UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Sašo Moškon

BREZKONTAKTNE PAMETNE KARTICE

Seminarska naloga pri predmetu

Kriptografija in teorija kodiranja 2

Mentor: prof. dr. Aleksandar Jurišić

Ljubljana, 2009

KAZALO

Povzetek

Od sodobne tehnologije pričakujemo učinkovitost, preprosto uporabo in varnost. Brezkontaktne pametne kartice so učinkovite, praktične, nam olajšajo in pohitrijo mnogo vsakdanjih opravkov. Le na področju varnosti bi se dalo še kaj postoriti, je pa tudi na tem področju napredek hiter in viden. Bistvena prednost brezkontaktnih pametnih kartic je njihova hitra in preprosta uporaba. Kartico enostavno približamo terminalu in v sekundi ali dveh je transakcija opravljena. Brezkontaktne pametne kartice nam omogočajo hitro plačevanje, uporabljajo se tudi na smučiščih, pri omejevanju dostopa v stavbe in poslovne prostore, kot vstopnice na prireditvah, v javnem prevozu, ... Žal pa je njihova razširjenost tudi posledica relativno nizke cene (glede na prednosti brezkontaktne tehnologije) in posledično šibkejših varnostnih mehanizmov.

V tej seminarski nalogi si bomo najprej ogledali kako delujejo brezkontaktne pametne kartice, kaj so njihove prednosti in kaj slabosti nato pa se bomo osredotočili predvsem na ranljivosti brezkontaktnih pametnih kartic, napade na njih in na to kako se pred napadi zaščititi. Primerjali bomo brezkontaktne pametne kartice z ostalimi karticami in RFID etiketami.

1 UVOD

Brezkontaktne pametne kartice se vse pogosteje pojavljajo v našem vsakdanu. Tako je zaradi njihove priročnosti, hitrosti in enostavne uporabe. Na smučišču nam omogočajo, da se le približamo terminalu in že se vratca odprejo, javni prevoz lahko ponekod plačamo tako, da približamo denarnico ustrezni napravi, vsakodnevno nam odpirajo vrata poslovnih prostorov, v Ameriki pa jih ljudje že uporabljajo kot kreditne in debetne plačilne kartice. Po podatkih podjetja MIFARE [1], ki si lasti 85% delež trga brezkontaktnih pametnih kartic, je bilo prodanih že več kot milijarda teh kartic. V Ameriki pa je v obtoku več kot 50 milijonov brezkontaktnih plačilnih kartic [2]. Brezkontaktne plačilne kartice sprejemajo na okoli 130.000 plačilnih mestih po vsej Ameriki, zelo dobro so jih sprejeli predvsem v okrepčevalnicah s hitro prehrano.

V drugem poglavju bomo predstavili različne načine uporabe pametnih kartic, njihove prednosti in slabosti. V tretjem poglavju se bomo osredotočili na njihove ranljivosti in nove vrste napadov, ki jih omogoča brezkontaktna tehnologija. V četrtem poglavju bodo predstavljeni nekateri napadi na brezkontaktne pametne kartice. V petem poglavju se bomo osredotočili na protiukrepe, torej na to kako kartice ustrezno zaščititi pred napadi. V šestem poglavju je predstavljena varnostna shema za obrambo pred napadom s ponavljanjem posnete seje in »distance bounding« protokol za obrambo pred napadom s prenosom signala. Sedmo poglavje je namenjeno predstavitvi nekaterih bistvenih razlik med brezkontaktnimi pametnimi karticami in nekaterimi drugimi karticami.

2 BREZKONTAKTNE PAMETNE KARTICE

2.1 Delovanje

Brezkontaktne pametne kartice so pasivne, brez lastnega napajanja. Aktivirajo se šele v bližini terminala, ki oddaja radijske valove. Napajajo jih radijski valovi, ki se na kartici s pomočjo posebnih induktorjev pretvorijo v električno energijo. Ko se kartica aktivira se za komunikacijo s terminalom uporabi RFID (identifikacija z radijskimi valovi) tehnologija. Način komunikacije je od kartice do kartice različen in odvisen tudi od varnostnih protokolov. Nekatere kartice omogočajo, da terminal enostavno prebere podatke iz njihovega pomnilnika, spet druge pa zahtevajo vzajemno avtentikacijo in kriptirano povezavo.

2.2 Prednosti

Bistvena prednost brezkontaktnih pametnih kartic je njihova priročnost in hitrost. Kartice namreč ni potrebno vstavljati v bralnike kartic ampak je dovolj, da jih enostavno približamo terminalu. Brezkontaktne pametne kartice s terminalom komunicirajo s pomočjo RFID

(identifikacija z radijskimi valovi) tehnologije [3]. Signali se torej prenašajo po zraku zato kartica ne potrebuje kontaktov. Ker kartice ni potrebno nikamor vstavljati tudi ni več potrebe po točno določeni obliki. Če upoštevamo še dejstvo, da je velikost čipa brezkontaktne pametne kartice že manj kot 1x1 mm [11], ugotovimo, da jo lahko vgradimo praktično kamorkoli. Tako so že v uporabi plačilne kartice vgrajene v obeske za ključe, ure in mobilne telefone. Posebej zanimivo je kombiniranje plačilne kartice z naprednimi elektronskimi napravami kot je mobilni telefon. Za uporabnika je to praktično saj bi se tako znebili odvečnih kartic v denarnici. Iz varnostnega stališča pa je to dobro, ker ima telefon lastno napajanje in relativno močan procesor, kar bi omogočilo uporabo naprednejših varnostnih rešitev. Lahko bi se uporabljalo računsko zahtevnejše kriptirne algoritme ali celo biometrične metode za identifikacijo uporabnika, kar bi bistveno izboljšalo varnost in omejilo možnosti zlorab.

