PREPREČEVANJE PRESTREZANJA ŠIFRIRNEGA KLJUČA S PAMETNIH KARTIC 71
7.4 UKREPI V ZVEZI Z OBRAVNAVO TAJNIH PODATKOV V ELEKTRONSKI OBLIKI 71
7.5 ZAŠČITNI UKREPI TEMPEST..... 75
8 DISKUSIJA 76
9 ZAKLJUČEK..... 78
10 LITERATURA..... 80
11 VIRI 85
11.1 PREDPISI, REGULATIVA, STANDARDI 85
11.2 DRUGI VIRI..... 86

SEZNAM KRATIC

AWG	*American Wire Gauge* (oznaka debeline vodnika)
CRT	*Catode Ray Tube* – katodna cev (računalniški zaslon)
EM	elektromagnetno (npr. sevanje)
EMC	elektromagnetna skladnost
EMI	elektromagnetna interferenca
IKT	informacijsko-komunikacijska tehnologija
IS	Informacijski sistem
LISN	*Line Impedance Stabilization Network* – naprava, ki omogoča merjenje konduktivnih emisij v napajalnih vodih
NRZI	*Non Return to Zero Inverted* – način kodiranja signala
RF	radiofrekvenčni (npr. spekter)
SDIP	*Security and evaluation agency Doctrine and Information Publication*
STP	*Shielded Twisted Pair* – oklopljena prepletena parica
TEAPOT	pojem, ki označuje proučevanje, raziskave in obvladovanje namerno povzročenega sevanja informacijskih in komunikacijskih sistemov
TEMPEST	oznaka, ki v osnovi določa zbirko predpisov za omejevanje EM emisij podatkov, v širšem smislu pa raziskave in študije tveganj, ki ga predstavlja sevanje informacijskih in komunikacijskih sistemov, kakor tudi za ukrepe za njihovo omejevanje
USB	*Universal Serial Bus* – univerzalno serijsko vodilo
UTP	*Unshielded Twisted Pair* – neoklopljena prepletena parica

POVZETEK

Pri uporabi informacijske in komunikacijske opreme smo izpostavljeni številnim tveganjem, ki jih predstavljajo različne možnosti nepooblaščenega razkritja podatkov. V nalogi sem se osredotočil na področje, ki mu običajno ne posvečamo posebne pozornosti. Vplivi na okolico, ki so stranski pojav uporabe informacijsko-komunikacijske tehnologije (IKT), so lahko neposredno povezani z obravnavanimi podatki ali podatki, ki se prenašajo po komunikacijskih povezavah. Po t. i. stranskih kanalih, kot so elektromagnetno (EM) sevanje, različne oblike parazitnih sklopov, napajalno omrežje in prevodna infrastruktura, lahko ti odtekajo v nenadzorovana območja. Njihovo prestrezanje pa je mogoče tudi na podlagi oddaljenega opazovanja, izkoriščanja odbojev slike, specifičnih zvočnih učinkov, analize porabe energije in drugih stranskih kanalov.

Med izpostavljene komponente IKT z vidika prestrezanja podatkov po stranskih kanalih spadajo periferne enote (zaslon, tipkovnica), komunikacijske povezave in tudi druga oprema, kot so pametne kartice, pri katerih obstaja tveganje prestrezanja tajnega kriptografskega ključa. V nalogi sem na podlagi pregleda sedanjih dosežkov in raziskav na navedenem področju ter s praktičnim primerom prikazal, da je uporaba običajne informacijske opreme v nekaterih primerih s tega vidika lahko zelo tvegana. Slednje je predvsem posledica nezadostnega upoštevanja priporočil za zmanjšanje EM vplivov na okolico.

Predpise in standarde z navedenega področja je treba obravnavati z dveh vidikov. Pri običajni osebni ali poslovni uporabi so ti večinoma omejeni na zagotavljanje EM skladnosti in interference ter minimiziranja škodljivih vplivov na človeški organizem, vendar ne zagotavljajo varnosti pred prestrezanjem podatkov. Na drugi strani so ukrepi zavarovanja pred tovrstnimi grožnjami pri obravnavanju tajnih podatkov stopnje zaupno in višje zakonsko predpisani.

Zloraba podatkov, ki so v nacionalnem interesu države, lahko resno ogrozi delovanje ključnih funkcij države in družbe. Ukrepi zavarovanja tajnih podatkov pred odtekanjem preko EM sevanja in drugih stranskih kanalov se zato izvajajo na različnih nivojih, njihova uvedba pa zaradi zahtevnosti v običajni poslovni ali osebni uporabi ni izvedljiva. V Sloveniji glede izvajanja zaščite povzemamo zahteve EU in NATO.

Vseeno pa obstaja vrsta priporočil in ukrepov, s katerimi lahko stopnjo tveganja do določene mere zmanjšamo tudi v običajnih okoljih. Upoštevanje navedene

problematike mora biti zato vključeno že v procesu načrtovanja informacijske in komunikacijske opreme. V praktičnem delu sem prikazal, da so med opremo, ki izpolnjuje enake kriterije evropske tehnične zakonodaje, vseeno lahko velike razlike.

KLJUČNE BESEDE

informacijski sistemi, varnost, odtekanje podatkov, elektromagnetno sevanje, TEMPEST, tajni podatki, varnostno območje, napadi po stranskih kanalih

ABSTRACT

While working with the information and communication technology we are being exposed to a number of risks in the form of various ways and possibilities of an unauthorized disclosure of data. My paper focuses upon an area that has not been usually taken into much consideration. The impact on the environment/s, as a collateral phenomenon in the use of the Information-communication Technology (ICT) may be directly linked to the processed data and those data that are transmitted through communication connections. These data my be flowing off into an unsupervised area through the side channels, by means of electromagnetic (EM) radiation, various forms of parasitic couplings, power lines and conducting infrastructure. It could be also possible to intercept them also on the basis of a long-distance observation control, immage rebound, specific sound effects, enery use analysis and other side channel attacks.

Taking into consideration the possibility of data interception through side channels, peripheral units (screen, keyboard), communication links and also other equipment, like smart cards, where there is a risk of intercepting the secret key of cryptographic algorithm, may be enlisted among the exposed ICT components. The paper illustrates, on the basis of an analysis of the results and research carried out in the field, the use of the usual information technology as highly risky from this point of view, mostly because of the impact of the EM on the surroundings.

Regulations and standards that regulate this field should be viewed from two points of view. When speaking about the usual personal or business use, these are mostly defined by guaranteeing EM conformity and interference and aimed at minimizing the dangerous impact on the human organism, but they do not guarantee safety against data leakage. On the other hand, provisions for protecting from such threats are prescribed by the law when dealing with confidential or classified data.

Misuse of data of the public, national interest can seriously jeopardize the work of the key functions of the State and the public area. Protection against classified data outflow through EM radiation and other side channel attacks is carried out on different levels, while it is impossible to apply the measures in the usual personal or business use sphere due to their complexity. As protection is concerned, in Slovenia we comply with the EU and NATO requirements.

Notwithstanding what previously said in regard, there is, however, a number of reccomandations and measures that can be used to also reduce the risk level in the personal and business sphere. To achieve the preset goal, security measures have to bet taken into account through from the very beginning, while planning the information and communication technology process. What I meant to demonstrate in the practical part of the paper was, that there may, however, exist quite some differences between tecnologies that still meet the requirements of the EU technical normative law.

KEY WORDS

Information systems, security, data leakage, electromagnetic radiation, TEMPEST, classified information, security area, side channel attacks

1 UVOD

Resolucija o strategiji nacionalne varnosti med vire ogrožanja uvršča tudi kibernetske grožnje in zlorabo informacijskih tehnologij ter sistemov. Motnje v delovanju sistemov kritične infrastrukture in nepooblaščeno razkritje podatkov, ki so v nacionalnem interesu države, lahko pomenijo resno grožnjo delovanju javnega in zasebnega sektorja ter ključnih funkcij države in družbe. Zaradi neizenačenih konvencionalnih vojaških zmogljivosti, ki jih posedujejo različni subjekti v mednarodnem varnostnem okolju, je treba glede varnostnih tveganj upoštevati tudi nove nekonvencionalne oblike ogrožanja varnosti z informacijsko tehnologijo. [Res1]

Za zavarovanje tajnih podatkov, tj. podatkov, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, so zato predpisani strogi ukrepi varovanja, ki preprečujejo možnost njihove zlorabe ne glede na njihovo pojavno obliko. [ZTP]

Med tveganja, ki jim v običajnem osebnem ali poslovnem okolju ne posvečamo posebne pozornosti, spada tudi odtekanje podatkov IKT po t. i. stranskih kanalih oziroma preko lastnosti, ki so stranski pojav obdelave ali prenosa podatkov v informacijskih sistemih. Podatki se v okolico širijo preko EM sevanja, različnih oblik parazitnih sklopov, napajalnega omrežja, prevodne infrastrukture ipd. Njihovo prestrezanje pa je mogoče tudi na podlagi oddaljenega opazovanja, izkoriščanja odbojev slike, specifičnih zvočnih učinkov in drugih neželenih vplivov na okolico.

Stopnja tveganja, ki smo ji pri tem izpostavljeni, ni enostavno določljiva, saj je odvisna od številnih dejavnikov, v največji meri od vrednosti podatkov, ki pa jih lahko obravnavamo na različnih nivojih (nacionalni interes države, finančna korist, osebni podatki …). Slednje je povezano z motivacijo napadalca in sredstev, ki jih je pripravljen vložiti za njihovo pridobitev. Iz številnih virov v strokovni literaturi izhaja, da so tovrstne zlorabe izvedljive že z uporabo preproste in nenamenske opreme.

Ukrepe, ki jih v zvezi s preprečevanjem neželenih EM emisij predpisuje regulativa EU in zveza NATO, povzema tudi slovenska zakonodaja. [SEU, EK] Ne glede na zahtevnost uvedbe in s tem povezanih stroškov so ti za zaščito nacionalnih interesov države vsekakor upravičeni. Zaradi različnih (mednarodnih) dejavnikov in okoliščin je namreč v oceni varnostnih tveganj treba upoštevati tudi možnost terorističnega napada, sabotaže, vojne ipd. [UKIS]

Obravnavana tema je zanimiva tudi z vidika uporabe IKT v običajne osebne ali poslovne namene in posledičnega tveganja, ki smo mu pri tem izpostavljeni zaradi neželenega odtekanja podatkov v okolico. Pred tovrstnimi napadi se je namreč težko zavarovati. Ne glede na potrdilo o izpolnjevanju vseh evropskih direktiv tehnične zakonodaje namreč ni mogoče pridobiti podatka o stopnji zaščite pred prestrezanjem podatkov na podlagi neželenih emisij.

V nalogi sem se zato osredotočil na pregled tveganj, ki jih predstavljajo napadi, ki izkoriščajo stranske kanale, in protiukrepom, s katerimi se pred njimi zavarujemo. Ob tem sem posebno pozornost namenil področju tajnih podatkov.

1.1 Motivacija in cilji

Uporaba informacijske opreme ima lahko različne vplive na okolico. Ti predstavljajo določen nivo motenj ali šuma, ki se v različnih oblikah širi okrog naprav. Če so ti vplivi posledica obravnave ali prenosa podatkov, lahko skupaj z njimi v okolico odtekajo tudi podatki. Tveganje povečuje dejstvo, da se podatki v sistemu večinoma obravnavajo v nešifrirani obliki in da tako poteka tudi komunikacija s perifernimi enotami.

V tem primeru je treba upoštevati tveganje nepooblaščenega prestrezanja teh vplivov, ki so stranski pojav uporabe IKT. To je še posebej pomembno, ker je zaradi pasivne narave njihovo zaznavanje težavno.

Motivacija za izdelavo naloge zato izhaja iz naslednjih vprašanj, ki se postavljajo v zvezi z opisano problematiko:

- Ali smo pri uporabi IKT v običajne poslovne in osebne namene dejansko izpostavljeni tveganju, ki ga predstavlja prestrezanje podatkov preko EM sevanja in drugih stranskih kanalov?

- Ali novejša tehnologija navedena tveganja zmanjšuje?

- Ali so visoki stroški uvedbe ukrepov, s katerimi ta tveganja preprečujemo, pri obravnavi tajnih podatkov upravičeni?

Na zastavljena vprašanja njih ni mogoče podati enoznačnih odgovorov. Odvisni so od konkretne situacije, umestitve opreme v prostor, poteka napajalnega in podatkovnega omrežja, lastnosti prevodne infrastrukture v bližini...

Glavni cilj naloge je torej kritično ovrednotenje stopnje tveganja, ki ga predstavlja nenadzorovano odtekanja podatkov informacijske opreme. Za boljšo ponazoritev sem prikazal tudi praktičen preizkus prestrezanja sevanih podatkov ter možnost aktivnega oddajanja podatkov prek elektromagnetnega sevanja.

Ne glede na relativno dobro pokritost področja v strokovni literaturi se vseeno pogosto porajajo dvomi o dejanski stopnji tveganja. To namreč tudi novejši viri pogosto ponazarjajo na zastareli tehnologiji. Zato dodatni motiv predstavlja prikaz tveganja pri uporabi aktualne opreme, in sicer na področju, ki ga nisem zasledil v strokovni literaturi. Med ključne vire emisij, ki so povezani s podatki, spadajo zaslon, tipkovnica in tiskalnik. Uporaba tipkovnica je kritična predvsem zaradi vnosa občutljivih podatkov, kot so gesla, elektronska sporočila, dokumenti ipd. V strokovni literaturi so izpostavljene predvsem tipkovnice z vodilom PS/2. Zaradi njegove obsoletnosti sem se osredotočil na novejše zasnovano vodilo USB in preveril, ali zagotavlja zadostno zaščito. Viri navajajo, da je pri USB tipkovnicah podatke mogoče prestreči na podlagi sevanja krmilnika, ki pa je občutno nižje jakosti kakor sevanje kabla PS/2.

Obravnavano področje sem zaokrožil s prikazom priporočil za splošno zmanjšanje nevarnosti tveganja pri uporabi opreme, namenjeni običajni poslovni ali osebni uporabi, ter protiukrepov na področjih, kjer se obravnavajo tajni podatki, ki so v nacionalnem interesu države.

1.2 Struktura naloge

Naslednje poglavje podaja pregled področja ter sedanjih dosežkov in raziskav v zvezi s tveganjem odtekanja podatkov po stranskih kanalih. Sledi pregled elektromagnetnih in drugih lastnosti, s katerimi informacijska oprema vpliva na okolico in preko katerih lahko nenadzorovano odtekajo podatki. Pregled predpisov, ki se nanašajo na zavarovanje pred tovrstnimi tveganji, je v četrtem poglavju. Sledi pregled najbolj izpostavljenih komponent sistema in možnosti rekonstrukcije obravnavanih podatkov v praksi. V šestem poglavju sem na praktičnem primeru prikazal možnost pasivnega in aktivnega prestrezanja podatkov po stranskih kanalih. Prvi primer prikazuje tveganje pri uporabi tipkovnice z vodilom USB, drugi pa namerno oddajanje podatkov preko emisij procesorja. Zadnje poglavje opisuje pregled varnostnih ukrepov, ki so predpisani za delo s tajnimi podatki, in ukrepov ter priporočil, s katerimi se lahko pred tveganji zavarujemo pri običajni poslovni ali osebni uporabi IKT.

2 PREGLED PODROČJA

V običajnem poslovnem okolju so informacijski sistemi varovani z ukrepi, ki zagotavljajo zaščito na različnih nivojih, kot so fizično in tehnično varovanje, gesla, šifrirni mehanizmi, požarni zidovi, protivirusna zaščita ipd. Ti ukrepi preprečujejo predvsem invazivne napade, ki bi lahko povzročili razkritje ali uničenje podatkov in po drugi strani onesposobitev sistemov, v katerih se ti obravnavajo. Šifrirni mehanizmi varujejo podatke pri prenosu po komunikacijskih kanalih in hrambi, vendar se ti znotraj računalniških sistemov večinoma obravnavajo v nešifrirani obliki. Primeri prenosa podatkov med posameznimi komponentami sistema brez uporabe šifriranja so npr. vnos besedila preko tipkovnice, prikaz slike na zaslonu ali zapisovanje podatkov na zunanji pomnilniški medij. Izpostavljene komponente sistema so tako tipkovnica, miška, zaslon, laserski tiskalnik, pametna kartica ipd.

Možnosti izvedbe napadov preko stranskih kanalov so različne. Ker vsaka elektronska naprava pri svojem delovanju v okolico oddaja EM vplive, ki so lahko neposredno povezani s podatki, je največja pozornost namenjena temu področju. Sinkovski [s3] ocenjuje, da je preko EM sevanja in konduktivnih emisij IKT mogoče prestreči od 1 do 2 % vseh podatkov, ki se obravnavajo v informacijskih sistemih.

Archambeault et al. [a3] izpostavljajo velik vpliv razvoja tehnologije in dviga frekvenc delovanja sistemov na oddano EM sevanje. Upoštevanje navedene problematike mora biti zato vključeno že v procesu načrtovanja vezja. Zaradi visokih frekvenc obdelave in prenosa podatkov so namreč valovne dolžine signala bistveno krajše. Zato lahko tudi kratke prenosne linije, usklajene z valovno dolžino signala, delujejo kot učinkovite oddajne antene.

Pomemben vir emisij podatkov predstavljajo tudi prenosi signala po podatkovnih vodilih. Smulders [s4] je leta 1990 izpostavil nevarnost odtekanja podatkov iz vodila RS-232. Vzroki so med drugim prenos signala po enem vodniku brez invertiranega para, oblika impulzov ipd. Ne glede na boljšo zasnovo pa so tudi emisije novejše zasnovanih vodil lahko precejšnje. Zaradi diferencialnega prenosa se vpliv signala medsebojno kompenzira. Fan et al. [f2] ugotavljajo, da majhna stopnja asimetrije ne vpliva na sam prenos signala, medtem ko ima po drugi strani lahko izjemen pomen glede oddanega sofaznega šuma in presluha signala na prevodnike v bližini. V [a3] kot vzroke med drugim navajajo minimalne razlike v dolžini vodnikov parice, kapacitivnosti kondenzatorjev za omejevanje časa dviga in spusta idr.

Vuagnoux in Pasini [v2, v3] sta izpostavila nevarnost razkritja zaupnih podatkov, ki se vnašajo s tipkovnico, kot so uporabniška imena, gesla, elektronska sporočila ipd. Pri tem sta se osredotočila na prestrezanje podatkov preko EM sevanja, ki je posledica posredovanja signala o kodi pritisnjene tipke. Hkrati sta izpostavila tudi vpliv posrednih emisij preko prevajalne infrastrukture.

Eden izmed virov najobčutljivejših podatkov, ki se obravnavajo v IS, je zaslon. Van Eck [e1] je leta 1985 na primeru CRT zaslona prvi ponazoril, da za prestrezanje podatkov ni potrebna sofisticirana oprema, saj zadošča že manjša prilagoditev običajnega televizijskega sprejemnika. Zajem slike z nekaterih modelov tedanjih zaslonov je bil mogoč celo z razdalje več kakor 1 km.

S prikazano sliko na računalniškem zaslonu je povezanih več virov EM sevanja in tudi konduktivnih emisij: DA konverter, podatkovni in napajalni kabel … [w1] Prestrezanje slike preprečujemo z namensko opremo, pa tudi s programskimi rešitvami in generatorji motenj.

Tanaka [t2] je razvil generator motenj, ki je lahko učinkovit in cenovno ugoden način preprečevanja prestrezanja podatkov preko EM sevanja. Karakteristike motilnega signala morajo prekriti emisije zaslona v celotnem radiofrekvenčnem območju. Hkrati pa mora biti skupno sevanje znotraj mej EM skladnosti in imuno na povprečenje signala. Podobno Suzuki in Akiyama [s7] motilni signal generatorja vodita v sistem kot sofazni šum. S tem sta zagotovila prekritost originalnih emisij v vseh smereh ne glede na oddaljenost od DP.

Ker je sevanje (analognega) podatkovnega vodila video signala vsota sevanj, ki so posledica sprememb signala osnovnih barvnih komponent, je rekonstrukcija prestreženih podatkov najučinkovitejša ravno pri prikazu kontrastnih vzorcev, kot je črno besedilo na beli podlagi. Zato sta Kuhn in Anderson [k8, k9] razvila modificiran način prikaza besedila, ki odreže zgornjo tretjino frekvenčnega spektra in tako zmanjša možnost rekonstrukcije. Posledično to vodi k nižjemu kontrastu med besedilom in ozadjem, kar povzroči nekoliko zamegljeno sliko. Tanaka et al. [t3] so s kombinacijo Fourijejeve in Gaussove transformacije zagotovili boljšo zaščito ob hkratnem izboljšanju kontrasta besedila.

Watanabe et al. [w2] so razvili metodo prikaza besedila, ki izkorišča lastnost očesa, da pri izpostavljenosti hitrim spremembam barv na podlagi t. i. aditivnega mešanja barv zazna zgolj eno barvo in ne sprememb. S hitro menjajočimi se barvnimi vzorci

se tako lahko generira očesu skoraj neopazni nivo šuma, ki pa ima izjemno velik vpliv na nižje stopnje EM sevanja in tako onemogoča rekonstrukcijo slike.

Sekiguchi in Seto sta prikazala, da je rekonstrukcija slike z zaslona mogoča tudi z izkoriščanjem konduktivnih emisij v napajalnih vodih. [s2]

Grzesiak in Przybysz [g3] sta ponazorila tveganje, ki ga predstavlja prestrezanje krmilnega signala laserskega žarka, s katerim se nevtralizira fotosenzitivni naboj na bobnu tiskalnika. Signal lahko v obliki EM sevanja oddajajo linije tiskanih vezij ali pa iz tiskalnika odteka preko konduktivnih emisij.

Ambros et al. [a1] izpostavljajo nevarnost prestrezanja šifrirnega ključa pametnih kartic, in sicer za različne algoritme, kot so DES, AES, RSA, SEAL ipd. Kot protiukrep predlagajo večprocesorsko zasnovo vezja kartice. Karakoyunlu et al. [k1] so dokazali, da so še bolj izpostavljena integrirana vezja, ki uporabljajo kriptografijo z eliptičnimi krivuljami, saj imajo v primerjavi z RSA krajši šifrirni ključ.

Kim in Quisquater [k2] navajata, da tveganje lahko predstavljajo tudi aktivni napadi na pametne kartice z injiciranjem napak na podlagi spreminjanja napetosti, frekvence signala ure, uporabe izven predpisanega temperaturnega območja, magnetnega polja ipd. Napaka v izvedbi šifrirnega algoritma v določenih primerih vodi k enostavnejši rekonstrukciji tajnega ključa.

Tiri in Verbauwhede [t4] sta razvila zasnovo vezja z redundančnimi komponentami, ki zagotavlja konstantno porabo energije ter hkrati minimizira parazitne vplive med posameznimi komponentami pametne kartice. S tem se onemogoči prestrezanje ključa na podlagi dinamične porabe energije, ki je sicer odvisna od obravnavanih podatkov.

Odtekanje podatkov preko stranskih kanalov pa ni omejeno zgolj na EM lastnosti naprav. Kuhn [k6] je predstavil možnost zajema slike na daljavo preko direktne linije pogleda na zaslon. Razdalje zajema slike so lahko zelo velike. Backes, Durmuth in Unruh [b2] pa analizirajo možnost prestrezanja slike preko odbojev od različnih predmetov v okolici zaslona na razdalje med 5 in 20 m.

Asonov in Agrawal [a4] sta prikazala možnost rekonstrukcije vnosov na tipkovnici preko akustičnega posnetka na podlagi razlik v zvoku, ki ga ustvarja pritisk različnih tipk na tipkovnici. Berger, Wool in Yeredor [b3] so uspešnost rekonstrukcije še izboljšali s primerjavo možnega besedila z besedami iz slovarja. Zaradi zastarelosti

tehnologije manjše tveganje predstavlja rekonstrukcija besedila na podlagi specifičnih zvočnih učinkov pri tiskanju besedila z matričnim tiskalnikom, ki jih izpostavljajo Backes et al. [b1]

Ukrepi zniževanja EM sevanja in drugih vplivov na okolico se morajo zato upoštevati že v procesu načrtovanja električnih vezij in naprav. Splošna priporočila izhajajo že iz samih tehničnih specifikacij (npr. za vodilo USB) in številnih virov s področja zagotavljanja elektromagnetne skladnosti ter strokovnih virov.

Posebni ukrepi, ki morajo biti izpolnjeni pri obravnavi podatkov, ki so v nacionalnem interesu države, so določeni z zahtevami mednarodnih organizacij, v katere smo vključeni. Naša zakonodaja v tem kontekstu povzema regulativo zveze NATO in EU. Auddy in Sahu [a5] ter številni drugi strokovni viri ponazarjajo zahtevnost uvedbe ukrepov, kot so načelo »separacije black/red«, obvezna uporaba opreme, skladne s standardom SDIP-27, zavarovanje ključnih komponent sistema v varnostnih območjih, obvezna akreditacija sistema, ki jo opravi pooblaščeni organ, ipd.

Nekoliko nejasnosti k obravnavanemu področju vsekakor prispeva tudi dejstvo, da standardi, ki obravnavajo navedeno področje, niso javno dostopni. To vsekakor poraja tudi nekatere dvome o dejanski nevarnosti, ki jo tovrstna tveganja predstavljajo. Slednje predvsem zaradi izjemno zahtevnih ukrepov, ki jih je treba izvesti pri obravnavanju tajnih podatkov, in na drugi strani zaradi odsotnosti predpisov, ki bi zagotavljali varnost glede uporabe informacijske opreme pri običajni poslovni ali osebni uporabi.

3 VRSTE IN LASTNOSTI STRANSKIH KANALOV

Uporaba informacijske opreme ima lahko različne vplive na okolico. Ti predstavljajo določen nivo motenj ali šuma, ki se v različnih oblikah razširja okrog naprav. Z vidika oddajanja motenj, ki so posledica delovanja naprave, je pomembna predvsem stopnja vpliva na delovanje drugih naprav in človeški organizem. Oddani šum je lahko tudi posledica obdelave ali prenosa podatkov in je z njimi lahko neposredno povezan. Podatki v obliki šuma tako neposredno odtekajo v okolico naprave. V tem primeru je poleg vpliva na okolico treba upoštevati tudi vidik tveganja, ki ga predstavlja prestrezanje teh vplivov, in možnost rekonstrukcije podatkov s strani nepooblaščenih oseb. Za napade, ki za dostop podatkov izkoriščajo navedene lastnosti, se je uveljavil izraz »side-channel attack«, saj pridobitev podatkov poteka po stranskih kanalih, na katere pri vsakdanji uporabi opreme običajno nismo dovolj pozorni. Podlago za rekonstrukcijo podatkov iz emisij, ki nenadzorovano odtekajo v okolico in jih izkoriščajo tovrstni napadi, predstavljajo:

- električne lastnosti (EM sevanje, parazitni sklopi …),
- LED in drugi indikatorji [d2],
- oddaljeno opazovanje in izkoriščanje odbojev slike,
- poraba energije,
- specifični zvočni učinki.

Možnost zlorabe podatkov z izkoriščanjem zgoraj opisanih lastnosti je močno odvisna od karakteristik opreme in okolja, v katerem se ta uporablja, ter po drugi strani od napadalčeve opreme, s katero izvaja napade. Pri običajni osebni ali poslovni uporabi se predvideva, da je možnost izvedbe takšnih napadov majhna. Kljub temu je pri obravnavi občutljivih podatkov priporočljivo upoštevati naslednja dejstva:

- običajna oprema IKT pred tovrstnimi napadi ni posebej zavarovana. Najvišjo stopnjo emisij določajo predpisi s področja zagotavljanja EM skladnosti (EMC); medtem ko uporabnik ne razpolaga z informacijo o njihovi korelaciji z obravnavanimi podatki,
- zlorabo je zaradi neinvazivne narave napadov težko odkriti,
- v določenih primerih je mogoče prestrezanje podatkov na velike razdalje,
- izvedba je večinoma mogoča že z uporabo neprilagojene opreme, ki je v splošni uporabi.

