Sigurnost hardvera

Sadržaj

- Uvodne napomene
- Kompromitujuće elektromagnetno zračenje
- Sigurnost smart kartica

Uvodne napomene

Da li je sigurnost softveskih rešenja dovoljan uslov?

- Veoma dobra softverska rešenja propisno projektovana i instalirana mogu, ipak, da se pokažu kao loša rešenja zaštite.
- Moguće je da dođe do nekontrolisanog odliva informacija putem:
  - elektromagnetnog zračenja,
  - indukcijom,
  - vibracijom.

Kompromitujuće elektromagnetno zračenje

Šta je kompromitujuće elektromagnetno zračenje (KEMZ)?

- Pojam se odnosi na sprečavanje nekontrolisanog odliva informacija preko indukovanih ili emitovanih elektromagnetnih signala.
- Vojni krugovi ulažu velike napore u sprečavanju odlivanja podataka sa računarske i druge elektronske opreme putem RF emitovanja.

Kompromitujuće elektromagnetno zračenje

Kako pojedini korisnici opreme gledaju na KEMZ?

- Većina korisnika elektronske opreme ne pridaje velike značaj KEMZ-u.
- Međutim, vojne organizacije troše podjednako na kriptografiju i na sprečavanje KEMZ-a.
- Industrija Smart kartica je takođe predmet napada preko analize naponskih signala i rekonstrukcije čuvanih podataka (npr. ključeva) na ovaj način.
- Napadač treba da “natera” vlasnika kartice da karticu postavi u prilagođen adapter koji će analizom napajanja u malom broju transakcija doći do tajnih podataka.
  - Nema tragova napada.

Kompromitujuće elektromagnetno zračenje

Neki primeri iz prošlosti.

- Krajem 19. veka je primećena pojava preslušavanja između dve telefonske žice.
- 1914. primećen odliv informacija preko telefonskih žica koje su povezivale vojne jedinice na frontu.
- 1960. u Britaniji je korišćen sistem za detekciju zračenja oscilatora TV prijemnika, s namenom kontrole plaćanja TV pretplate.
- 1960. MI5 je upozorio Britanskog ambasadora da se uz šifrat prenosi i dodatni signal (otvoreni tekst).

Kompromitujuće elektromagnetno zračenje

Neki primeri iz prošlosti.

- Do sedamdesetih godina prošlog veka godina ovo nije bila javna tema.
- 1985. Wim van Eck, danski istraživač, objavio je rad koji objašnjava kako može da se rekonstruše slika sa monitora na osnovu KEMZ-a.
- 1996. Markus Kuhn je objavio da mnoge smart kartice mogu da se analiziraju preko napona napajanja CPU.
- 2000. prikazan je napad na smart kartice pomoću malih senzora EM polja postavljenih u neposrednoj blizini kartice.
- Pokazano je da mnogi kriptosistemi mogu da se “razbiju” preciznom merenjima EM zračenja, napona napajanja, itd.

Kompromitujuće elektromagnetno zračenje

Problem.

- Jedan od ciljeva sigurnosti informacionih sistema je sprečavanje neautorizovane strane da dođe do poverljivih podataka.
- Svi računari stvaraju EM zračenje u radio frekvencijskom (RF) domenu.
  - To zračenje može da se detektuje odgovarajućim uređajima.
  - Ako napadač u tome uspe, može da dođe do važnih informacija.
- EM zračenje u RF domenu predstavlja neželjeni komunikacioni kanal koji često nije pod kontrolom vlasnika informacija.

Kompromitujuće elektromagnetno zračenje

Poreklo problema.

- EM zračenje je posledica promene jačine struje u provodniku.
- Ako struja menja jačinu, menja se i jačina EM polja.
- Ako se u promenljivom EM polju nalazi strujni provodnik, u provodniku će se indukovati struja proporcionalna brzini promene EM polja.
- Promenljiva struja $\rightarrow$ promenljivo EM polje $\rightarrow$ indukcija u drugom provodniku.

Kompromitujuće elektromagnetno zračenje

Poreklo problema – signali.

- **Video signali**.
  - Koriste se za prenos slike (npr. TV) i nose informaciju o intenzitetu (boji) svakog piksela na ekranu.
  - Skup ovih informacija daje sliku.
  - Svako ko može da primi video signal i ima odgovarajući monitor, može da prikaže originalnu sliku.
- **Serijski podaci**.
  - Podaci se često prenose kao niz bita, što predstavlja promenu struje u provodniku.
  - Promena struje $\rightarrow$ stvaranje EM polja.
  - Ako neko registruje promenu EM polja, znaće promenu struje, samim tim i sadržaj signala.

