POREDBENA ANALIZA TEMPEST ZAŠTITE U UPRAVLJANJU SAJBER BEZBJEDNOSTI TAJNIH PODATAKA

[1,2]Igor Burić, [2]Ivana Ognjanović, [2]Ramo Šendelj
[1]Agencija za nacionalnu bezbjednost Crne Gore, Podgorica, Crna Gora
igorburi@gmail.com
[2]Univerzitet Donja Gorica, Podgorica, Crna Gora
{ivana.ognjanovic,ramo.sendelj}@udg.edu.me

Ključne riječi: TEMPEST, KEMZ, tajni podaci, zoniranje, ometanje, filtriranje, elektromagnetno zračenje, Soft TEMPEST, van Eck phreaking, Faradejev kavez

SAŽETAK:

U vremenu široke upotrebe informaciono - komunikacionih tehnologija, bezbjednost informacija je na prvom mjestu. Sadašnje rašireno interesovanje o elektromagnetnom zračenju i elektromagnetnom prisluškivanju je fenomen koji nije od skora. Vojska i obavještajne agencije su znale da svi električni uređaji, bez odgovarajuće zaštite, generišu visok nivo signala iz radio frekfentnog spektra. Ovaj signal je sofisticiranom opremom moguće "uhvatiti" i rekonstruisati u čitljive informacije. Po svojoj prirodi ***elektromagnetno zračenje*** *je ista pojava kao elektromagnetne smetnje sa jednom bitnom razlikom, radi se o signalima koji nose informaciju koja ne smije biti dostupna okolini. U zapadnoj literaturi se ova problematika najčešće podvodi pod akronimom američke vlade* ***TEMPEST*** *. U ovom radu će biti prikazani najpoznatiji TEMPEST napadi, urađena poredbena analiza najefikasnijih mjera TEMPEST zaštite i generisane preporuke u cilju povećanja bezbjednosti informacija.*

1. UVOD

Elektronska oprema emituje elektromagnetne talase koji nose informacije o podacima koji se obrađuju tom opremom. Ove informacije je moguće presresti i rekonstruisati koristeći radio prijemnike i savremene tehnike obrade signala. Shodno tome, ova tema predstavlja potencijalnu prijetnju po bezbjednost informacija [1]. Ova problematika se danas najčešće podvodi pod akronimom američke vlade **TEMPEST**. Iako postoje mnoga tumačenja ovog termina, TEMPEST je neklasifikovano ime koje se odnosi na istraživanja, studije i kontrolu kompromitujućeg elektromagnetnog zračenja kao i mjere zaštite za njihovo sprječavanje [2]. TEMPEST zaštita predstavlja veoma značajan element u upravljanju sajber bezbjednosti tajnih podataka koji se obrađuju u informaciono komunikacionim sistemima. To potvrđuju Evropska Unija i NATO koji svojim Uredbama i bezbjednosnim direktivama nalažu primjenu TEMPEST mjera zaštite tajnih podataka [2]. Informaciono komunikacioni sistemi koji se koriste za obradu tajnih podataka pokazali su se kao izuzetno atraktivni ciljevi za protivnike poput stranih obavještajnih službi, teroriste, pripadnike organizovanog kriminala, koji su tehnički i kadrovski opremljeni za iskorišćavanje TEMPEST ranjivosti ovih sistema. Zbog opšteg nedostatka saznanja i opasnosti koje se odnosi na TEMPEST, ovoj problematici nije posvećivana adekvatna pažnja. Trend masovnog korišćenja savremenih informacionih tehnologija za obradu osjetljivih informacija ističe u prvi plan problem zaštite državnih, vojnih, naučnih, poslovnih i finansijskih tajni koji se njima obrađuju. Da bi postigli zaštitu od curenja informacija putem elektromagnetnog zračenja i uspješno upravljali utvrđenim rizikom potrebno je preduzeti niz mjera. TEMPEST zaštita se postiže instaliranjem Faradejevih kaveza [1] [2], nabavkom TEMPEST zaštićene opreme [2], vršenjem TEMPEST zoniranja prostorija [2], filtriranjem signala [1], primjenom Soft TEMPEST tehnika [11] i pravilnom instalacijom opreme