V okoljih, kjer je ohranjanje zaupnosti zelo pomembno, mora biti zato onemogočena vsaka možnost prestrezanja podatkov preko invazivnih in neinvazivnih napadov. Za

ohranjanje zaupnosti, celovitosti in razpoložljivosti podatkov se zato v teh primerih zahtevajo ukrepi na različnih nivojih, ki v medsebojni povezavi kar najbolj preprečujejo možnost izvedbe kakršnega koli napada na podatke ali opremo.

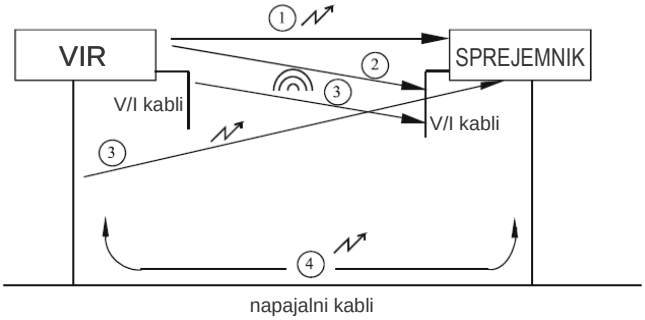
Najširše področje napadov preko stranskih kanalov predstavljajo napadi, ki izrabljajo neželene električne lastnosti, s katerimi oprema IKT vpliva na okolico. Za slednje se je uveljavil izraz »napadi TEMPEST« (angl. TEMPEST attacks).

3.1 Prenosne poti signala preko električnih lastnosti

Vse elektronske naprave pri svojem delovanju v okolico oddajajo določen nivo EM emisij. Če ti vplivi niso povezani z osnovno funkcionalnostjo naprave (kot na primer brezžični prenosi ali mobilna telefonija), so večinoma nezaželeni in imajo lahko različne negativne učinke na delovanje drugih električnih naprav v bližini in na človeški organizem. Vpliv je poleg jakosti odvisen tudi od frekvenčnega območja emisij, ki se širijo okrog naprave. Glede na namen uporabe so predpisane različne dopustne vrednosti vpliva na okolico.

Vir RF energije je lahko naprava, vhodno-izhodni vodnik (podatkovni ali napajalni), medtem ko sprejemnik signala predstavlja katera koli naprava ali vodnik, ki ni nujno del informacijskega sistema ali infrastrukture, ki zagotavlja njegovo delovanje. Obstaja več možnih transportnih poti prenosa RF energije [m2]:

- direkten prenos RF signala iz vira na sprejemnik,
- prenos RF signala iz vira na V/I napajalne ali komunikacijske kable sprejemnika,
- prenos RF signala iz V/I kablov vira na V/I napajalne ali komunikacijske kable sprejemnika,
- prenos RF signala preko prevodnosti, ki je posledica skupne napajalne ali podatkovne infrastrukture.



Slika 1:
Viri sevanja, možni sprejemniki in poti prenosa signala pri uporabi elektronskih naprav (povzeto po [m2]).

Možni načini prenosa signala so:

- prevodniški (konduktivni),
- EM,
- preko dominantnega magnetnega polja,
- preko dominantnega električnega polja.

3.2 Elektromagnetno sevanje

EM sevanje je pojav, pri katerem se EM polje oddalji od vira in se samostojno širi v prostor. Neposredno ob anteni se ustvari bližnje polje, kjer imata električno in magnetno polje komponente v prostoru v vseh smereh. Jakost teh komponent pa pada s prvo, drugo in tretjo potenco. Za vmesnim bližnjim in vmesnim prostorom valovanje preide v EM sevanje. Tu sta električna in magnetna poljska jakost med seboj pravokotni. Jakost EM sevanja se zmanjšuje s kvadratom razdalje, ker se prostor (površina ploskev) v prostoru kvadratno povečuje. Pri tem razmerje med električnim in magnetnim poljem ostaja konstantno, enako valovni upornosti, in znaša 120 π (~377 Ω). [b4]

Radiofrekvenčni spekter EM valovanja predstavlja del EM spektra od 30 kHz do 300 KHz. Nižje od 30 kHz je območje nizkih frekvenc. V tem območju ni EM polj, ampak prevladujejo električna in magnetna polja. V več kakor 99 odstotkih so njihovi povzročitelji omrežje za prenos električne energije, hišne električne napeljave, železnica in električni gospodinji aparati. [b4]

RF spekter zajema naslednja frekvenčna območja [b4]:

Frekvenca		Valovna dolžina	Mednarodna oznaka	Možni viri
od	do	med		
30 kHz	300 kHz	10 km–1 km	LF *(low)*	radio – dolgi val
300 kHz	3 Mhz	1 km–100 m	MF *(medium)*	radio – srednji, kratki val
3 MHz	30 Mhz	100 m–10 m	HF *(high)*	radio – kratki val
30 MHz	300 MHz	10 m–1 m	VHF *(very high)*	radio – FM, TV, ura – Frankfurt, radioamaterji
300 MHz	3 Ghz	1 m–10 cm	UHF *(ultra high)*	TV, mobilna telefonija
3 GHz	30 GHz	10 cm–1 cm	SHF *(super high)*	komunikacije, zveze, sateliti
30 GHz	300 GHz	1 cm–1 mm	EHF (*extremly high*)	zveze, sateliti

V RF delu EM frekvenčnega spektra poteka tudi obdelava podatkov z IKT:

- procesorji: frekvenca delovanja 1–4 GHz,
- zaslon: EM sevanje, povezano s prikazano sliko 300–500 MHz,

in prenos podatkov:

- tipkovnice, miške: 1,5 Mb/s,
- USB 1.1: do 12 Mb/s,
- USB 2.0: do 480 Mb/s,
- USB 3.0: do 5 Gb/s,
- UTP: od 100 Mb/s do 1 Gb/s.

Viri EM sevanja pri obdelavi in prenosu podatkov so prisotni v različnih območjih RF spektra. Osnovni signal lahko modulira na drug, nosilni signal z drugačno frekvenco. Možnost rekonstrukcije je odvisna od razmerja med signalom in šumom pri določeni frekvenci. Nevarnost odtekanja podatkov na podlagi EM sevanja in konduktivnih emisij je zato treba obravnavati v širokem frekvenčnem razponu.

3.3 Parazitni sklopi med prevodniki

Med različnimi tokokrogi obstajajo neželene medsebojne električne lastnosti, ki niso neposredno povezane s funkcionalnostjo naprave, vendar imajo lahko različne negativne učinke na delovanje sistemov. Na njihovi podlagi se med sistemi, ki bi sicer morali biti popolnoma neodvisni, tvorijo različne oblike sklopov. Te so posledica neželenih, t. i. parazitnih kapacitivnosti, induktivnosti in prevodnosti, ki obstajajo med različnimi tokokrogi. Preko parazitnih kapacitivnosti in induktivnosti se lahko signal prenese iz osnovnega na drug tokokrog, ki se nahaja v bližini, čeprav z njim nima neposrednega stika. Ta tokokrog je lahko del obravnavanega sistema, del druge naprave ali infrastrukture, ki ni z njim v nikakršni povezavi.

Primer prenosa signala predstavlja presluh (angl. »crosstalk«) med prevodniki, ki potekajo v medsebojni bližini. Lahko je posledica medsebojne kapacitivnosti, induktivnosti, obravnavamo pa ga lahko tudi z vidika skupne prevodnosti. Običajno je njegov negativni učinek pomemben pri prenosu signala med vzporedno ležečimi vodniki kot posledica kapacitivnega (in / ali induktivnega) sklopa. Posebno izrazit je pri dolgem vzporednem poteku večžilnih kablov (npr. kabli UTP), kjer opazujemo prenos signala med posameznimi prevodniki.

Šum, ki se v sprejemnem (parazitnem) prevodniku generira na določenem segmentu, se lahko širi po infrastrukturi. Kadar je šum posledica obdelave podatkov in je z njimi neposredno povezan, lahko podatki na tej podlagi nenadzorovano odtekajo iz sistema. Potencialni prevodniki in naprave, preko katerih je mogoče odtekanje podatkov in niso del obravnavanega sistema, so:

- oprema IKT,
- komunikacijske povezave, razen optičnih,
- vodi napajalne infrastrukture,
- druga infrastruktura, ki omogoča prenos električnega signala.

Glede na vrsto medsebojne električne lastnosti, ki obstaja med sistemi, ločimo:

- kapacitivni sklop,
- induktivni sklop,
- sklop preko skupne prevodnosti in
- sklop preko EM sevanja.

3.3.1 Sklop na podlagi skupne prevodnosti

Pri tem sklopu je več tokokrogov povezanih preko skupne impedance (prevodnosti). V praksi sta večinoma dva razloga za njegov nastanek, in sicer:

- sklop preko nezadostne izolacije,
- sklop preko nezadostne ozemljitve. [dv3]

Sistemi v tem primeru niso povsem ločeni, saj med njimi obstaja neka skupna točka, preko katere se prenaša šum. Ne glede na to z vidika obravnavanih naprav obstaja tudi med povsem ločenimi sistemi. Skupno točko lahko namreč predstavlja napajalno omrežje, v katero so priključene naprave ali podatkovna povezava med sistemi.

3.3.2 Kapacitivni sklop

Na podlagi razlike v napetosti med dvema prevodnikoma se med njima razvije električno polje, ki lahko v sosednjem vodniku inducira napetost. Preko impedance sprejemnika v tokokrogu steče električni tok, ki je (med drugim) odvisen od hitrosti spremembe napetosti. [m2]

$V_2 = c_m Z_2(dV/dt)$, $I = c(dV/dt)$

Kapacitivni sklop je najbolj izrazit pri dolgem vzporednem poteku prevodnikov, ki so v neposredni bližini, to so na primer vodniki znotraj istega večžilnega kabla ali daljši vzporedni poteki vodnikov z majhnim medsebojnim razmikom. Medsebojna

kapacitivnost med dvema vzporednima linearnima prevodnikoma je odvisna od debeline prevodnikov, medsebojnega razmika ter dolžine sklopa in je določena z naslednjim izrazom:

$$C = \frac{0.0885 \bullet L \bullet \pi}{acosh\frac{D}{d}}$$

kjer je L dolžina sklopa v cm, D razmik med vodnikoma, d debelina vodnikov, c pa kapacitivnost sklopa v pF [m2].

Kapacitivnost sklopa se s povečevanjem razmika med prevodnikoma hitro zmanjšuje. Največji padec je v neposredni bližini prevodnika, medtem ko s povečevanjem razdalje upad ni več tako izrazit.

Preglednica 1 prikazuje odvisnost medsebojne kapacitivnosti od medsebojnega razmika za standardne debeline vodnikov, ki se uporabljajo za prenos podatkov. Premeri podatkovnih vodnikov po standardu *American wire gauge* so:

- za kable UTP tipično med AWG 23 in 20,
- USB 2.0 med AWG 28 in 20.
- USB 3.0 za UTP parice med AWG 34 in 28,
- USB 3.0 za SuperSpeed parice med AWG 34 in 26.

Na izbrano debelino podatkovnih vodnikov vplivajo dolžina kabla (razdalja, na kateri poteka prenos signala), material in frekvenca prenosa.

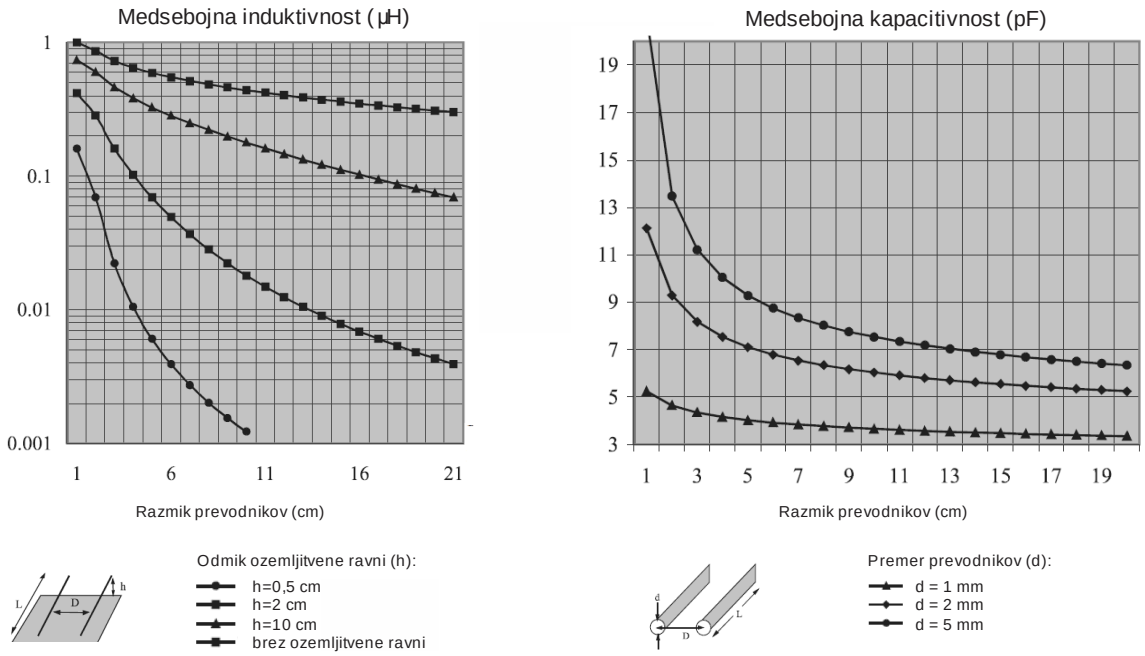
	AWG 20		AWG 26		AWG 28	
D [mm]	d [mm]	C [pF]	d [mm]	C [pF]	d [mm]	C [pF]
1	0,89	56,487	0,483	20,494	0,381	17,166
2	0,89	19,185	0,483	13,245	0,381	11,871
3	0,89	14,746	0,483	11,064	0,381	10,100
4	0,89	12,734	0,483	9,917	0,381	9,139
6	0,89	10,710	0,483	8,659	0,381	8,062
10	0,89	8,939	0,483	7,468	0,381	7,020
20	0,89	7,307	0,483	6,295	0,381	5,974
40	0,89	6,181	0,483	5,441	0,381	5,200
100	0,89	5,135	0,483	4,614	0,381	4,439
150	0,89	4,777	0,483	4,323	0,381	4,169
180	0,89	4,632	0,483	4,204	0,381	4,058
200	0,89	4,552	0,483	4,138	0,381	3,997

Preglednica 1:
Kapacitivnost sklopa med dvema vzporednima vodnikoma v odvisnosti od razdalje.

3.3.3 Induktivni sklop

Analogno kapacitivnemu sklopu, ki je posledica obstoja skupne kapacitivnosti, se na podlagi medsebojne induktivnosti tvori induktivni sklop. Kadar magnetno polje, ki je posledica tokovne zanke, teče skozi zanko drugega tokokroga, se v njem na podlagi medsebojne induktivnosti generira šum, ki je določen z naslednjim izrazom:

$$V_2 = M_{12}(dI_1/dt)$$



Slika 2:
Odvisnost medsebojne induktivnosti in kapacitivnosti od razmika med vodniki [m2].

Presluh signala preko kapacitivnega ali induktivnega sklopa pri večjem razmiku med prevodniki zaradi upada kapacitivnosti in induktivnosti ni učinkovit. Prenos dodatno slabijo ali onemogočajo prepreke med virom in sprejemnikom (oklop, zaslon, drugi prevodniki).

3.4 Vrste sevanja

Slika 3 na primeru zanke, ki jo sklepa vodnik s povratno povezavo, prikazuje vir sofaznih in protisofaznih emisij. Običajno so z vidika zagotavljanja EM skladnosti najbolj problematične sofazne emisije. Po drugi strani so protifazne spremembe

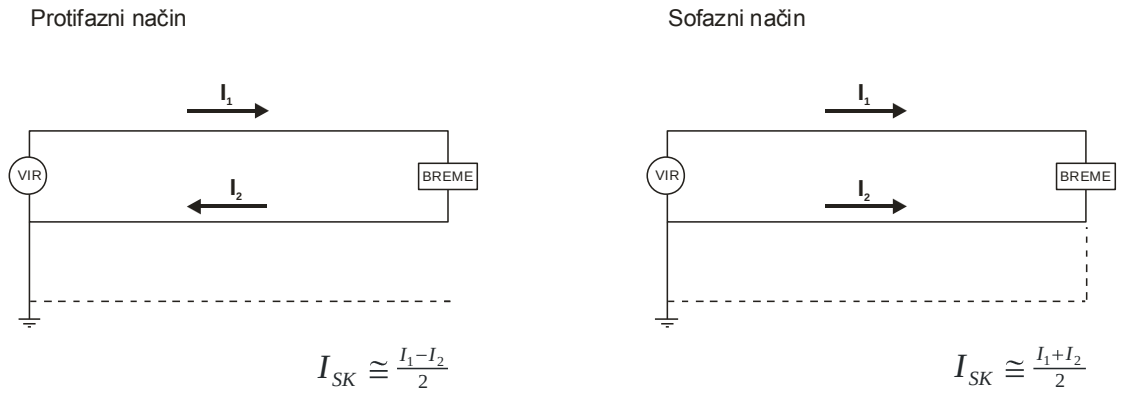
lahko posledica obdelave ali prenosa podatkov in so lahko vir emisij preko katerih odtekajo podatki.

Protifazni (angl. »differential mode«) – medvodniški način sevanja

Sevanje povzročajo tokovi visokih frekvenc, ki tečejo po t. i. tokovnih zankah in se lahko tvorijo npr. na vhodno-izhodnih kablih pri povratnih povezavah. V splošnem moramo biti pozorni na večje tokovne zanke. Te običajno tvorijo podatkovna ali naslovna vodila in dolgi vhodno-izhodni kabli. Zanke se obnašajo kot velike antene, ki sevajo elektromagnetno energijo v okolico in generirajo tok v bližnjih vezeh in žicah. Kot je razvidno iz slike 3, je sevano električno polje DM tokov prispevek razlike polj, ki jih povzročata toka I1 in I2. Če sta tokova I1 in I2 enaka, se polji zaradi DM tokov medsebojno izničujeta. [dv2]

Sofazni (angl. »common mode«) – vodniški način sevanja

So običajno glavni izvor sevanja, ki ga oddajajo naprave. Merjeno sevano električno polje CM tokov je seštevek polj, ki jih povzročata tokova I1 in I2 (slika 3). Povzročajo ga npr. nenamerni napetostni padci v vezju. Oddaja energije v prostor je sorazmerna velikosti antene, ki jo predstavljajo prevodniki, po katerih se prenaša signal. Antena je najbolj občutljiva, kadar je njena velikost usklajena z valovno dolžino signala in manj, kadar je valovna dolžina večja od velikosti antene. [dv2]



Slika 3:
Sofazni in protifazni tok v električnem vezju.

Pretvorba protifaznega toka v sofazni tok

Zaradi različne impedance prevodnikov, po katerih teče tok v električnih vezjih, prihaja do pretvorbe protifaznega toka v sofazni tok. Zaradi parazitnih kapacitivnosti

znotraj ohišja in med prevodniki tok ne steče direktno skozi breme. Pri prenosu signala v diferencialnem načinu morata biti zato oba signala v vodnikih usklajena, prav tako morata biti vodnika usklajena tudi v smislu parazitnih električnih lastnosti. [m2]

3.5 Konduktivne emisije

Konduktivne emisije za prenos izkoriščajo prevodno infrastrukturo, preko katere lahko odtekajo v nenadzorovana območja. Primer so povratne konduktivne emisije v napajalne vode. Če so segmenti infrastrukture, po katerih se širi signal, usklajeni z njegovo valovno dolžino, lahko posredno oddajajo EM sevanje. Rekonstrukcija na podlagi konduktivnih emisij je tako mogoča v nenadzorovanih prostorih, drugih stavbah in podobno.

Potencialni prevodniki so:
- napajalno omrežje,
- kabli UTP,
- povezave alarmnega sistema,
- telefonski kabli,
- konzole in povezave klimatskih naprav,
- neozemljeni deli cevi ogrevalnega ali klimatskega sistema ipd. [s3]

3.6 Emisije podatkovnih vodil

Kakor izhaja iz prejšnjih podpoglavij, gradniki sistema med seboj tvorijo različne oblike sklopov, preko katerih lahko odtekajo podatki. Zaradi izjemnega števila različnih podatkovnih vodil in posledičnih virov sevanja v sistemu sem se v nalogi omejil zgolj na bolj izpostavljena (razširjena) podatkovna vodila, ki so potencialni vir emisij podatkov.

Pred časom zelo razširjeno vodilo RS 232 je v primerjavi z novejšimi oblikami prenosa podatkov še posebej izpostavljeno zaradi:
- prenosa signala po enem prevodniku (brez invertiranega para),
- relativno visoke amplitude signala,
- kratkih časov dviga in spusta signala,
- preprostega kodiranja signala,
- pogosto neustrezno izvedene ozemljitve in oklopa. [s4]

Podobno velja tudi za vodilo PS/2, ki je bilo izjemno razširjeno predvsem pri tipkovnicah in miškah. Ker se po vodilu hkrati s podatki prenaša tudi signal ure, je oddano sevanje kombinacija obeh signalov. Kakor je razvidno iz nadaljevanja, je stopnja tveganja, ki ga predstavlja uporaba slednjega, neprimerno višja kakor pri novejše zasnovanem vodilu USB.

Vodilo VGA, ki se uporablja pri analognem prenosu slike zaslona, je naslednji primer podatkovne komunikacije, ki poteka v nediferencialni obliki. Osnovne barvne komponente analognega signala se ločeno prenašajo po treh prevodnikih (R, G in B). Oddano EM sevanje je zato kombinacija (vsota) treh EM sevanj, ki so posledica spremembe nivoja signala v teh prevodnikih. Možnost rekonstrukcije slike je zato še posebej izrazita pri prikazu kontrastnih oblik, kot je npr. prikaz črnega besedila na beli podlagi. V takšni obliki pa je predstavljena večina pomembnejših podatkov. Delež opreme, ki za prenos uporablja takšen prenos slike, pa je danes še vedno izjemno visok. Zaradi splošne razširjenosti in zagotavljanja kompatibilnosti namreč 15-pinski VGA priklop zagotavlja tudi najnovejša oprema. Hkrati pa nediferencialen način prenosa omogoča tudi vodilo DVI v analognem načinu delovanja (DVI-A). Starejša oprema za prikaz slike na zaslonu je bila neprimerno bolj izpostavljena tveganju glede prestrezanja signala, vendar zaradi številnih virov EM emisij pri prenosu in prikazu video signala tveganje obstaja tudi pri uporabi najnovejše opreme.

Pri prenosu podatkov brez invertiranega para lahko prevodnik pri usklajenosti njegove dolžine s frekvenco prenosa deluje kot učinkovita oddajna antena, ki v okolico razširja EM sevanje s podatki.

Za razliko od RS 232, PS/2 in VGA pri novejše zasnovanih vodilih prenos podatkov poteka v diferencialnem načinu, kar pomeni, da teče tok v dvojicah vodnikov v nasprotnih smereh. Električno in magnetno polje, ki se generira zaradi prenosa signala v navedenih vodnikih, je zato pri večji oddaljenosti od podatkovnega kabla načeloma izničeno oziroma se medsebojno kompenzira. V okolici kabla lahko tako zaznavamo samo polje, ki je posledica odstopanja od idealnih razmer, kot je stopnja asimetrije kabla, razlike absolutne vrednosti signalov ali časovne neusklajenosti signalov (zamika nastopa začetka ali konca impulza). Za prenos ni pomemben potencial, temveč razlika napetosti med vodniki v parici. Po drugi strani pa je prenos odporen tudi proti zunanjim motnjam, saj sofazne motnje v enaki meri vplivajo na oba vodnika, zato ostane razlika napetosti nespremenjena. Tako se lahko posledično zagotovijo tudi zelo visoke hitrosti prenosa in prenos na daljše razdalje.

Primer predstavlja prenos podatkov po podatkovnih vodilih UTP, STP, USB, Firewire, HDMI ipd. Kabel UTP običajno sestavljajo 4 pari medsebojno prepletenih vodnikov, zato so njegove emisije kombinacija več različnih medsebojno izničujočih se polj. Čeprav so jakosti EM sevanja kabla UTP ali STP v določenih primerih lahko zelo visoke, je posledično razmerje med koristnim signalom in šumom zelo majhno. Zato so se že leta 1993 pojavile nekatere tendence, da bi pri povezovanju sistemov TEMPEST uporabili kable UTP kategorije 5 [STP]. EM emisije, ki jih oddajajo kabli UTP višjega kakovostnega razreda, so dejansko zelo majhne. Neodvisno testiranje NSA pooblaščenega laboratorija Dayton T. Brown Inc. je potrdilo, da so emisije kabla UTP kategorije 7 (Siemon's TERA, Category 7 / Class F) glede oddanih EM emisij skladne z zahtevami standardov TEMPEST. [UTP7] Ne glede na to pa je zdaj prenos tajnih podatkov v nešifrirani obliki možen samo po optični napeljavi znotraj upravnega območja. [UKIS]

Večje tveganje lahko predstavlja serijski prenos podatkov z enim diferencialnim parom, kot je to na primer pri vodilu USB. Pri pomanjkljivi izvedbi zahtev EMI lahko emisije neposredno predstavljajo podatke, ki se po vodilu prenašajo.

Ne glede na to, da diferencialna oblika prenosa omogoča boljšo integriteto signala, lahko vseeno vodi k problemom sevalne narave. Visoka stopnja sevanja sofazne narave, ki pri prenosu nastane, je lahko predvsem posledica:

- asimetrije,
- rahlega zamika signala (ob dvigu ali spustu impulza) in
- razlike v amplitudi signala

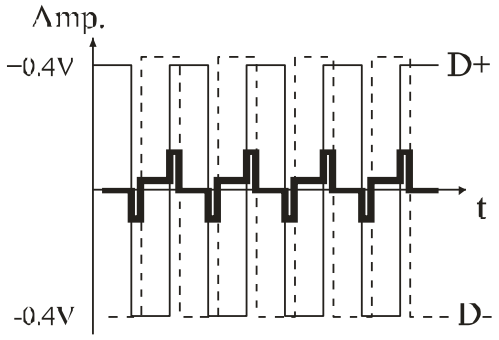
v paru prevodnikov. [f2]

Ta sofazni signal ima lahko izjemno velik učinek na izpolnjevanje zahtev v zvezi z elektromagnetno skladnostjo in tudi vpliva na:

- presluh signala na bližnje prevodnike (*crosstalk*),
- sevanje na podlagi pretvorbe protifaznega v sofazni šum. [f2]

Na te razlike pa lahko vpliva več dejavnikov, kot so npr. razlika v dolžini vodnikov parice, kapacitivnosti kondenzatorjev za omejevanje časa dviga in spusta ipd. [a3]

Da nevarnost nenadzorovanega odtekanja podatkov v okolico obstaja tudi pri vodilu USB, sem na praktičnem primeru prikazal v nadaljevanju. Slednje je predvsem posledica neupoštevanja priporočil glede EM interference, ki so posledica nižanja stroškov izdelave.



Slika 4:
Sofazni šum vodila USB (prikazano z debelejšo črto) zaradi razlike v amplitudi in zamika signala (prirejeno po [y1]).