Kompromitujuće elektromagnetno zračenje

Poreklo problema - signali.

- **Spektar signala**.
  - Bilo koji signal može da se predstavi kao suma sinusnih signala različitih frekvencija, amplituda i faza.
  - Predstavljanje signala u frekvencijskom domenu se naziva spektar signala.
  - Usled različitih uzroka, osnovni spektar signala može da se translira u viši frekvencijski opseg i da se nađe u radio frekvencijskom delu spektra.
- **Putevi EM zračenja**.
  - EM zračenje ne mora da bude direktno.
  - EM zračenje može da se indukuje u različitim delovima opreme i da se odatle emituje.
  - EM zračenje može da se indukuje i izvan opreme, npr. u vodovima za napajanje, spojnim kablovima, itd.

Kompromitujuće elektromagnetno zračenje

Prijem EM zračenja.

- Za prijem direktnog zračenja je neophodna antena.
  - Karakteristike antene treba da su takve da omogućavaju prijem RF signla odgovarajućeg frekvencijskog opsega.
  - Snaga signala i frekvencijski opseg signala bitno utiču na izbor opreme napadača.
- Kod detekcije signala koji su indukovani u linije za napajanje, postupak detekcije je jednostavniji a oprema često jeftinija.
- Za prijem video signla, koji se pojavljuju u frekvencijskom opsegu od 20MHz do 200MHz sa spektrom širine 5MHz, tehničko rešenje može da bude još jednostavnije.

