

TRENDOVI PRIMENE I NOVE PRETNJE SIGURNOSTI SMART KARTICA

Docent dr Dušan Bulatović, Informatika ad, Beograd
email: dusanb@informatika.com

Apstrakt: *Finansijske institucije i komercijalne firme koriste smart kartice za smeštaj poverljivih informacija i uzdaju se, kao i korisnici tih kartica, u njihovu sigurnost. Ovaj rad daje pregled mogućih napada na smart kartice i cilj mu je da ukaže da se deklarirana sigurnost smart kartica mora uzeti sa rezervom. Neophodno je unaprediti postupak testiranja pouzdanosti smart kartica, a aplikacije koje ih koriste ne bi smele biti tako projektovane da njihova celokupna bezbednost zavisi od bezbednosti individualne kartice .*

USAGE TRENDS AND NEW THREATS TO SMART CARDS SECURITY

Abstract: *Financial institutions and commercial companies are relying on smart cards security, as well as end user do. This paper will give a survey of possible attacks on smart cards, and its intention is to show that declared smart cards security must be taken with reserve. Testing procedures of smart card security should be improved, and application security should not depend on security of an individual card.*

1. UVOD

Stotine miliona smart kartica se koriste danas u hiljadama aplikacija koje uključuju mobilnu telefoniju, plaćanje TV programa, kontrolu pristupa računarima, skladištenje medicinskih informacija, identifikacione kartice, kreditne kartice itd. Ove kartice se po pravilu koriste za izvršavanje kriptografskih transformacija što se izvode pod kontrolom tajnih ključeva ugrađenih u njihovoj zaštićenoj memoriji. Cilj napadača jeste da izvuče ove tajne ključeve iz fizički zaštićene kartice, u cilju da se modifikuje sadržaj kartice, da se kreira duplicirana kartica, ili da se generiše neautorizovana transakcija.

Smart kartice su po pravilu jeftine, pogodne za korišćenje, sa malom količinom memorije, nekim osnovnim kompjutacionim mogućnostima i određenim ulazno/izlaznim portovima preko kojih dobijaju napajanje i sinhronizacione impulse (clock).

U idealnom slučaju kartice su otporne na svaki pokušaj pristupa njihovom sadržaju (tamper-proof) izuzev preko dozvoljenog pristupa kriptografskim operacijama putem ulazno/izlaznog porta, tako da tajni podaci iz memorije kartice ne mogu biti izvučeni. Napadač može biti neko ko je ukradio smart karticu, njen legitimni korisnik, ili neko ko pokušava da pristupi kartici putem portova. U praksi je bilo mnogo uspešnih pokušaja napada na smart kartice. Evo nekih primera scenarija korišćenja smart kartice i šta može da bude posledica ukoliko je kartica kompromitovana i njen zaštićeni sadržaj otkriven:

- Banka proverava autentičnost korisnika na bankomatu, ili trgovac proverava identitet korisnika kreditne smart kartice. Smart kartica čuva tajni ključ korisnika i učestvuje u protokolima provere autentičnosti korišćenjem specifičnih kriptografskih operacija. Jedna od pretnji je da napadač ukrade smart karticu i pokuša da dođe do tajnog ključa legitimnog korisnika sa ciljem da podigne novac sa njegovog računa. Drugi rizik je da maliciozni bankomat u interakciji sa karticom pokuša da dođe do ključa.
- Kod plaćanja TV programa sirovi TV signal se enkriptuje a smart kartica sadrži tajni ključ i kôd algoritma za dekripciju. Na ovaj način je moguće lako i na jeftin način menjati ključ i algoritam za dekripciju. U ovom slučaju i korisnik kartice može biti napadač pa sam poželeti da dopre do tajnog ključa sa svoje kartice. Ovo bi mu omogućilo da prodaje klonirane kartice na crnom tržištu, što se u praksi i dešava i takve kartice je moguće nabaviti.

Razlikuju se dva tipa napada na kartice:

1. Aktivni napadi, u kojima čip sa smart kartice može biti izvučen, modifikovan, premeravan i delimično uništen, ili korišćen u neuobičajenom okruženju. Aktivni napad ostavlja jasno vidljive znake napada, pa se zato ovakav napad obično izvodi na ukradenim karticama ili u situacijama kada sam vlasnik kartice želi da naruši njenu sigurnost. Ovakvi napadi obično obuhvataju napade izazivanjem greške, testiranje merenjem, mikrohirurgiju čipa pomoću fokusiranog jonkog zraka itd. Oni obično zahtevaju značajno vreme, sofisticirane uređaje i detaljno poznavanje fizičkog dizajna čipa. Ovakvi napadi su izuzetno moćni u otkrivanju informacija o smart card sistemu ali se zbog svoje cene retko koriste da bi se došlo do tajnih podataka nekog individualnog korisnika.

2. Pasivni napadi u kojima kartica može biti samo eksterno posmatrana za vreme njene normalne interakcije sa (eventualno modifikovanim) čitačem smart kartice. Ovakav napad se preferira kada je vlasnik smart kartice zainteresovan u očuvanju njene bezbednosti, naprimer, kod finansijskih aplikacija. U slučaju otkrivenih zloupotreba tog tipa smart kartica se od strane vlasnika vraća onome ko je izdao karticu na ispitivanje. Pasivni napadi uključuju, vremenski napad, napad impulsima napona ili signala i analizu napajanja. Ovi napadi zahtevaju minimalno investiranje i relativno malo poznavanje kartice, a mogu da se izvedu prema velikom broju smart kartica korišćenjem malog broja modifikovanih čitača kartica.