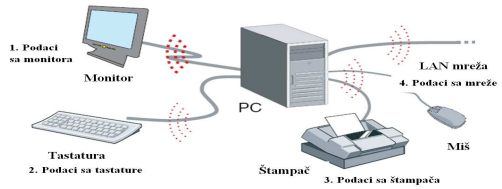
i kablova [2]. U radu je prikazan istorijski razvoj TEMPEST-a i poznatih TEMPEST napada. Dat je osvrt na poznate standarde koji propisuju ovu oblast kao i problemi u njihovoj implementaciji. Napravljena je poredbena analiza TEMPEST mjera zaštite i njihovog uticaja na upravljanje utvrđenim rizikom u odnosu na sajber bezbjednost tajnih podataka. Na osnovu dobijenih rezultata analize generisane su i preporuke u cilju povećanja bezbjednosti tajnih podataka koji se obrađuju elektronskim putem.

2. POZNATI TEMPEST NAPADI

Najstariji TEMPEST napadi desili su se početkom prvog svjetskog rata [3]. Kablovi koji su povezivali telefonske i telegrafske centrale na bojnom polju emitovali su signal koji se mogao prisluškivati sa udaljenosti od 100 metara za telefon i 250 metara za telegraf. Jedan od najpoznatijih TEMPEST napada dogodio se 1957. godine kada je britanski premijer izdao naredbu o nadgledanju francuske ambasade, kako bi se ustanovio njihov stav u vezi s pristupanjem Britanije Evropskoj ekonomskoj zajednici. Naučnici MI5 su opremom za presrijetanje elektromagnetnog zračenja, pored šifrovanog saobraćaja, uhvatili i slabi sekundarni signal. Taj signal je bio nosilac otvorenog teksta koji su britanski naučnici uspješno rekonstruisali [8]. Elektromagnetno zračenje kao bezbjednosni rizik po računarske sisteme se prvi put pominje u otvorenoj literaturi 1967. godine kada je dr. Willis Ware jasno prepoznao ranjivosti kao što su zračenje procesora, komunikacione linije, komutacione opreme i perifernih uređaja [4]. Jedan od prvih detaljnijih opisa TEMPEST prijetnji je bio u Švedskoj 1983. godine [5]. TEMPEST problem je javno eskalirao tek 1985. godine kada je Wim van Eck koristeći kombi s elektronskom opremom BBC-ja i VHF antenski sistem, uspješno prisluškivao uređaje sa CRT monitorima sa velike udaljenosti [6]. Ovaj napad je poznat kao "***van Eck phreaking***" *napad*. Njegove rezultate su potvrdili Möller, Bernstein i Kolberg [7]. Iako su CRT monitori podložniji curenju signala, ni LCD monitori nijesu sigurni u odnosu na elektromagnetno zračenje. To su potvrdili naučnici sa Univerziteta Cambridgeu koji su 2004. godine uspješno izvršili prisluškivanje LCD monitora sa udaljenosti od 10 metara [10]. Istraživanja pokazuju da su neki LCD monitori mnogo ranjiviji od CRT monitora [11]. Vlada Holandije je zabranila korištenje **NewVote** elektronskih glasačkih mašina proizvođača SDU na nacionalnim izborima 2006. godine, pod uvjerenjem da tajnost glasanja ne može biti zagarantovana usled eventualnog TEMPEST napada. TEMPEST napad koji je kompromitovao očuvanje tajnosti glasanja prilikom provjere elektronskog glasanja dogodio se 2009. godine u Brazilu. U januaru 2015. godine istraživači sa Instituta za tehnologiju iz Džordžije, SAD su na Univerzitetu Ben Gurion u Izraelu demonstrirali TEMPEST napad tako što su prisluškivali tastaturu računara na kome je bio instaliran softver za generisanje modulisane frekvencije za tipke tastature. Za prijemnik je korišćen mobilni telefon sa Android platformom [12][13].

3. PROCJENA RIZIKA U ODNOSU NA IZVOR INFORMACIJA

Danas se TEMPEST ne odnosi samo na uređaje na kojima se vrši kripto obrada informacija već je to slučaj i sa komercijalnom informatičkom opremom (računari, tableti, mobilni telefoni...).