2.3 Slabosti

Glavna slabost je ta, da komunikacija med kartico in terminalom poteka po zraku. To odpira možnosti za nove napade in olajša nekatere napade, ki so bili uspešni že na karticah s kontakti. Močno olajšano je predvsem prisluškovanje. Omogočeno je tudi nepooblaščeno branje kartic. Ker je za aktivacijo kartice dovolj že bližina terminala, ki oddaja radijske valove, lahko našo kartico napadalec aktivira enostavno tako, da se nam približa. To lahko seveda stori brez naše vednosti. Nato lahko, prav tako brez naše vednosti kartici pošilja različne ukaze in poskuša pridobiti informacije, morda celo tajni ključ. Testi prve generacije plačilnih kartic [4], ki so jih izdali v Ameriki in so temeljile na karticah z magnetnim trakom, so pokazali, da so te kartice zelo ranljive. Na nekaterih je bilo možno celo ponavljanje posnetih transakcij. Podatki, ki jih je napadalec z lahkoto pridobil preko RFID komunikacije (seveda brez vednosti lastnika kartice), pa so uspešno služili za spletne nakupe in nakupe preko telefona.

2.4 Uporaba

Brezkontaktne pametne kartice se uporabljajo za plačevanje javnega prometa, kot uradne in poslovne identifikacijske kartice, dokumenti (elektronski potni list) in kot brezkontaktne plačilne kartice. Uporabljajo se tudi kot vstopnice na športnih prireditvah in koncertih. Po svetu obstaja že kar nekaj sistemov, ki temeljijo na brezkontaktnih pametnih karticah. Taki sistemi so Octopus card v Hong Kong-u, Oyster card v Londonu in T-money v Južni Koreji. Večina takih sistemov je bila sprva uvedena za plačilni promet v javnem prevozu. Kasneje se je uporaba teh kartic razširila še na plačevanje v restavracijah s hitro prehrano, trgovinah, parkiriščih ponekod z njimi celo preverjajo prisotnost pri pouku. Postale so torej univerzalno in priročno plačilno sredstvo. Zanimiv podatek je, da je v Hong Kongu v obtoku 17 milijonov Octopus kartic [5], s katerimi je opravljenih 10 milijonov transkacij dnevno, prebivalcev pa je ''le'' 7 milijonov.

3 NEVARNOSTI SPECIFIČNE ZA PAMETNE KARTICE

Kot že omenjeno je glavna razlika med kontaktnimi in brezkontatktnimi karticami v tem, da pri brezkontaktnih karticah komunikacija poteka po zraku preko radijskih signalov pri kontaktnih pa preko kontaktov. Posledica brezkontaktne komunikacije je večja priročnost takih kartic, saj jih ni potrebno vstavljati v bralnike kartic, dovolj je že da jih približamo. Vendar pa taka komunikacija odpira vrata novim napadom.

3.1 Sledenje

Trgovci bi lahko zbirali podatke o kupcih na nedovoljen način. Pri tem scenariju gre za spremljanje števca transakcij na kartici. Trgovec s spremljanjem tega števca lahko ugotovi ali je bila kartica od zadnjega nakupa uporabljena pri kakem drugem trgovcu. Možno je tudi, da trgovec poleg kartice, ki jo kupec uporabi za plačilo, dostopa do ostalih kartic, ki jih ima kupec v denarnici. Poleg tega pa se namesto črtnih kod vedno pogosteje uporabljajo RFID etikete. Predvsem so pogoste v čevljarski industriji. In čeprav znajo te etikete le pošiljati številko, ki je shranjena v njih, pa delujejo na razdalji tudi do nekaj metrov. Če si trgovec ob nakupu v tabelo zabeleži ID številko čevljev in identiteto kupca, lahko kasneje spremlja tega kupca preko RFID etikete v čevljih.

3.2 Napad s ponavljanjem, napad s prenosom

Pri napadu s ponavljanjem napadalec enostavno ponovi posneto sejo transkacije med terminalom in brezkontaktno pametno kartico. Če obstajajo mehanizmi, ki to preprečujejo (enkratno geslo, izziv-odgovor, timestamp) lahko še vedno uspe nekoliko zahtevnejši napad – napad s prenosom. Ta napad deluje tako, da se signal preko nekega prenosnega medija prenaša od kartice do terminala. Žrtev ima lahko na primer kartico v žepu. Napadalec se postavi poleg žrtve z bralcem kartic. Njegov sodelavec pa stoji ob terminalu z ustrezno opremo za prenos signalov. Signal se preko prenosnega medija prenese od terminala med napadalcema do kartice. Kartica se aktivira in začne komunikacijo s terminalom. Ker sta oba, kartica in terminal, avtentična, bo transkacija uspela. Največja razdalja kartice od terminala, da bo napad še uspešen, je odvisna od latence, ki jo dopušča terminal. Tak napad je bil uspešen na večini brezkontaktnih plačilnih kartic prve generacije [4], izdanih v Ameriki.