Što se tiče napadača i oni se mogu klasifikovati pa se prema IBM taksonomiji razlikuju tri klase napadača i to:

Klasa I (vešti autsajderi)

Ovi napadači su često veoma inteligentni ali možda nemaju dovoljno znanja o sistemu. Oni imaju pristup samo umereno sofisticiranim uređajima i alatima. Najčešće pokušavaju da iskoriste neku poznatu slabost sistema ali ne pokušavaju da i sami generišu novu.

Klasa II (Insajderi sa tehničkim znanjem):

Ovi napadači imaju značajno tehničko i specijalističko obrazovanje i iskustvo. Oni imaju različite stepene poznavanja delova sistema ali imaju pristup najvećem delu takvih informacija. Često imaju veoma sofisticirane alate i instrumente za analizu.

Klasa III (Organizacije sa velikim fondovima):

Ovakve organizacije mogu da sakupe timove specijalista sa komplementarnim znanjem, podržanim značajnim novčanim resursima. U stanju su da naprave iscrpnu analizu sistema, projektuju sofisticirane napade i koriste najsavremenije alate za analizu. Mogu da koriste i napadače iz klase II kao deo tima.

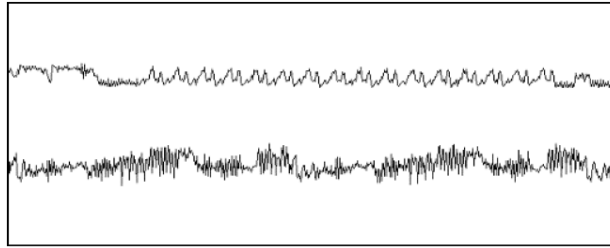
Kritično pitanje kod napada na smart kartice je da li napadač ima nenadgledani pristup kartici. Ako je odgovor ne, tada relativno jednostavne mere mogu biti dovoljne. Ali, u sve većem broju aplikacija oponent može imati potpuno nenadgledan pristup i to ne samo jednoj kriptografskoj kartici nego na više njih. Zato su takvi sistemi u praksi i meta sve većeg broja dobro pripremljenih napada.

2. ANALIZA NAPAJANJA KARTICE

Analiza napajanja kartice je pasivni napad, veoma laka je za izvođenje a veoma teško ju je izbeći. Ona se bazira na zapažanju da detaljna kriva potrošnje napajanja od strane tipične smart kartice, (koja predstavlja kako se spoljna struja napajanja menja tokom vremena), sadrži veliku količinu informacija o operacijama koje se izvode na kartici. Sa dovoljno osetljivim uređajima za merenje moguće je posmatrati egzaktnu sekvencu događaja (u formi pojedinačnih strujnih kola koja se otvaraju ili zatvaraju) za vreme izvršavanja mikro koda svake instrukcije. Naprimera, profili potrošnje struje operacija sabiranja i množenja su potpuno različiti, a i potrošnja napajanja kod upisivanja jedinica ili nula u memoriju takođe se može registrovati, tako da je moguće, naprimera, vizuelno dobiti tajni ključ RSA operacije na osnovu toga što se zna kada se izvodi modularno kvadriranje a kada modularno množenje. Razlikuju se dve varijante ove vrste napada i to **prosta analiza napajanja** i **diferencijalna analiza napajanja** (Simple Power Analysis – SPA i Differential Power Analysis – DPA).

2.1 Prosta analiza napajanja

Ideja izvođenja ovog napada je jednostavna i sastoji se u pasivnom posmatranju potrošnje kartice tokom vremena i zaključivanja na osnovu tog posmatranja o operacijama koje se izvode na kartici. Naprimera DES ima 16 rundi i kriva potrošnje struje će pokazati 16 ispupčenja. Svaka runda koristi različiti deo tajnog ključa. Smeštanje bita 1 u registar ima različitu potrošnju struje od smeštanja bita 0. Na osnovu toga amplituda ispupčenja na krivoj potrošnje će dati mnogo informacija o korišćenom tajnom ključu a ponekad i ceo ključ.



Slika 1. Kriva napajanja kartice

Slika 1 prikazuje krivu napajanja kartice prilikom izvođenja jedne DES operacije. Gornja kriva prikazuje celu DES operaciju, uključujući inicijalnu permutaciju, 16 DES petlji i konačnu permutaciju.

Kod RSA i Diffie-Helman baziranih kriptosistema takođe je moguće izvesti jednostavan napad. U ovim sistemima se najčešće dati podatak c podiže na stepen d modul n , gde je d tajni ključ. Algoritam eksponenciranja je po pravilu "ponavljano kvadriranje" koji ispituje bitove ključa d i uslovno ih množi sa akumulatorom, a potom kvadrira akumulator:

```
// compute  $c^d \bmod p$ , for  $d \geq 0$ 
exponentiate( $c, d, p$ ):
    total = 1
    s = c
    while( $d > 0$ )
        if  $d$  is odd:
            total = total * s
        d = d - 1
        s =  $s^2$ 
        d = d / 2
    return total
```

Svako uslovno množenje u algoritmu predstavlja dodatnu operaciju koja traži ekstra potrošnju napajanja, tako da se tajni podatak d može direktno dobiti analizom napajanja.