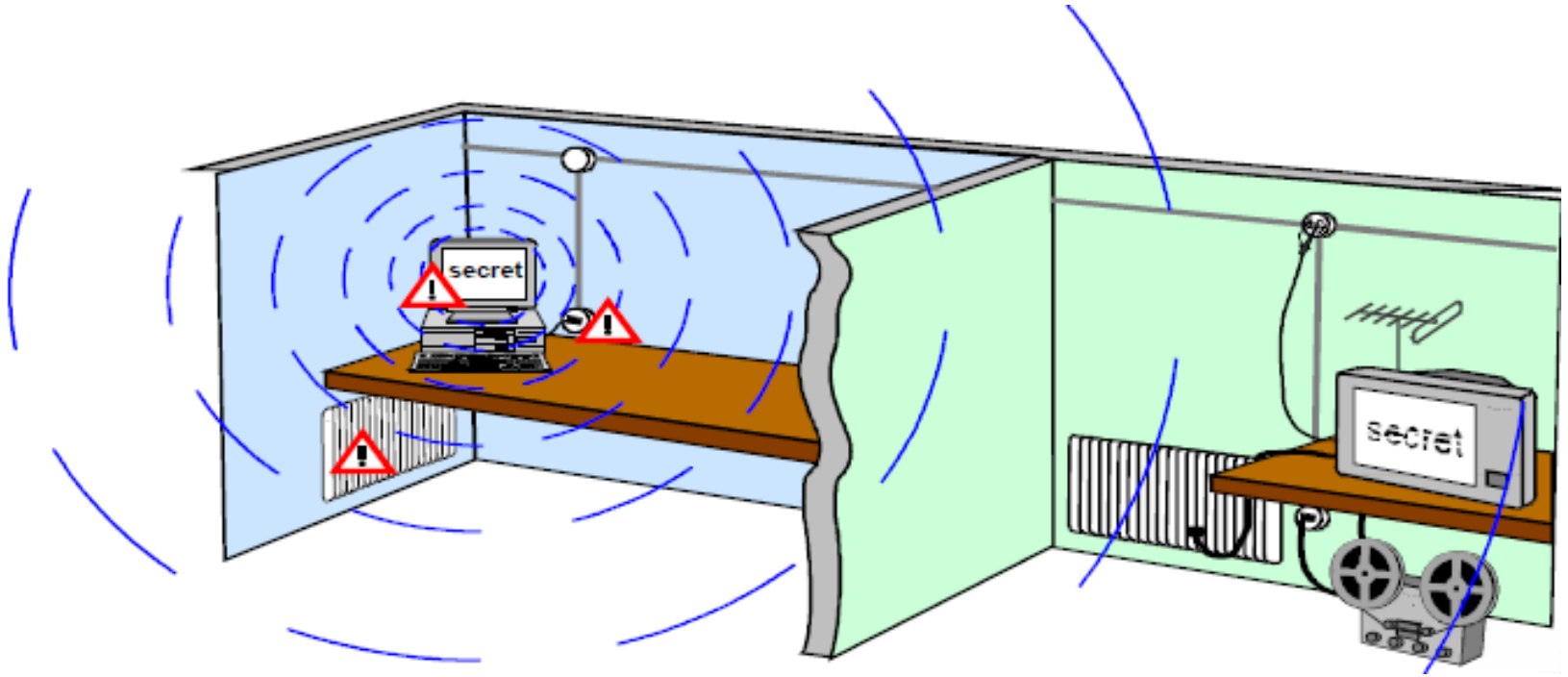
Kompromitujuće elektromagnetno zračenje

Video signali.

- Svi uređaji za prikaz slike emituju (slabe) TV signale (VHF ili UHF) modulisane sa slikom koja se prikazuje, osim ako su namenski razvijeni da do ovoga ne dođe.
- Uz odgovarajuću opremu ovi signali mogu da se detektuju i rekonstruišu.
- Suprotno ustaljenom mišljenju, LCD displeji takođe emituju KEMZ.

Kompromitujuće elektromagnetno zračenje

Primer KEMZ.



Kompromitujuće elektromagnetno zračenje

Odbrana.

- Rešenje se svodi na smanjenje intenziteta EM zračenja na nivo električnog šuma koji je prisutan u opremi ili u okruženju.
- Ovo se može postići na više načina:
  - razdvajanjem opreme,
  - povećanjem rastojanja od napadača,
  - maskiranjem,
  - korišćenjem dodatne opreme,
  - posebnom konstrukcijom uređaja.

Kompromitujuće elektromagnetno zračenje

Odbrana.

- **Razdvajanje opreme**.
  - Razdvojiti opremu na kojoj se nalaze poverljivi podaci (otvoreni tekst) od one koja služi za slanje (šifrat).
  - U praksi je ovo veoma teško, krito-sistemi su upravo suprotan primer.
  - Neophodne su dodatne mere.

Kompromitujuće elektromagnetno zračenje

Odbrana.

- **Povećanje rastojanja od potencijalnog napadača**.
  - Dobre strane:
    - jednostavan i jeftin metod,
    - snaga EM zračenja opada sa kvadratom rastojanja.
  - Loše strane:
    - nije rešenje za indukovane signale u npr. naponskim vodovima, cevima za ventilaciju, itd.,
    - dodatni problem se stvara ukoliko napadač na neki način sakrije prijemne uređaje u blizinu uređaja.

Kompromitujuće elektromagnetno zračenje

Odbrana.

- **Maskiranje**.
  - Što je više signala prisutno u spektru, napadaču je teže da izdvoji onaj od interesa.
  - Postoje komercijalni uređaji koji mogu da generišu ometajuće signale željenog frekvencijskog opsega i snage.
  - Potrebno je da se signali spektralno preklapaju.
  - Postoji etički (zakonski) problem kod emitovanja ometajućih signala.
  - Maskiranje ipak nije garancija za odbranu, zato što može samo da oteža posao napadaču.

Kompromitujuće elektromagnetno zračenje

Odbrana.

- **Posebna oprema**.
  - Postoje dva načina da se spreči neželjeno EM zračenje opreme:
    - dizajnirati uređaj na takav način da se EM zračenje svede na minimum,
    - oklopiti već gotov uređaj.

Kompromitujuće elektromagnetno zračenje

Odbrana.

- **Dizajn sigurnog uređaja**.
  - Metal na putu EM zračenja izaziva njegovo slabljenje (oko 30dB).
  - Oklapanjem se može postići slabljenje i do 120dB.
  - Potrebno je:
    - staviti filtre na linije za podatke i linije za napajanje kako bi se “prigušile” viskoko frekvencjekse komponente,
    - napraviti linije za masu tako da imaju što veću površinu i da se prostiru po svim delovima štampane ploče,
    - podeliti delove uređaja po funkcionalnosti i posebno oklopiti (metalnom kutijom) svaki blok,
    - filtrirati vodove koji spajaju pojedine funkcionalne blokove.
  - Poseban problem predstavljaju ekrani (metalizacija), otvori za ventilaciju, dugmad i tasteri, itd.