3.3 Nedovoljena uporaba podatkov

Napadalec lahko podatke, pridobljene s kartice preko radijskih signalov, uporabi na nedovoljen način. Podatke o imenu imetnika, številki kartice in datumu poteka kartice lahko uporabi za izdelavo kartice z magnetnim trakom ali pa za spletne nakupe, naročila preko telefona in preko spletne pošte.

3.4 Prisluškovanje

Ena izmed ranljivosti brezkontaktne komunikacije med terminalom in kartico je ta, da je komunikacijo zelo lahko prestreči. Komunikacija namreč poteka preko zraka in to omogoča prisluškovanje z ustrezno napravo, postavljeno dovolj blizu. Obstaja več različnih napadov s prisluškovanjem. Lahko le snemamo komunikacijo in iz nje poskušamo ugotoviti kaj koristnega. Lahko tudi sami sprožimo odgovor kartice, tako da se ji strezno približamo s terminalom za komunikacijo z brezkontaktnimi karticami. Možen je tudi »man-in-the-middle« napad, kjer napadalec ne le prisluškuje komunikaciji, ampak sporočila prestreže, spremeni in šele nato pošlje naprej. Kot bomo opisali v naslednjem razdelku sta za reševanje takih težav potrebna vsaj dva ukrepa, avtentikacija terminala in enkripcija podatkov, ki se pošiljajo.

3.5 Prekinitev operacije

Naslednja pomanjkljivost brezkontaktnih kartic je omejeno področje delovanja in nevarnost nenadne prekinitve operacije, ki se trenutno izvaja na kartici. Brezkontaktne kartice so pasivne, torej brez lastnega napajanja. Delovati začnejo šele ko pridejo v elektronsko polje terminala. Seveda se lahko kajhitro zgodi, da kartica ni več v elektronskem polju in se delovanje prekine. Torej je potrebno poskrbeti za robustno zaščito in zagotoviti, da se vse operacije končajo regularno kljub prekinitvi delovanja.

3.6 Denial of service

Z neprimernimi elektronskimi valovi lahko kartice spraznemo ali uničimo. S takim napadom se lahko lotimo lastne kartice in upamo, da bomo s tem razširili njeno uporabnost na funkcije, ki jih nismo plačali.

3.7 Skimming, covert transactions - skrite transakcije

Obstaja več različnih napadov, ki uporabljajo skrite transkacije. Napadalec lahko brez naše vednosti sproži komunikacijo med svojim terminalom in kartico, ki jo imamo na primer v žepu. Lahko tudi namesto ene transkacije, katere se zavedamo, izvede več transkakcij ali pa transakcijo velikega zneska prikrije s transakcijo manjšega. Obstaja veliko vrst skritih transkacij, možna zaščita pa je močna vzajemna avtentikacija med terminalom in brezkontaktno kartico, ki po možnosti temelji na javni kriptografiji in potrebuje nekakšno interakcijo (potrditev) uporabnika. Lahko bi na primer uporabnik vsako transkacijo potrdil s pritiskom gumba na kartici. Vsekakor mora sistem uporabniku pomagati, da sprejema le legitimne transakcije.

3.8 Kartice, ki omogočajo brezkontaktno in kontaktno komunikacijo

Ena izmed možnih ranljivosti je tudi možna uporaba komunikacije s pomočjo kontaktov in brezkontaktne komunikacije. Kartice, ki omogočajo oba načina komunikacije imajo en čip, torej je edina razlika v tem kako pridejo podatki do čipa. Taka je večina plačilnih kartic, ki omogočajo brezkontaktno delovanje. Dva možna načina komunikacije omogočata napadalcu, da med samim napadom menja načine komunikacije in tako lažje izkorišča pomanjkljivosti. Na taki kartici morajo biti protiukrepi učinkovito implementirani na obeh vmesnikih (kontaktnem in brezkontaktnem), oba načina komunikacije pa morata biti strogo ločena. Kartica torej ne sme dopuščati hkratne uporabe obeh načinov komunikacije ali prekplapljanja med njima med izvajanjem posamezne transakcije.

3.9 Radio frequency analysis

Analiza radijskih frekvenc je nov tip »side-channel« napada, ki je mogoč samo na brezkontaktnih karticah. Pri tem napadu se namesto toka analizira radijske frekvence. Ta napad izkorišča dejstvo, da se brezkontaktna kartica napaja s pomočjo radijskih valov. Torej se magnetno polje okoli kartice spreminja kot funkcija porabe električne energije na kartici. Kot bomo videli kasneje na primeru, je napad uspešen tudi na karticah, ki imajo že implementirane protiukrepe proti standardnim »side-channel« napadom. Tak ukrep je na primer stabilizator toka, ki poskrbi, da je tok na kartici nespremenjen ne glede na operacije, ki jih kartica izvaja. Tak protiukrep nam prepreči, da bi iz analize toka dobili kakršnekoli koristne informacije.