Protiv mera koja onemogućava ovakvu analizu može da se sastoji u tome da se obe operacije izvode bezuslovno a da se potom odbacuje nepotrebnii podatak. Operacija odbacivanja uvek ima istu potrošnju napajanja bez obzira na sadržaj podatka koji se odbacuje. Shamir [1] je dao i hardversko rešenje ovog problema kod kojeg se ne mora voditi računa o načinu implementacije algoritma radi izbegavanja pasivne analize napajanja.

2.2 Diferencijalna analiza napajanja

Diferencijalna analiza napajanja (DPA) je mnogo opasnija: napadač analizira mnogo krivih potrošnje napajanja snimljenih prilikom više izvršavanja algoritma sa različitim ulazima i koristi statističku razliku rezultata da na automatski način pronađe bitove ključa.

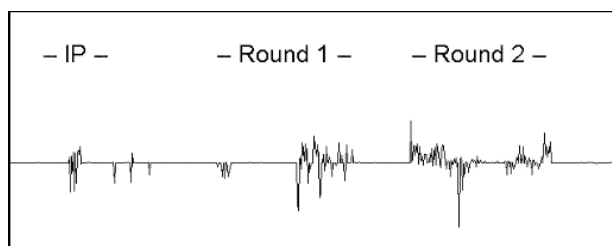
Metod diferencijalne analize napajanja su otkrili Kocher Jaffe i Jun [2]. On može da otkrije tajne podatke i u slučajevima kada su podaci o algoritmu dobijeni putem analize potrošnje napajanja predstavljeni na mnogo manje jasan način. Ideja kod DPA analize se sastoji u tome da se algoritmu koji se izvršava na smart kartici daju različiti ulazi,

naprimer, u samo jednom bitu, i da se posmatra razlika u korišćenju napajanja u dužem vremenskom intervalu.

S obzirom da je kriptografski algoritam poznat napadaču, on može da prati kako se razlika u jednom bitu širi kroz algoritam i vrši interakciju sa delovima tajnog ključa. Korišćenjem statističke analize rezultata velikog broja merenja, može se doći do tajnog ključa. Štaviše, napad se može automatizovati i u opštem slučaju zahteva samo hiljadu uzoraka merenja.

Slika 2 prikazuje razliku u potrošnji napajanja promenom jednog bita izvornog teksta. U inicijalnoj permutaciji (IP) taj bit se unosi u registar a njegov uticaj se oseća na napajanje prve runde algoritma a dosta snažno i druge. Rezultat je dobijen nakon 1000 merenja mada se razlike zapažaju i znatno ranije.

Autori ovog napada su javno objavili da su korišćenjem DPA tehnike uspeli da probiju praktično sve tipove smart kartica korišćenih do tada od strane finansijskih institucija.



Slika 2. Diferencijalna analiza napajanja

2.3 Tehnike zaštite od napada analizom napajanja

Dok se od proste analize napajanja može zaštititi korišćenjem određenih jednostavnih i u opštem slučaju uspešnih protivmera, mnogo je teže zaštititi hardver od DPA napada. Pokušaji da se napravi potrošnja napajanja smart kartice absolutno uniformnom promenom njenog dizajna nije uspeła, jer se i sasvim male razlike napajanja mogu uhvatiti pomoću osetljivog digitalnog osciloskopa. Pored toga, prisiljavanje da se kod svih instrukcija uključi isti broj tranzistora je potpuno neprirodan način koji povećava ukupnu potrošnju i usporava operacije.

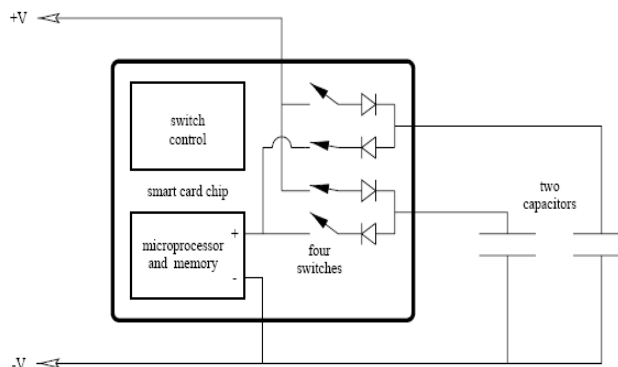
Jedno predloženo rešenje sastoji se u tome da se doda kondenzator na linijama napajanja kartice koji bi ublažio krivu promene napajanja. Međutim, fizičko ograničenje veličine kondenzatora čini i njegov kapacitet nedovoljnim, tako da ostaje dovoljno neuniformnosti napajanja da se DPA napad može izvesti. Jedna slična tehnika bi se sastojala u tome da se čipu smart kartice doda senzor koji bi merio struju napajanja i pokušao da je ujednači napajanjem dodatog opterećenja. Ipak, promene struje napajanja su tako brze da nijedna kompenzaciona tehnika ne može u potpunosti da ih prati i ostaje dovoljno neravnomernosti u napajanju koje su jasno vidljive.