Slika 1: Tipovi informacija skriveni u elektromagnetnom zračenju

Najjače elektromagnetno zračenje na računarima proizlazi iz monitora i ostalih grafičkih komponenti i ono predstavlja veći rizik u odnosu na zračenje sa perifernih uređaja. Osnovno načelo prisluškivanja je očitavanje električnih signala visoke frekvencije koju stvara monitor. Oscilirajući električni tokovi

stvaraju elektromagnetno zračenje koje je u uskoj vezi sa slikom prikazanom na monitoru pa je iz tog zračenja relativno lako izvršiti rekonstrukciju originalne informacije upotrebom savremenih radio prijemnika i tehnika obrade signala. Smulders je dokazao da je moguće presresti signale koje prenosi zaštićeni RS-232 kabal [9]. Konektori kabla formiraju rezonantne krugove koji se sastoje od indukcije kabla i kapaciteta između uređaja i uzemljenja. Ovo pobuđuje komponente visokih frekvencija što rezultira da visokofrekventne oscilacije emituju elektromagnetno zračenje. Kabal RS-232 se koristi i za povezivanje procesora bankomata sa čitačem kartica i PIN tastaturom. Postoje brojni dokumenti koji pokazuju mogućnost hvatanja PIN-a i sadržaja kartice na daljinama do 8 metara [9].
Podaci koji se unose sa tastature su takođe podložni oticanju zračenjem stim što je snaga zračenja u ovom slučaju znatno manja nego kod monitora. Samim tim napadač mora biti bliže meti prilikom napada. Podaci koji su na najviše podložni ovom napadu su korisničko ime i lozinka.
Podatke sa štampača je veoma teško rekonstruisati jer je potrebno demodulirati signal sa njegovog interfejsa. U ovom slučaju samo štampane informacije mogu biti kompromitovane.
Nivo važnosti i količina podataka koji mogu biti kompromitovani sa LAN mreže je visoka, međutim njih je teško rekonstruisati zbog male snage zračenja i teške demodulacije signala sa LAN interfejsa.

Tabela 1: Procjena rizika po bezbjednost informacija u odnosu na izvor informacije [1]

Izvor informacija	**Važnost i količina informacija**	**Težina rekonstrukcije originalne informacije**	**Snaga zračenja**	**Rizik od gubljenja informacija**
Monitor	Visoka (sve sa monitora)	Lako	Jaka	Visok
Tastatura	Niska - Srednja (Samo tekst)	Teško (potreban kod za dekripciju vezan za svaku tipku)	Slaba	Srednji
Štampač	Niska (štampane informacije)	Teško (potrebno demodulirati signal sa interfejsa)	Slaba	Nizak
Mreža	Srednje -Visoko (podaci sa mreže)	Teško (potrebno demodulirati signal sa LAN interfejsa)	Slaba	Srednji

4. POREDBENA ANALIZA TEMPEST MJERE ZAŠTITE

U ovom radu je izvršena poredbena analiza šest konvencionalnih TEMPEST mjera zaštite. Ove mjere obuhvataju kako one koje su definisane standardima (oklopljena prostorija, oklopljen uređaj, zoniranje) tako i one koje nijesu (filtriranje, soft TEMPEST, ometanje). Poredbena analiza se odnosi na nivo zaštite, cijenu, primjenu na mobilnoj opremi i da li su ove mjere propisane standardima.

4.1 Oklopljena prostorija

Najsigurniji metod TEMPEST zaštite je osiguranje područja oko elektronske opreme kojom se obrađuju tajni podaci. Ovo se postiže smještanjem opreme u Faradejev kavez tjs. u prostoriju i/ili zgradu koja je oklopljena materijalima koji sprečavaju elektromagnetno zračenje. Instalacija Faradejevog kaveza je u većini slučajeva teško izvodljiva, ekstremno skupa i nepraktična. Prilikom izgradnje prostorije za obradu tajnih podataka potrebno je pridržavati se standarda **NATO SDIP-29 (bivši AMSG 719G)** koji definiše zahtjeve za instalaciju opreme za obradu tajnih podataka.