Razlogi, zaradi katerih vodilo USB vseeno oddaja emisije, so tako predvsem:

- asimetrija kabla,
- neobvezna zahteva po zunanjem oklopu (pri nizkih frekvencah prenosa),
- neobvezna zahteva po prepleteni parici (pri nizkih frekvencah prenosa),
- neobvezna zahteva po notranjem oklopu – aluminijasti foliji, s katero so oviti vodniki v kablu (pri nizkih frekvencah prenosa),
- neobvezna zahteva po odvodnem vodniku (pri nizkih frekvencah prenosa),
- možnosti poškodbe aluminijaste folije, ki lahko nastane zaradi prepogibanja kabla ali dotrajanosti,
- neustrezna izvedba povezave oklopa kabla s konektorjem,
- resonančne lastnostih kabla in oklopa pri določeni frekvenci prenosa.

Težavo pri uporabi vodila USB lahko predstavljajo tudi konduktivne emisije, in sicer tako sofazne kakor tudi diferencialne. Pri opremi, ki je povezana preko vodila USB in je na ta šum občutljiva, lahko celo vpliva na njeno delovanje, zato je slednje treba upoštevati pri obravnavi celotnega sistema. [s5]

3.7 Drugi stranski kanali

Stranski kanali, po katerih odtekajo podatki, niso omejeni zgolj na EM lastnosti in prevodne lastnosti infrastrukture. Oprema vpliva na okolico tudi preko drugih lastnosti, ki so prav tako lahko povezane z obravnavanimi podatki. Tovrstne stranske kanale predstavljajo optične lastnosti, specifični zvočni učinki, poraba energije, razlike v temperaturi ipd.

4 STANDARDI IN PREDPISI

4.1 Varnost, ki jo zagotavljajo predpisi o elektromagnetni skladnosti

EM združljivost (EMC) opredeljuje vpliv EM sevanj na elektronske naprave. Vse elektronske naprave namreč pri svojem delovanju v okolico oddajajo EM emisije. Hkrati so naprave, ki vsebujejo polprevodniška vezja, občutljive na zunanje motnje v obliki EM emisij. Najbolj so občutljive naprave, ki sprejeti motilni signal preoblikujejo in ojačijo. Posebne zahteve so predpisane v okoljih, kjer lahko motnje povzročijo večjo škodo (npr. medicinska oprema, promet). Proizvajalci morajo zato zagotoviti imunost za predpisano (standardizirano) izpostavljenost EM polju. Skladnost se za področje EU zagotovi z izpolnjevanjem zahtev usklajenih standardov po Direktivi 2004/108/ES Evropskega parlamenta in Sveta z dne 15. 12. 2004. Pri nas direktivo uvaja Pravilnik o elektromagnetni združljivosti (EMC) (Uradni list RS, št. 132/2006). Namen pravilnika je zagotoviti, da so aparati, nepremični sestavi, telekomunikacijska in radiokomunikacijska omrežja vključno s sprejemanjem radiodifuznih in radioamaterskih storitev ter omrežja za dobavo električne energije ustrezno zaščiteni pred elektromagnetnimi motnjami, ki bi jih povzročali aparati ali nepremični sestavi. Pravilnik ne velja za določena specifična področja (medicina, letalski proizvodi, radioamaterska oprema …).

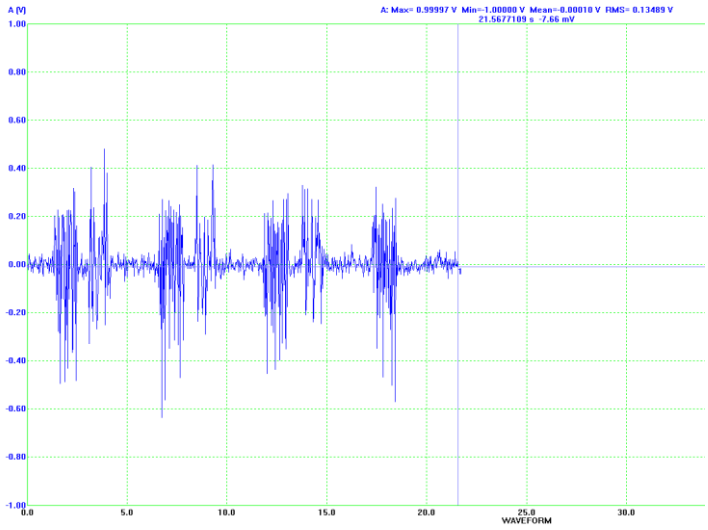
Zahteve, ki izhajajo iz priloge pravilnika, vključujejo:

1. Zaščitne zahteve
   Oprema mora biti zasnovana in izdelana z upoštevanjem stanja tehnike, ki zagotavlja, da:
   – elektromagnetne motnje, ki jih povzroča, ne presegajo ravni, nad katero radijska in telekomunikacijska oprema ter druga oprema ne morejo delovati, kakor je predvideno;
   – ima raven odpornosti pred elektromagnetnimi motnjami, kot se pričakujejo pri predvideni uporabi, kar omogoča delovanje opreme za njen namen brez nesprejemljivega poslabšanja delovanja.
2. Posebne zahteve za nepremične sestave
   Pri namestitvi nepremičnih sestavov se uporabi dobra inženirska praksa s področja EMC in upoštevajo podatki o predvideni uporabi njenih sestavnih delov, da se izpolnijo zaščitne zahteve iz 1. točke. Zadevna dokumentacija pa mora biti na voljo pristojnemu inšpektoratu za pregled, dokler nepremični sestav deluje.

Emisije informacijske opreme opredeljuje standard EN 55022 (Oprema za informacijsko tehnologijo, karakteristike občutljivosti na radijske motnje – mejne vrednosti in merilne metode), ki se sklicuje na referenčni dokument CISPR 22.

Oznaka »CE« zagotavlja ustreznost naprave glede izpolnjevanja vseh evropskih direktiv tehnične zakonodaje za določeno vrsto naprave.

Primer vpliva uporabe običajne informacijske opreme na radiofrekvenčni spekter je razviden iz slike 5. Prikazano je oddano EM sevanje v radijskem (FM) frekvenčnem območju, ki je posledica uporabe USB flash diska pri zapisovanju in branju datotek. Pomnilniški medij je bil na prenosnik priključen preko dvojno oklopljenega kabla. Signal je bil sprejet z radijskim sprejemnikom v običajnem delovnem okolju na frekvenci 82 Mhz, z razdalje 3 m od vira sevanja. Slika 5 prikazuje emitirano EM sevanje, ki je posledica izmeničnega pisanja in branja štirih različnih datotek, med katerimi so kratki časovni presledki. Antena je bila usmerjena tako, da je zagotavljala najugodnejše razmerje med virom sevanja in šumom.



Slika 5:
Vpliv uporabe USB flash diska na FM območje RF spektra oziroma na motnje radijskega sprejema.

Ker pa so oddane emisije lahko neposredno povezane s podatki, ki se obravnavajo v sistemu, se postavi vprašanje, ali predpisane meje sevanja hkrati zagotavljajo zaščito pred odtekanjem podatkov.

Nivo varnosti pred prestrezanjem podatkov, ki jo zagotavljajo meje dopustnih emisij standardov s področja EM skladnosti, je razviden iz naslednjega primera. Najvišje dovoljene EM emisije elektronskih naprav namreč niso tako zelo odmaknjene od

nivoja signala, ki še zadošča za nemoten sprejem radijskih ali televizijskih programov. Primer se nanaša na UHF frekvenčno območje, v katerem je mogoče zaznati emisije, ki so neposredno povezane s podatki slike, ki je prikazana na zaslonu. Hkrati se v tem frekvenčnem območju oddaja televizijski program preko zemeljskih oddajnikov. Minimalne zahteve pri načrtovanju RF spektra za pokritost terena, ki omogoča kakovosten sprejem digitalnega televizijskega signala v UHF frekvenčnem območju za najnižjo električno poljsko jakost, določajo najmanj 50 dBµV/m. Najnižja poljska jakost, ki omogoča nemoten sprejem digitalne televizije s standardno opremo v UHF območju, je 44,6 dBµV/m [DTV-A]. Pri tem je treba upoštevati, da se pri načrtovanju pokritosti terena predvideva uporaba običajnih antenskih sistemov in ne profesionalne opreme, s katero so mogoči višji dobitki. Za uspešno rekonstrukcijo podatkov pa »popolnoma nemoten sprejem« večinoma ni potreben. Standarda CISPR 22/EN 55022 in FCC Part 15 za to frekvenčno območje dopuščata naslednje najvišje vrednosti oddanih EM emisij glede na razred naprave in glede na oddaljenost od vira sevanja, ki ga predstavlja naprava [o1]:

Razdalja od naprave – vira sevanja FCC	Meja dopustnih emisij – naprave razreda A	Meja dopustnih emisij – naprave razreda B
1 m	* 66,5 dBµV/m	* 55,5 dBµV/m
3 m	* 57,0 dBµV/m	46,0 dBµV/m
10 m	46,5 dBµV/m	35,5 dBµV/m

Razdalja od naprave – vira sevanja CISPR 22	Meja dopustnih emisij – naprave razreda A	Meja dopustnih emisij – naprave razreda B
1 m	* 67,0 dBµV/m	* 57,0 dBµV/m
3 m	* 57,5 dBµV/m	47,5 dBµV/m
10 m	47,0 dBµV/m	37 dBµV/m

Preglednica 2:
Meje dopustnih emisij sevanja, ki jih predpisujeta standarda CISPR 22 in FCC Part 15
(izračunane vrednosti)*

Najvišje dopustne vrednosti emisij so predpisane pri določeni oddaljenosti od vira sevanja, kjer se izvajajo meritve. Dopustne vrednosti emisij pri drugačni oddaljenosti od naprave se lahko preračunajo na podlagi izraza:

$$E_1\ (\mathrm{dB\mu V/m}) = E_0\ (\mathrm{dB\mu V/m}) + 20 \log (d_0/d_1),$$

kjer je E0 predpisana mejna vrednosti pri razdalji d0 od vira sevanja, E1 pa mejna vrednost pri oddaljenosti d1 [m2].

Na tej podlagi je mogoče podati oceno, da sprejemni del običajne televizijske opreme lahko sprejema EM signal v UHF frekvenčnem območju, katerega jakost je ekvivalentna dopustnemu EM sevanju opreme »razreda A« na razdalji 13,2 m oziroma opreme »razreda B« na razdalji 4,2 m.

Iz zgoraj opisanega izhaja, da lahko prilagojeni sprejemni deli radijske in televizijske opreme predstavljajo osnovo za sprejem emitiranih podatkov. To je še bolj očitno ob dejstvu, da za to frekvenčno območje obstaja široka ponudba cenovno dostopnih anten z visokim dobitkom. Zaradi prilagojenosti moduliranemu signalu neposrednega zajema brez ustreznih predelav sicer ne omogočajo. Če napadalec uporabi profesionalno opremo, pa so možnosti prestrezanja podatkov še veliko večje. Za zajem EM sevanja se lahko uporabi širokopasovna antena, ki je preko ojačevalnika priključena neposredno na vhod osciloskopa in spektralnega analizatorja.

Kuhn [k7] zato za zagotavljanje varnosti pred prestrezanjem podatkov na podlagi EM sevanja predlaga občutno nižje vrednosti emisij, kakor izhajajo iz standardov s področja zagotavljanja EM skladnosti (preglednica 3).

Vir	Namen	Najvišja dovoljena vrednost
CISPR 22	EMC	68
MIL-STD-461E/R102	EMI/RFI (am. – Dep. of Defence)	44
Kuhn [k7]	Varnost pred prestrezanjem podatkov	7

Preglednica 3:
Najvišje dovoljene vrednosti spektralne gostote glede na standarde EM skladnosti v primerjavi z mejo, ki zagotavlja varnost pred nepooblaščenim prestrezanjem podatkov [k7] (pri 100 MHz, na razdalji 1 m, v dBµV/mMHz) [k7]

Podobno kot Kuhn ugotavljata tudi Zoyousefein in Ghorbani [z1], ki v RF spektru od 30 kHz do 1 GHz za zagotavljanje varnosti pred prisluškovanjem predlagata 20 dB nižje meje dopustnih emisij, kakor jih določajo standardi za zagotavljanje EM skladnosti.

Glede na IEEE *Standard for Information Technology*: *Hardcopy Device and System Security* [SIT] samo omejevanje emisij z vidika EMC ni dovolj, saj je bolj kakor sama amplituda emisij pomembna njihova korelacija s podatki.

Pri uporabi običajne informacijske in komunikacijske opreme ob upoštevanju zgoraj navedenih referenčnih vrednostih električnega polja namreč ne moremo zagotoviti, da zlorabe podatkov na osnovi oddanih EM emisij niso mogoče. Tveganje je še

veliko večje, če napadalec pri prestrezanju podatkov napada uporabi prilagojeno opremo z zelo učinkovitim sprejemnim delom, ki dejansko omogoča sprejem zelo nizkih jakosti EM sevanja.

4.2 EM emisije v odvisnosti od razvoja tehnologije

Razvoj tehnologije na področje zagotavljanja EMC prinaša nove izzive. Leta 1990 so bile frekvence obdelave in prenosa signala večinoma pod 25 MHz, zato temu področju v fazi načrtovanja integriranih vezij ni bilo treba posvečati toliko pozornosti. EMI/EMC načrtovanje je bilo večinoma omejeno na prilagajanje oblike signala v smeri daljših časov dviga in spusta impulza s kapacitivnimi filtri ter filtriranja V/I signalov. Večina emisij je izvirala iz priključnih kablov, saj so ti zaradi svoje dolžine bolj ustrezali oddajni anteni kot sama naprava. V današnjem času so zaradi visokih frekvenc obdelave in prenosa signala valovne dolžine signala bistveno krajše. Za signal s frekvenco 30 MHz mora biti dolžina prenosne linije z lastnostjo oddajnega monopola 250 cm, medtem kot je ta pri 3 Ghz samo 2,5 cm. [a3]

Okvire najvišjega dopustnega EM sevanja v okolico postavljajo standardi za zagotavljanje EMC skladnosti. Ti sicer ne določajo varnosti pred prisluškovanjem, vendar se dopustne meje sevanja z razvojem predpisov počasi znižujejo. Če je bilo mogoče neposredno EM sevanje CRT zaslonov pred leti prestreči z razdalje več kakor 1 kilometer, so stopnje emisij sodobne opreme občutno nižje. To pa ne pomeni, da podatkov z večjih razdalj ni več mogoče prestreči. Pri prenosu signala na prevodno infrastrukturo ali z modulacijo na signal komunikacijske opreme se lahko širi po njem tudi na izjemno velike razdalje. Razširjenje je omejeno zgolj s potekom in lastnostmi prevodne infrastrukture ter vplivom motenj na poti prenosa. Prestrezanje podatkov na podlagi direktnih ali posrednih emisij tako tudi pri najnovejši IKT lahko predstavlja visoko tveganje glede izgube zaupnosti.

Na emisije, ki so posledica prenosa podatkov, v prvi vrsti vpliva vrsta podatkovnega vodila in sama hitrost prenosa. Zaščita je večinoma odvisna od usklajenosti valovne dolžine EM valovanja z dolžino prevodnika, uporabe diferencialnega prenosa, oklapljanja, ozemljitve in oblike signala.

4.3 Predpisi s področja zaščite pred prestrezanjem podatkov

Pojem »TEMPEST« je v osnovi oznaka ameriške vlade, ki določa zbirko standardov za omejevanje električnih in EM emisij, ki jih pri delovanju oddaja električna, elektronska, elektromehanska in elektrooptična oprema. Ne glede na širšo

uveljavljenost pojma na področju nadzora nad EM emisijami pri obravnavi zaupnih podatkov sam pomen izraza ni uradno razložen. Obstaja sicer več neuradnih razlag, kot so »Telecommunication and Electronic Material Protected from Emanating Spurious Transmission«, »Transient Electro-Magnetic Pulse Emanation Standards«, »Transient Emanations Protected from Emanating Spurious Transmissions«, »Temporary Emanation of Spurious Transmission« ipd. [a5]

Razvoj standardov, ki opredeljujejo področje emisij podatkov, temelji na standardu iz 50. let prejšnjega stoletja z oznako NAG1A. Ta je bil v 60. letih nato revidiran in objavljen pod oznako FS222 ter pozneje kot FS222A. Obsežna revizija v 70. letih je vodila k izdaji dokumenta *National Communications Security Information Memorandum 5100*, ki je širše poznan pod oznako NACISM 5100. [a5] Ta standard je v nekoliko okrnjeni različici tudi javno objavljen na spletu. Vsi aktualni standardi in njihovi predhodniki še vedno niso javno dostopni. V veljavno skupino standardov z oznako SDIP (*Security and evaluation agency Doctrine and Information Publication*) se s tega področja uvrščajo:

- SDIP 27 – postopki in zahteve evalvacije NATO TEMPEST (nasledil standarde AMSG-720B / AMSG-788A / AMSG-784),
- SDIP 28 – postopki NATO coniranja,
- SDIP 29 – zahteve načrtovanja in instalacije opreme za obravnavanje tajnih podatkov,
- SDIP 30 – instalacije električne opreme za obravnavanje tajnih podatkov.

V Nemčiji so z oznako tajnosti označena tudi imena standardov, ki se nanašajo na varnost pred prestrezanjem podatkov preko EM emisij. S standardi upravlja agencija *Bundesamt für Sicherheit in der Informationstechnik* (BSI). [k4]

Standardi s področja zagotavljanja elektromagnetne skladnosti, ki sicer določajo dopustne emisije elektronskih naprav v okolico, večinoma ne predpisujejo zahtev, ki bi preprečevale zlorabo podatkov na tej osnovi. Izjeme so splošne narave, kakor npr. člen 15.9 standarda FCC, ki se nanaša na prepoved uporabe predpisane merilne opreme za namene prestrezanja podatkov.

Sklep Sveta EU z dne 19. marca 2001 o sprejetju predpisov Sveta o varovanju tajnosti (2001/264/ES) glede zaščite podatkov v sistemih informacijske tehnologije in v komunikacijskih sistemih določa protiukrepe TEMPEST kot ukrepe varovanja tajnosti, katerih namen je varovanje opreme in komunikacijske infrastrukture pred ogrožanjem tajnih podatkov zaradi nenamernih elektromagnetnih oddajanj. Glede varovanja tajnosti v zvezi s sevanjem opreme IKT predpisuje naslednje zahteve:

- sistemi, ki obdelujejo tajne podatke na stopnji EU CONFIDENTIAL (zaupno) in višje, se zaščitijo tako, da njihove varnosti ne morejo ogroziti škodljiva sevanja, katerih proučevanje in nadzor sta določena kot »TEMPEST«,
- protiukrepe TEMPEST, ki veljajo za namestitve v GSS in decentraliziranih agencijah EU, pregleda in odobri organ TEMPEST, ki ga določi varnostni organ GSS. Za namestitve na nacionalni stopnji, v katerih se obdelujejo tajni podatki EU, odobritev izda na nacionalni ravni priznani organ TEMPEST.

Sklep Evropske komisije z dne 29. novembra 2001 o spremembah njenega poslovnika oziroma v Pravilniku o varnosti glede varovanja tajnih podatkov EU v sistemih informacijske tehnologije in v komunikacijskih sistemih določa tudi tehnične varnostne ukrepe na področju varnosti v zvezi z namestitvijo in sevanjem.

V Sloveniji glede izvajanja zaščite TEMPEST upoštevamo navedene zahteve EU in zveze NATO. [m1]

Področje zaščite pred neželenim elektromagnetnim sevanjem je v Sloveniji opredeljeno v [UKIS], ki s tem v zvezi predpisuje naslednji zahtevi:

- vse sestavine sistemov, v okviru katerih se obravnavajo tajni podatki stopnje tajnosti ZAUPNO ali višje, morajo biti zaščitene pred neželenim elektromagnetnim sevanjem,
- zaščito pred neželenim elektromagnetnim sevanjem zagotavljajo upravljavci sistemov, v katerih se obravnavajo tajni podatki in so del načrta varovanja. O ugotovitvah meritev obveščajo Urad Vlade RS za varovanje tajnih podatkov,

ter določa pristojne organe za izvajanje meritev pred neželenim elektromagnetnim sevanjem in nosilca priprave zahtev glede izvajanja zaščitnih ukrepov.

Komisija za informacijsko varnost je 19. 11. 2008 izdala Navodilo o izvajanju zaščite pred neželenim elektromagnetnim sevanjem v komunikacijskih in informacijskih sistemih, v katerih se obravnavajo tajni podatki [UVTP1]. Na podlagi navodila mora imeti vsa delujoča oprema, razen kriptografske, za obdelovanje, prenos in hranjenje tajnih podatkov v elektronski obliki ustrezno potrdilo TEMPEST in biti ustrezno označena z nalepko, na kateri je naveden nivo zaščite TEMPEST. Potrdila, ki določajo ustrezen nivo zaščite TEMPEST, so tudi del dokumentacije, na podlagi katere se pridobiva varnostno dovoljenje za delovanje sistema.

Coniranje TEMPEST

EM sevanje je najmočnejše v neposredni bližini vira in upada s kvadratom razdalje. Ker je nevarnost razkritja podatkov odvisna od razdalje, se prostor okoli vira sevanja razdeli na več con glede na stopnjo tveganja, ki jo predstavlja odtekanje podatkov. V bolj ogroženih conah je treba uporabiti stroge zaščitne ukrepe, na manj ogroženih področjih pa so ukrepi blažji. Od stopnje uporabljenih ukrepov je namreč zelo odvisna cena uporabljene opreme in kompleksnost drugih varnostnih ukrepov. V splošnem standardi razločijo 3 do 4 cone. Skladno s tem proizvajalci izdelujejo rangirano opremo, ki je certificirana za uporabo v določeni coni. Da bi dosegli poenotenje meril, so v standardih za določitev cone uvedli bodisi merilo fizične razdalje od virov neželenega sevanja (sistema) ali pa meritve ekvivalentnega dušenja radijskih signalov skozi stene merjenih prostorov. Meritve je treba izvesti na širokem frekvenčnem spektru, da zajamejo večino možnih pojavnih oblik neželenega sevanja. Ko je določena cona prostora, kjer bo nameščen sistem, je treba skladno s tem izbrati primerno opremo in način namestitve, ki ustreza stopnji tajnosti in coni. [m1]

Meritve TEMPEST

Za pravilno namestitev primerne opreme v posameznih prostorih je treba izvesti tudi t. i. meritve TEMPEST. V prvi vrsti so to meritve prostorov za določitev cone in jih običajno izvaja za ta namen usposobljena skupina strokovnjakov. Za meritve se uporablja posebej prilagojena merilna oprema, izvajajo pa se po natančno predpisanih metodah. [a5, m1]

Sledijo meritve opreme za pridobitev določenega varnostnega potrdila TEMPEST. Izvajajo jih namenski laboratoriji, ki so bodisi v okviru državnih ustanov ali pa v lasti specializiranih podjetij z ustreznimi potrdili za opravljanje takih meritev. Nekatere države na spletu tudi objavljajo seznam opreme in vrsto varnostnega potrdila, ki ga posedujejo, na primer:

- SDIP-27 Level A – najstrožje zahteve – opremo lahko namestimo v NATO coni 0, kjer ima potencialni napadalec skoraj neposredni dostop do opreme,
- SDIP-27 Level B nekoliko milejše zahteve – opremo lahko namestimo v NATO cono 1,
- SDIP-27 Level C še milejše zahteve – opremo lahko namestimo v NATO cono 2. [m1]

5 PRESTREZANJE PODATKOV PREKO STRANSKIH KANALOV

V prvem delu poglavja podajam pregled tveganj, ki ga predstavlja prestrezanje podatkov z izkoriščanjem električnih lastnosti, s katerimi IKT med svojim delovanjem vpliva na okolico, v drugem delu poglavja pa pregled tveganj zaradi izrabe drugih lastnosti.

5.1 Prestrezanje podatkov preko električnih lastnosti

V celotnem oddanem RF spektru emisij, ki jih med svojim delovanjem oddaja neka naprava, so v določenih frekvenčnih območjih te lahko neposredno povezane z obravnavanimi podatki. [p1] Najvišje predpisane meje emisij zagotavljajo elektromagnetno skladnost med napravami in dopusten vpliv na organizem, medtem ko v običajnem poslovnem okolju ali pri osebni uporabi neposredno ne varujejo pred možnostjo odtekanja podatkov, ki s tem v zvezi obstaja. Tako imenovani napadi TEMPEST za prestrezanje podatkov izkoriščajo električne vplive na okolico, ki jih oddajajo elektronske naprave med svojim delovanjem ali pri komunikaciji z drugimi napravami in perifernimi enotami. Možnosti izvedbe teh napadov so zelo raznolike, napadalci pa izbirajo metode, ki so prilagojene vrsti naprav, okolju in komunikacijskim povezavam.

Ocenjuje se, da je mogoče na podlagi EM sevanja in konduktivnih emisij zajeti okrog 1–2 % vseh podatkov, ki se obravnavajo v informacijskih sistemih. Na prvi pogled stopnja tveganja torej ni izjemno velika, toda ob upoštevanju dejstva, da se večina zaupnih podatkov obravnava z opremo IKT, lahko 2 % vseeno pomeni veliko nevarnost. [s3]

Kakor je razvidno iz slike 9, lahko signal, ki nosi podatke, zajamemo neposredno (npr. preko EM sevanja) ali posredno preko prevodne infrastrukture, na katero se signal prenese preko sevanja ali različnih oblik sklopov, ki so posledica neželenih medsebojnih odvisnosti sistemov.

Pri obravnavi elektromagnetne skladnosti med napravami je šum neželeni pojav, ki moti delovanje druge naprave, ki jo v tem primeru definiramo kot žrtev. Pri obravnavi napadov TEMPEST pa sta vlogi zamenjani, sprejemnik izkoriščamo za prestrezanje signala s podatki naprave, ki predstavlja vir sevanja. Žrtev je v tem primeru vir sevanja, ki obravnava podatke, šum pa predstavljajo vse emisije, ki niso povezane s podatki. Napad TEMPEST se zato običajno izvede na ozkem frekvenčnem območju,

na katerem so emisije povezane s signalom, ki predstavlja podatke in kjer je razmerje med signalom in šumom dovolj ugodno, da je mogoča rekonstrukcija izvornih podatkov. [t1]

Napadi TEMPEST na podlagi prestrezanja EM sevanja zaradi pasivnega načina izvedbe ne puščajo sledi in so zato težko izsledljivi. V okoljih, kjer je zaupnost podatkov visokega pomena in lahko vpliva na ogrožanje nacionalne varnosti države, so predpisani ukrepi, ki preprečujejo možnosti tovrstnih zlorab. Te vključujejo uporabo namenske opreme, skladne s standardom SDIP 27, obravnavo podatkov v akreditiranih varnostnih območjih, kriptografsko zaščito ipd. Vendar tveganje obstaja tudi pri uporabi opreme v osebne ali poslovne namene, kjer uporaba tovrstne opreme ni mogoča. Pri običajni poslovni in tudi osebni uporabi opreme s standardno informacijsko opremo ima lahko izguba zaupnosti podatkov prav tako hude posledice na ravni poslovnega sistema ali na osebni ravni. Ogroženi so lahko osebni podatki, finančno stanje, poslovne skrivnosti ipd. Zaščita pri uporabi standardne IKT je lahko strojna (oz. fizična) in tudi programska. [t1]

Zaradi nekajkrat višje cene namenske opreme za zaščito pred napadi TEMPEST je njena uporaba večinoma omejena na okolja, v katerih se obravnavajo tajni podatki. Možnost prestrezanje podatkov je po drugi strani mogoče omejevati tudi s cenejšimi ukrepi, vendar je njihova učinkovitosti v praksi vprašljiva. Protiukrepi so tako lahko izvedeni tudi s programskimi rešitvami ali generatorji motenj. [t1]

Pri učinkovitosti navedenih protiukrepov pa obravnava z vidika elektromagnetne skladnosti naprav predstavlja predvsem dve težavi:

- emisije lahko nastopajo v širokem frekvenčnem območju (rekonstrukcija podatkov je mogoča na različnih frekvenčnih območjih RF spektra) in
- učinkovitost ukrepov je nejasna, saj ne glede na dopustne vrednosti emisij EMC ni znana stopnja emisij naprave in tveganja, ki jo te emisije predstavljajo. Hkrati ne poznamo mejne vrednosti EM sevanja, pri kateri lahko napadalec podatke še zajame in rekonstruira. [t1]

5.1.1 Pregled objavljenih primerov

V strokovni literaturi tveganje prestrezanja podatkov preko stranskih kanalov izpostavljajo številni viri. Po drugi strani pa je število objavljenih primerov dejanske izvedbe manjše. Zato je do neke mere še vedno neznanka tudi realna ocena tveganja, ki ga predstavljajo tovrstne grožnje.