Druge tehnike predlažu korišćenje hardverskih generatora slučajnog šuma, izvršavanje neuobičajenih instrukcija, paralelno izvršavanje više instrukcija i slično. Međutim, hardverski šum se može eliminisati ako se posmatra više krivih napajanja i uzimanjem prosečne vrednosti, a softverske tehnike ne pomažu ako se mogu slediti individualne instrukcije, tako da je efekat i ovih mera ograničen.

Rešenje koje bi podrazumevalo zamenu spoljašnjeg izvora napajanja sa napajanjem kartice pomoću baterije obezbedilo bi da se napajanje ne može meriti izvana. Međutim, debljina kartice je samo 0,76 mm i tako tanka baterija bi bila suviše skupa, trajala kratko vreme, i bila teško zamenljiva tako da ni to ne bi bilo praktično. Alternativna varijanta sa baterijom koja se dopunjava prilikom svakog stavljanja kartice i čitač takođe ima nedostatke jer se takve baterije brzu suše, a kod uobičajenog korišćenja kartice koje

je povremeno i slučajno, dolazilo bi do neprihvatljivo dugog punjenja i već posle nekoliko stotina korišćenja bateriju bi bilo potrebno zameniti.

Shamir [1] je predložio rešenje sa potpunim odvajanjem napajanja od kartice pomoću dva kondenzatora (slika 5).



Slika 3. Smart kartica sa odvojenim napajanjem

Za vreme prve polovine ciklusa kondenzator 1 se puni od spoljnog izvora napajanja, a kondenzator 2 prazni napajajući karticu, a u drugoj polovini ciklusa njihove uloge se menjaju. Ovo rešenje onemogućava DPA napad izvan kartice, ali ako se izvrši fizičko otvaranje čipa i merenja na samom čipu kartice (o takvim tehnikama će biti kasnije više reči), napad bi i dalje bio moguć.

3. DIFERENCIJALNA ANALIZA GREŠKE

Model analize greške je uveden od strane Boneh-a [3] a kasnije je analiziran i od strane drugih. On pretpostavlja da ako se čip izloži niskom nivou jonizujuće radijacije ili nekog drugog uticaja sa sličnim efektom tada generisana greška u jednom bitu može dovesti u kompromitujuće stanje senzitivni materijal, posebno materijal ključa.

Anderson i Khun su u [4] opisali da takav napad može biti uspešno izveden i od strane hakera amatera na, naprimer, kartice za plaćanje TV programa. Ideja je da se na čip primeni brzi tranzijent napona napajanja ili clock-a (clock mnogo uži od normalnog), što će uticati na funkcionisanje samo nekih tranzistora u čipu. Variranjem parametara CPU može biti doveden u stanje da izvršava potpuno pogrešne instrukcije, ponekad čak i instrukcije koje nisu podržane mikro kodom. Mada se ne zna unapred koji će tranzijent izazvati kakvu grešku sistematska analiza grešaka može biti izvedena na relativno jednostavan način.

Tipična sabrutina koja se nalazi u sigurnosnim procesorima je petlja koja piše sadržaj nekog ograničenog memorijskog opsega na serijski port:

```
1 b = answer_address
2 a = answer_length
3 if (a == 0) goto 8
4 transmit(*b)
5 b = b + 1
6 a = a - 1
7 goto 3
8 ...
```

Ideja je da se pronađe tranzijent koji normalno uvećava program counter ali zato transformiše uslovni skok na liniji 3 ili decrement petlje na liniji 6 u nešto drugo. Nakon toga, ponavljajući taj tranzijent, celokupan sadržaj memorije može biti isčitana.

Izlazne petlje su samo jedan od ciljeva napada tranzijentima. Drugi ciljevi mogu biti provera lozinke, prava pristupa, ili sam protokol, gde narušavanje samo jedne instrukcije može u potpunosti poništiti zaštitu. Kada se napad primeni na sam algoritam umesto na kontrolni kôd, može se pokazati kao veoma efikasan, kao što će se videti u nastavku teksta. Napad baziran na unošenje greške u kôd instrukcije je lakše izvodljiv i daje više informacija napadaču nego napad izveden na podacima.

3.1 Napad na RSA algoritam

Jedna od varijanti napada može se odvijati na sledeći način: Pretpostavimo da kartica računa RSA digitalni potpis **S** poruke **M** nad modulom **n = pq**, tako što ga računa nad modulom **p** i **q** odvojeno a potom kombinuje rezultat korišćenjem teoreme kineskog ostatka. Ako se greška unese u bilo koje od zadnja dva računanja tada se **n** može faktorisati praktično odmah. Ako je **e** javni eksponent i ako je digitalni potpis **S = M^d(mod pq)** korektan za modul **p** a netačan za modul **q** tada se **p** lako dobija kao:

$$p = \gcd(n; S^e - M)$$

Ovo je idealna situacija za napad tranzijentom napona ili impulsa. Kako kartica provodi najveći deo vremena u računanju digitalnog potpisa **mod p** i **mod q** to će bilo koji tranzijent koji utiče na rezultat završiti posao; napadač ne mora da pazi da primeni tranzijent selektivno na nekoj izabranoj instrukciji. Digitalni potpis se u komunikaciji koristi samo jedanput, pa ovaj napad može biti izveden i on-line. Unapred pripremljeni terminal, u radnji koja pripada nekome što izvodi napad, može primeniti tranzijent na karticu u momentu plaćanja, faktorisati module, izračunati digitalni potpis kakav stvarno treba da bude i završiti transakciju u realnom vremenu.