4.2 Oklopljen uređaj

Drugi siguran metod TEMPEST zaštite je upotreba sertifikovane opreme. Saradnjom SAD i NATO saveza nastao je niz standarda za oklopljenu opremu:

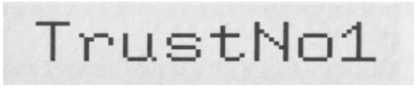
NATO SDIP-27 Level A (ranije AMSG 720B) i **USA NSTISSAM Level I** - najstrožiji standard za uređaje, prilikom kojeg se pretpostavlja da napadač ima direktan pristup računaru. Upotrebom ove opreme smatra se da ne postoji kompromitujuće elektromagnetno zračenje.
NATO SDIP-27 Level B (ranije AMSG 788A) i **USA NSTISSAM Level II** - blaži standard u odnosu na Level A. Pretpostavka je da napadač ne može doći na manje od 20 metara od uređaja ili je uređaj ograđen sigurnim zidovima,
NATO SDIP-27 Level C (ranije AMSG 784) i **USA NSTISSAM Level III** - još blaži kriterijum, smatra se da je napadač udaljen više od 100 metara ili je zračenje spriječeno sa dovoljno zidova.
TEMPEST sertifikovani uređaji su prilagođeni kako bi se kompromitovana zračenja svela na minimum. To se postiže stavljanjem metalnih kućišta, zaštićenih konektora i kablova i modifikovanih napajanja. Ove modifikacije podižu cijenu računarskoj opremi. Cijena TEMPEST zaštićenog lap topa, standarda SDIP-27 Level A, je između 5000 i 10000 eura. Teško je primjenljivo na mobilne uređaje.

4.3 Filtriranje

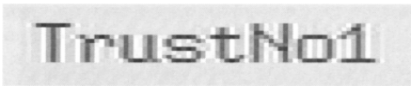
Filtriranje je efikasna metoda TEMPEST zaštite. Postiže se umetanjem filtera u komunikacione interfejs kablove i kablove za napajanje. Filteri trebaju biti podešeni na frekvenciju emisije. Nedostatak ove metode je to što je efikasna samo za suzbijanje emisije iz kablova, nikako iz samog računara ili monitora [1]. Fizičko filtriranje treba koristiti uz druge metode TEMPEST zaštite. Filtriranje je moguće za implementaciju na mobilne uređaje. Ova mjera zaštite nije standardizovana.

4.4 Soft TEMPEST

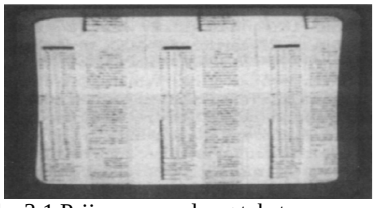
Soft TEMPEST koristi softver za filtriranje ili maskiranje kako bi informaciju koju emituje uređaj učinio nerazumljivom. Snaga zračenja se može smanjiti upotrebom posebno dizajniranih fontova [11] [14]. Ova tehnologija se koristi i u komercijalnim proizvodima (e-mail Encription Package PGP). Kuhn i Anderson su otkrili da je većina informacija koje se emituju iz monitora koncetrisana u vrhu spektra [11]. Koristeći pogodne low-pass filtere uklonili su 30% signala od Furijeove transformacije standardnog fonta. Ovo filtriranje je imalo neprimjetan efekat na sadržaj ekrana korisnika (slika 2.2). Razlika uhvaćenog signala je ogromna, što je prikazano na slici 3.1 i 3.2.

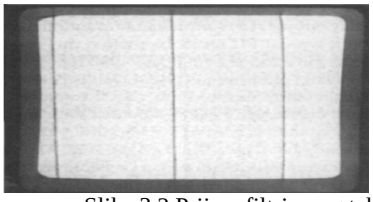


Slika 2.1 Normalan tekst



Slika 2.2 Isti tekst, filtriran


Slika 3.1 Prijem normalnog teksta


Slika 3.2 Prijem filtriranog teksta

Soft TEMPEST je efikasan za izmjenu fonta slova, međutim za slike i grafike nije primjenljiv. Ova tehnika smanjuje kompromitujuće elektromagnetno zračenje sa monitora između 10 i 20 dB, što u kombinaciji sa TEMPEST zoniranjem može donijeti značajne uštede prilikom TEMPEST opremanja prostorija. I druge napade je moguće potpuno blokirati pomoću adekvatnog softvera. Napad na tastaturu može biti sproveden kada mikrokontroler prolazi kroz petlju skenirajući tastere dok ne naiđe na onaj koji je pritisnut. Pritisnuti taster se modulira i emituje iz tastature. Šifrovanjem redosleda kojim se skeniraju tasteri na tastaturi, ova vrsta napada može biti potpuno blokirana. Pogodno je za implementaciju na mobilne uređaje. Ova mjera zaštite nije standardizovana.