Prvi znani primeri problema EM emisij, ki so povezani z ohranjanjem zaupnosti podatkov, se nanašajo na obsežen razvoj telefonskih omrežij v 19. stoletju, ki je imel za posledico zelo zgoščene omrežne povezave. Zaradi presluha med posameznimi telefonskimi linijami so uporabniki omrežja lahko nehote prisostvovali pogovorom drugih uporabnikov. [v3] Težavo je prvič izpostavila britanska vojska ob ekspedicijah v dolino reke Nil in Suakin v letih 1884 in 1885. [a2]

V prvi svetovni vojni je nemška vojska uspešno prisluškovala telefonskim pogovorom nasprotnika. Za komunikacijo med različnimi vojaškimi enotami na bojišču se je uporabljala povezava s samo eno izolirano žico, s čimer so znižali težo kablov, ki so jih morale enote prenašati s seboj. Zanka je bila zaključena skozi zemljo. Tok povratne zanke je preko ojačevalcev izkoristila nemška vojska. Tako so lahko prestrezali telefonske pogovore na 90 m, signal Morsejeve abecede pa celo na trikrat daljšo razdaljo. Leta 1915 so se tega problema zavedle britanske in francoske sile ter uvedle protiukrepe, ki so vključevali prestavitev ozemljitvenih konektorjev za sto in pozneje za več tisoč metrov od prvih strelskih jarkov, prepletene kable, znižanje jakosti toka … [k4, a2]

Leta 1918 je ameriška vojska naložila organizaciji Black Chamber, ki jo je vodil Herbert Yardly, naj razvije metode zaznavanja in prestrezanja vojaških telefonskih in radijskih sistemov. Poročilo je izpostavilo, da uporaba »neprilagojene opreme« na podlagi številnih tehničnih slabosti omogoča odtekanje zaupnih podatkov. Na podlagi teh ugotovitev so začeli razvijati metode za preprečevanje neželenih EM emisij. [a5]

V drugi svetovni vojni je ameriška vojska uporabljala teleprintersko komunikacijo. Za kriptiranje povezave se je uporabljala naprava Bell 131-B2. Čisto po naključju so v Bellovem laboratoriju odkrili, da njena uporaba sproža impulzne odzive na oddaljenem osciloskopu v istem prostoru, ki so neposredno povezani z besedilom v nekriptirani obliki. Poskus so ponovili iz 25 m oddaljene stavbe na drugi strani ceste in rekonstruirali 75 % podatkov. [NSA]

V Vietnamski vojni je senzor »Black Crow«, ki so ga uporabljali bombniki AC 130, lahko na razdalji 10 milj zaznal EM sevanje, ki so ga oddajali motorji tovornjakov na transportnih povezavah Ho Chi Minh Trail. [v3]

Leta 1960 so v Veliki Britaniji na podlagi EM sevanja odkrivali lastnike neprijavljenih televizijskih sprejemnikov. [dv1]

Istega leta je med pogajanji o pridružitvi Evropski uniji britanska tajna služba MI5 prisluškovala francoski ambasadi. Zaradi bojazni, da bo francoski predsednik De Gaulle blokiral pridružitev Velike Britanije, so strokovnjaki MI5 in GCHQ prestregli signal z linije telefaksa in ga speljali v bližnji Hyde Park Hotel. Kriptografske zaščite sporočila niso uspeli razbiti, vendar so uspeli iz linije izkoristiti šibak nekodiran EM signal, ki ga je oddajala oprema pri šifriranju podatkov. [N1, 50]

Leta 1984 je tajna služba Nemške demokratične republike MfS na podlagi EM sevanja prestrezala podatke zunanjega ministrstva. [dv1]

Leta 1985 je bilo v Veliki Britaniji prvič javno predstavljeno prisluškovanje z izkoriščanjem elektromagnetnega sevanja računalnikov, in sicer zajem slike z računalniških zaslonov, ki so ga izvedli iz vozila pred stavbo New Scotland Yarda v Londonu. S tem so prvič javnosti prikazali resnično nevarnost kompromitiranja podatkov v računalniških sistemih. [m1]

Konduktivne emisije pametnih kartic so v 90. letih izkoristili hekerji za zajem kriptografskega ključa plačljivih televizijskih programov [a2].

Eden izmed bolj znanih in odmevnih primerov, ki je izpostavil nevarnost odtekanja podatkov preko EM sevanja, pa je bil napad na nizozemske volilne naprave. Nizozemska je že od poznih osemdesetih let prejšnjega stoletja izvajala volitve z elektronskimi volilnimi napravami, ki so v primerjavi s klasičnimi papirnimi glasovnicami poenostavile glasovanje, pospešile štetje glasov in odpravile dileme glede neveljavnih glasov. [j1]

Za izvedbo volitev so večinoma uporabljali volilne naprave nizozemskega proizvajalca Nedap, v zadnjih letih pa tudi novejše, ki jih je izdelovalo drugo domače podjetje Sdu. Ne glede na to, da so te naprave pri volitvah uporabljali vrsto let brez večjih težav in da so naprave izpolnjevale vse predpisane zahteve, je skupina posameznikov z zelo odmevno akcijo dokazala njihovo neustreznost in preprečila njihovo nadaljnjo uporabo. Jeseni 2006 se je začela kampanja proti volilnim napravam z naslovom »We don’t trust voting computers«. Glavni razlog za nezaupanje je bilo dejstvo, da je mogoče z napadom TEMPEST razkriti glas volivca. Posledično izvedba volitev ni zagotavljala tajnosti glasovanja. V predstavitvi, ki je bila na nacionalni televiziji predvajana mesec in pol pred razpisanimi volitvami, so predstavili slabosti volilnih naprav. [j1] Izkazalo se je, da je mogoče glas volivca z naprave Sdu prestreči do razdalje 40 m, z naprave Nedap pa do razdalje okrog 5 m. Pri slednjih so uspeli z manjšim tehničnim posegom izboljšali varnost glede izvedbe

napada TEMPEST. Bolj kritične so bile emisije zaslona na dotik, ki jih je oddajala volilna naprava Sdu. Tri tedne pred volitvami so zato preklicali certifikat o njihovi ustreznosti. Volitve so dovolili izvesti z napravami, pri katerih je bila zagotovljena varnost znotraj 5 m, kar je ustrezalo sevanju naprav Nedap. Ta dopuščena meja, znotraj katere je mogoče prestreči glas, je bila tudi podlaga za nadaljnjo razpravo o tehnični primernosti in iskanje ustreznih rešitev na področju regulative ter tehnične izvedbe naprav. [p2]. Na območjih, kjer so se uporabljale naprave Sdu, so zato leta 2006 izvedli glasovanje s presežnimi napravami Nedap ali pa s papirnimi glasovnicami. V letu 2007 je Sdu pripravil različico z nižjimi elektromagnetnimi emisijami in jo ponovno predložili v akreditacijo. Sprememba naprave glede odpornosti proti napadom TEMPEST je znižala svetilnost zaslona, kar je vodilo k zavrnitvi iz razloga neprimernosti za volivce z barvno slepoto. [j1].

Po izvedenih volitvah je nizozemska vlada leta 2007 ustanovila dve komisiji neodvisnih strokovnjakov, ki naj bi dali mnenje o preteklih elektronskih volitvah in priporočila za prihodnost. Eden od predlogov, ki se je nanašal na EM emisije, je bila zahteva po skladnosti s standardom SDIP 27 level B, kar je bilo zaradi tajnosti standarda v nasprotju z načelom javnosti izvedbe volilnega postopka. V tem času so pripravili tudi prototip volilne naprave TEMPEST, ki pa je bila zaradi kovinskega oklopa pretežka in neprimerna za uporabo. Nizozemska vlada je za pripravo normativa glede sevanja volilnih naprav pooblastila nemško podjetje GBS. V poročilu, ki ga je to podjetje pripravilo, je normativ 5 metrov temeljil na aperturi sprejemne antene velikosti 1 m^2. To je pomenilo, da bi zmogljivejša antena lahko signal zajela tudi na večji razdalji, hkrati pa bi bilo mogoče signal na krajši razdalji prestreči tudi z manjšimi antenami. Še večjo težavo so predstavljali postopki za izvajanje meritev emisij in postopki akreditacije. Skladnost glede oddajanja emisij bi se preverjala na dveh nivojih, in sicer na nivoju akreditacije modela in meritve skladnosti vsake posamezne naprave. Prva meritev bi trajala 4 ure, druga 25 minut. Za testiranje vseh 10.000 naprav bi bilo tako potrebnih 50 tednov, meritve pa bi bilo treba ponoviti vsaki dve leti. V postopku testiranja bi naprave namesto volilne aplikacije izvajale program, s katerim bi maksimirali oddane emisije. Poročilo je predvidevalo tudi omejitve pri postavitvi naprav v prostoru, prepoved približevanja mobilnih telefonov ipd. Po analizi poročila, ki jo je opravila ekspertna skupina, se je vlada odločila, da zahteve niso sprejemljive. Izpolnitev zahtev z uvedbo prilagojenih vojaških standardov bi namreč vodila k visokim stroškom, pretežkim napravam in velikim organizacijskim ter logističnim problemom glede izvajanja meritev sevanja. Nizozemska je zato v letu 2008 ukinila glasovanje z volilnimi napravami in se vrnila h klasičnemu načinu glasovanja. Naslednje volitve so bile na Nizozemskem izvedene s papirnimi glasovnicami. Volilne naprave so na podlagi vprašljive tehnične ustreznosti

in civilnih pobud ukinili tudi v nekaterih drugih državah, na podlagi ustavne sodbe leta 2009 tudi v Nemčiji. [j1, p2]

5.1.2 Prestrezanje podatkov pri uporabi tipkovnice

Prestrezanje podatkov, ki v okolico odtekajo z uporabo tipkovnice, lahko predstavlja nevarnost zaradi izjemno občutljive vsebine, ki se na ta način vnaša v računalniški sistem. S tipkovnico se pri osebni uporabi in uporabi v poslovne ali službene namene vpisujejo osebni in drugi občutljivi podatki, kot so uporabniška imena in gesla, s katerimi se prijavljamo v operacijski sistem, omrežje, internetne portale, spletne banke, dostopamo do elektronske pošte in podobno. EM emisije, iz katerih je mogoče razbrati podatke, lahko oddaja kabel ali krmilnik tipkovnice. Podobno sicer velja tudi za druge naprave, ki so priključene na delovno postajo preko USB ali drugih serijskih vodil, vendar je specifika tipkovnice v tem, da se pri njeni uporabi prenašajo izjemno majhne količine podatkov z občutljivo vsebino. Ker ni potrebe po obsežnejši podatkovni komunikaciji, tipkovnice tudi ne izkoriščajo celotnih zmožnosti prenosa in zaščite, ki jo sicer omogoča vodilo USB. Prav tako je prenos podatkov uniformiran in ponovljiv, saj ena posredovana sekvenca vedno ustreza isti pritisnjeni tipki.

Da možnost zlorabe podatkov, ki se vnašajo preko tipkovnice, predstavlja dejansko nevarnost, sta s praktičnim preskusom potrdila Vuagnoux in Pasini [v3]. Pri tem sta se osredotočila samo na EM sevanje, ki nastopi ob pritisku tipke in posledičnem prenosu podatkovne sekvence do delovne postaje. V preskus sta vključila 12 tipkovnic z različnimi zasnovami, in sicer tako PS/2, USB kakor tudi brezžične ter integrirane tipkovnice prenosnikov. Potrdila sta, da je zloraba podatkov možna pri vseh modelih tipkovnic, razlikujejo pa se razdalje, iz katerih je mogoče zagotoviti pravilno rekonstrukcijo.

Avtorja sta prikazala več različnih tehnik zajema, na podlagi katerih je mogoče prestreči signal:
– *Falling Edge Transition Technique (FETT),*
– *Generalized Transition Technique (GTT),*
– *Modulation Technique (MT),*
– *Matrix Scan Technique (MST)*.

Izkazalo se je, da je s prvimi tremi tehnikami večinoma mogoče prestreči signal s tipkovnic, ki uporabljajo vodilo PS/2, in prenosnih računalnikov, medtem ko je zadnja metoda primerna predvsem za vodilo USB in brezžične tipkovnice. Uspešno izvedbo

testa je pomenila 95-odstotna pravilnost rekonstrukcije sporočila v dolžini 500 znakov.

Za tipkovnice, ki uporabljajo vodilo PS/2, se lahko uporabi vsaj ena od prvih treh tehnik. Te izrabljajo dejstvo, da je emitirani signal kombinacija podatkovnega signala in signala ure. Prva tehnika sloni na rekonstrukciji signala iz kombinacij, ki ustrezajo prehodom signala iz stanja 1 v 0. Druga tehnika kodira stanje vsote amplitude obeh signalov. Tretja tehnika pa izrablja modulacijo signala pri višjih frekvencah (pogojenih s frekvenco interne ure mikrokontrolerja tipkovnice), iz katerih se rekonstruirata podatkovni signal in signal ure.

Zaradi nižje stopnje emisij podatkovnega vodila USB se lahko signal tipkovnic, ki uporabljajo to vodilo, rekonstruira posredno preko emisij krmilnika na podlagi merjenja zamika v njegovem delovanju. Večina tipkovnic zazna pritisk tipke, če je ta pritisnjena 10 ms, kar pomeni, da mora biti znotraj tega intervala zaznan pritisk katere koli tipke ali kombinacije. Iz navedenega izhaja, da se mora pregled stanja posameznih tipk izvajati pri visoki frekvenci. Poenostavitev se lahko doseže z razvrstitvijo tipk v matriko. Krmilnik tipkovnice v zaporedju prebira signal, ki ustreza posameznim stolpcem matrike. Ker tipkovnice večinoma uporabljajo 8-bitne krmilnike, imajo matrike tipkovnic večinoma 8 vrstic, matrika pa predstavlja 192 tipk, od katerih so nekatera mesta nezasedena (običajne tipkovnice imajo okrog 105 tipk). Krmilnik v zaporedju pregleduje posamezne stolpce tipkovnice in ko ugotovi, da je v stolpcu pritisnjena tipka, sproži prenosno rutino, ki ustreza pritisnjeni tipki. Tehnika MST izrablja lastnost, da zagon rutine za prenos za nekaj časa zamakne branje naslednjega stolpca. Podatek o pritisnjeni tipki se posledično razbere iz stolpca, pri katerem je nastopila zakasnitev.

Pri brezžičnih tipkovnicah zajem signala ne predstavlja težave, možnost rekonstrukcije podatkov pa je odvisna od metode kodiranja. Zasnova *wireless* USB omogoča visoko stopnjo zaščite pred prestrezanjem [WUSB]. Ne glede na to je tudi vnose pri brezžičnih tipkovnicah mogoče prestreči na podlagi emisij krmilnika oziroma metode MST. Podobno velja za tipkovnice prenosnih računalnikov, kjer se je izkazalo, da sta poleg MST lahko učinkoviti tudi metodi FETT in GTT.

Različne tehnike zajema so različno učinkovite v odvisnosti od razdalje prestrezanja. Zaradi najvišje frekvence se je za najučinkovitejšo tehniko izkazala MT, na podlagi katere je podatke mogoče prestreči z razdalje okrog 20 m tudi skozi stene. To pa je mogoče le pri tipkovnicah, ki za komunikacijo uporabljajo vodilo PS/2. To je v tem trenutku že povsem zastarelo, saj ga je že popolnoma nadomestilo novejše

zasnovano vodilo USB, ki daje boljšo zaščito. Zato sta avtorja pri USB tipkovnicah vnose rekonstruirala na podlagi sevanja krmilnika z uporabo tehnike MST. Razdalje možnega zajema podatkov pa so v tem primeru bistveno nižje. V realnem okolju na širjenje elektromagnetnega sevanja vplivajo tudi prepreke, kot so na primer stene med prostori in EM motnje v okolici, ki ga oddajajo druge naprave. Minimalno razmerje med signalom in šumom, ki še zagotavlja rekonstrukcijo signala, je 6 dB. Razdalje, pri katerih je zagotovljeno ustrezno razmerje med signalom in šumom, so tako v EM gluhi sobi do 22 m (FETT 10 m do 18 m, GTT 8 m do 15 m, MT od 16 m do 22 m in za MST od 2,5 m do7 m). Zaradi prostorske omejenosti gluhe sobe 7 m x 7 m so bile najvišje teoretične vrednosti preračunane glede na dejansko jakost polja in najnižjo jakost polja, ki še zagotavlja rekonstrukcijo.

Zaradi EM motenj razdalje v običajnem pisarniškem okolju predstavljajo zgolj polovico izmerjenih v EM gluhi sobi. Stene med pisarnami (iz mavca ali lesa) oslabijo razmerje med signalom in šumom še za okrog 3 dB. V realnem okolju so tako najvišje možne razdalje zajema za metode FETT, GTT, MT od 3 m do 10 m in pri MST od 1 m do 3 m. V določeni konkretni situaciji pa lahko nekateri kovinski elementi ali strukture, kot so vodovodne cevi ali vodniki omrežnega napajanja, delujejo kot antene in občutno izboljšajo možnost zajema podatkov. Presenetljivo dobri rezultati prestrezanja signala so bili tako dobljeni med etažami. Najvišja izmerjena razdalja v realnem okolju je predstavljala 20 m [v2]. Slaba zaščita pred EM emisijami je predvsem vpliv optimiziranja stroškov izdelave. Vsekakor nepreverjene tipkovnice niso primerne za vnos občutljivih podatkov. [g2] Dodatno težavo pri izbiri predstavlja tudi dejstvo, da je edini objavljeni podatek glede sevanja zgolj skladnost s standardom CISPR ali FCC, podatka o varnosti pred prisluškovanjem pa razen pri namenski opremi ni mogoče pridobiti.

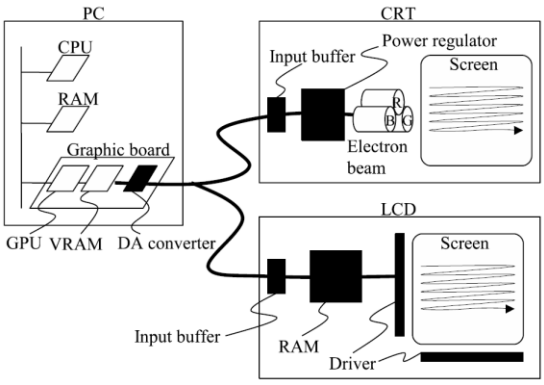
5.1.3 Prestrezanje slike z zaslona

Iz številnih raziskav izhaja, da je v običajnem delovnem okolju glede nenadzorovanega odtekanja podatkov zelo izpostavljen tudi računalniški zaslon. Običajno je ravno zaslon tisti del informacijske opreme, s katerim se obravnava največ občutljivih vsebin. Razvoj tehnologije je sicer nevarnost odtekanja podatkov zmanjšal, vendar je ni odpravil. Po eni strani je to posledica številnih virov emisij, ki jih oddajajo različne komponente sistema, potrebne za prikaz slike. Po drugi strani pa emisije, na podlagi katerih je mogoča rekonstrukcija slike, nastopajo v različnih delih frekvenčnega spektra. Običajno je najučinkovitejša rekonstrukcija slike v UHF območju, kjer obstajajo učinkoviti nizkocenovni antenski sistemi, namenjeni vsakodnevni uporabi pri sprejemu televizijskega signala. Posledično to pomeni, da je

rekonstrukcija slike mogoča že z uporabo nenamenske opreme. Drug kanal, preko katerega je mogoče odtekanje video podatkov, predstavljajo konduktivne emisije v napajalne vode.

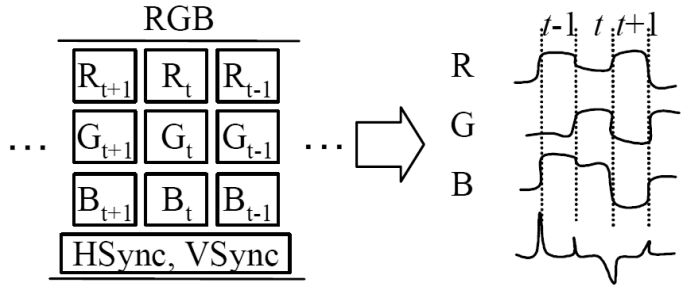
Tehnično osnovo za zajem EM sevanja, ki je povezano s prikazano sliko na zaslonu, lahko v realnem pisarniškem okolju predstavlja širokopasovna antena z ojačevalcem, spominski osciloskop in spektralni analizator. Signal se tako najprej zajame in prenese v računalnik, na katerem se nato demodulira in dekodira. Navedena strojna zasnova pa ni omejena zgolj na EM sevanje, ki je posledica prikaza slike na zaslonu, temveč je primerna tudi za zajem EM sevanja vodila USB, procesorja, trdega diska … Frekvenca vzorčenja osciloskopa mora biti prilagojena frekvenčnemu spektru EM sevanja, hkrati mora spominski osciloskop omogočati shranjevanje vrednosti pri visoki frekvenci. [y1] Naknadna obdelava signala, zajetega s širokopasovno anteno, je uporabna tudi pri nižjih frekvencah, npr. pri zajemu EM sevanja s tipkovnice [g2].

Iz slike 6 izhaja, da je virov EM sevanja, ki nosijo informacijo o prikazani sliki na zaslonu, več in niso omejeni na zasnovo zaslona ali način prenosa slike. [w1]



Slika 6:
Viri EM sevanja ob prikazu slike na zaslonu [w1].

Kakor je razvidno iz slike 7, spremembe stanja posameznega prevodnika povzroči impulzni EM odziv. Oddano EM sevanje v okolici vodila je zato kombinacija (vsota) EM sevanj, ki ustrezajo trem osnovnim barvnim komponentam (RGB: rdeča, zelena in modra). [w2]



Slika 7:
EM sevanje kot posledica kombinacije treh impulznih odzivov na spremembe signalov [w2].

EM sevanje zaslona je v veliki meri odvisno od konkretne opreme in morebitnih zaščitnih ukrepov. Z vidika EM sevanja, ki ga oddaja kabel, sta Fan in He [f1] analizirala diferencialni šum v okolici kabla, s katerim je delovna postaja povezana z zaslonom. Zaradi kontrasta med barvo pisave in ozadja (črno / belo) so posledično spremembe amplitude signalov posameznih barvnih komponent visoke. EM sevanje, ki je neposredna posledica teh sprememb, zato omogoča učinkovito rekonstrukcijo slike predvsem ob prikazu besedila. Pri prikazu bitne grafike je kontrast posameznih detajlov slike manj izrazit. Posledično so manjše tudi spremembe v nivojih signala posameznih barvnih komponent, kar vodi k manjši učinkovitosti rekonstrukcije slike.

Čeprav zasloni s katodno cevjo skoraj niso več v praktični uporabi, jih je treba omeniti zaradi izjemno visokih emisij EM sevanja s podatki o prikazani sliki. Elektromagnetno sevanje v smislu potencialne nevarnosti zlorabe informacij informacijskih sistemov je bilo širši javnosti prvič predstavljeno leta 1985 z opisom metode zajema in rekonstrukcije slike na daljavo ravno na primeru zaslona s katodno cevjo [e1]. Koncept »Van Eck Phreaking« je imenovan po vodji projekta, ki je potekal od leta 1983 v PTT Dr. Neher Laboratories na Nizozemskem. Wim van Eck je opozoril, da je zaradi visoke jakosti emitiranega EM sevanja in frekvenčnega območja več 100 MHZ signal mogoče prestreči na velike razdalje. Pri CRT zaslonih je visoka stopnja sevanja posledica visokih napetosti signala pred vstopom v katodno cev in možnost njegove resonance. Kadar je v resonančni krog vključena tudi napajalna napetost, je signal z zaslona mogoče prestreči tudi z razdalje več kakor 1 kilometer. V nekaterih primerih je bilo mogoče sliko rekonstruirati že z uporabo nekoliko prilagojenega televizijskega sprejemnika, kjer je generator impulzov nadomeščen z nastavljivim horizontalnim in vertikalnim oscilatorjem. Glede na frekvenco valovanja se za zajem uporabijo VHF ali UHF usmerjene antene z ojačevalnikom. Na podlagi slednjega je mogoč prikaz slike zaslona z razdalje nekaj 100 m, medtem ko so pri uporabi bolj sofisticirane sprejemne in dekodirne opreme

lahko sprejemne razdalje še veliko večje. Bistvena ugotovitev, ki jo je izpostavil, pa je dejstvo, da za prestrezanje slike ni potrebna posebna namenska oprema. Zadošča že manjša prilagoditev običajnega televizijskega sprejemnika.

Trenutno še vedno velik delež opreme za prikaz slike uporablja nediferencialni način prenosa video signala. Zaradi splošne razširjenosti in zagotavljanja skladnosti namreč analogni priklop zagotavlja tudi najnovejša oprema. Nediferencialni način prenosa hkrati podpira tudi novejše vodilo DVI v analognem načinu (DVI-A).

Možnost prestrezanja elektromagnetnega sevanja s podatki o prikazani sliki na zaslonu zato ni omejena na analogno tehnologijo prenosa in prikaza. Ranljivi so tudi LCD zasloni delovnih postaj, ki uporabljajo digitalni prenos video signala, in zasloni prenosnih računalnikov. Razdalje, na katere je mogoče prebrati signal, so sicer občutno nižje, saj signal ni tako ojačan kakor pri zaslonih s katodno cevjo, vendar vseeno predstavljajo visoko tveganje pred izgubo zaupnosti podatkov. Kuhn [k5] opisuje metodo zajema niza podatkov z LCD zaslona, ki neposredno ustrezajo posameznim točkam slike na zaslonu. Avtor je predstavil rekonstrukcijo slike z razdalje 10 m v prostorih, ločenih s steno, ki je lahko v primerjavi s sliko, dobljeno iz CRT zaslona, občutno boljše kakovosti.

Rekonstrukcija slike zaslona je poleg izkoriščanja EM sevanja mogoča tudi na podlagi prestrezanja podatkov iz konduktivnih emisij v napajalnih vodih. To sta v raziskavi potrdila tudi Sekiguchi in Seto [s2]. V postopku ugotavljanja EM skladnosti elektronskih naprav se vpliv konduktivnih emisij na napajalne vode izvaja v frekvenčnem območju od 150 hHz do 30 Mhz. Avtorja navedene raziskave sta prikazala možnost rekonstrukcije slike v območju od 50 MHz do 1 GHz. Podobno kot pri EM sevanju je rekonstrukcija slike možna pri različnih frekvencah, vendar ta vpliva na njeno kvaliteto.