3.10 Ostali napadi

Seveda obstajajo tudi napadi, neodvisni od načina komunikacije. Torej napadi, ki jih poznamo iz kontaktnih kartic in so uporabni tudi pri brezkontaktnih karticah. Taki napadi so na primer fizični napad na čip ali pa tako imenovani »side-channel« napadi. Pri slednjih se spremlja nihanje toka na kartici, nihanje elektromagnetnega sevanja ali nihanje časa, ki ga kartica potrebuje za posamezne operacije in te podatke uporabi za pridobitev koristnih informacij o kartici.

4 PRIMERI NAPADOV

4.1 Napad na brezkontatktno kartico s pomočjo analize radijskih frekvenc

V tem razdelku bomo predstavili napad na kartico z dvojnim načinom delovanja- s kontakti in brezkontaktno delovanje. Tak napad je natačneje opisan v [6]. Uporabljena kartica uporablja RSA algoritem za kriptografijo z javnim ključem in 1024 bitni ključ.

4.2.1 Algoritem RSA

Imamo sporočilo m, veliki praštevili p in q, modul n = p*q in tajni eksponent d. Sporočilo podpišemo tako da izračunamo:

$$s = m^d (mod\ n)$$

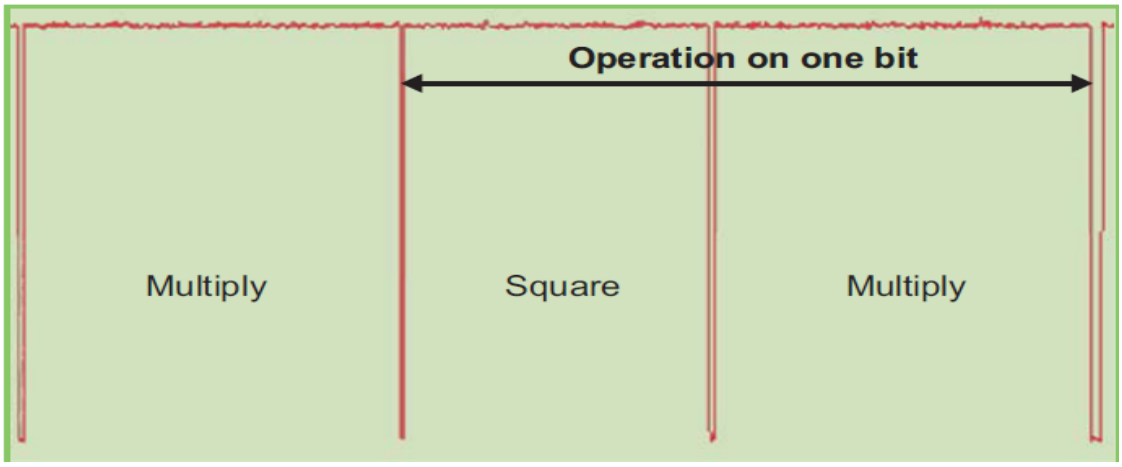
Cilj napada je odriti tajni ključ d. Implementacije za pametne kartice uporabljajo varen "vedno kvadriraj in množi" algoritem za podpisovanje sporočil.

$$Vhod: Sporočilo\ \boldsymbol{m}, javni\ RSA\ modul\ \boldsymbol{n}, tajni\ eksponent\ \boldsymbol{d}\ velikosti\ k\ bitov$$
$$Let\ s := m$$
$$for\ i = k - 2\ down\ to\ 0$$
$$Let\ s = s^2 (mod\ n) \quad * kvadriranje$$
$$if\ (bit\ i\ of\ d\ is\ 1)$$
$$Then\ s = s\ x\ m\ (mod\ n) \quad * množenje$$
$$Else\ s = s'\ x\ m\ (mod\ n) \quad * nadomestno\ množenje$$
$$Izhod: javni\ RSA\ podpis\ \boldsymbol{s = m^d (mod\ n)}$$

Algoritem opisan v zgornji psevdo kodi tudi v primeru, da je ustrezni bit enak nič izvede množenje, katerega rezultat zavrže. Tako se vedno izvedejo enake operacije, ne glede na to ali je bit enak ena ali nič.