Kompromitujuće elektromagnetno zračenje

Odbrana.

- **Dizajn sigurnog uređaja**.
  - Materijali za oklapanje – preporučuje se upotreba aluminijuma i čelika.
  - Spojevi – preporuka je da svi spojevi na metalnim kutijama budu kontinualni (vareni, lemljeni, itd.)
  - Otvori (rupe) potrebni za tastere, potenciometre, itd. predstavljaju put za RF talase – treba ih svesti na minimum i koristiti namenske tastere (prekidače, itd.) posebno dizajnirane za ovu svrhu.

Kompromitujuće elektromagnetno zračenje

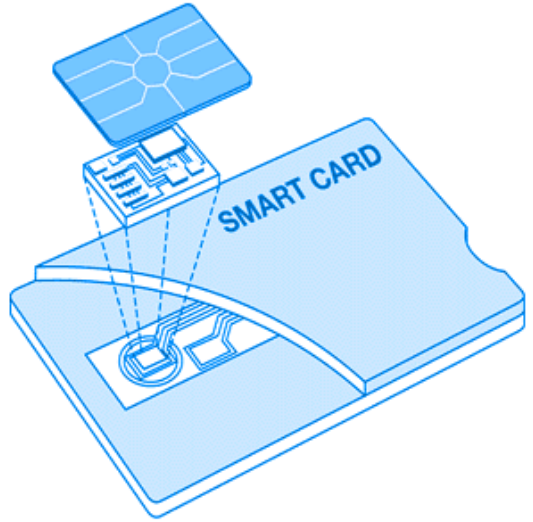
Odbrana.

- **Dizajn sigurnog uređaja**.
  - Oprema često treba da se otvori: popravka, izmena komponenti, podešavanja, itd.
  - Delovi koji se otvaraju, treba da imaju metalne kontakte otporne na fizička izobličenja i elastična svojstva.

Smart kartice

Šta su smart kartice?

- Smart kartice su plastične kartice veličine bankarske kartice sa ugrađenim čipom.
- Postoje dva osnovna tipa:
  - sa memorijskim elementima,
  - sa mikroprocesorom.
- Mogu biti:
  - kontaktne,
  - bezkontaktne.
- Imaju operativni sistem.