4.5 Zoniranje

Zoniranje kao TEMPEST mjera zaštite se koristi radi kvalitetnog odabira prostorija u kojima će se elektronski obrađivati tajni podaci. Poželjno je da se prostorija nalazi u podrumu zgrade, da nema prozore, da su zidovi izgrađeni od čvrstog materijala (beton, armaturno željezo...), da je opremljena blind vratima itd. Ukoliko je ta prostorija fizički obezbijeđena perimetrom koji pokriva pojas od 20 metara, možemo govoriti o srednje zaštićenoj prostoriji. Ukoliko je taj perimetar veći od 100 metara možemo reći da je to sigurna prostorija. Prostoriju je najbolje odabrati nakon TEMPEST zoniranja prostorija. Za TEMPEST zoniranje prostorija se koristi mjerna oprema i postupak u skladu sa Procedurama EU za TEMPEST zoniranje **IASG 7-02** i NATO procedurama TEMPEST zoniranja **NATO SDIP-28.** U zavisnosti od rezultata mjerenja vrši se opremanje prostorije. Zoniranje je nepraktično za primjenu na mobilnim uređajima.

4.6 Ometanje

Ometanje je TEMPEST mjera zaštite čija je osnovna namjena da preklopi glavni signal. Postiže se pomoću generatora signala (buka ili besmisleni signali), koji utiče na korisni signal i zajedno daju signal koji je neupotrebljiv za napadača. Ova oprema je veoma jednostavna za izradu i jeftina za nabavku. Može se koristiti na mobilnim uređajima. Grupa naučnika iz Japana je napravila TEMPEST Guard uređaj koji uspijeva da zaštiti PC od nenamjernog curenja informacija putem monitora [15]. Ometanje je pogodno za implementaciju na mobilni uređaj. Ova mjera zaštite nije standardizovana.

Tabela 2: Uporedna tabela TEMPEST mjera zaštite

Mjere zaštite	Nivo zaštite	Cijena	Zaštita mobilnih uređaja	Standardizovano
Oklopljena prostorija	Visok	Veoma visoka	Nemoguće	**DA**
Oklopljena oprema	Visok	Visoka	Neugodno za upotrebu	**DA**
Zoniranje	Visok	Niska-Srednja	Teško za implementaciju	**DA**
Ometanje	Visok	Niska-Srednja	Moguće	**NE**
Soft TEMPEST	Srednji	Niska-Srednja	Moguće	**NE**
Filtriranje	Nizak-Srednji	Niska	Moguće	**NE**

4.7. Zaključci poredbene analize

Poredbena analiza se odnosila na nivo zaštite, cijenu implementacije, mogućnost primjene na mobilne uređaje i da li su ove mjere propisane obaveznim standardima. Analiza je pokazala da su najefikasniji metodi TEMPEST zaštite oklopljena prostorija i oklopljena oprema. Međutim, primjena ovih metoda je ujedno i najskuplje rješenje. Ukoliko bi se standardizovala upotreba svih pobrojanih metoda adekvatno bi zaštitili podatke od kompromitujućeg elektromagnetnog zračenja a postigla bi se i značajna novčana ušteda. Upotrebom Soft TEMPEST tehnika, koje su se pokazale kao izuzetno efikasne a veoma jeftine, elektromagnetno zračenje se smanjuje za 10-20dB što je dovoljno da se za jednu zonu poboljša rezultat TEMPEST zoniranja i samim tim upotrijebi jeftinija oprema u zoniranim prostorijama. Filtriranje se pokazalo kao efikasan metod za suzbijanje zračenje iz interfejsa kablova. Jedna od veoma značajnih mjera zaštite je i ometanje, koje u poslednje vrijeme bilježi sve bolje rezultate uz relativno nisku cijenu implementacije.