4.2.2 Radio frequency analysis

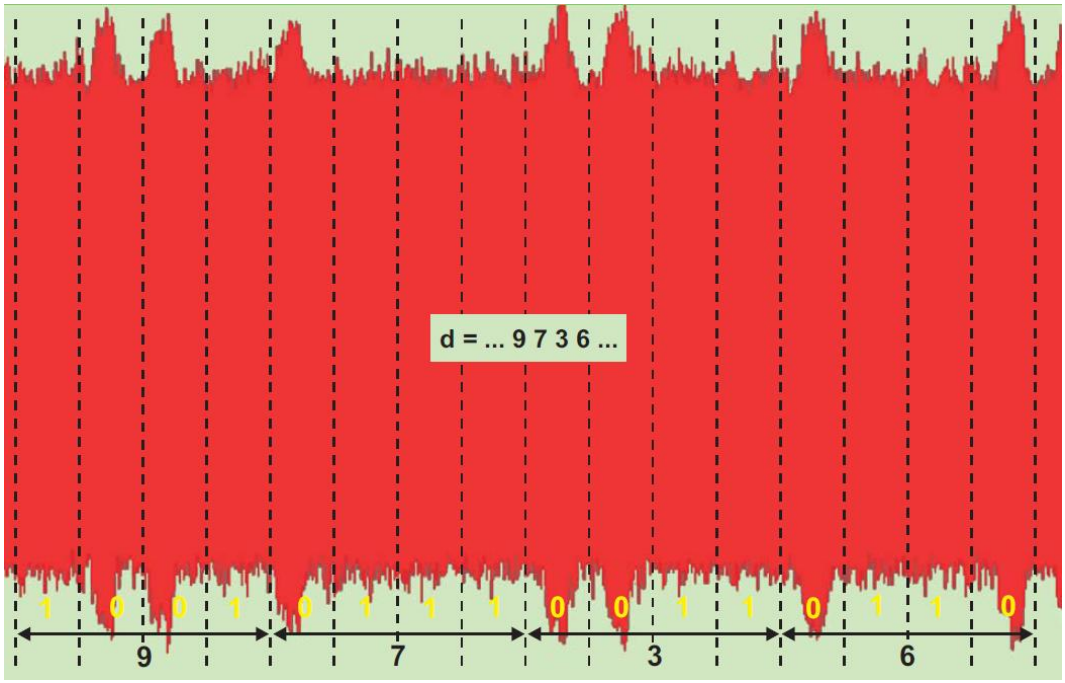
Kartica na kateri je bil prikazan napad s pomočjo analize radijskih frekvenc je že imela implementirane protiukrepe, ki so preprečevali osnovne »side-channel« napade. Napad z analizo toka na kartici je neuspešen, saj je tok, kot je razvidno iz slike 1, konstanten ne glede na operacije, ki jih kartica izvaja.



SLIKA 1: Krivulja prikazuje tok na kartici med izvajanjem podpisovanja z RSA algoritmom

Nekoliko več informacij pridobimo z analizo elektromagnetnega sevanja kartice. Pri tem postopku je potrebno fizično odstraniti zgornji sloj čipa na kartici. Nato najdemo mesto na čipu kjer je elektromagnetno sevanje najmočnejše in uporabimo osciloskop, ki nam sevanje pretvori v krivulje, ustrezne za analizo. Pri tej tehniki so kljub protiukrepom že vidne razlike med obdelavo ničel in enic pri množenju in kvadriranju.

Za najbolj obetavno se izkaže tehnika analize radijskih frekvenc. Ta tehnika je možna le pri brezkontaktnih karticah. Fizični posegi na kartici niso potrebni. Ideja je v tem, da merimo magnetno polje okoli kartice. Uporabimo bakreno zanko, ki meri magnetno polje in njegova nihanja ter osciloskop, ki nam meritve prikaže v obliki krivulj, primernih za analizo. Kot je razvidno iz slike 2, je iz teh krivulj možno bit po bitu razbrati skrivni eksponent d.



SLIKA 2: Prikaz meritev magnetnega polja

Torej so »side-channel« napadi uspešni kljub temu, da je proizvajalec kartic že implementiral ukrepe proti najbolj pogostemu- analizi toka na kartici.

Iz tega primera lahko ugotovimo, da je osnovna zaščita proti »side-channel« napadom potrebna, ne pa zadostna. Zaradi ranljivosti brezkontaktne komunikacije je možno napad z analizo radijskih frekvenc izvesti popolnoma neopaženo in brez posegov na kartici. Za zaščito pred takimi napadi bi bilo potrebno uvesti naprednejše programske protiukrepe kot sta randomizacija sporočila in skrivnega eksponenta. K sreči so taki protiukrepi že znani in

implementirani na kontaktnih karticah, torej je to znanje potrebno le prenesti v brezkontaktni svet.

4. 2 Napad na MIFARE Classic kartico

MIFARE sistem je dobro poznan in zelo razširjen. Družina izdelkov MIFARE spada pod okrilje podjetja NXP Seminconductors. Po podatkih izdelovalca je bilo prodanih že 1 milijarda MIFARE brezkontaktnih kartic. Trenutno naj bi bilo v uporabi 200 milijonov MIFARE Classic kartic po vsem svetu. To pomeni, da MIFARE pokriva 85% celotnega trga brezkontaktnih pametnih kartic.

Napad objavljen v [1] se osredotoča na MIFARE Classic kartico. Kartica omogoča vzajemno avtentikacijo in varovanje podatkov. Varnost temelji na algoritmu imenovanem CRYPTO-1. CRYPTO-1 je tokovna šifra, ki uporablja 48 bitni skrivni ključ. Algoritem je last podjetja NXP in je tajen.