Na ovaj način napadači mogu doći do RSA tajnih ključeva a da pri tom ni korisnik kartice niti banka nemaju nikakve podatke koji bi ih upućivali na mesto na kojem je došlo do otkrivanja tajnog ključa. Ako se zna da u prosečnoj implementaciji EMV elektronskog novčanika ima oko 10,000 različitih RSA ključeva po jednoj banci, može se zaključiti da na ovaj način napadači mogu doći u mogućnost da zloupotrebe platne kartice velike populacije korisnika.

3.2 Napad na DES algoritam

Kada je napadač u mogućnosti da izabere instrukciju na kojoj će izazvati grešku primenom tranzijenta, tada se otvara mogućnost nekoliko direktnih napada na DES. Moguće je u zadnjim dvema petljama šifrovanja izbaciti jednu od 8-bit **xor** operacija koje se koriste da kombinuju ključeve petlje sa S tabelama i ponoviti ovaj postupak za sve bajtove ključa. Pogrešni rezultat šifrovanja koji se dobija nakon ovog napada će se razlikovati od originalnog šifrovanog teksta na izlazu obično dva a ponekad tri S box-a. Korišćenjem tehnike diferencijalne kriptanalize moguće je doći do informacije za pet bita od osam bita ključa koji nisu korišćeni u xor operaciji zbog unesene greške. Tako, naprimer, šest šifrovanih tekstova sa pogrešnom zadnjom petljom će dati 30 bita ključa i na taj način učiniti jednostavnim pretraživanje ključa.

Još brži napad je ako se redukuje broj petlji DES-a na jednu ili dve, narušavanjem odgovarajuće varijable ili uslovnog skoka, kao i u napred opisanom napadu na protokol.

Potom se ključ može pronaći isprobavanjem. Praktičnost ovog napada zavisi od detalja implementacije.

Na taj način DES može biti napadnut pomoću jednog do deset poznatih šifrovanih tekstova. Ipak, postavlja se pitanje koliko je realna pretpostavka da se može odabrati za napad izabrana instrukcija?

U većini smart kartica proizvođač daje određeni broj rutina u ROM-u. Mada se nekada predstavlja kao "operativni sistem" kôd ROM-a je pre biblioteka ili aplikacioni kit koji omogućava programeru da kontroliše komunikaciju i ostale funkcije. Ove rutine obično uključuju i DES algoritam i sa kupovinom proizvođačevog smartcard development toolkit-a (obično za cenu od nekoliko hiljada dolara) napadač dobija punu dokumentaciju plus primerke za testiranje tako da je mogućnost napada individualne instrukcije realna.

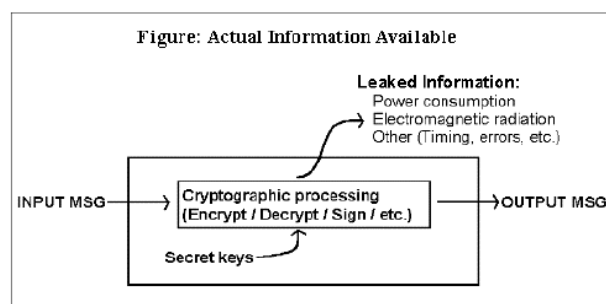
Kada je u pitanju neuobičajena aplikacija potrebno je malo više eksperimentisati (što u svakom slučaju mora da se radi da bi se dobili potrebni parametri tranzijenta koji se primenjuje na karticu. Međutim, prostor za pretraživanje je mali, pa se na osnovu iskustva sa nekoliko implementacija DES algoritma može reći da je uvek moguće prepoznati izbacivanje jedne instrukcije iz bilo koje od zadnje dve petlje.

Tranzijenti napona ili impulsa se uvek mogu primenjivati sve dok prosti statistički testovi iznenada ne pokažu veliku zavisnost ulaznih i izlaznih bita kriptografske transformacije, što je indikacija da je došlo do umanjivanja broja petlji enkripcije. Ovakav pristup može biti praktičan čak i kad nisu poznati detalji implementacije, što ukazuje na zaključak da moguće koristiti ovu tehniku sa ciljem da se izvrši rekonstrukcija nepoznatog algoritma, kao što je Skipjack, bez potrebe za korišćenjem skupih uređaja za testiranje čipa.

4. NAPADI MERENJEM VREMENA ENKRIPCije

Kriptosistemima je najčešće potrebno različito vreme da obrade različite ulaze. Razlozi za to su mnogobrojni i zavise od postojanja grananja ili uslovnih instrukcija u algoritmu, pristupa memoriji, procesorskih instrukcija (kao što su množenje i deljenje) koje se ne izvršavaju u fiksnom vremenu i drugih različitih uzroka. Performansa po pravilu zavisi od ključa i ulaznih podataka (npr, otvorenog teksta ili šifrata). Vremenski kanal daje određene informacije izvan kriptografske kartice koje mogu biti dovoljne da se iskoriste od strane napadača da bi pomoću njih, vršeći merenja na osetljivim sistemima, došao do celog tajnog ključa.

Vremenski napad predstavlja napad izvan kartice (side-channel attack) kao što su to i analiza napajanja kartice ili emitovana elektromagnetna radijacija sa kartice (tempest). Kriptografska naprave (kartica ili token), ne daje samo rezultat kriptografske operacije na svom izlazu, nego su raspoložive i druge informacije koje mogu poslužiti kao osnova za napad (slika 5).