Za TEMPEST certifikovanje sistema kojim se obrađuju tajni podaci propisana je upotreba tri mjere TEMPEST zaštite i to: oklopljena prostorija, oklopljen uređaj i zoniranje. One su ujedno i najskuplje rješenje. Obzirom da većina TEMPEST standarda nosi stepen tajnosti, nije moguće jasno zaključiti zašto se ne primjenjuju jeftinije mjere zaštite. Kako bi se postigla optimalna i jeftinija TEMPEST zaštita potrebno je i druge TEMPEST mjere zaštite propisati standardom. Naučnicima bi veoma koristio pristup tajnim dokumentima koja definišu ovu oblast kako bi dali svoj maksimalan doprinos.

5. ZAKLJUČAK

Kada pominjemo TEMPEST gotovo uvijek se misli na zaštitu tajnih podataka koji se obrađuju u informaciono komunikacionim sistemima. U vremenu široke upotrebe informacionih tehnologija, bezbjednost informacija je na prvom mjestu. Kompromitujuće elektromagnetno zračenje nastavlja da bude veoma interesantno za naučnike, iako ovo polje nije u dovoljnoj mjeri istraženo u dostupnoj literaturi. Visoki troškovi fizičke zaštite prostora i opreme kao i stalno povećanje takta frekfencije modernih računara koje uzrokuju veće zračenje, ukazuju da ovaj problem neće biti lako riješen. Ukupnu situaciju pogoršava pojava jeftinog softvera koji na univerzalnim radio prijemnicima vrši demodulaciju i rekonstrukciju primljenog signala. Savremena tehnologija omogućava nisko budžetnim napadačima sprovođenje sofisticiranih TEMPEST napada koji su ranije bili mogući samo sa naprednom i skupom opremom. U ovom radu je prikazan kratak istorijski osvrt na razvoj TEMPEST napada, prikazani su najpoznatiji TEMPEST napadi, izvršena je poredbena analiza poznatih TEMPEST mjera zaštite i date preporuke za njihovo korišćenje.
TEMPEST oblast je veoma široko polje za dalje istraživanje. Posebnu pažnju treba posvetiti jeftinijim mjerama TEMPEST zaštite kao što su ometanje i soft TEMPEST tehnike.

4. LITERATURA

[1] Y. Suzuki, M. Masugi, K. Tajima, and H. Yamane: *"Countermeasure Technique for Information Leakage by the Electromagnetic Emissions from Personal Computers"*, Annual meeting IEE Japan, Symposium 1-S2-8, Fukuoka, 2008,
[2] THE COUNCIL OF THE EUROPEAN UNION, "COUNCIL DECISION on the security rules for protecting EU classified information", Official Journal of the European Union, 2013
[3] Kuhn M: *"Compromising emanations: eavesdropping risks of computer displays"*, 2003,
[4] Highland J. Harold: *"Electromagnetic Radiation Revisited"* Computers & Security vol 5, 1986,
[5] Kristian Beckman, "*L¨ackande Datorer [Leaking Computers]"*. Štokholm, 1984
[6] van Eck "*Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*", 1985
[7] E.Möller, L.Bernstein, F.Kolberg: "*Protective Measures Against Compromising Electro Magnetic Radiation Emitted by Video Display Terminals*". Labor f¨ur Nachrichtentechnik, Aachen
[8] Peter Wright: "*Spycatcher*", Heinemann (Australia), str. 109-112,1987
[9] Peter Smulders: "*The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables*", Computers & Security vol 9, 1990
[10] Markus G. Kuhn: "*Electromagnetic Eavesdropping Risks of Flat-Panel Displays*", 4th Workshop on Privacy Enhancing Technologies 2004
[11] M.Kuhn, R.Anderson: "*Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations"*, 2004
[12] Robert Callan, Alenka Zajic, Milos Prvulovic: "*A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events*", 2015,
[13] https://www.youtube.com/watch?v=2OzTWiGl1rM, pristupio dana 18.05.2015. godine
[14]H. Tanaka, O. Takizawa, and A. Yamamura: "*Evaluation and Improvement of the Tempest Fonts*" Information Security Applications, Lecture Notes in Computer Science, Vol. 3325, 2005.
[15]Y. Suzuki, M. Masugi, H. Yamane, K. Tajima: "*Countermeasure Technique for Preventing Information Leakage Caused by Unintentional PC Display Emanations*", International Symposium on Electromagnetic Compatibility, Kyoto, 2009