Z »reverse engineering« metodo najprej razkrijemo kriptografski algoritem in protokol za avtentikacijo. To naredimo z analizo komunikacije med terminalom in kartico. Ko imamo algoritem in avtentikacijski protokol lahko izvedemo napad. Za napad potrebujemo le eno ali dve avtentikaciji iz terminala in že lahko razkrijemo skrivni ključ v manj kot sekundi in z uporabo le 8 MB pomnilnika. Če napadalec prisluškuje komunikaciji med terminalom in kartico, lahko s to metodo pridobi vse ključe uporabljene v komunikaciji in dekriptira vsa sporočila. To nam priskrbi dovolj informacij za branje, kloniranje ali obnovitev kartice v prejšnje stanje. Kopiranje kartice traja le deset sekund. Napadi so bili konec leta 2008 uspešno izvedeni tudi v praksi in sicer na sistemih Oyster Card v Lonodonu in OV-Chipkart na Nizozemskem. Ker sistem s karticami MIFARE Classic ne omogoča nadgradnje na naprednješe varnostne protokole, je edina možna zaščita pred napadi menjava sistema ali pa uvedba dodatnih varnostnih ukrepov. Kartica MIFARE Classic je zaradi nizke cene namreč zelo razširjena v sistemih za plačevanje javnega prevoza, kot tudi v sistemih za nadzor dostopa v stavbe, poslovne prostore itd.

5 ZAŠČITA PRED NAPADI

5.1 Težave pri zaščiti brezkontaktnih kartic

Kriptografija javnih ključev in kriptografski koprocesor morata biti optimizirana, da lahko delujeta na kartici. Brezkontaktne kartice imajo strožje časovne omejitve in omejitve porabe energije zato je uvedba naprednejše kriptografije lahko težja in cenovno manj učinkovita kot pri navadnih karticah. Pogosto se sklepajo kompromisi med ceno in varnostjo. Tako so v Ameriki zaradi lažje integracije in ugodne cene na trg poslali brezkontaktne pametne plačilne kartice, ki so temeljile na simetrični kriptografiji. Te kartice so se izkazale za zelo ranljive. Lahko jih je bilo ponarediti in zlorabiti za nepooblaščene transkacije. Na očitke, da bi morali za te kartice

uporabiti naprednejšo tehnologijo, ki bi temeljila na EMV standardih, pa so izdajatelji teh kartic odgovorili, da stopnja zlorab enostavno ni dovolj visoka, da bi opravičila stroške za zamenjavo obstoječega sistema.

5.2 Varnostni mehanizmi za preprečevanje napadov

5.2.1 Vzajemna avtentikacija

Brezkontaktna pametna kartica preveri avtentičnost terminala in dokaže svojo avtentičnost terminalu. S tem preprečimo nepooblaščen dostop do kartice. Dandanes že obstajajo predlogi vzajemne avtentikacije, ki temeljijo na javni kriptografiji z uporabo eliptičnih krivulj [7]. Take rešitve preprečujejo prikrite transakcije in onemogočajo neavtentičnim terminalom komunikacijo s kartico.

5.2.2 Močna varnost podatkov

Za aplikacije, ki zahtevajo zaupnost podatkov shranjenih na kartici, lahko podatke na kartici kriptiramo. Prav tako lahko kriptiramo komunikacijo med kartico in terminalom. S tem preprečimo prisluškovanje. Dodatni varnostni ukrepi se lahko uvedejo tudi za zagotavljanje integritete podatkov.

5.2.3 Močna varnost brezkontaktne naprave

Kartice imajo lahko vgrajene mehanizme, ki preprečujejo podvajanje kartic. Obstaja veliko strojnih in programskih rešitev, ki zaznajo poskus podvajanja in ustrezno odreagirajo ter pomagajo preprečiti zlorabe.

5.2.4 Avtentičen in pooblaščen dostop do podatkov

Sposobnost brezkontaktne pametne kartice, da procesira podatke in se odziva na okolje ji omogoča avtenticiranje dostopa do podatkov. Kartica lahko preveri identiteto osebe, ki zahteva podatke, ter dovoli dostop le do določenih podatkov. Dostop do shranjenih podatkov je lahko tudi dodatno zaščiten s PIN kodo ali celo biometričnimi metodami.

5.2.5 Ščitenje in blokiranje

Eden izmed načinov zaščite pred napadi s prenosom signala, skritimi transkacijami in nepooblaščenim dostopom do podatkov na brezkontaktni pametni kartici je ščitenje kartice s posebnimi ovojnicami. Faraday-eva kletka je primer take zaščite. Dandanes je možno kupiti ovitke za kartice in celo denarnice, ki imajo lastnosti Faraday-eve kletke. Seveda taka zaščita nima nobenega pomena ko kartico uporabljamo. Smotrno bi bilo, da bi izdajatelji kartic tako zaščito uporabljali pri pošiljanju kartic uporabnikom.

Bolj dovršena zaščita, ki je tudi bolj priročna je kartica s stikalom opisana v naslednjem razdelku.