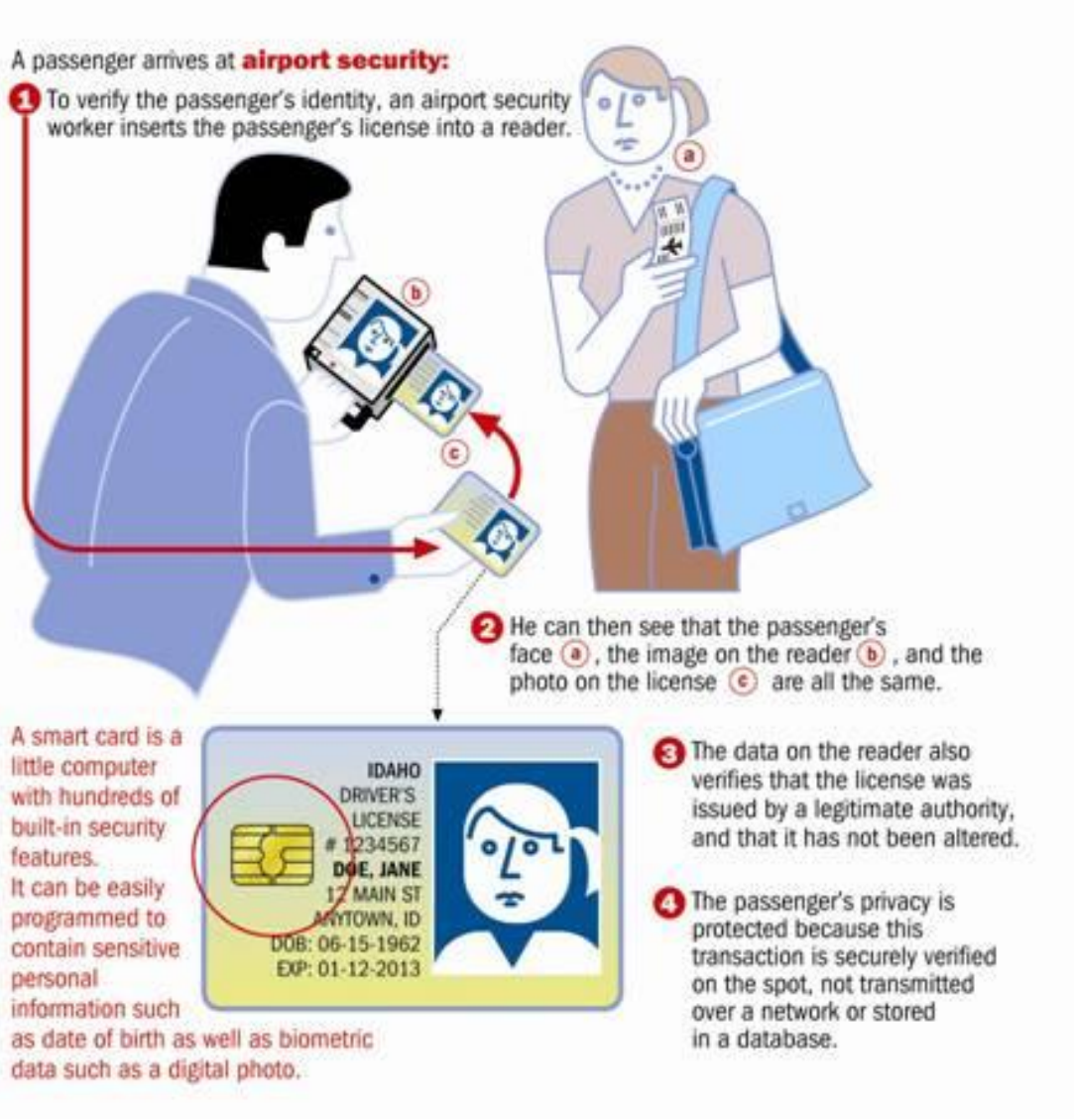
Smart kartice

Prednosti smart kartica.

- Smart kartica može da čuva mnogo više informacija nego magnetna kartica, a informacije mogu lako da se ažuriraju.
- Magnetne kartice su osetljive na različite napade.
- U smart kartice mogu da se implementiraju različiti kriptografski algoritmi.
- Jedna smart kartica može da se koristi za više različitih aplikacija (e-novčanik, identifikacija, kontrola pristupa, itd.)
- Smart kartica može da obezbedi trostuku autentifikaciju:
  - PIN (nešto što zna),
  - posedovanje (nešto što ima) i
  - biometrija (nešto što jeste).

Smart kartice

Primer upotrebe.



Smart kartice

Sigurnost smart kartica.

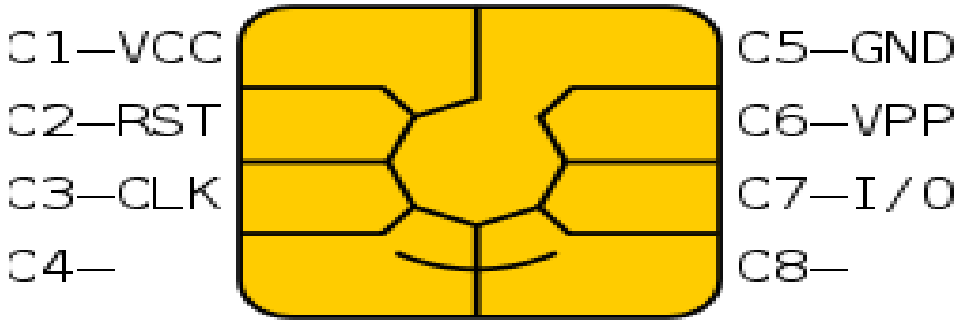
- Impelemntirani PKI algoritmi (3DES, RSA ECC).
- Mogućnost generisanja parova ključeva.
- 0.6 mikronske komponente.
- Podaci koji se čuvaju na kartici su šifrovani.
- Moguće je blokirati karticu usled višestruke greške kod unosa PIN-a.

Smart kartice

Sigurnost smart kartica.

- Poverljivost se postiže šifrovanjem podataka na smart kartici.
- Autentifikacija je obezbeđena primenom PKI i trofaktorskom autentifikacijom.
- Integritet se postiže ugrađenim mehanizmima za kontrolu greške.
- Svaka transakcija se autentifikuje i može da se beleži tako da je obezbeđena i neporecivost.

Signali.