5.1.4 Tiskalnik

Poleg zaslona in tipkovnice med periferno opremo IKT, s katero se obravnavajo zaupni dokumenti, spada tudi tiskalnik. Vir emisij, ki so povezane s podatki, so lahko vgrajeni elektronski sestavi, USB in napajalni kabel. Procesor (*Raster Image Processor*) generira signal, ki ponazarja bitno grafiko izpisanega dokumenta. Ta krmili laserski žarek, s katerim se nevtralizira fotosenzitivni naboj na bobnu tiskalnika. Signal lahko v obliki EM sevanja oddajajo linije tiskanih vezij ali pa iz tiskalnika odteka na podlagi konduktivnih emisij. [g3]

5.1.5 Pametne kartice

Za napad na pametne kartice obstaja več razlogov. Namenjene so izvajanju zaupnih operacij, obenem pa so v osnovi zelo preproste naprave. Za razliko od osebnih računalnikov v določenem trenutku tipično izvajajo samo eno operacijo. Nimajo lastnega napajanja in signala ure. Poleg tega so majhnih dimenzij, lastniki jih nosijo s seboj in so lahka tarča žeparjev. [k3]

Napadi preko stranskih kanalov tako predstavljajo največjo grožnjo glede prestrezanja šifrirnega ključa pametne kartice. Napadalec izkorišča prestrezanje zunanjih manifestacij, kot so:

- čas procesiranja posameznih operacij,
- EM sevanje,
- poraba energije.

Na podlagi korelacije navedenih lastnosti z obravnavanimi podatki je mogoče rekonstruirati šifrirne ključe različnih algoritmov, kot so DES, AES, RSA, SEAL ipd. [a1]

Časovni napadi (angl. timing attacks) izkoriščajo lastnost, da je čas izvedbe operacije odvisen od obravnavanih podatkov. Na podlagi natančne analize porabljenega časa posameznih operacij je mogoče razbrati skrito informacijo iz integriranega vezja. [k3]

Največjo nevarnost glede prestrezanje tajnega ključa s pametnih kartic predstavljajo napadi na podlagi analize dinamične porabe energije. Temelj tovrstnih napadov predstavlja dejstvo, da je poraba odvisna od podatkov, ki se obdelujejo, oziroma od signala, ki v določenem segmentu predstavlja tajni ključ. Zaradi polnjenja kapacitivnosti na izhodu CMOS logičnih vrat pri prehodu iz 0 v 1 mora napajalni vir zagotoviti tok, medtem ko je obremenitev pri ostalih prehodih (0 v 0, 1 v 1 in 1 v 0) manjša. [t4]

Še bolj so izpostavljena integrirana vezja, ki uporabljajo kriptografijo z eliptičnimi krivuljami. Zaradi manjše dolžine ključa v primerjavi z RSA je zajem ključa enostavnejši ne glede na samo večjo učinkovitost algoritma. [k1]

Namesto analize porabe energije se lahko tajni ključ rekonstruira tudi na podlagi EM sevanja v bližnjem polju, ki ga pri procesiranju oddaja integrirano vezje na kartici (*simple/differential EM analyses*). Učinkoviti so predvsem v neposredni bližini kartice ali ob odstranitvi zaščite, pri merjenju signala neposredno ob vezju. V nekaterih primerih je ta metoda lahko celo bolj učinkovita kakor pa analiza porabe energije. Na

podlagi prenosa signala preko parazitnih sklopov s prevodniki v bližini pa lahko podatki odtekajo tudi na večje razdalje (5 m). Tako so mogoči tudi neinvazivni napadi brez (začasne) posesti kartice. [k3]

Visoko učinkovitost dosegajo tudi aktivni napadi z injiciranjem napak. Na podlagi napake v izvedbi šifrirnega algoritma lahko napadalec v določenih primerih lažje pridobi tajni ključ kakor pri zgoraj opisanih napadih. Možnost injiciranja so različne:

- spreminjanje napetosti ali frekvence signala ure,
- uporaba kartice izven predpisanega temperaturnega območja,
- svetloba (fotoelektrični efekt): laserski žarek je mogoče usmeriti na izbrano mesto vezja in mu spreminjati valovno dolžino,
- magnetno polje [k2],
- mikrovalovno sevanje [k3].

5.1.6 Škodljiva koda

Procesor pri izvajanju določene programske kode oddaja EM sevanje, preko katerega lahko sporoča določene informacije, ki bi jih lahko na daljavo sprejemali v RF območju, čeprav sistem ne bi bil priključen v omrežje ali povezan s spletom [k9].

Tovrstne napade označuje oznaka TEAPOT, s katero se opisuje proučevanje, raziskovanje in obvladovanje tveganj zaradi namerno povzročenega sevanja informacijskih in komunikacijskih sistemov. [a2]

Z vidika protiukrepov TEMPEST so ti obravnavani s posebno pozornostjo, saj se prav zaradi njihove programsko zasnovane narave lahko generira sevanje z nepričakovanimi karakteristikami. [a2] navaja, da je virus TEMPEST za gospodarsko vohunjenje v nekaterih evropskih državah izkoriščala ameriška obveščevalna služba CIA.

5.1.7 Napadi »NONSTOP«

EM sevanje, ki je posledica obravnave podatkov z opremo IKT, se lahko modulira na signal, ki ga oddajajo naprave, namenjene brezžični komunikaciji. Tveganje, ki ga ti napadi predstavljajo, je tudi razlog, da pri obravnavi tajnih podatkov opremi IKT ne smemo približevati vključenih mobilnih telefonov. Posebna pozornost napadom »NONSTOP« je namenjena v mornarici zaradi številnih brezžičnih komunikacijskih povezav. [a2]

5.2 Prestrezanje podatkov preko drugih lastnosti

Opisani načini zajema za prestrezanje signala izrabljajo električne lastnosti, ki jih oddaja oprema IKT med svojim delovanjem. V nekaterih specifičnih situacijah pa lahko tveganje predstavljajo tudi druge vrste napadov.

5.2.1 Specifični zvočni učinki

Dokaj učinkovita rekonstrukcija besedila, ki se vnaša s tipkovnico, je mogoča tudi na podlagi akustičnega posnetka [a4]. Ta vrsta napada izrablja dejstvo, da pritisk različnih tipk na tipkovnice ustvarja specifičen zvok, na podlagi katerega je mogoče razbrati vnos. Razlike je mogoče identificirati ne glede na to, da človeško uho med različnimi dogodki ne zazna bistvenih razlik.

Razlogi za nastanek specifičnega zvoka vsake tipke so predvsem:

- interakcija zvoka s sosednjimi elementi, kot so druge tipke ali ohišje tipkovnice,
- razlike v izdelavi tipk,
- razlika v legi glede na ohišje, vodi k različnim zvočnim učinkom, podobno kot pri udarcih na različne dele opne bobna.

Oprema za izvedbo takšnega napada je izjemno poceni, saj temelji zgolj na uporabi mikrofona in snemalnika zvoka. Običajni PC mikrofoni so ustrezni za napade do razdalje 1 m, medtem ko se za večje razdalje uporabi parabolični mikrofon. [a4] Ta s parabolični odsevnikom zbira in usmerja odbito zvočno valovanje na sprejemnik podobno kakor pri satelitski anteni. Mikrofon sprejema in ojača zvočni signal pred paraboličnim mikrofonom v ozkem kotu in tako omogoča slišnost z večjih razdalj [a4].

S slednjimi se lahko zajame zvok s tipkovnice tudi do razdalje 17 m ne glede na prisotnost zvočnega šuma. Z analizo zvočnega posnetka se posameznim zvočnim vzorcem priredijo ustrezne ASCII vrednosti in rekonstruira vneseno besedilo. Razlike med posameznimi zvočnimi vzorci enakih modelov tipkovnic se medsebojno le malo razlikujejo. [s1]

S primerjavo možnega besedila z besedami iz slovarja je rekonstrukcija mogoča z 90-odstotno zanesljivostjo pri dolgih besedah in 73-odstotno pri kratkih. To je še eden od razlogov, zaradi katerega pri izbiri gesla ni dopustna izbira besed s pomenom oziroma iz slovarja [b3].

Poleg tega ni omejena zgolj na namizne tipkovnice ali prenosnike, temveč lahko predstavlja nevarnost tudi pri uporabi telefonskih aparatov, mobilnikov, bankomatov ipd. [a4]

Na podoben način kakor pri tipkovnicah je v nekaterih primerih mogoče na podlagi zvočnega posnetka razbrati tudi izpis besedila tiskalnika. Slednje je sicer omejeno zgolj na matrične tiskalnike, saj pri brizgalnih ali laserskih tiskalnikih ni korelacije med oddanim zvokom in tiskano vsebino. Ne glede na zastarelost tovrstne opreme je treba upoštevati, da se v nekaterih okoljih zaradi specifičnega načina izpisa, ki temelji na fizičnem odtisu, takšni tiskalniki še vedno uporabljajo. Tak primer je na primer sočasen izpis dokumenta z indigo kopijami. Podobno kakor pri tipkovnici je v tem primeru na podlagi analize zvočnega posnetka mogoče razbrati tudi natisnjeno besedilo. Avtorji navajajo do 72-odstotno uspešnost rekonstrukcije besedila, ob znanem kontekstu izpisanega besedila pa tudi do 95-odstotno, vendar le v primerih, ko je mikrofon v neposredni bližini tiskalnika. Ker se pri večji oddaljenosti učinkovitost metode hitro zmanjšuje, je stopnja tveganja tovrstnih napadov zanemarljiva, kar ponazarja tudi podatek, da je v razdalji 2 m od tiskalnika mogoče razbrati le še 6 odstotkov tiskane vsebine [b1].

5.2.2 Optični napadi

Prestrezanje slike zaslona na daljavo je mogoče pri neposrednem pogledu na zaslon ali preko odboja slike od različnih predmetov, ki so v bližini ekrana [d2, b2].

Možnost izvedbe tovrstnih t. i. optičnih napadov je sicer omejena in odvisna od konkretne situacije, vendar je v nekaterih primerih njihova izvedba vseeno mogoča, na primer:

- neposredna linija pogleda na ekran skozi okno (iz stavb na drugi strani ulice, vozila na ulici …),
- neposredna linija pogleda na objekt, na katerem je dobra odbojna slika skozi okno (iz stavb na drugi strani ulice, vozila na ulici …),
- vnaprej pripravljena skrita oprema v določenem prostoru.

Razdalje, iz katerih lahko zajamemo sliko pri neposredni liniji pogleda na zaslon, so lahko zelo velike [k6]. Iz Rayleighovega kriterija izhaja, da je z uporabo teleskopa s premerom vhodne leče 300 mm sliko z ekrana mogoče zajeti z razdalje več kakor 60 m:

$\Theta = 1{,}22*\lambda / D$, $\Theta = (r / d) * \cos \alpha$

$d = D * r * \cos \alpha / (1{,}22 * \lambda)$

Ob predpostavki:
valovna dolžine svetlobe $\lambda = 500$ nm,
kot opazovanja 60^o,
velikost točke na zaslonu (Full HD, diagonala 24", število točk: 1920 x 1080, razmerje slike 16 : 9):

$r = \sqrt{(256/337)} * d / nx = \sqrt{(256/337)} * 24 * 2{,}54 / 1920$ cm = 0,277 mm

Za navedene vrednosti je razdalja opazovanja: d = 68 m.

Če ni neposrednega pogleda na zaslon, se lahko uporabi možnost odboja slike od predmetov v prostoru, ki so v neposredni bližini. Rekonstrukcija je tako mogoča preko odseva na predmetih, kot so kozarci, jedilni pribor, očala, plastenke ali zenice uporabnika delovne postaje. Tovrstni napadi so še posebno zanimivi, ker se pred njimi težko zavarujemo ali pa jim ne posvečamo dovolj velike pozornosti.

Avtor je s praktičnimi primeri prikazal, da v običajnem delovnem okolju obstaja cela vrsta predmetov, ki omogočajo zelo dober odboj slike. Navaja nekaj primerov rekonstrukcije preko odboja slike od površine:

- čajnika na 10 m,
- očal, kozarca, plastenke in žlice (z notranje in zunanje strani) na 5 m.

Rekonstrukcija slike zaslona iz predmeta v prostoru se lahko v praksi izvede z razdalje 10 m z uporabo običajne opreme (zrcalnorefleksni fotoaparat z 10 MP in senzorja 22,2 mm × 14,8 mm ter teleskop s premerom vhodne leče 235 mm). Z uporabo dodatnih optičnih komponent je možna rekonstrukcija do razdalje 20 m.

Navedene vrednosti ustrezajo pogojem v notranjosti prostora, kar pomeni, da sta zaslon in oprema za zajem v istem prostoru. Tovrstni napadi pa so mogoči tudi iz okolice objekta, pri čemer na kakovost reprodukcije slike vplivajo naslednji dejavniki:

- zajem odboja skozi okensko steklo lahko doda šum ali dodatne odboje,
- ogrevanje povzroča kroženje zraka in posledično znižanje kakovosti slike,
- dež, veter …

Vpliv teh dejavnikov v povprečju vodi k polovični resoluciji rekonstruirane slike glede na idealne pogoje v notranjosti.

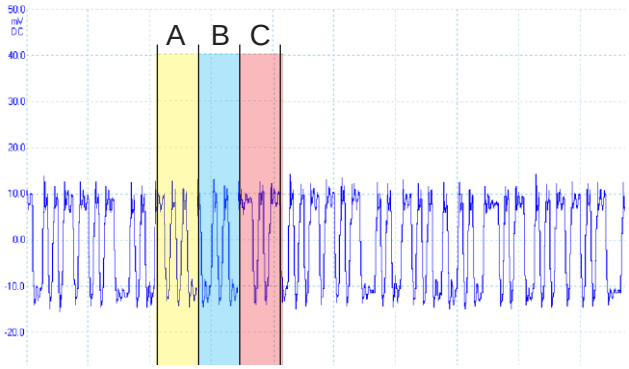
Tveganje, ki ga predstavlja prestrezanje slike preko odboja z zenice očesa, je zaradi številnih omejitev bolj teoretično. Zaradi majhne dimenzije zenice, ki ima v povprečju premer le 7,8 mm, so potrebne visoke povečave slike. To posledično pomeni majhno količino svetlobe, ki je na voljo pri opazovanju, in daljši čas osvetlitve tipala. Daljši intervali odprte zaslonke kamere hkrati niso mogoči zaradi stalnega premikanja očesa, saj bi to zameglilo sliko. Da bi se odpravila zameglitev in izboljšala ostrina, se zato slika obdela z ustreznimi algoritmi. Zrcalnorefleksna kamera zato ni primerna za tovrstni zajem in je namesto nje bolj učinkovita uporaba kamere z višjo svetlobno občutljivostjo, kakršna je na primer astronomska monokromatska kamera v kombinaciji s teleskopom.

6 PRAKTIČNI PRIMERI IZVEDBE PRESTREZANJA PODATKOV

6.1 Rekonstrukcija podatkov

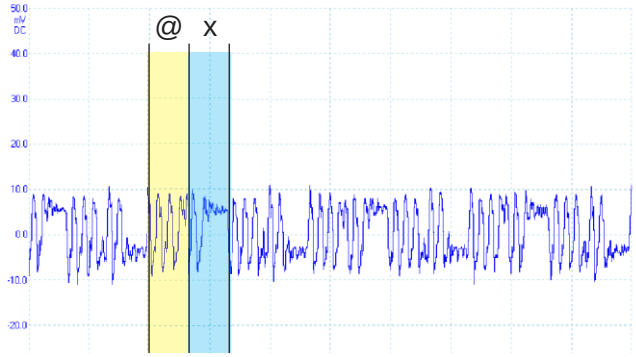
Večinoma se podatki z opremo IKT obdelujejo v nešifrirani obliki. Običajno tako poteka tudi komunikacija med delovno postajo in perifernimi enotami. Zato je v primerih, ko napadalec uspe prestreči EM sevanje ali konduktivne emisije, ki so povezane s podatki, rekonstrukcija večinoma enostavna. Sliki 8 *a* in 8 *b* prikazujeta segment prenosne sekvence signala vodila USB pri zapisovanju datoteke s ponavljajočo se vsebino na USB pomnilniški medij (*flash disk*). Iz prikazanega primera je razvidno, da posamezni bajti pri prenosu neposredno ustrezajo podatkom, ki se na medij zapisujejo.

Prenos podatkov v skladu s protokolom USB poteka z uporabo kodiranja NRZI, pri katerem prehodi med stanji predstavljajo logično ničlo, zadržanje stanja pa logično »1«. Na podlagi analize prenosne sekvence je tako mogoča enostavna rekonstrukcija podatkov.



SEKVENCA	10000010010000101100001010000010010000101100001 0
A	10000010 10000010
B	01000010 01000010
C	11000010 11000010

Slika 8 a:
Segment podatkovne sekvence pri komunikaciji z USB pomnilniškim medijem (sekvenca »ABC«, datotečni sistem: FAT32).



SEKVENCA	00000010000111100000001000011110
@	00000010 00000010
X	00011110 00011110

Slika 8 b:
Segment podatkovne sekvence pri komunikaciji z USB pomnilniškim medijem (sekvenca »@x, datotečni sistem: NTFS).

Pri zaslonih, tiskalnikih in izmenjavi podatkov s pomnilniškimi mediji je frekvenca prenosa višja, zato je treba obdelati večjo količino podatkov. Sprejemni sistem mora biti sposoben zajeti signal, ločiti koristno informacijo od šuma in shraniti veliko količino podatkov v realnem času.

Za sprejem signala preko EM valovanja se uporabi antena z ojačevalnikom in filtrom, ki je prilagojena frekvenčnemu območju signala. Zmogljivi antenski sistemi z možnostjo ojačitve nizkih vrednosti EM polja so dostopni večinoma za vsa območja radiofrekvenčnega spektra. Tako lahko v določenih primerih signal učinkovito zajamemo z uporabo navadne žice ali s televizijsko VHF ali UHF anteno z ojačevalcem.

6.2 Praktičen preskus prestrezanja podatkov s tipkovnice

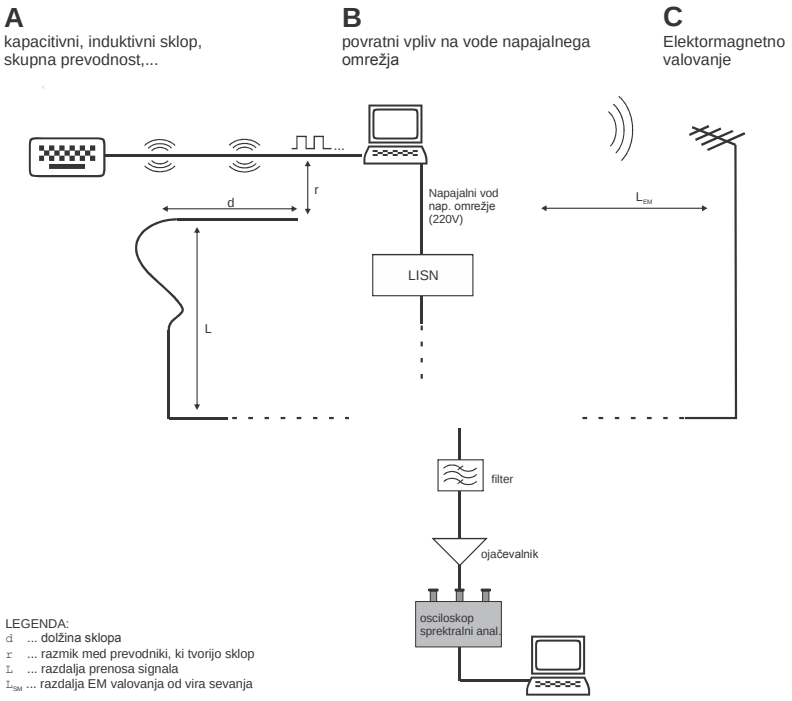
V strokovni literaturi so opisani številni primeri, ki prikazujejo nevarnost napadov TEMPEST na različne komponente komunikacijske in informacijske opreme. Med njimi sta izpostavljena predvsem zaslon in tipkovnica kot ključni del opreme, s katero se obravnavajo občutljivi podatki. Tudi novejši viri se pri opisu možnosti izvedbe napadov TEMPEST na tipkovnico osredotočajo predvsem na že zastarelo vodilo PS/2, pri brezžičnih in USB tipkovnicah pa na prestrezanje emisij krmilnika, ki pa ne omogoča takšnih možnosti za rekonstrukcijo. Že sama zasnova vodila USB namreč daje relativno visoko stopnjo zaščite pred odtekanjem podatkov. Zdaj so v običajni osebni in poslovni uporabi večinoma samo še tipkovnice, ki podatke prenašajo brezžično ali pa prenos poteka po vodilu USB. Tipkovnice PS/2, ki so bile izjemno

razširjene pred leti, so večinoma na voljo le še kot nizkocenovne alternative. Ker za obravnavo tajnih podatkov brezžične tipkovnice zaradi oddajanja EM sevanja niso primerne navkljub šifriranemu prenosu podatkov, sem se osredotočil na tiste, ki uporabljajo vodilo USB. S praktičnim preskusom sem zato želel preveriti, kakšne so emisije in morebitna tveganja, ki smo jim izpostavljeni pri njihovi uporabi.

Izkazalo se je, da ima velik delež tipkovnic, ki so na voljo na trgu, pomanjkljivo izvedene ukrepe in priporočila, predpisana s specifikacijami USB. Uporaba takšnih tipkovnic lahko v nekaterih primerih dejansko predstavlja določeno stopnjo tveganja glede prestrezanja emisij. Če pri tem upoštevamo še emisije krmilnika, je stopnja tveganja glede izgube zaupnosti podatkov, ki ga predstavlja njihova uporaba, še večja.

Nizke frekvence, pri katerih poteka komunikacija USB tipkovnice z delovno postajo, ne omogočajo učinkovitega zajema EM valovanja v frekvenčnem območju prenosa podatkov. Tipkovnice, ki sem jih preskusil, so podatke prenašale s hitrostjo, ki je ustrezala predpisani 1,5 Mbps, in sicer od 1435 kbps do 1533 kbps. Da bi kabel tipkovnice pri prenosu deloval kot učinkovita oddajna antena, bi morala biti njegova dolžina usklajena z valovno dolžine valovanja, kar pomeni, da bi moral biti kabel dolg več sto metrov. Analogno velja za oddaljenost, pri kateri se konča bližnje polje in se okrog vira sevanja v okolico začne širiti EM sevanje ($d = \lambda/2\pi$). Zaradi medsebojnega kompenziranja vpliva vodnikov in upada jakosti polja z razdaljo zato zajem signala preko neposrednega EM sevanja ne predstavlja visokega tveganja.

Zato sem se pri preskusu osredotočil predvsem na možnost odtekanja podatkov preko prevodne infrastrukture v bližini tipkovnice. Obravnavani in merilni sistem sem medsebojno popolnoma izoliral, tako da sta oba delovala na lastno baterijsko napajanje brez fizičnega stika in brez povezave z napajalnim omrežjem. Prestreženi signal sem zajel z digitalnim spominskim osciloskopom in na podlagi tako zajetih podatkov rekonstruiral kodo, ki ustreza pritisnjeni tipki.



Slika 9:
Prestrezanje podatkov z uporabo osciloskopa – zajem signala s prevodne infrastrukture (levo), vodov napajalnega omrežja z LISN (sredina) in oddanega EM valovanja z anteno (desno).

Na sliki 9 so prikazane možnosti prestrezanja in rekonstrukcije podatkov na podlagi:

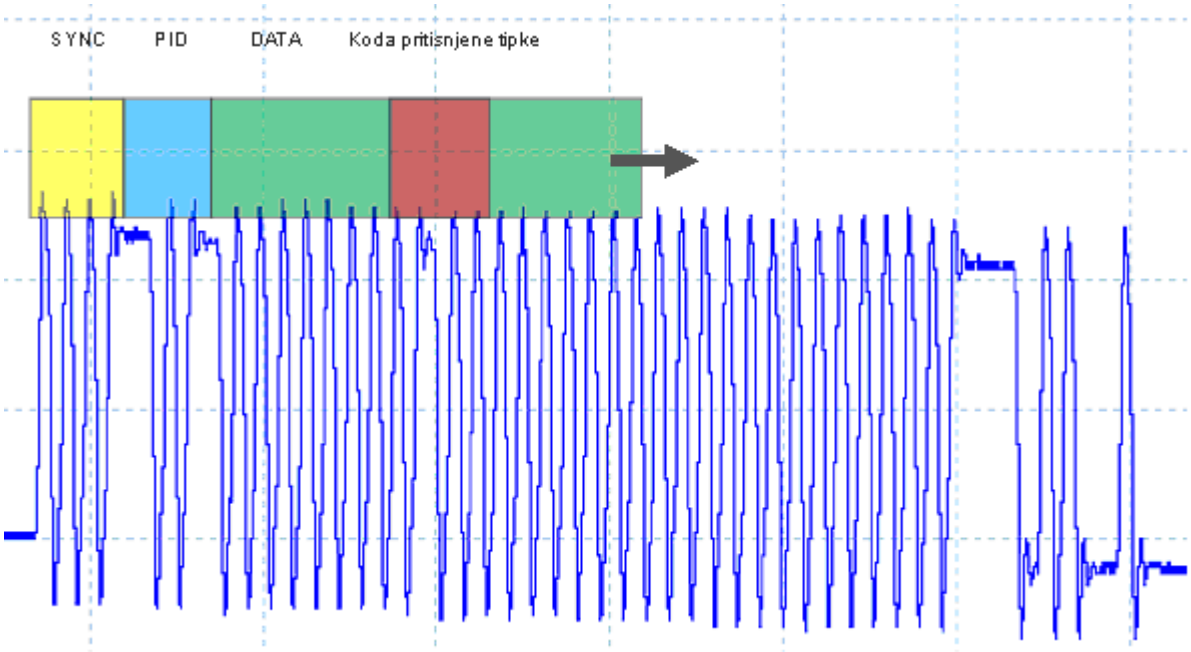
- obstoja medsebojne kapacitivnosti, induktivnosti in prevodnosti (A),
- povratnih konduktivnih emisij v napajalne vode in
- elektromagnetnih emisij.

Ne glede na vrsto emisij je za njihov zajem mogoče uporabiti digitalni spominski osciloskop. V realnem delovnem okolju se EM motnje iz okolice pred ojačanjem signala ustrezno filtrirajo na frekvenčno območje signala.

V konkretnih primerih sem se osredotočil na nevarnost, ki jo lahko predstavlja prenos signala med podatkovnim vodnikom tipkovnice (periferne enote USB) in prevodno infrastrukturo, ki je v bližini (slika 9 – primer A). Z izbiro parametrov sem želel ponazoriti, da smo pri uporabi običajne informacijske opreme lahko izpostavljeni tveganju nenadzorovanega odtekanja obravnavanih podatkov preko prevodne infrastrukture v okolici delovne postaje, perifernih enot in medsebojnih podatkovnih povezav. Zato se vsi primeri nanašajo na zajem signala s prevodnika – žice, ki ponazarja del napajalnega ali podatkovnega omrežja.

Podatki o meritvah in opremi, ki je bila uporabljena pri prikazu zajema podatkovnih sekvenc prenosa naprav USB (glede na sliko 9):

- digitalni spominski USB osciloskop Picotech,
- prenosnik Lenovo ThinkPad T500,
- preizkušena oprema: 7 aktualnih modelov tipkovnic različnih proizvajalcev (vse nabavljene v letu 2011), miške USB;
- dolžina sklopa (d): 60 cm;
- prevodnik za zajem signala:
  - izolirana žica debeline AWG24 – UTP kabel ali
  - izolirana žica debeline 0,75 mm – napajalno omrežje;
- razmik med prevodniki, ki tvorijo sklop (r): od 2 cm do 25 cm;
- dolžina prevodnika, po katerem se prenaša signal – od vira sevanja ali mesta sklopa (L): od 1 m do 10 m;
- meritve sem izvedel v območju z majhnim vplivom EM šuma okolice brez filtriranja signala ter vsaj 5 m od drugih elektronskih naprav, komunikacijskih povezav in vodnikov napajalnega omrežja.



Slika 10:
Prenos podatkovne sekvence po vodilu USB, ki je posledica pritiska tipke na tipkovnici (Logitech K120).

Prenos podatkov s tipkovnice poteka na podlagi prekinitvenega načina prenosa (angl. interrupt transfer), ki ga uporabljajo naprave, ki redko pošiljajo ali sprejemajo majhne količine podatkov, vendar zahtevajo hiter odziv. Pri tem se garantira čas, v katerem so podatki posredovani, in ob neuspešnem prenosu ponovitev prenosa v naslednji periodi. Poleg tipkovnice predstavlja tipičen primer tudi računalniška miška.