5.2.6 Switch cards [8] – kartice s stikalom

Na trgu se pojavljajo tudi kartice s posebnim stikalom, s katerim jih lahko vključimo oziroma izključimo. Tako stikalo nam omogoča večji nadzor nad našo kartico in do neke mere preprečuje nepooblaščene dostope brez naše vednosti. Še vedno pa mora biti poskrbljeno za zaščito podatkov, prav tako pa morajo biti implementirani varnostni ukrepi za primere ko je kartica aktivna. Ko držimo stikalo se taka kartica namreč obnaša enako kot kartica brez stikala.

5.2.7 Zaznavanje uporabnikove namere

Kot alternativa fizični zaščiti kartice je možno kartico prirediti tako, da bo delovala le ko bo uporabnik to želel. Na kartico lahko vgradimo že prej omenjeno stikalo ali celo senzorje svetlobe in toplote. S slednjimi bi lahko omogočili delovanje kartice le ko jo držimo v roki in je na svetlobi (ni v denarnici). Morda bi lahko vgradili senzorje gibanja, ki bi zaznali posebno trajektorjio gibanja kartice. Še najboljša rešitev pa bi bila povečanje računske moči in uporaba biometričnih metod, kot je na primer zaznava prstnega odtisa. Računsko zahtevnejše metode so seveda možne le ob ustreznem viru energije. To pa ni težavno saj so dandanes čipi brezkontaktnih pametnih kartic lahko vgrajeni v naprednejše elektronske naprave kot je mobilni telefon.

5.2.8 Boljša kriptografija

Še dandanes celo kartice, ki zaradi svojih aplikacij potrebujejo najvišji nivo varnosti, temeljijo na tehnologiji kartic z magnetnim trakom. Veliko bolje bi bilo, če bi brezkontaktne pametne kartice prevzele EMV standarde, ki se uporabljajo za plačilne kartice v evropi. Seveda pa bi implementacija naprednejše kriptografije potrebovala več elektirčne energije, več procesorske moči in več prostora.

5.2.9 Upravljanje s ključi pri simetričnih sistemih (DES, 3-DES)

Kot opozarjajo v [9] je ključe potrebno menjavati in izbirati naključno. Če na primer pri DES-u kjer so ključi 7 bajtni, namesto naključnih 7 bajtov uporabimo le male črke angleške abecede, dobimo 9-milionkrat $((256/26)^7)$ šibkejše ključe. To pomeni da bi »brute-force« napad, ki sicer traja 100 let, na šibkejši množici ključev trajal le 6 minut.

6 Primeri varnostnih shem

V tretjem poglavju smo med nevarnostmi specifičnimi za brezkontaktne kartice omenili tudi napad s ponavljanjem in napad s prenosom. Na tem mestu se bomo posvetili postopkom za zaščito pred tema napadoma.

6.1 Enkratno geslo (One Time Password - OTP)

V nadaljevanju bo podan primer sheme ki uporablja koncept enkratnega gesla. Shema prepreči napad s ponavljanjem in še nekaj drugih napadov. Shema uporablja tudi vzajemno avtentikacijo. Ta shema je bila predstavljena v [12].

6.1.1 Prva faza: Registracija

V tej fazi se uporabnik registrira v sistem.

Faza registracije je prikazana na sliki 3.

Postopek:

1.) Strežnik izda kartico, ki vsebuje skrivni SEED. SEED je veliko naključno število, ki ga generira strežnik.

2.) Strežnik izbere naključno število D_0. Nato izračuna

$$SEED \oplus D_0 \text{ in } H(D_0)$$

in ju pošlje uporabniku. H() je enosmerna zgoščevalna funkcija brez trkov.

3.) Uporabnik preveri, če velja

$$H\big(SEED \oplus (SEED \oplus D_0)\big) = H(D_0).$$

Nato izračuna

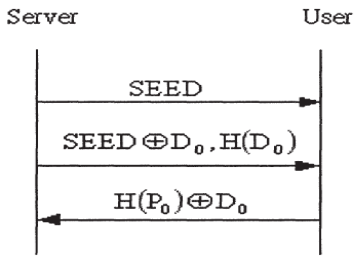
$$H(P_0) \oplus D_0 \text{ kjer je } P_0 = H^{F(D_0)}(K \oplus SEED)$$

F() je ponovno enosmerna zgoščevalna funkcija brez trkov. Sedaj uporabnik pošlje P_0 strežniku po varnem kanalu.

4.) Strežnik shrani

$$D_0 \oplus X, H(P_0), SEED \oplus X$$

kjer je X skrivni parameter sistema.



SLIKA 3: Registracija

6.1.2 Druga faza: Prijava v sistem

V tej fazi se uporabnik t-tič prijavi v sistem.

Ta faza je prikazana na sliki 4.

Postopek:

1.) Strežnik izračuna

$X \oplus (SEED \oplus X)$ in $X \oplus (D_{t-1} \oplus X)$

da dobi SEED in D_{t-1} . Nato strežnik naključno izbere število D_t . Izračuna

$SEED \oplus D_t$ in $H^2(D_t) \oplus H^2(P_{t-1}||T)$

z uporabo shranjene vrednosti $H(P_{t-1})$, kjer je T časovni žig in

$P_{t-1} = H^{F(D_{t-1})}(K \oplus SEED)$. Nato strežnik pošlje rezultat izračuna in $F(D_{t-1})$ s T-jem uporabniku.