- VCC – osnovno napajanje.
- RST – reset, može biti eksterni ili interni.
- CLK – signal takta.
- GND – referentni napon (masa).
- VPP – napon programiranja.
- I/O – linija za prenos serijskih podataka u/iz kartice.

Smart kartice

Napadi na smart kartice.

- Postoji nekoliko tipova napada.
- Napad na protokol.
  - Više primera iz naplate TV.
- Zabrana promene sadržaja EEPROM-a.
  - Čuvaju se ključevi i brojači (e-novčanik, npr.)
  - Ukinuti napon VPP (prekriti PIN na kartici).
  - Onemogućava se blokiranje kartice.
  - Ne može se promeniti stanje brojača.
  - Rešenje: generisati VPP interno iz napona napajanja VCC.
  - Nije potpuno sigurno.

Smart kartice

Napadi na smart kartice.

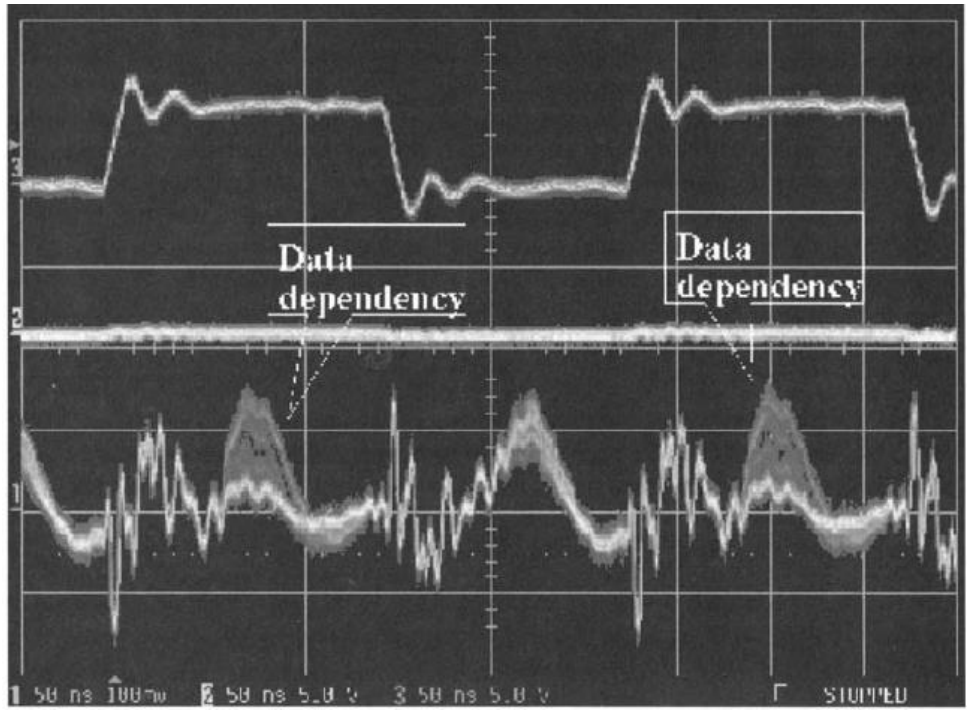
- Usporavanje frekvencije rada kartice.
  - Moguće je, u nekim slučajevima pročitati sadržaj RAM-a nakon reseta.
  - Rešenje: detekcija frekvencije rada i blokiranje rada kartice.
  - Problem: verovatnoća lažnog alarma.
- Analiza fizičkih karakteristika čipa.
- Oštećenje vitalnih komponenti čipa.
  - Instrukcijski dekoder, npr, i izvršvanje instrukcija po želji.

Napadi na smart kartice.

- **Napad analizom napona napajanja**.
  - Različite instrukcije zahtevaju različitu potrošnju.
  - Zahtev za napajanjem je takođe uslovljen sadržajem podataka koji se obrađuju.
    - U zavisnosti od dizajna, jačina struje može da se menja i za nekoliko stotina mikro-ampera u toku milisekunde za svaki bit koji menja vrednost.
    - Čitanje i pisanje u EEPROM može dati i dodatne informacije.
    - Napad je neinvazivan.
    - Moguće ga je realizovati u čitaču kartica (“prodavca”).

Napadi na smart kartice.

- Primer promene napona napajanja sa promenom vrednosti signala.



Literatura

1. M. Stamp (2006): *Information Security*. John Wiley and Sons.

Hvala na pažnji

Pitanja su dobrodošla.