Slika 4. Stvarno raspoložive informacije

Osnovna ideja kod vremenskog (timing) napada jeste da se meri vreme koliko dugo određena kriptografska operacija traje. Svaka kriptografska operacija kojoj je potrebno različito vreme zavisno od upotrebljenih tajnih podataka, potencijalno daje informaciju o tim podacima. Naprimera, RC5 rotira bajtove za određeni broj pozicija koji zavisi od tajnog ključa. Ako smart kartica nema "barrel shifter", operacija rotiranja mora biti izvedena kao skup rotacija za jedno mesto izvedenih u sekvenci. Merenje vremena otkriva broj izvedenih rotacija, koji omogućava otkrivanje tajnog ključa.

Druga mogućnost izvođenja vremenskog napada je na otkrivanje faktorisanje RSA modula $n = pq$. U slučaju uspešnog faktorisanja ovog modula probijena je zaštita RSA algoritma i lako se otkriva tajni ključ. Radi efikasnosti rada, RSA implementacija se najčešće izvodi korišćenjem teoreme kineskog ostatka pa kada se vrši operacija redukovanja podatka y po modulu n , izvodi se tako što se prvo redukuju $y \bmod p$ i $y \bmod q$ a potom dobijeni rezultati kombinuju. Ova inicijalna redukcija po modulu je osetljiva na vremenski napad: izabere se ulaz y koji je blizu broja p , pa se vrši vremensko merenje da se utvrdi da li je y veće ili manje od p (ako je y veće od p vrši se operacija deljenja/oduzimanja). Kada se odredi uži opseg u kojem se nalazi broj p tada se korišćenjem binarnog pretraživanja dolazi do podatka p i otkriva faktorisanje modula n .

Merenje vremena može da se iskoristi i u Diffie-Hellman protokolu razmene ključa ili u punom RSA protokolu. Da bi napad bio izvodljiv, žrtva mora da izvede nekoliko operacija stepenovanja poruke nad modulom, pri čemu napadač, pasivnim prisluškivanjem treba da dođe do poruke koja se stepenuje i vremena potrebnog za stepenovanje. Algoritam eksponenciranja koji je po pravilu "ponavljano kvadriranje" ispituje bitove ključa i uslovno ih množi sa akumulatorom. Na osnovu vremena trajanja svake iteracije može se doći do bita ključa od kojeg u toj iteraciji zavisi da li se izvodi ili ne operacija množenja [5].

Najdirektniji način u sprečavanju vremenskog napada jeste da se napravi da sve operacije traju isto vreme. Nažalost, to je često teško izvesti. Napraviti da softver radi isto vreme pogotovu nezavisno od platforme na kojoj se izvršava, je teško izvesti zbog organizacije kompajlera, tajminga instrukcija i drugih faktora koji unose neočekivane vremenske varijacije. Ako se koristi tajmer da napravi kašnjenje na specifikirano vreme, faktori kao što su odziv sistema ili potrošnja napajanja ipak su promenljivi toliko da ih je moguće detektovati.

Drugi pristup bi bio da se napravi da merenje vremena nije pouzdano i da se tako učini napad neizvodljivim. Slučajna kašnjenja koja bi se dodavala vremenu obrade bi zaista napravila da bude potreban veći broj uzoraka šifrovanog teksta, ali napadač to može kompenzovati povećanim brojem merenja.

Postoje i efikasnija rešenja. Tehnike koje se koriste za dobijanje slepog potpisa [6] mogu se adaptirati da spreče napadača da sazna ulaz za funkciju modularnog stepenovanja. Pre izvođenja operacije modularnog stepenovanja izabere se par brojeva $(v_i; v_f)$ takav da je $v_f^{-1} = v_i^x \bmod n$. Pre modularnog stepenovanja ulazna poruka se množi sa $v_i \bmod n$ da bi se potom rezultat korigovao množenjem sa $v_f \bmod n$. Sistem treba da odbaciti poruke jednake $0 \bmod n$.

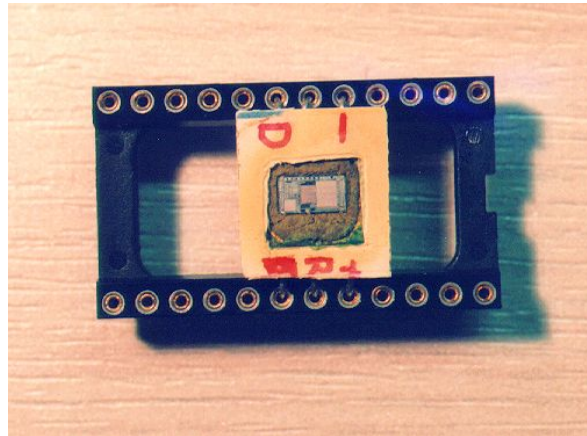
5. HARDVERSKI NAPADI NA KARTICU

Fizička otpornost na napad (tamper resistance) nije apsolutna: oponent koji raspolaže testnim uređajem za poluprovodnike može doći do podataka ključa sa smart kartice direktnom opservacijom i manipulacijom komponenta čipa. Opšte je verovanje da sa dovoljnom investicijom zaštita bilo kojeg uređaja veličine čipa može biti probijena.