Slika 10 ponazarja prenos podatkovnega paketa po vodilu USB, ki se sproži ob pritisku tipke na tipkovnici in nosi informacijo o pritisnjeni tipki. Prenos podatkov se v skladu s protokolom USB začne s sinhronizacijskim segmentom, ki mu sledi podatkovni paket. Tega sestavljajo identifikator, podatkovno polje in CRC kontrolni zapis. Sinhronizacijskemu polju (SYNC) sledi dvakrat zapisan 4-bitni identifikator (PID), prvič v običajni in drugič v invertirani obliki, kar predstavlja skupno dolžino identifikatorja 1 byte.

Polje SYNC je tako določeno s sekvenco NRZI: KJKJKJKK. Sinhronizacijsko polje ni del podatkovnega paketa in služi zgolj uskladitvi prenosa s signalom ure.

Sinhronizacijskemu polju sledi sekvenca NRZI, ki določa identifikator polja, s katerim je določena vrsta podatkovnega paketa, in ustreza vrednosti »00111100«, kar predstavlja dvakrat zapisano vrednost »0011«, tj. v običajni in invertirani obliki. Navedeni identifikator označuje podatkovno polje vrste »DATA0«.

Sledi podatkovno polje, v katerem je vsebina paketa, ki se prenaša in v konkretnem primeru nosi informacijo o pritisnjeni tipki. Specifikacija »Universal Serial Bus HID Usage Tables« [HID] določa kode posameznih tipk na tipkovnic, ki jih mora podpirati vsaka tipkovnica, izdelana po standardu USB. Iz konkretnega primera se lahko razbere, da vsebina prenesenega paketa »00000100« ustreza vrednosti 4. Iz specifikacije (preglednice 12) izhaja, da ta koda ustreza dogodku, ki označuje pritisk tipke »A« na tipkovnici. Kode, ki označujejo dogodke večinoma neodvisne od vrste sistema in so tako enake za PC ali Mac. Nad sekvenco podatkovnega polja je izračunana tudi vrednost kontrolnega polja (CRC), ki pa je izračunana samo nad podatkovnim delom prenesene sekvence, saj ima identifikator PID ločeno kontrolo (ponovljeno invertirano polje).

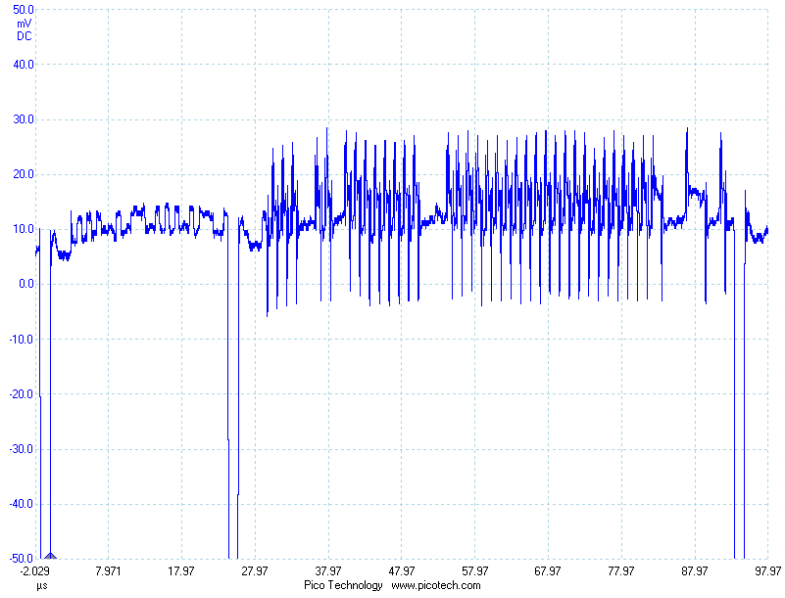
Iz slik 12 do 14 je razvidno, da je razlika v zapisu dogodkov, ki so posledica pritisnjenih tipk na tipkovnici, predvsem v zelo ozkem delu podatkovne sekvence oziroma v enem bajtu.

Ob spremembah napetosti v prepletenih vodnikih, ki niso protifazne, se pojavijo porasti v EM emisijah, ki pa ne izražajo podatkov, ki se prenašajo po vodniku. V trenutkih nenadnih porastov električnega polja se namreč signal spreminja samo v enem prevodniku. Primer takšnega prehoda napetosti v vodnikih predstavlja signal za konec podatkovnega paketa, ki ga označuje stanje na vodnikih SE0 (*single-ended* 0) v trajanju prenosa 2 bitov. Na podlagi teh impulzov je mogoče razbrati informacijo o nastopu dogodka, ki sproži prenos. Emisije, ki neposredno izražajo prenos

podatkov, so tako v bližini kabla, pri slabo zaščitenih tipkovnicah okrog 20-krat nižje jakosti. Ta značilnost olajša zajem podatkovnega paketa, saj lahko z njimi prožimo zajem podatkov na osciloskopu. Tako podatkovno sekvenco dejansko zajamemo samo ob pritisku tipke in ne ob drugih dogodkih, za rekonstrukcijo pa ni treba obdelati velike količine podatkov.

Primer podatkovne sekvence, ki se prenese ob pritisku tipke, je razviden iz slike 12. Ključni del podatkovne sekvence, ki nosi informacijo o kodi tipke in se prenese med tipkovnico in delovno postajo, je ponazorjen v spodnji tabeli. Iz slike, ki je bila zajeta z osciloskopom, je razviden nastop navedenega segmenta približno 50 µs po trenutku proženja. Koda ali »usage ID« 31, ki jo v binarni obliki zapišemo kot 00011111, ustreza pritisku tipke »2«.

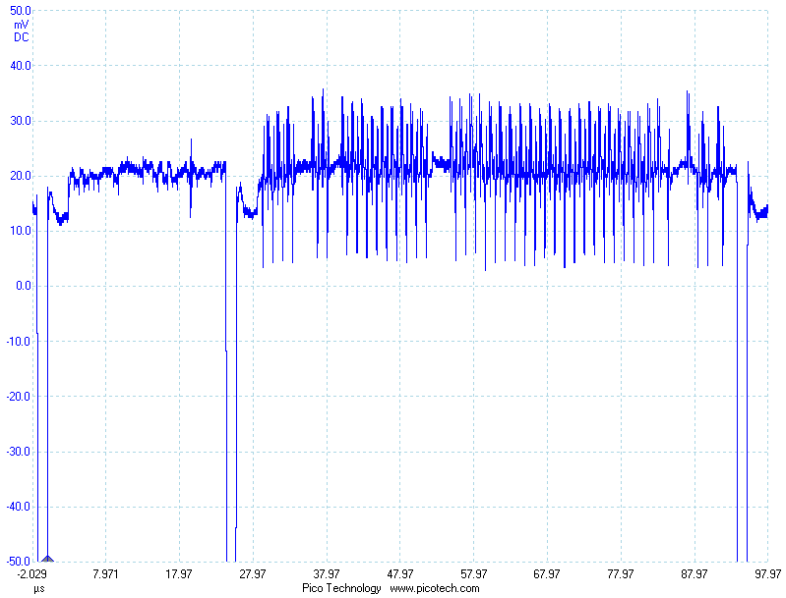
			(lsb)							(msb)			
…	…	…	1	2	4	8	16	32	64	128	…	…	…
0	0	0	1	1	1	1	1	0	0	0	0	0	0



Slika 12: Podatkovna sekvenca, ki ponazarja dogodek pritiska tipke »2«.

Iz medsebojne primerjave različnih podatkovnih sekvenc se enostavno opazi razlika v podatkih, ki identificirajo pritisnjeno tipko. Na naslednji sliki je prikazana podatkovna sekvenca, ki ustreza pritisku tipke »F3«.

			(lsb)							(msb)			
…	…	…	1	2	4	8	16	32	64	128	…	…	…
0	0	0	0	0	1	1	1	1	0	0	0	0	0



Slika 13: Podatkovna sekvenca, ki ponazarja dogodek pritiska tipke »F3«.

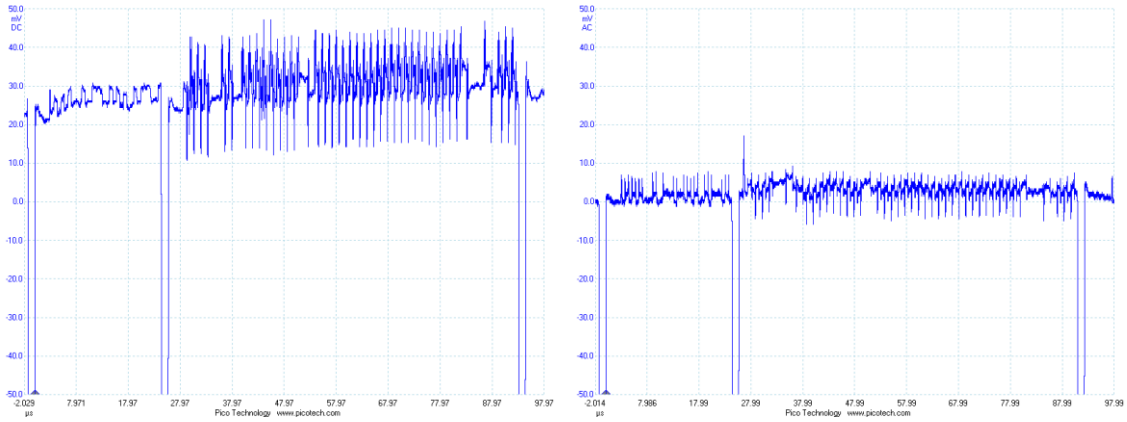
Ker različni modeli tipkovnic USB (tudi različnih proizvajalcev) za komunikacijo uporabljajo isti protokol, so razlike med podatkovnimi sekvencami minimalne. Največje razlike, ki izhajajo iz praktičnega preskusa, so v:

- frekvenci prenosa podatkov,
- stopnji uporabljene zaščite kabla.

Da so razlike v prenosu podatkovnih sekvenc med različnimi modeli tipkovnic oziroma različnimi proizvajalci majhne, je razvidno iz naslednje slike, kjer je prikazana podatkovna sekvenca, ki se prenese ob pritisku tipke »S«.

Pritisnjena tipka: »S«
Usage ID: 22
Prenesena sekvenca:

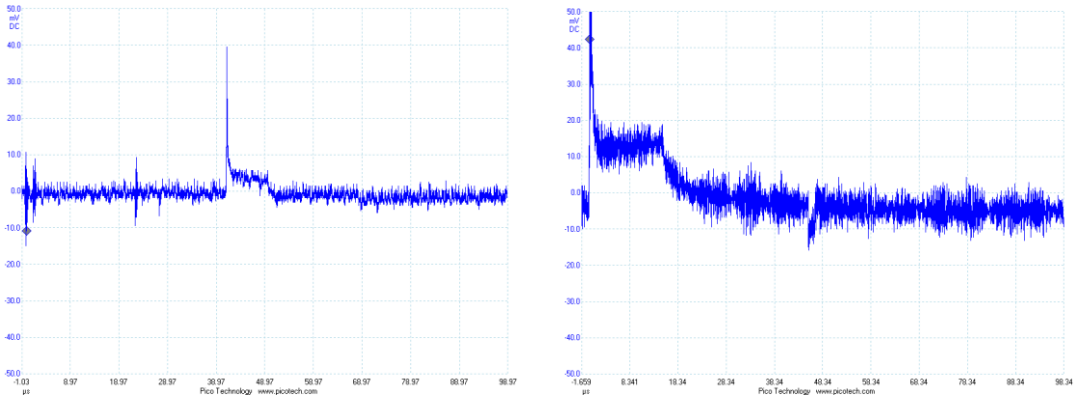
			(lsb)							(msb)			
…	…	…	1	2	4	8	16	32	64	128	…	…	…
0	0	0	0	1	1	0	1	0	0	0	0	0	0



Slika 14:
Razlike v emisijah, ki so posledica pritiska tipke »s« pri različnih modelih tipkovnic.

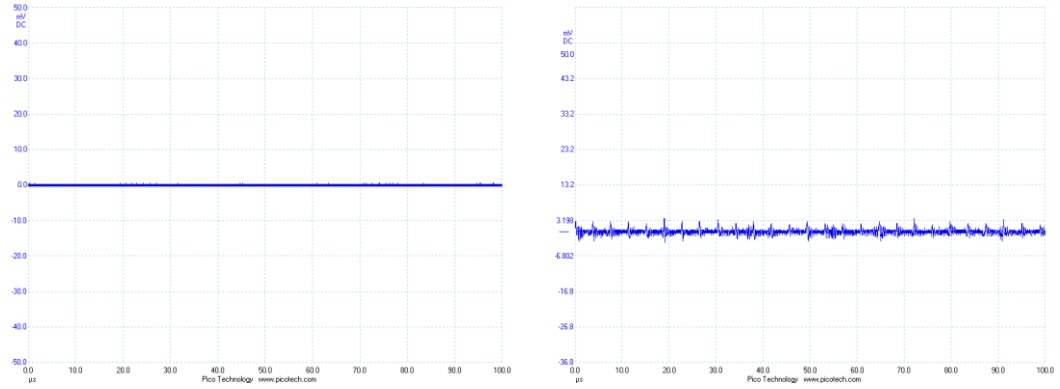
Podatkovne sekvence, ki ustrezajo pritiskom različnih tipk na tipkovnici (slike 12 do 14), se razlikujejo zgolj v zelo omejenem segmentu. V celotni prenosni sekvenci je tako ključen samo en byte, ki nosi informacijo o pritisnjeni tipki. Podatek je še toliko lažje razbrati, ker večji del sekvence sestavljajo vrednosti 0 in zato koda v dolgem monotonem nizu izstopa.

Navkljub relativno visokim emisijam pa pri nekaterih modelih tipkovnic z ustreznejšo izvedbo EMI zaščite te niso povezane z obravnavanimi podatki (slika 15). Emisije so tako zgolj posledica sofaznih sprememb v podatkovnem paru, medtem ko so emisije protifaznih sprememb prenizke za uspešno rekonstrukcijo. V tem kontekstu je treba rezultat upoštevati z vidika uporabljene opreme, kar ne pomeni, da podatkov ne bi bilo mogoče rekonstruirati tudi z uporabo zmogljivejše opreme. Tu je treba poudariti, da z vidika uporabnika ni mogoče pridobiti informacije o zaščiti pred odtekanjem podatkov preko EM emisij. Vsaka naprava ima namreč navedeno le informacijo ali izjavo proizvajalca o izpolnjevanju zahtev glede EM skladnosti. Ta navedba pa zagotavlja samo omejitev emisij znotraj predpisanih meja in ne zagotavlja varnosti pred prestrezanjem podatkov.



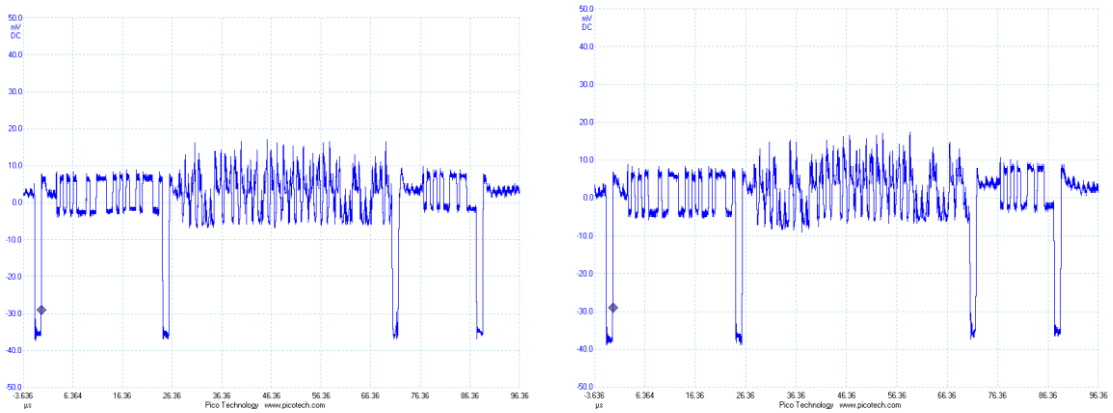
Slika 15:
Emisije USB tipkovnic z ustreznejšo izvedbo zaščite.

Ob enakih merilnih pogojih kakor v zgoraj opisanih primerih sem poskusil prestreči tudi signal z opreme, skladne z najvišjim nivojem zaščite pred EM sevanjem – SDIP 27 Level A. Zaščita se v praksi izkaže za izjemno učinkovito, saj signala ob enakih merilnih pogojih ni bilo mogoče zaznati niti v neposredni bližini kabla.



Slika 16:
Emisije USB SDIP 27 level A tipkovnice (levo) in miške (desno).

Poleg tipkovnice sem preskusil tudi nekatere druge naprave. Za slabo zaščitene so se poleg tipkovnic izkazale predvsem računalniške miške. Zaradi enostavnega nabora različnih sekvenc, ki se posredujejo ob uporabi, je rekonstrukcija podatkov o njihovi uporabi še toliko enostavnejša. Tveganje odtekanja podatkov pri uporabi pa je vseeno minimalno zaradi nizke uporabne vrednosti podatkov. Tudi v tem primeru podatkov z miške, skladne z nivojem zaščite SDIP 27 Level A, ni bilo mogoče zaznati niti v neposredni bližini. V tem primeru gre za miško proizvajalca HP, ki jo je podobno kakor prej opisano tipkovnico predelalo podjetje Eurotempest.

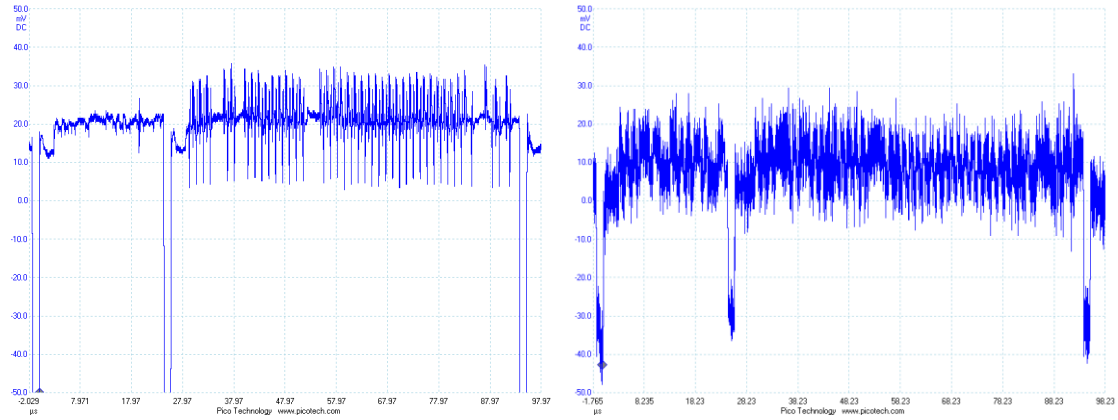


Slika 17:
Podatkovni sekvenci pri uporabi miške USB, ki ustrezata dvema različnima dogodkoma.

Z večjo oddaljenosti od kabla postaja razmik med vodniki D+ in D– v razmerju z razdaljo, ki jo predstavlja točka opazovanja, vse bolj zanemarljiv. Vsota dveh nasprotno usmerjenih polj se tako z večjo oddaljenostjo izničuje. Posledično se povečuje tudi razmerje med odzivom, ki je posledica sofaznih sprememb v primerjavi s protifaznimi. V večji oddaljenosti od kabla so zato neposredne emisije, ki bi bile posledica protifaznih sprememb signala, zanemarljive [s6]. Hkrati se z razdaljo niža tudi medsebojna kapacitivnost in induktivnost med prevodniki, kar slabi prenos signala preko kapacitivnega ali induktivnega sklopa.

Ne glede na to pa se lahko signal na določenem delu prenese na drug prevodnik v bližini in se po njem širi tudi na večje razdalje. Te so odvisne od samega poteka prenosne infrastrukture in možnosti filtriranja signala glede na šum iz okolice. To tveganje obstaja tudi pri uporabi opreme TEMPEST, ki mora biti zato ustrezno umeščena v delovni prostor.

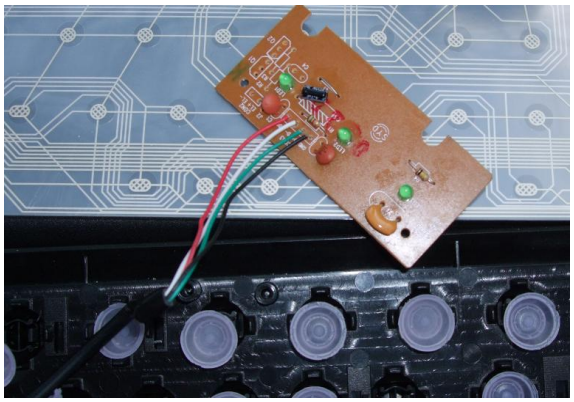
Kadar se signal širi po mediju, kjer je vpliv okolja na prenos majhen, so lahko razdalje prenosa zelo velike. Slika 18 prikazuje prestreženo podatkovno sekvenco s tipkovnice v oddaljenosti 8 m od vira emisij oziroma mesta prenosa signala.



Slika 18:
Primer vpliva motenj na prenos signala po prevodni infrastrukturi na razdalji 1 m (levo) in 8 m (desno).

Razlogi za visok nivo emisij so v neupoštevanju priporočil, ki jih določa specifikacija USB. Kabli naprav, ki uporabljajo nizke frekvence prenosa signala, so lahko brez ustreznega oklopa in ozemljitve. Iz slike 19 je razvidna konstrukcijska slabost, ki zaradi nezadostne zaščite vodi k nenadzorovanim emisijam. V konkretnem primeru je prikazana tipkovnica brez zunanjega oklopa iz bakrene pletenice, aluminijaste zaščitne folije, odvodnega vodnika (»drain wire«) in brez prepletanja vodnikov parice D+ in D–. Zaradi velikega premera kabla, v katerem je podatkovni par zelo razmaknjen, je izničenje polja podatkovnih vodnikov neučinkovito.

Na sliki 20 pa je prikazana ustrezno izvedena zaščita kabla tipkovnice in konektorja, ki je skladna z najvišjo stopnjo zaščite po standardu SDIP 27 – level A. Ob enakih merilnih pogojih emisij v okolici navedene tipkovnice in kabla, na podlagi katerih bi bila mogoča rekonstrukcija podatkov, v praktičnem preskusu nisem zaznal. V osnovi gre za tipkovnico proizvajalca HP (model SK 2885), ki jo je z zaščito pred EM emisijami (oklop, kabel, priključki) predelalo podjetje Eurotempest. Čeprav deluje po protokolu USB, namesto standardnih priključkov uporablja prilagojene DSUB 9 pin. Oprema TEMPEST tako že v izhodišču z uporabo specifične izvedbe priključkov onemogoča priklop in uporabo neustrezne opreme na prenosnikih ali delovnih postajah.

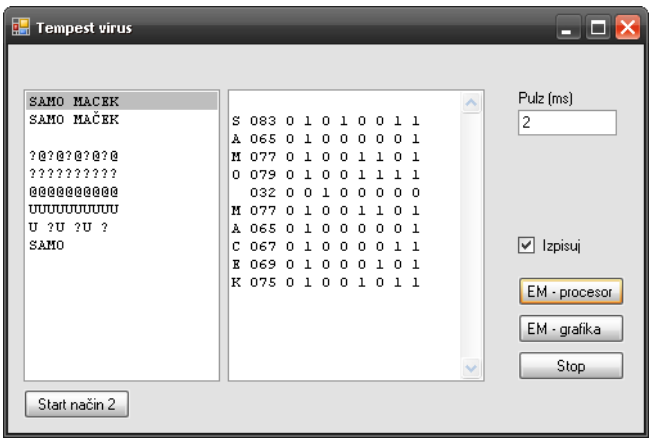


Slika 19:
Nezadostna zaščita USB kabla – ni oklopa, zaščitne folije, odvodnega vodnika, prepletenosti vodnikov parice (Speedlink).

Slika 20:
Močna zaščita USB kabla in konektorja – izvedba v skladu z nivojem zaščite SDIP 27 level A (Eurotempest).

6.3 Virus TEMPEST

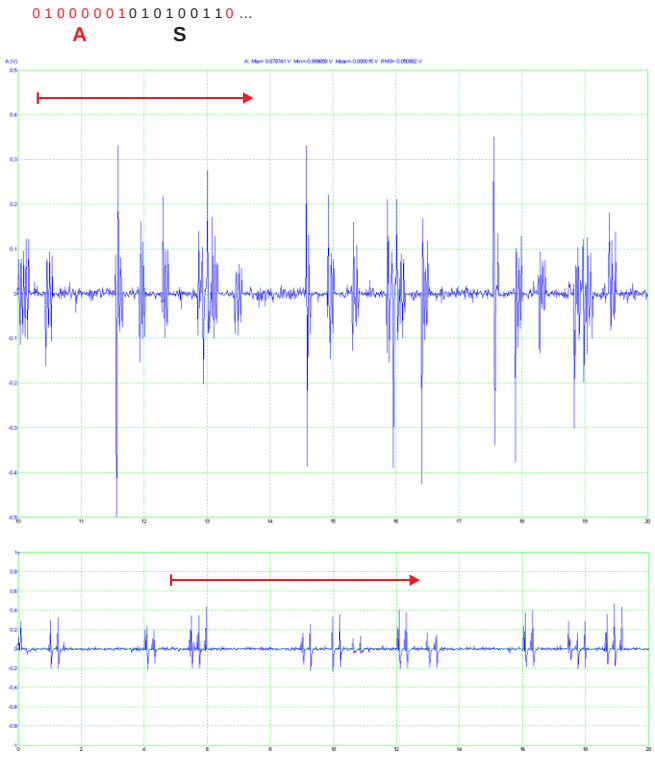
Možnost »oddajanja podatkov« preko EM sevanja, ki je posledica izvajanja specifičnih operacij posameznih komponent sistema, sem preskusil tudi v praksi. S programsko kodo (C#), ki je razvidna iz primera, generiramo EM sevanje v srednjevalovnem RF območju z moduliranim signalom, na podlagi katerega lahko v okolico oddajamo določene podatke. Izvedba funkcije fnoise2 kratkotrajno obremeni eno jedro procesorja, kar ima za posledico impulz v emitiranem EM sevanju. Zanka (dogodek bsend1_CheckedChanged) v zaporedju bere posamezne bite podatkovne sekvence in ob stanju »1« izvede funkcijo fnoise2. Ob stanjih »0« je aplikacija v mirovanju. Na podoben način lahko EM sevanje oddajajo tudi nekatere druge komponente sistema. Izvedba funkcije fnoise3 znotraj iste zanke generira EM sevanje s hitro izmenjavo barve ozadja aplikacije. Ker kovinska ohišja in prepreke, ki jih predstavljajo drugi elementi sistema, sevanje slabijo, je to bolj izrazito pri prenosnikih kakor pri namiznih delovnih postajah.



```
static string besedilo = @"TEST";   // podatki
byte[] c = Encoding.ASCII.GetBytes(besedilo);
byte[] wbin = new byte[8] {128,64,32,16,8,4,2,1};
bool wizpis = false;
int wby = 0, wbi = 0;
double kpulse = 2;  // dolžina impulza v ms (hitrost prenosa)

void fnoise2(double k, bool b)  // obremenitev procesorja
{
    DateTime t0 = DateTime.Now;
    while ((DateTime.Now - t0).TotalMilliseconds < k);
}

void fnoise3(double k, bool b) // izmenjava barvnih vzorcev
{
    DateTime t0 = DateTime.Now;
    while ((DateTime.Now - t0).TotalMilliseconds < k)
    {
        this.BackColor = Color.White;
        this.Refresh();
        this.BackColor = Color.Black;
        this.Refresh();
    }
}

private void bsend1_CheckedChanged(object sender, EventArgs e) // proži bproc1 ali bgraf1
{
    if ((sender as CheckBox).Checked) textBox1.Clear();
    besedilo = listBox1.SelectedItem.ToString();
    c = Encoding.ASCII.GetBytes(besedilo);
    kpulse = Convert.ToDouble(ed_pulse.Text);
    wizpis = cb_izpis.Checked;
    wby = 0;
    wbi = 0;
    bstop.Focus();
    while ((sender as CheckBox).Checked)
        {
            if (wbi == 8)
            {
                wby++;
                wbi = 0;
            }
            if (wby >= c.Length) wby = 0;
            int w = c[wby];
            if ((w & wbin[wbi]) != 0)
            {
                if (sender == bproc1) fnoise2(kpulse, true); // obremenitev procesorja
                if (sender == bgraf1) fnoise3(kpulse, true); // izmenjava barvnih vzorcev
            }
            else System.Threading.Thread.Sleep((int)kpulse);
            if (wizpis) textBox1.Text += ((wbi == 0) ? ("\r\n" + (char)w + " " +
             string.Format("{0:000}", w)) : ("")) + " " + (((w & wbin[wbi]) != 0) ? "1" : "0");
            wbi++;
            Application.DoEvents();
        }

    }
```

Primer 1:
Programska koda za generiranje EM sevanja s podatki.

Emitirane podatke lahko prestrežemo v RF spektru z običajnim radijskim sprejemnikom. Primer EM emisij, ki so posledica izvedbe kode na prenosniku Lenovo ThinkPad T500, je razviden iz slike 21. EM sevanje sem v obeh primerih zajel v srednjevalovnem RF območju, in sicer pri funkciji fnoise2 na frekvenci 800 kHz, pri fnoise3 pa na frekvenci okrog 520 kHz.



Slika 21:
Virus TEMPEST – oddajanje podatkov preko EM sevanja na podlagi izmenjave barvnih vzorcev na zaslonu (zgoraj) in kratkotrajnih obremenitev procesorja (spodaj).

7 VARNOSTNI PROTIUKREPI IN PRIPOROČILA

V prvem delu poglavja navajam nekatere splošne zahteve in priporočila, s katerimi lahko dosežemo nižje stopnje emisij z načrtovanjem električnih vezij, naprav in komunikacijskih vodil, v drugem pa posebne ukrepe za zavarovanje tajnih podatkov. Ti se izvajajo na različnih nivojih in so odvisni od najvišje stopnje tajnosti obravnavanih podatkov.

7.1 Splošne metode in sredstva za zmanjševanje EM sevanja

Učinkovito zmanjšanje nivoja emisij se začne z ustreznim načrtovanjem električnih vezij. Pri obravnavi sevanja, ki je povezano s podatki, je treba posebno pozornost nameniti vsem električnim sestavom, v katerih se obravnavajo podatki. Ker imajo vodniki, po katerih se prenaša digitalni signal, pri visokih frekvencah sevalni značaj, je treba posebno pozornost nameniti ustrezni zaščiti prenosnih poti.

Splošna načela, ki jih je priporočljivo upoštevati pri načrtovanje električnih vezij, so [s3, p3, v1, d1]:

- nižja frekvenca sistemske ure,
- počasnejši prehodi signala,
- manjša površina magnetnih zank na tiskanem vezju,
- namestitev linij signala blizu ozemljitvene površine,
- postavitev identičnih tokokrogov na način, ki medsebojno kompenzira vplive,
- čim večje razdalje med prevodniki, po katerih potekajo signali, in čim krajše sklopne dolžine linij. Linije na nasprotnih straneh se morajo srečevati pravokotno,
- kakovostno napajalno vezje:
  Načrtovanje nizkega nivoja emisij se običajno začne pri napajalnem vezju. Kakršen koli šum na napajalnem ali ozemljitvenem vezju (Vcc, GND) se pozna tudi na izhodih že v samem ohišju. Na slabšem so vezja, ki ležijo blizu vezij, ki preklapljajo,
- dobra izvedba ozemljitve:
  Ozemljitev je ena od osnovnih metod za minimiziranje neželenih šumnih motenj. Primerne metode ozemljitve morajo biti upoštevane pri zasnovi tiskanih vezjih, oklop in zaslonov,
- uporaba zaslonov – ozemljenih kovinskih preprek med virom in sprejemnikom:
  Zaslanjanje je v RF območju učinkovit ukrep, vedeti moramo le, kateri material bomo uporabili. Običajni kovinski materiali zadoščajo za ločitev signalov v

celotnem RF območju, le pri nizkih frekvencah moramo uporabiti posebne materiale,

- zaščita odprtin v ohišju:
  Odprtine v ohišju oddajajo energijo v okolico podobno kot antena. Nekatere odprtine v ohišju so nujno potrebne, zato jih je treba, če je le mogoče, oklopiti. Pri tem lahko uporabimo posebno žično mrežo z majhnimi prezračevalnimi luknjicami ali posebna tesnila.

Največ EMC problemov sevalne narave povzročajo vhodno/izhodni kabli, zato je za prenos signala treba zagotoviti kakovostne prenosne poti. Slednje namreč že zaradi svoje narave delujejo kot oddajne antene. Kakor je razvidno iz praktičnega primera, so problemi tudi posledica nižanja stroškov izdelave na račun neupoštevanja priporočil.

Posebno pozornost je zato treba nameniti zaščitnim ukrepom pri prenosu podatkov po komunikacijskih poteh. Smernice, ki jih pri njihovem načrtovanju upoštevamo, so v splošnem [USB3, USB2, p3, v1, d1]:

- nižje frekvence prenosa,
- diferencialni način prenosa podatkov – vpliv sevanja prevodnikov v paru se medsebojno kompenzira,
  - uporaba kablov z nizko stopnjo asimetrije,
  - usklajena oblika signalov v vodnikih parice,
- počasnejši prehodi med stanji signala,
- uporaba ustreznega premera prevodnikov – nizko razmerje med premerom in medsebojnim razmikom prevodnikov,
- preprečevanje presluha
  - prepletenost parice,
  - večji medsebojni razmik med prevodniki, po katerih potekajo signali, in krajše sklopne dolžine linij,
- uporaba oklopa kablov,
  hitre digitalne signale vodimo iz ohišja po oklopljenih kablih; pri višjih frekvencah uporabimo večkratne oklope,
- ustrezna izvedba ozemljitve oklopa,
  oklopi kablov morajo biti dobro ozemljeni, povezava oklopa na priključek pa kakovostno izvedena (pravilo 360°: oklop je s kovinskim ohišjem priključka povezan tako, da z njim čim bolj pokriva polni kot),
- zaščita in ozemljitev konektorjev,

- vezje, ki generira izhodni signal, moramo postaviti čim bližje izstopne točke – izhodne linije je treba voditi daleč proč od hitrih digitalnih signalov in jih ločiti z ozemljenim zaslonom,
- filtriranje napajalnih kablov,
- filtriranje vhodno-izhodnih kablov z uporabo filtrov, ki ne vplivajo na obliko signala,
- ustrezna dolžina prenosnih linij – večina anten v RF spektru učinkovito seva na 1/4 ali 1/2 valovne dolžine signala. Linije morajo biti zato v primerjavi z valovno dolžino signala čim krajše.

Zaradi visokih frekvenc, pri katerih se prenašajo podatki po vodilu USB ali *Firewire*, in relativno velikih dovoljenih dolžin kabla lahko ta deluje kot oddajna antena, ki v okolico emitira EM valovanje. Ukrepi, s katerimi lahko znižamo jakost emitiranega EM valovanja, so različni. Zaradi diferencialnega načina prenosa podatkov je eden od ključnih dejavnikov, ki jih je treba upoštevati, tudi oblika signala. Za zmanjševanje šuma se pogosto uporabljajo filtri (*choke*), ki se namestijo na kabel, običajno na mestu pred priključkom v delovno postajo. Če niso pravilno načrtovani, ima lahko njihova uporaba v nekaterih primerih povsem nasproten učinek. Popačenje oblike signala lahko povzroči neusklajenost med nasprotnima signaloma v podatkovnih vodnikih parice, kar vodi k porastu sofaznega šuma, ki ga naprava oddaja v okolico. Neustrezna izvedba filtrov ima lahko zato neposreden vpliv na obliko signala in posledične emisije v okolico [y1].

Specifikacija USB predpisuje nekatere ukrepe, s katerimi se minimizira oddana EM emisija v okolico, kot so:

- zunanji oklop kabla – bakrena pletenica,
- notranji oklop kabla – aluminijaste folije (poliestrska folija, metalizirana z nanosom aluminija) z odvodnim vodnikom,
- omejitev časa vzpona in upada impulza,
  - »low speed« (tipkovnica, miška …): čas vzpona in upada mora biti med 75 ns in 300 ns, signal pa mora v tem času doseči območje ciljne vrednosti ± 20 %,
  - »full speed«: čas vzpona in upada mora biti med 4 ns in 20 ns, signal pa mora v tem času doseči območje ciljne vrednosti ± 10 %,
  - high speed – na podlagi meritve pri referenčni obremenitvi linij D+ in D– proti zemlji s 45 Ω.

Zaradi visokih hitrosti prenosa, ki pri USB 3,0 dosegajo 5 Gb/s, specifikacija USB v posebnem poglavju predpisuje smernice, ki jih morajo načrtovalci opreme upoštevati

za zmanjševanje sevanja. Neupoštevanje EMI priporočil pri visokih hitrostih prenosa podatkov lahko vodi k preseganju predpisanih mej za zagotavljanje EM skladnosti.

7.2 Protiukrepi za preprečevanje prestrezanja slike z zaslona

Protiukrepi, s katerimi se omejujejo tveganja nenadzorovanega odtekanja podatkov z zaslona, za zmanjševanje razmerja signal/šum so mogoči [w2]:

- z uporabo namenske opreme, zaščitene pred EM sevanjem in konduktivnimi emisijami,
- z redukcijo jakosti oddanega valovanja – obdelava prikazane slike ali besedila,
- z generiranjem šuma – dodatni izvor šuma se namesti v bližino vira EM sevanja, ki se sinhronizira s frekvenco oddanega valovanja;
- s programskim vsiljevanjem šuma na prikazano sliko ob nezaznavnem vplivu na kakovost prikaza. [w2]

7.2.1 Programske metode

Kakor je bilo že pojasnjeno, je odtekanje podatkov preko EM sevanja pri prikazu slike na zaslonu največje pri prikazu kontrastnih vzorcev, kot je črno besedilo na beli podlagi. Ker so na zaslonu običajno najpomembnejše informacije prikazane v berljivi in ne slikovni obliki, to pomeni, da je najučinkovitejše prav prestrezanje podatkov z občutljivejšo vsebino. Zato je bila leta 1999 razvita metoda prikaza besedila na način, ki znižuje oddane EM emisije in možnost njegove rekonstrukcije [k8, k9]. Ugotovljeno je bilo, da je večina radiofrekvenčne energije, ki jo oddaja zaslon, koncentrirana v zgornjih 30 % frekvenčnega spektra. Prikaz besedila z uporabo t. i. tipografije *soft-tempest* zato odreže zgornjo tretjino frekvenčnega spektra oziroma zmanjša kontrast med besedilom in ozadjem ter tako zniža stopnjo emitiranega EM valovanja. Zaradi slabšega kontrasta je rezultat nekoliko zamegljen prikaz besedila. Tipografija je bila brezplačno na voljo na medmrežju in je bila vključena tudi v različne programske pakete s področja zaščite podatkov. Tako npr. PGP (od verzije 6.0.2) za prikaz besedila uporablja tipografijo »soft tempest font« v modulu »Secure Viewer«.

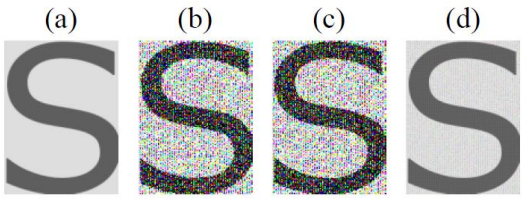
Slika 22:
Tipografija »Soft Tempest«, preprečevanje prestrezanja podatkov iz EM sevanja zaslona (Zero Emission Pad, Freeware, v 2.0, Camridbe University Computer Laboratory).

Z razvojem programske in strojne opreme je tipografija »soft tempest« izgubila na pomenu, kar so na svoji spletni strani objavili tudi avtorji, tako da ni več v praktični uporabi. Ne glede na to so se metode preprečevanja EM emisij na podlagi modifikacije prikaza besedila na zaslonu izpopolnjevale.

Način izpisa z uporabo tipografije *soft tempest* na podlagi Fourijejeve transformacije izloči zgornji del frekvenčnega spektra. Visokofrekvenčni del spektra namreč vodi k visokim konicam v oddanem EM valovanju, ki jih je enostavno mogoče ločiti od šuma v okolici. Uporaba nizkoprepustnega filtriranja sicer možnost zlorabe omeji, vendar se je izkazalo, da v nekaterih primerih ne zagotavlja zadostne zaščite. S kombinacijo Fourijejeve in Gaussove transformacije je mogoče ob hkratnem izboljšanju kontrasta besedila zagotoviti višjo stopnjo zaščite. [t3]

Oko pri izpostavljenosti hitrim spremembam barv ne opazi sprememb, temveč na podlagi t. i. aditivnega mešanja barv zazna samo eno barvo. Metoda, ki izkorišča navedeno lastnost očesa, besedilo prikaže v obliki hitro menjajočih se barvnih vzorcev. Tako se generira očesu skoraj neopazni nivo šuma, ki pa ima izjemno velik vpliv na oddano EM sevanje. Signal, ki ga lahko prestrežemo pri prenosu slike na zaslon, se namreč modificira do te mere, da rekonstrukcija slike na ta način ni več mogoča. [w2]

Namesto originalnega besedila se konstanta barva nadomesti s hitro menjavo dveh nadomestnih vzorcev, ki v skladu z metodo aditivnega mešanja barv generira za človeško oko praktično nespremenjeno sliko (slika 23). [w2]



Slika 23:
Metoda »aditivnega mešanja barv«:
a) izsek originalne slike na ekranu zaslona,
b) in c) menjajoča se vzorca,
d) rezultat hitre menjave barvnih vzorcev, kakor jih zazna človeško oko [w2].

Spremenjen način prikaza slike na ekranu pa navkljub nezaznavnim spremembam v kakovosti slike za človeško oko pomeni bistveno spremembo v oddanem EM sevanju podatkovnega signala slike. Iz slike 24 je razvidno, da rekonstrukcija slike ali besedila iz tako modificiranega EM valovanja ni več mogoča. [w2]

a) Prikaz besedila – slika na zaslonu.

b) Rekonstruirano besedilo na podlagi EM sevanja.

c) Neuspešna rekonstrukcija; protiukrep – aditivno mešanje barv.

Slika 24:
Rekonstrukcija slike brez (b) in s (c) uporabo metode aditivnega mešanja barv [w2].

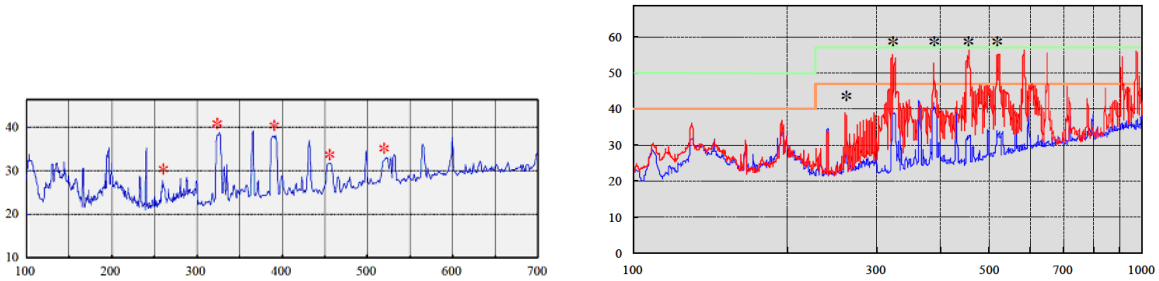
7.2.2 Generatorji motenj

Uporaba generatorjev motenj je lahko učinkovit ukrep zmanjševanja EM emisij, ki je v primerjavi z uporabo namenske opreme cenovno ugoden. Pri praktični uporabi pa je treba upoštevati tudi nekaj omejitev, ki so z njimi povezane. Karakteristike motilnega signala morajo prekriti emisije zaslona v celotnem radiofrekvenčnem območju. Emisije, ki so povezane s podatki s prikazane slike, izstopajo na več mestih frekvenčnega spektra. Zato mora motilni signal:

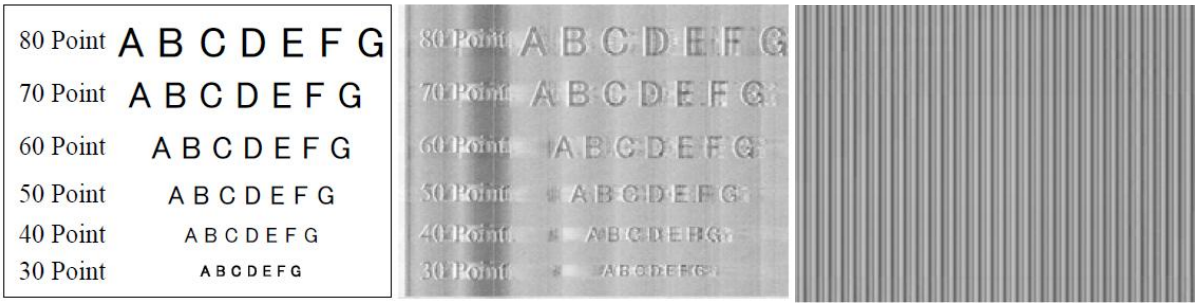
- vsebovati harmonske komponente originalnega signala in
- imeti usklajeno jakost z originalnim signalom.

Pri slabem razmerju med nosilcem in šumom se zajem izboljša s povprečenjem signala. Ta tehnika je ena od glavnih metod, ki se pri napadih TEMPEST uporabljajo

za pridobitev izrazitejšega signala. Generator motenj mora zato oddajati signal, ki bo na slednjo imun. Slabost metode po drugi strani izhaja iz daljšega časa, ki je potreben za obdelavo signala in sposobnosti obdelave večjih količin podatkov. [t2]



Slika 25:
Levo: EM valovanje zaslona, označene so frekvence z ustreznim razmerjem S/N, ki omogoča rekonstrukcijo slike.
Desno: Skupne emisije zaslona in motilnega signala ter mejne vrednosti (FCC) za zagotavljanje EMC, povzeto po [s7].



Slika 26:
Originalna slika na zaslonu, rekonstrukcija na podlagi emisij zaslona, rekonstrukcija na podlagi emisij zaslona in generatorja motenj [s7].

Kakor je razvidno iz slike 25, mora motilni signal prekriti emisije zaslona na mestih, kjer je razmerje med signalom in šumom dovolj ugodno za rekonstrukcijo podatkov. Zaradi specifične oblike signala lahko napadalec namesto originalne slike pridobi le sliko z nespremenljivim vzorcem.

Težavo pri generiranju motilnega signala lahko predstavlja tudi dejstvo, da morajo biti skupne emisije z zaslonom znotraj predpisanih mej EM skladnosti.

Če motilni signal vstopa v sistem kot sofazni šum, celoten sistem deluje kot antena, ki ta signal oddaja na enak način kakor originalni video signal. S tem se zagotovi prekritost originalnih emisij v vseh smereh in ne glede na oddaljenost od delovne postaje. [s7]

7.3 Ukrepi za preprečevanje prestrezanja šifrirnega ključa s pametnih kartic

Protiukrepi so izvedeni na različnih nivojih. Najenostavnejši so generatorji šuma, ki naj bi z naključnim signalom vplivali na dinamično porabo energije. Zapolnitev segmentov, ko sistem ne izvaja šifrirnih algoritmov, maskiranje podatkov, programske prilagoditve algoritma. Najbolj učinkovito pa je načrtovanje enakomerne porabe že z ukrepi na nivoju načrtovanja električnega vezja. [k1]

Prvotno so bili protiukrepi izvedeni z maskiranjem podatkov. Pri tem se pred šifriranjem podatki maskirajo z naključno masko, ki se po obdelavi odstrani, ne da bi to vplivalo na spremembo rezultata. Zaradi vsakokratne izvedbe postopka ob šifriranju pa je njihova učinkovitost omejena. Novejše metode zato namesto kodiranja podatkov slonijo na preprečevanju odtekanja podatkov. [a1]

Napadi na podlagi analize dinamične porabe energije se lahko preprečijo z zagotavljanjem konstantne porabe. To se zagotovi tako, da se pri vsakem urinem ciklu izvede eno polnjenje kapacitivnosti, ter z zasnovo električnega vezja, ki minimizira parazitne vplive med posameznimi komponentami. [t4]

Še naprednejša zasnova vezja uporablja večjedrni procesor. Obe jedri uporabljata skupno uro in šifriranje izvajata sočasno. Medtem ko eno jedro izvaja originalno enkripcijo, drugo jedro izvaja komplementarno. S tem obe jedri učinkovito izničujeta možnost prestrezanja podatkov preko DPA za različne metode šifriranja (DES, AES). [a1]

7.4 Ukrepi v zvezi z obravnavo tajnih podatkov v elektronski obliki

Ukrepi preprečevanja odtekanja podatkov po stranskih kanalih v okoljih, kjer se obravnavajo podatki, ki so v nacionalnem interesu države, se izvajajo na različnih nivojih. Ti skupaj zagotavljajo visoko varnost pred njihovim nepooblaščenim razkritjem, spremembo ali uničenjem.

Zahteve IS za obravnavanje tajnih podatkov

Zavarovanje tajnih podatkov se izvaja z ukrepi in postopki na fizičnem, organizacijskem in tehničnem nivoju. Prilagojeni so najvišji stopnji tajnosti podatkov v sistemu in se nanašajo na same podatke in tudi na ključne komponente sistema za njihovo obravnavanje. S tem se zagotavlja tajnost, celovitost in razpoložljivost podatkov ter celovitost in razpoložljivost samih sistemov.

Fizični in organizacijski ukrepi

Ključne komponente sistema, s katerimi se obravnavajo tajni podatki v nešifrirani obliki, morajo biti postavljene v varnostno območje, ki ga za obravnavano stopnjo tajnosti akreditira Urad Vlade RS za varovanje tajnih podatkov.

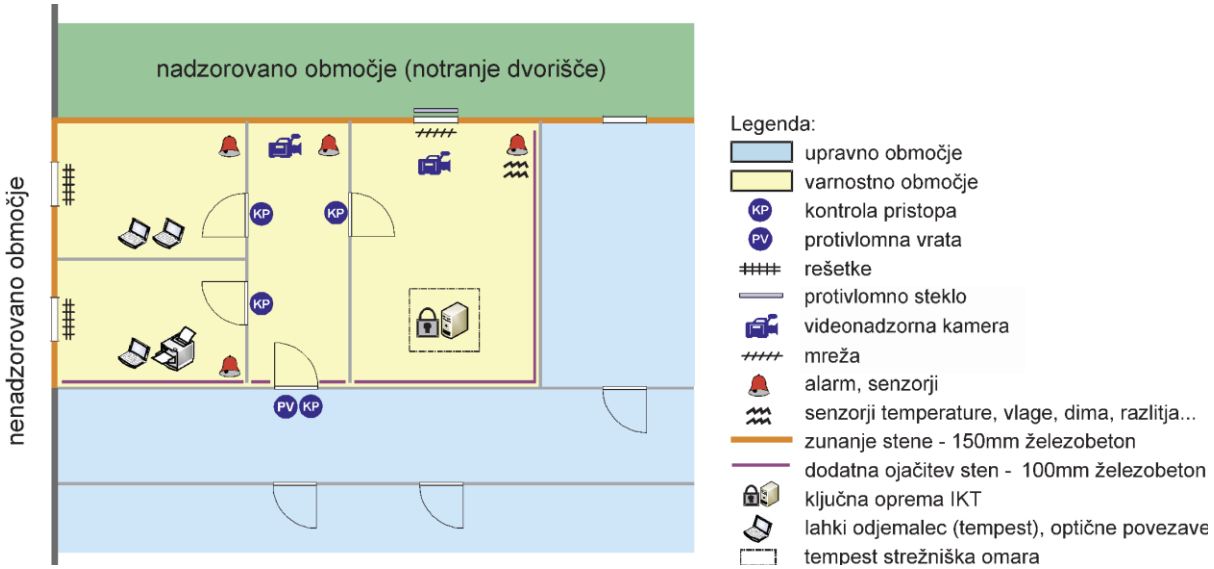
Prenos podatkov v nešifrirani obliki je mogoč izključno po optičnih povezavah v upravnem območju.

Zaščitne ukrepe, ki se nanašajo na prostor – varnostno območje, v katerem se hranijo ključne komponente sistema, predpisuje Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja [SV1].

Za ponazoritev zahtevnosti ukrepov navajam samo nekatere zahteve, ki se nanašajo na izvedbo, prikazano na sliki 27:

- zunanji zidovi morajo biti iz armiranega betona debeline 150 mm ali drugega materiala enake mehanske trdnosti,
- notranji zidovi (ki mejijo na upravno območje) morajo biti iz armiranega betona debeline 100 mm ali drugega materiala enake mehanske trdnosti,
- protivlomna vrata morajo imeti vsaj tritočkovno zapiranje in morajo ustrezati standardu SIST EN 1627 stopnje 4,
- zunanji del protivlomnih vrat se opremi s slepo kljuko in protivlomno zaščito ključavnice,
- z notranje strani oken v pritličju ali kletnih prostorih varnostnega območja se vgradi kovinska zaščitna plošča debeline 2 mm z odprtinami 20 mm, ki preprečuje vnos ali iznos kakršnih koli stvari ali predmetov,
- na okna varnostnega območja, ki mejijo na nenadzorovano površino, se do višine 5,5 m namestijo varnostne rešetke, tako da so vzidane ali pritrjene z notranje strani oken. Izdelane morajo biti iz železnih elementov ali drugega materiala enake mehanske trdnosti premera najmanj 20 mm. Razmik med elementi rešetk ne sme biti večji od 150 mm (ali alternativno s protivlomnim steklom),
- odprtina za zajem zraka se zaščiti z varnostno mrežo, katere odprtine ne smejo biti večje od 200 cm2,
- sistem nadzora gibanja, ki zagotavlja, da osebe vstopajo v varnostno območje samo v spremstvu pooblaščenih oseb ali ob drugi enakovredni obliki nadzora, zagotavlja, da bo oseba vstopila samo v dele območja, povezane z namenom obiska in, če je to potrebno, se bo seznanila le s tistimi tajnimi podatki, ki so povezani z namenom obiska,

– vnos opreme, s katero bi bilo mogoče tajne podatke nepooblaščeno posneti, odnesti ali prenesti, ni dovoljen,
– po končanem delovnem času se varnostno območje varuje s sistemom fizičnega ali protivlomnega varovanja oziroma s fizičnimi nadzorom.



Slika 27:
Primer uvedbe ukrepov fizične in tehnične zaščite pri zaščiti ključnih komponent IS za obravnavanje tajnih podatkov.

Tajni podatki pa se lahko z ustrezno opremo obravnavajo tudi zunaj varnostnega območja v fizično ali tehnično varovanem prostoru, kjer je seznanitev s temi podatki onemogočena nepooblaščenim osebam. Primer takšne uporabe bi lahko predstavljal lahki odjemalec ali lahki kripto odjemalec, ki za svoje delovanje izrablja vire strežnika (brez pomnilniških medijev), skladen s stopnjo zaščite pred oddajanjem neželenih emisij SDIP 27 – level A, z optičnimi omrežnim priključkom. Prijava je mogoča na podlagi pametne kartice, ki se ob možnosti razkritja podatka izvleče, pri tem pa se prekine celotna seja skupaj z začasnimi podatki (prikaz na zaslonu, pomnilniku).