Fizički napadi na neke mikrokontrolere su skoro trivijalni. Naprimera, lock bit određenih naprava sa ugrađenim EPROM-om može biti pobrisa fokusiranjem UV svetla na bezbednosnu ćeliju, koja je obično udaljena dovoljno daleko od ostatka memorije.

Savremene smart kartice je nešto teže napasti ali ipak ne suviše teško. One po pravilu imaju malo zaštite koja sprečava direktan pristup silikonu. Obučeni napadač sa velikim budžetom može da uradi mnogo toga. Međutim i napadač iz klase I, korišćenjem raznovrsnih hemijskih tehnika može skinuti epoksi smolu sa čipa, skinuti gornje slojeve zaštite, prekinuti veze ili pristupiti instrumentom direktno na interne veze. Slika 5 prikazuje potpuno funkcionalan mikroprocesor sa smart kartice sa skinutim plastičnim prekrivačem u cilju mikro eksperimentisanja. Alat potreban za ovakvu pripremu čipa je dobijen za 30\$ u apoteci.

Kao što se na slici vidi cela unutrašnjost čipa je izloženu posmatranju i testiranju dok za to vreme čip može da radi normalno. Takav jedan napad je obeshrabrujući: ništa od podataka korišćenih od strane mikroprocesora ne može ostati tajno.



Slika 5. Fizički napad

Korišćenjem naprednijih tehnika napadač iz klase III može skidati jedan po jedan sloj štampe sa čipa, skenirati čip sa snažnim mikroskopom i doći do njegovog celokupnog dizajna. Postoje takođe i manje invazivne metode: pod svetlošću određene talasne dužine silikon postaje transparentan i otkriva metalne veze unutar čipa.

Zaštita od takve vrste napada je veoma teška. U osnovi, veoma je teško sačuvati dizajn čipa od motivisanog oponenta koji ima dovoljno vremena i veliki budžet. Ipak, postoji nekoliko strategija koje mogu napraviti napad težim:

- Postaviti čip u kontejner pod pritiskom i programirati štampana kola da se deaktiviraju ako se oseti gubitak pritiska
- Postaviti veze u epoksi smolu koja obavija čip koje detektuju oštećenje epoksi smole i onemogućavaju čip da radi
- Uključiti mehanizam za samodestrukciju koji detektuje pokušaj fizičkog narušavanja čipa.

Savremena poluprovodnička laboratorija sa uređajima potrebnim za reverzibilni inženjering čipa može koštati milione dolara. Ipak, kao što će se videti u nastavku teksta, postoje napadi na smart karticu koji mogu biti realizovani od strane napadača sa mnogo manjim budžetom.

5.1 Napad na sadržaj čipa

Tamo gde je implementacija algoritma na kartici poznata postoji više načina da se izvuku ključevi sa kartice tako što se dejstvuje na tačno određena kola ili osigurače, ili tako što se nanovo upiše neki sadržaj memorije. Bovenlander [7] je opisao proboj zaštite kartice uz pomoć dve mikro probe sa kojima se premosti osigurač koji je nakon proizvodnje i testiranja kartice predviđen da pregoreva. Potom se ponovo aktivira test

rutina i može se pročitati celokupan sadržaj memorije. Čak i gde ovaj metod nije moguć, memorijske ćelije se ipak mogu uspešno napasti, pri čemu to može biti realizovano sa relativno malim budžetom.

5.2 Napad na sadržaj ROM-a

Pojedini biti u ROM-u mogu biti prepisani korišćenjem laserskog zraka, a tamo gde je implementacija DES-a dobro poznata, može se pronaći jedan bit (ili mali broj bita) sa osobinom da ako se oni promene tajni ključ može biti lako dobijen. Detalji zavise od implementacije ali je sasvim moguće da se uslovna instrukcija napravi bezuslovnom i na taj način broj petlji algoritma redukuje na jednu ili dve. Mogu se takođe progresivno izbacivati instrukcije kao što je exclusive-or ili materijal ključa.

Kada ne postoji kompletna informacija o implementaciji, sadržaj ROM-a se može napasti na drugi način. Naprimer, DES S boksovi u ROM-u mogu biti identifikovani i njihov sadržaj prepisan sa drugim tako da funkcija enkripcije postane linearna transformacija. Nakon toga se ključ može dobiti pomoću samo jednog para šifrovanog i odgovarajućeg nešifrovanog teksta.

5.3 Napad modifikacijom EEPROM-a

Kada se algoritam nalazi u EEPROM-u pomoću dve mikro probe se može setovati i resetovati ciljni bit [8]. Ova tehnika može da se koristi i u prethodnim napadima, ali činjenica da možemo i setovati i resetovati bit otvara još više mogućnosti.

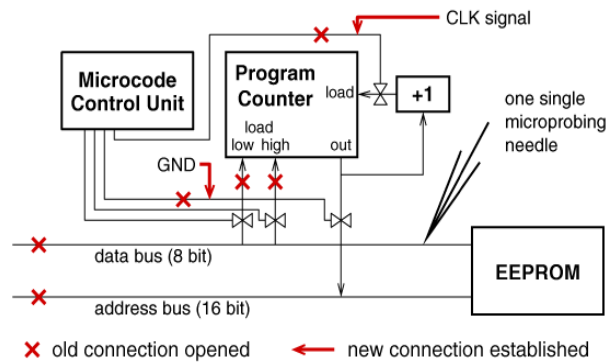
Pošto DES algoritam koristi ključ sa proverom neparne parnosti, ukoliko broj bita ključa nije neparan, korektna implementacija treba da javi grešku. Pretpostavimo da je poznata lokacija DES ključa u EEPROM-u ali mu se ne može pristupiti direktno zbog nedostatka neophodnih uređaja opisanih u [4]. Tada se može napad izvesti na sledeći način. Setuje se prvi bit EEPROM-a na 1 (ili 0, izbor nije bitan) pa ako algoritam i dalje ispravno funkcioniše bit ključa je bio 1. Potom se prelazi na sledeći bit i ponovo proverava funkcionalnost.

Potrebni alat za ovaj napad su dve mikro probe i laserski rezač koji se često mogu naći i u laboratorijama univerziteta, gde im eventualno može i student neovlašćeno pristupiti. Napadači iz klase I mogu ovakve uređaje kupiti za nekoliko hiljada dolara.

5.4 Napad prekidom strujnih kola u čipu

Napadi izvedeni od strane pirata na određene kartice za plaćanje TV programa koristili su radnu stanicu sa fokusiranim jonskim zrakom. Ovaj uređaj može da prekine veze na metalizovanom sloju čipa i da uspostavi nove veze ili slojeve izolacije. Cena ovakvih mašina je nekoliko miliona dolara ali napadači sa niskim budžetom mogu doći do njih tako što ih rentiraju od različitih poluprovodničkih kompanija.

Opremljen sa takvim alatom napadi na smart kartice postaju mnogo prostiji i mnogo moćniji. Tipičan napad pretpostavlja odvajanje skoro celog procesora od ostatka čipa, ostavljajući samo EEPROM i CPU komponente koje mogu generisati pristup čitanjem. Naprimer, programski brojač može biti ostavljen da bude povezan, na takav način da se pristupa memorijskim lokacijama po redu kada se na uređaj primeni clock (slika 6).



Slika 6. Napad prekidom strujnih kola čipa

Kada se to uradi, napadaču je potrebna samo jedna mikro proba ili optička proba da pročita ceo sadržaj EEPROM-a. Ovo omogućava mnogo lakšu analizu programa nego u pasivnim napadima, jer je potrebno samo jedanput izvršiti merenje. Takođe, na taj način se izbegavaju mehaničke poteškoće primene više proba na čip u isto vreme, gde su veze širine, naprimer, reda mikrona.

6. ZAKLJUČAK

Većina napada na smart kartice kao što su side-channel napadi (npr., analiza napajanja ili diferencijalna analize greške), dešavaju se ad hoc, isto kao i preduzimanje kontra mera protiv takvih napada. Takvo stanje nije zadovoljavajuće zato što nikada ne možemo biti sigurni da li su podaci u kartici (ili tokenu) uopšte zaštićeni.

Videli smo da se pomoću jeftinih i široko raspoloživih uređaja, kao što su mikro probe ili laserski rezač, moguće je izvesti napad na površinu čipa, da bi se potom lako dobili podaci o tajnom ključu iz procesora sa smart kartice, za kojeg smo prethodno smatrali da je fizički bezbedan. Pri tome redundantnost ključa kao što je bit parnosti kod DES-a samo olakšava takve napade.

Zbog takvih okolnosti inženjerska praksa treba da bude izbegavanje situacija u kojim proboj sigurnosti na jednom mestu narušava sigurnost čitavog sistema (single points of failure). Ovo je posebno potrebno zbog činjenice da su hardverska otpornost smart kartica i drugih komercijalnih proizvoda bili dugo vremena ne proveravani. Zbog toga se tvrdnje o njihovoj sigurnosti moraju uvek uzeti sa oprezom.

Jedan novi pristup fizičkoj sigurnosti koji uzima u obzir navedene činjenice o sigurnosti smart kartica sastoji se, ne u zahtevu za postizanjem apsolutne zaštite podataka u hardveru, već u obezbeđenju da do određene mere siguran hardver bude korišćen na dokazivo siguran način. U svakom slučaju iskustvo pokazuje da projektovanje sigurnosnih sistema mora da se izvodi sa mnogo pažnje a da pri tome ni njihovo testiranje ne sme nikako da bude zanemareno.

REFERENCE:

1. Shamir: Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies, <http://jya.com/dfa.htm> 2000.
2. P. Kocher, J. Jaffe, and B. Jun, Introduction to Differential Power Analysis and Related Attacks, <http://www.cryptography.com/dpa/technical/index.html>, 1998.
3. D Boneh, RA DeMillo, RJ Lipton, "On the Importance of Checking Computations", preprint, 11/96
4. RJ Anderson, MG Kuhn, "Tamper Resistance - a Cautionary Note", in The Second USENIX Workshop on Electronic Commerce Proceedings (Nov 1996)
5. P. Kocher, "Timing Attacks on Implementations of Dffie-Hellman, RSA, DSS, and Other Systems", Proceedings of Crypto 96, Springer-Verlag, 1996.
6. D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983..
7. E Bovenlander, invited talk on smartcard security, Eurocrypt 97
8. O Kocar, "Hardwaresicherheit von Mikrochips in Chipkarten", in Datenschutz und Datensicherheit v 20 no 7 (July 96).