Dovoljenje za dostop do tajnih podatkov

Eden od bistvenih ukrepov glede omejevanja dostopa je dovoljenje za dostop do tajnih podatkov, ki ga izdajo MNZ, Policija, MORS ali SOVA. Dovoljenje se izda samo v primeru, da iz postopka varnostnega preverjanja ne izhajajo varnostni zadržki. To so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo dvomi o zanesljivosti in lojalnosti osebe, ki naj bi dobila dovoljenje. Vrsta preverjanja se določi glede na predvideno potrebno stopnjo tajnosti.

Varnostna odobritev sistema

Pred začetkom obravnavanja tajnih podatkov v sistemu je treba potrditi izvajanje vseh ukrepov in postopkov za zagotovitev varnega delovanja sistema. Za sisteme, v katerih se obravnavajo podatki stopnje tajnosti ZAUPNO ali višje, je predpogoj varnostno dovoljenje, ki ga izda Urad Vlade RS za tajne podatke. Uradu je treba omogočiti varnostni pregled sistema, s katerim preveri izpolnjevanje ukrepov in postopkov za zagotovitev varnega delovanja sistema.

V postopku izdaje varnostnega dovoljenja je treba pripraviti naslednjo dokumentacijo:

- načrt varovanja sistema, ki vsebuje opis sistema, načrt sestavin in povezav sistema, varnostne zahteve sistema, varnostna okolja, varnostne protiukrepe in varnostno upravljanje sistema;
- oceno varnostnih tveganj, ki vsebuje oceno trenutnega stanja sistema z oceno stopnje tveganja;
- varnostna navodila za delo v sistemu, ki vsebujejo varnostno upravljanje in organiziranost varnosti sistema, informacijsko varnost, načrtovanje ukrepov ob nepredvidenih dogodkih, upravljanje in spreminjanje konfiguracije/nastavitev sistema, splošna varnostna navodila za uporabnike in odgovorno osebje.

Identifikacija in overitev dostopa uporabnikov v sistem

Vzpostavitev postopkov identifikacije in overitve dostopa za vse uporabnike sistema v skladu z določili Komisije za informacijsko varnost.

Tehnično-informacijski ukrepi

Povezovanje sistemov

Povezovanje sistemov je dovoljeno le po nadzorovanih in varovanih vstopno-izstopnih točkah, skozi katere potekajo vsi servisi in storitve.
Sistemi stopnje zaupno ali višje ne smejo biti povezani z internetom.
Vse povezave morajo biti izvedene skladno z varnostnimi zahtevami za povezovanje sistemov, ki jih določi Komisija za informacijsko varnost. Prenos podatkov v nešifrirani obliki je mogoč samo po optičnih povezavah v upravnem območju.

Izvajanje zaščite pred neželenim elektromagnetnim sevanjem

Vse komponente sistemov, v okviru katerih se obravnavajo tajni podatki stopnje zaupno ali višje, morajo biti zaščitene pred neželenim elektromagnetnim sevanjem. Meritve pred neželenim elektromagnetnim sevanjem opravljajo Ministrstvo za obrambo, Policija, Slovenska obveščevalno-varnostna agencija in drugi pooblaščeni organi.

Načelo separacije black/red

Vsaka informacija je na vhodu in izhodu sistemov vedno v analogni (ljudem razpoznavni) obliki (zvok, slika, besedilo). V sistemih, kjer se obravnavajo tajni podatki, so informacije lahko v različnih oblikah (razpoznavne – odprte in nerazpoznavne – šifrirane oblike). Zato je smiselno vpeljati pojma »črno« in »rdeče«, kjer črno pomeni varni del omrežja ali sistemov in so informacije v zaščiteni obliki (črno, *black*, varno), ter rdeče (opozorilna barva), ki pomeni tisti del sistemov, v katerih so informacije v nezaščiteni (odprti, berljivi, razpoznavni) obliki. Pozornost je treba nameniti predvsem rdečemu delu sistema, saj je tam nevarnost uhajanja podatkov največja. Zato je v standardih vpeljan in predpisan podroben sistem postavitve obeh delov, ki vključuje fizičen razmik med njima, RF oklapljanje in izolacijo rdečega dela, filtriranje vseh vhodno-izhodnih točk rdečega dela in enosmeren prehod med rdečim in črnim delom sistemov. [m1]

7.5 Zaščitni ukrepi TEMPEST

Najpomembnejši del področja TEMPEST so zaščitni ukrepi, ki preprečujejo EM sevanje opreme in konduktivne emisije ter s tem potencialno odtekanje podatkov. Ti ukrepi vključujejo [a5, m1]:

- oklapljanje prostorov, izbiro primernih gradbenih materialov,
- prilagojeno izvedbo instalacij v prostoru,
- izbiro primerne opreme z ustreznim potrdilom TEMPEST,
- pravilno postavitev opreme v prostor, upoštevanje razmikov med rdečim in črnim delom sistemov in drugih instalacij ter naprav,
- filtriranje vseh vhodno-izhodnih vodnikov,
- uporabo EM nepredušnih omaric,
- usposabljanje uporabnikov za pravilno ravnanje z opremo,
- pravilno vzdrževanje opreme in instalacij.

8 DISKUSIJA

Uporaba informacijske in komunikacijske opreme lahko predstavlja tveganje glede odtekanja podatkov po stranskih kanalih. Stopnja tveganja pri običajni poslovni ali osebni uporabi je odvisna od vrste opreme, namestitve sistema, izvedbe komunikacijske in napajalne infrastrukture, izpolnjevanja zahtev in priporočil EMC/EMI, zavedanja uporabnika opreme in številnih drugih dejavnikov. Pri tem pa je treba upoštevati tudi, da je:

- v nekaterih primerih podatke mogoče prestreči s povsem običajno (nizkocenovno) opremo,
- tveganje odvisno od motivacije napadalca oziroma zaupnosti podatkov,
- tovrstne zlorabe zaradi njihove neinvazivnosti težko odkriti.

Standardi in predpisi s področja zagotavljanja EM skladnosti določajo najvišje dopustne vplive na delovanje drugih naprav in organizem, vendar večinoma ne predpisujejo varnosti pred nepooblaščenim prestrezanjem podatkov po stranskih kanalih. Ob tem uporabnik ne razpolaga z informacijo o morebitni zaščiti pred odtekanjem podatkov.

Tveganje, ki ga predstavlja odtekanje podatkov preko stranskih kanalov, je v strokovni literaturi relativno dobro pokrito. Ne glede na to pa so primeri pogosto utemeljeni na zastareli tehnologiji.

Tako na primer Vuagnoux in Pasini v novejšem viru (2010) [v1, v2] navajata, da je mogoče EM sevanje, ki nastane pri uporabi tipkovnice, prestreči z razdalje do 20 m. Izkaže se, da se ta podatek nanaša na tipkovnice, ki uporabljajo zastarelo vodilo PS/2, medtem ko se tveganje pri tipkovnicah z vodilom USB v realnem okolju zniža na vsega 1,5 m do 3 m. Po drugi strani je treba upoštevati, da sta zaradi osredotočenosti na EM sevanje izločila druge načine prenosa, ki omogočajo učinkovitejše širjenje. To velja za vpliv skupne prevodnosti oziroma priklopa opreme v napajalno omrežje ter odtekanje podatkov preko parazitnih sklopov in posledičnega širjenja po prevodni infrastrukturi. Slednje sem potrdil tudi v praktičnem delu naloge.

Za tveganje, ki ga predstavlja uporaba zaslona, velja podobno kakor za tipkovnice. Prestrezanje EM sevanja z razdalje, večje kakor 1 km, kar je leta 1985 izpostavil Eck, ni več aktualno. Zanimivo je, da tudi novejši viri v strokovni literaturi izpostavljajo predvsem EM sevanje analognega vodila RGB.

Diferencialna zasnova obdelave in prenosa signala stopnjo tveganja glede odtekanja podatkov zmanjšuje. To sledi tako iz virov, ki navajajo zaščitne ukrepe pred prestrezanjem, kakor iz navedenega v prejšnjih dveh odstavkih.

Tveganje je po eni strani vedno manjše zaradi sodobnejše zasnove opreme in podatkovnih vodil, po drugi strani pa se povečuje zaradi višjih frekvenc delovanja opreme. Razvoj tehnologije zaradi upoštevanja priporočil EMC/EMI pri načrtovanju vezij tveganje zmanjšuje, vendar se odpirajo novi problemi. Če so bili pred leti problemi v zvezi z EM sevanjem omejeni večinoma na kable V/I, je danes potencialnih virov več in se prenašajo v višje območje frekvenčnega spektra. S tem pa lahko tudi kratke linije, po katerih se signal prenaša, zaradi usklajenosti z valovno dolžino signala delujejo kot učinkovite oddajne antene.

Pri tem se odpira tudi vprašanje ekonomske upravičenosti uvedbe ukrepov in opreme, ki preprečuje EM emisije, in sicer predvsem ob hkratnem upoštevanju naslednjih dejavnikov:

- standardi, ki obravnavajo navedeno področje, niso javno objavljeni,
- za obravnavo tajnih podatkov v IS je uvedba varnostnih ukrepov predpisana z zakonodajo,
- visoki dobički maloštevilnih podjetij, ki delujejo na tem področju. [bs]

Ne glede na izpostavljene dileme menim, da je za zaščito nacionalnih interesov države uvedba ukrepov v zvezi z zavarovanjem tajnih podatkov upravičena. Upoštevati je treba, da so podatki lahko razkriti ali uničeni v terorističnih napadih, sabotaži, vojni … Zaradi visoke cene, nestandardnih priključkov in lastnosti opreme (večja masa in dimenzije) pa je sama uvedba ukrepov v običajnem delovnem in poslovnem okolju vprašljiva.

9 ZAKLJUČEK

V nalogi sem proučil tveganja, ki jih predstavlja nenadzorovano odtekanje podatkov preko stranskih kanalov kot stranski pojav uporabe informacijske in komunikacijske opreme. Elektronske naprave pri obdelavi podatkov namreč oddajajo šum, ki se v različnih oblikah širi v okolico naprav in komunikacijskih povezav. Ta je lahko neposredno povezan z obravnavanimi podatki. Med prevodniki, ki so v bližini, se signal prenese na podlagi medsebojnih parazitnih kapacitivnosti in induktivnosti ter zaradi nepopolne izolacije in ozemljitve na podlagi skupne prevodnosti. Pri višjih frekvencah podatkovne linije delujejo kot oddajne antene, ki v okolico razširjajo elektromagnetno sevanje. Na drugi strani konduktivne emisije za prenos izkoriščajo prevodno infrastrukturo, preko katere lahko odtekajo v nenadzorovana območja, kot so druge sobe, stavbe … Pri odtekanju podatkov preko prevodne infrastrukture lahko posamezni segmenti, ob usklajenosti dolžine s frekvenco signala, posredno oddajajo elektromagnetno sevanje. Obstaja tudi nevarnost, da se to sevanje s podatki modulira na signal, ki ga oddajajo naprave za brezžično komunikacijo (npr. mobilni telefoni). V tem primeru je njihova rekonstrukcija neodvisna od razdalje in lokacije. V nekaterih konkretnih situacijah pa lahko napadalec izkoristi tudi druge stranske kanale. Sliko z zaslona lahko prestreže v neposredni liniji pogleda na večje razdalje ali pa izkoristi odboj slike od predmetov v njegovi bližini. Določeno stopnjo tveganja lahko predstavljajo tudi specifični zvočni učinki, ki nastanejo pri uporabi informacijske opreme.

Med izpostavljene enote informacijske opreme, ki sem jih v nalogi opisal, spadajo zaslon, tipkovnica, laserski tiskalnik, pametne kartice idr. Na drugi strani je zelo izpostavljen tudi prenos podatkov po določenih vrstah podatkovnih vodil.

Zaradi neinvazivnosti tovrstnih napadov je njihovo zaznavanje izjemno težavno. Pri obravnavi tajnih podatkov stopnje zaupno ali višje so zato predpisane stroge varnostne zahteve na različnih nivojih, s katerimi onemogočamo tovrstne zlorabe. Te vključujejo fizične, tehnične in organizacijske ukrepe, kot so:

- zavarovanje ključne opreme v varnostnem območju,
- varnostno preverjanje oseb, ki imajo dostop do opreme in podatkov,
- uporaba posebne opreme, ki zagotavlja varnost pred EM sevanjem in konduktivnimi emisijami ali uporaba opreme v oklopljenih prostorih (v t. i. gluhih sobah),
- ločitev infrastrukture tajnega in javnega dela (separacija črno/rdeče),
- šifriran prenos podatkov,

– pridobitev mnenja Urada Vlade RS za varovanje tajnih podatkov o izpolnjevanju varnostnih zahtev: varnostnega območja, v katerem se namestijo ključne strojne komponente IKT, in informacijskega sistema za obravnavo tajnih podatkov v elektronski obliki.

Za zaščito nacionalnih interesov države je uvedba navedenih ukrepov v zvezi z zavarovanjem tajnih podatkov vsekakor upravičena. V teh primerih moramo namreč med drugim upoštevati tudi možnost terorističnega napada, sabotaže, vojne ipd. Zaradi zahtevnosti uvedbe in tajnosti predpisov s tega področja pa ti ukrepi za osebno in poslovno uporabo niso relevantni. Z upoštevanjem splošnih priporočil lahko do določene mere tveganja sicer zmanjšamo, vendar ne moremo zagotoviti, da nevarnost odtekanja podatkov ne obstaja.

Pri uporabi informacijske opreme je zato treba upoštevati tudi nevarnost razkritja podatkov, ki odtekajo preko neželenega elektromagnetnega sevanja in po drugih stranskih kanalih.

10 LITERATURA

[a1] J. A. Ambrose, R. G. Ragel, S. Parameswaran, A. Ignjatovic, »Multiprocessor information concealment architecture to prevent power analysis-based side channel attacks«, *IET Computers & Digital Techniques*, zv. 5, št. 1, str. 1–15, januar 2011.

[a2] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Publishing Inc., Indianapolis, ZDA, 2008.

[a3] B. Archambeault, C. Brench, S. Connor, »Review of Printed-Circuit-Board Level EMI/EMC Issues and Tools«, *IEEE Transactions On Electromagnetic Compatibility*, zv. 52, št. 2, str. 455–461, maj 2010.

[a4] D. Asonov, R. Agrawal, 2004, »Keyboard acoustic emanations, Security and Privacy«, *IEEE Symposium on Digital Object Identifier*, maj 2004, str. 3–11.

[a5] A. Auddy, S. Sahu, 2008, »TEMPEST: Magnitude of Threat and Mitigation«, v zborniku *10th International Conference on Electromagnetic Interference & Compatibility*, Bangalore, Indija, november 2008, str. 603–611.

[b1] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, C. Sporleder, »Acoustic side-channel attacks on printers«, v zborniku *19th USENIX Security Symposium, Washington DC*, ZDA, avgust 2010.

[b2] M. Backes, M. Dürmuth, D. Unruh, 2008, »Compromising Reflections or How to Read LCD Monitors Around the Corner«, v zborniku IEEE *Symposium on Security and Privacy*, Oakland, Kalifornia, ZDA, maj 2008, str. 158–169.

[b3] Y. Berger, A. Wool, A. Yeredor, »Dictionary attacks using keyboard acoustic emanations«, *13th ACM Conference on Computer and Communications Security*, Alexandria, ZDA, oktober 2006, str. 245–254.

[b4] J. Budin et al., *Elektromagnetna sevanja*, 2004, Inštitut za telekomunikacije, Ljubljana.

[d1] S. B. Dhia, M. Ramdani, E. Sicard, *»Electromagnetic Compatibility of Integrated Circuits - Techniques for low emission and susceptibility«*, New York: Springer, 2006.

[d2] M. Dürmuth, »*Novel Classes of Side Channels and Covert Channels*«, doktorska disertacija, Naturwissenschaftlich-Technischen Fakultäten der Universität des Saarlandes, Nemčija, 2009.

[e1] W. van Eck, »Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?«, *Computers & Security*, zv. 4, št. 4, 1985, str. 269–286.

[f1] J. Fan, L. He, »The study on video information leakage of computer«, v zborniku *2009 Network Infrastructure and Digital Content*, Peking, Kitajska, november 2009, str. 991–994.

[f2] J. Fan, X. Ye, J. Kim,B. Archambeault, A. Orlandi, »Signal Integrity Design for High-Speed Digital Circuits: Progress and Directions«, *IEEE Transactions On Electromagnetic Compatibility*, zv. 52, št. 2, str. 392–400, maj 2010.

[g2] N. N. Gorobets, A. V. Trivaylo, »Compromising emanations: overview and system Analysis«, *Vestnik Karazin Karkhov National University*, št. 883, 2009, str. 83–88.

[g3] K. Grzesiak, A. Przybysz, »Emission security of laser printers«, v zborniku *Military Communications and Information Systems Conference*, Wroclaw, Poljska, september 2010, str. 353–363.

[j1] B. Jacobs, W. Pieters, »Combatting Electoral Traces: The Dutch Tempest Discussion and Beyond«, *Lecture Notes in Computer Science*, zv. 5705, 2009, str. 121–144.

[k1] D. Karakoyunlu, F. K. Gurkaynak, B. Sunar, Y. Leblebici, »Efficient and side-channel-aware implementations of elliptic curve cryptosystems over prime fields«, *IET Information Security*, zv. 4, št 1, str. 30–43, marec 2010.

[k2] C. H. Kim, J. J. Quisquater, »Faults, Injection Methods, and Fault Attacks«, *IEEE Design & Test archive*, zv. 24, št. 6, str. 544–545, november 2007.

[k3] F. Koeune, F. X. Standaert, »A Tutorial on Physical Security and Side-Channel Attacks«, *Lecture Notes in Computer Science*, zv. 3655, Foundations of Security Analysis and Design III, 2005, str. 78–108.

[k4] M. G. Kuhn, *Compromising emanations: eavesdropping risks of computer displays*, 2003, tehnično poročilo, University of Cambridge, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.html, dostop 14. 6. 2011

[k5] M. G. Kuhn, »Electromagnetic Eavesdropping Risks of Flat-Panel Displays«, 2005, *Lecture Notes in Computer Science*, zv. 3424, 2005, str. 88–107.

[k6] M. G. Kuhn, »Optical time-domain eavesdropping risks of CRT displays«, v zborniku *2002 IEEE Symposium on Security and Privacy*, Berkeley, Kalifornia, ZDA, maj 2002, str. 3–18.

[k7] M. G. Kuhn, »Security Limits for Compromising Emanations«, *Lecture Notes in Computer Science*, zv. 3659, str. 265–279, 2005.

[k8] M. G. Kuhn, R. J. Anderson, »Soft Tempest – An Opportunity for NATO«, v zborniku *Protecting NATO Information Systems in the 21st Century*, Washington DC, ZDA, oktober 1999, str. 5.1–5.5.

[k9] M. G. Kuhn, R. J. Anderson, »Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations«, *Lecture Notes in Computer Science*, zv. 1525, 1998, str. 124–142.

[m1] D. Mohorovič, »Elektomagnetno sevanje v informatiki – TEMPEST«, članek v zborniku in predstavitev *Dok_sis 2008 - XVII. Posvetovanje Sistemi za upravljanje z dokumenti*, Kranjska gora, september 2008

[m2] M. I. Montrose, E. M. Nakauchi, *Testing for EMC Compliance - Approaches and Techniques*, IEEE Press, 2004

[o1] H. W. Ott, *Electromagnetic compatibility engineering*, New Jersey: 2009, John Wiley and Sons

[p1] S. Pennesi, S. Sebastiani, »Information Security and Emissions Control«, v zborniku *2005 IEEE International Symposium on Electromagnetic Compatibility*, avgust 2005, str. 777.

[p2] W. Pieters, »Combatting Electoral Traces: The Dutch Tempest Discussion and Beyond«, *Lecture Notes in Computer Science*, zv. 5767, 2009, str. 172–190.

[p3] M. Podberščič, V. Matko, M. Šegula, »Pravila za zmanjšanje elektromagnetne emisije«, v zborniku *Elektrotehniške in računalniške konference*, Portorož, zv. A, september 2004, str. 73–76.

[s1] D. Salomon, *Elements of Computer Security*, poglavje 1, Springer Verlag, London, 2010, str. 17–35.

[s2] H. Sekiguchi, S. Seto, »Measurement of computer RGB signals in conducted emission on power leads«, *Progress In Electromagnetics Research*, zv. 7, str. 51–64, 2009.

[s3] S. Sinkovski, »Zaštita informacija od kompromitujućeg elektromagnetnog zračenja«, *Nauka, tehnika, bezbednost*, 2004, zv. 14, št. 1, str. 61–79.

[s4] P. Smulders, »The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables«, *Computers & Security*, zv. 9, št. 1, 1990.

[s5] K. Sridhar S. Prasad L. Punitha S. Karunakaran, »EMI issues of Universal Serial Bus and Solutions«, v zborniku *8th International Conference on Electromagnetic Interference and Compatibility*, Chennai, Indija, december 2003, str. 97–100.

[s6] R. Stolle, »Electromagnetic coupling of twisted pair cables«, *IEEE Journal on selected areas in communications*, zv. 20, št. 5, junij 2002, str. 883.

[s7] Y. Suzuki, Y. Akiyama, »Jamming Technique to Prevent Information Leakage Caused by Unintentional Emissions of PC Video«, v zborniku *2010 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Fort Lauderdale, Florida, ZDA, julij 2010, str 132–137.

[t1] H. Tanaka, »Information Leakage Via Electromagnetic Emanations and Evaluation of Tempest Countermeasures«, *Lecture Notes in Computer Science*, zv. 4812, 2007, str. 167–179.

[t2] H. Tanaka, »Information Information leakage via electromagnetic emanation and effectiveness of averaging technique«, v zborniku *International Conference on Information Security and Assurance*, Busan, Južna Koreja, april 2008, str. 98–101.

[t3] H. Tanaka, O. Takizawa, A. Yamamura, »Evaluation and Improvement of the Tempest Fonts«, *Lecture Notes in Computer Science*, zv. 3325, str. 457–469, 2005.

[t4] K. Tiri, I. Verbauwhede, »A Digital Design Flow for Secure Integrated Circuits«, *IEEE transactions on computer-aided design of integrated circuits and systems*, zv. 25, št. 7, str. 1197–1208, julij 2006.

[v1] G. Vasilescu, »Methods of Reducing Emission of Interfering Signals«, 2005, *Signals and Communication Technology, Electronic Noise and Interfering Signals*, II. del, str. 389–409, 2005.

[v2] M. Vuagnoux, S. Pasini, »An Improved Technique to Discover Compromising Electromagnetic Emanations«, v zborniku *2010 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Fort Lauderdale, Florida, ZDA, str. 121–126.

[v3] [49] M. Vuagnoux, S. Pasini, »Compromising Electromagnetic Emanations of Wired and Wireless Keyboards«, v zborniku *18th USENIX Security Symposium*, Montreal, Kanada, avgust 2009, str. 1–16.

[w1] T. Watanabe, H. Nagayoshi, H. Sako, »A Display Technique for Preventing Electromagnetic Eavesdropping Using Color Mixture Characteristic of Human Eyes«, *Lecture Notes in Computer Science*, zv. 5284, 2008, str. 1–14.

[w2] T. Watanabe, H. Nagayoshi, T. Urano, T. Uemura, H. Sako, »Countermeasure for Electromagnetic Screen Image Leakage based on Color Mixing in Human Brain«, v zborniku *2010 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Fort Lauderdale, Florida, ZDA, julij 2010, str. 138–142.

[y1] W. Yang, Y. Lu, J. Xu, »Video information recovery from EM leakage of computers based on storage oscilloscope«, *Frontiers of Electrical and Electronic Engineering in China*, zv. 5, št. 2, str. 143–146, 2010.

[y2] P. Yeh, A. Wang, B.C. Tseng, »High Speed Data Transmission Common Mode Noise Suppression - Appplication to USB 2.0 and IEEE 1394«, v zborniku *4th International Symposium on Electronic Materials and Packaging*, december 2002, str. 488–491.

[z1] M. Zoyousefein, A. Ghorbani, »Design of a new emission-security standard for radiated emission EMC test«, v zborniku *2009 IEEE Student Conference on Research and Development (SCOReD)*, Serdang, Malezija, str. 513–516, 2009.

11 VIRI

11.1 PREDPISI, REGULATIVA, STANDARDI

[UVTP1] (2008) Komisija za informacijsko varnost, Navodilo o izvajanju zaščite pred neželenim elektromagnetnim sevanjem v komunikacijskih in informacijskih sistemih, v katerih se obravnavajo tajni podatki, št. 02210-1/2008/85 (19. 11. 2008). Dostopno na: www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Navodilo_em_sevanje_v_KIV.pdf.

[SEU] (2001) Sklep Sveta EU z dne 19. marca 2001 o sprejetju predpisov Sveta o varovanju tajnosti, Uradni list Evropske unije, št. 2001/264/ES.

[EK] (2001) Sklep Evropske Komisije z dne 29. novembra 2001 o spremembah njenega Poslovnika, Uradni list Evropske unije, št. 2001/844/ES.

[SV1] (2005) Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja, Uradni list RS, št. 74/2005.

[Res1] (2010) Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1), Uradni list RS, št. 27/2010.

[ZTP] (2006) Zakon o tajnih podatkih (ZTP), Uradni list RS, št. 50/2006 – UPB2 in nasl.

[UVTP] (2005) Uredba o varovanju tajnih podatkov, Uradni list RS, št. 74/2005.

[UKIS] (2007) Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Uradni list RS, št. 48/2007.

[HID] (2001) USB Implementers' Forum, Universal Serial Bus HID Usage Tables, v. 1.11. Dostopno na: www.usb.org.

[USB3] (2008) Universal Serial Bus 3.0 Specification, rev. 1.0. Dostopno na: www.usb.org.

[USB2] (2000) Universal Serial Bus 2.0 Specification, rev. 2.0. Dostopno na: www.usb.org.

[WUSB] (2010) Wireless Universal Serial Bus Specification, rev. 1.1. Dostopno na: www.usb.org.

[SIT] (2008) IEEE Computer Society, *IEEE Standard for Information Technology: Hardcopy Device and System Security*. Dostopno na: http://ieeexplore.ieee.org.

11.2 DRUGI VIRI

[DTV-A] (2005) Australian Broadcasting Authority, Digital Terrestial Television Broadcasting Planning Handbook. Dostopno na: http://www.acma.gov.au.

[dv1] (2009) A. Shirvani, Emission Security (EMSEC), *2st systems security conference*, Teheran, Iran, Dostopno na: http://www.slideshare.net/abe8512000/emission-securitytempest-attacks.

[dv2] M. Podberščič, *Reševanje EMC problematike CPU modula*, Poročilo o individualnem raziskovalnem delu, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, 2001.

[dv3] J. Korenčan, *Ozemljitve, prenapetostna in EM zaščita sistemov strukturiranih ožičenj*, diplomsko delo, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, 2009.

[bs] (2005) D. Huang, Computer and Network Security, Lecture 4. Dostopno na: http://enpub.fulton.asu.edu/iacdev/courses/cse591m/lecture_notes/lecture4.pdf.

[UTP7] (2006) Siemon, Government Levels of Security Enhanced with TERA® Cabling System. Dostopno na: http://www.siemon.com/us/white_papers/06-03-02-tera-security-government.asp.

[NSA] (2007) National Security Agency, TEMPEST, A Signal Problem. Dostopno na: http://www.nsa.gov/public info/ files/cryptologic spectrum/tempest.pdf.

[STP] (2004) SYSTIMAX, Structured Connectivity Solutions and Information Security. Dostopno na: http://docs.commscope.com/Public/information_security.pdf.