2.) Ko uporabnik sprejme

T, $SEED \oplus D_t, H^2(D_t) \oplus H^2(P_{t-1}||T) in\ F(D_{t-1})$

uporabnik najprej preveri, če je T zapadel. Če ni izračuna

$$H^2\big(SEED \oplus (SEED \oplus D_t)\big) \oplus H^2(H^{F(D_{t-1})}(K \oplus SEED)||T)$$

in preveri ali se rezultat izračuna ujema z

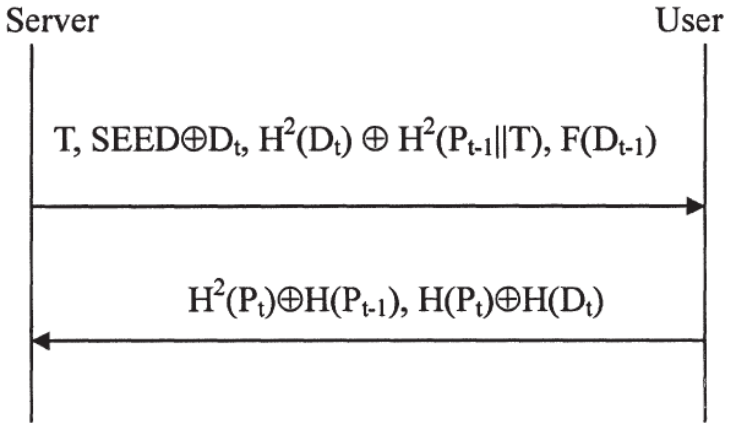
$$H^2(D_t) \oplus H^2(P_{t-1}||T)$$

Če se ne ujema potem pošiljatelj ni pravi strežnik. Sicer uporabnik izračuna

$H^2(P_t) \oplus H(P_{t-1})$ in $H(P_t) \oplus H(D_t)$

kjer je

$P_{t-1} = H^{F(D_{t-1})}(K \oplus SEED)$ in $P_t = H^{F(D_t)}(K \oplus SEED)$



SLIKA 4: Faza prijave v sitem za t-to prijavo

6.1.3 Tretja faza: faza dokaza

V tej fazi uporabnik dokaže svojo identiteto.

Ko strežnik sprejme

$H^2(P_t) \oplus H(P_{t-1})$ in $H(P_t) \oplus H(D_t)$

Izračuna

$$H(P_{t-1}) \oplus (H^2(P_t) \oplus H(P_{t-1}))$$

Da dobi $H^2(P_t)$. Pri tem je bil $H(P_{t-1})$ shranjen pri prejšnji prijavi. Nato strežnik izračuna

$$H(D_t) \oplus (H(P_t) \oplus H(D_t))$$

Da dobi $H(P_t)$. Če velja

$$H\big(H(P_t)\big) = H^2(P_t)$$

Je uporabnik avtenticiran. Nato se D_{t-1} in $H(P_{t-1})$ ustrezno zamenja z D_t in $H(P_t)$.

6.1.4 Varnost opisane sheme

Shema preprečuje nepooblaščeno branje kartic:

-V fazi registracije in fazi prijave v sistem lahko uporabnik preveri avtentičnost strežnika. Avtentikacija temelji na poznavanju velikega števila SEED. Komunikacija med nepravim strežnikom (terminalom) in uproabnikom (kartico) je torej neuspešna.

Shema preprečuje napadalcu, da se izdaja za nekega drugega uporabnika:

- Napadalec, ki se bo skušal izdajati za nekega drugega uporabnika, bo od strežnika prejel T, $SEED \oplus D_t, H^2(D_t) \oplus H^2(P_{t-1}||T) in\ F(D_{t-1})$
  Ker je naključno generirana vrednost T, D_t zaščitena z vrednostjo SEED, ki je napadalec ne pozna, ne more izračunati D_t. Napadalec prav tako ne pozna ključa K, zato je tudi tretja faza neuspešna.

Shema je varna pred napadom s ponavljanjem:

- Prvi mehanizem, ki preprečuje napad s ponavljanjem posnete seje je časovni žig T. Na začetku faze prijave v sistem lahko uporabnik enostavno preveri če je T zapadel in ustrezno ukrepa.
- Če napadalec zamenja T z drugim T' se še vedno ne more uspešno avtenticirati, saj $H^2(D_t) \oplus H^2(P_{t-1}||T') \neq H^2(D_t) \oplus H^2(P_{t-1}||T)$

Shema je varna pred "stolen-verifier" napadom

- To je napad pri katerem naadalec uporabi podatke, ki jih strežnik uporablja za preverjanje uporabnika. Ti podatki so $D_t \oplus X, H(P_t), SEED \oplus X$. Ker je X skrivni parameter sistema, napadalec ne more izračunati SEED ali D_{t-1}. S prislkuškovanjem t-ti prijavi uporabnika bi lahko napadalec pridobil kvečjemu podatke za izračun $H(D_t), H^2(D_t), H(P_{t-1}) in\ H^2(P_{t-1}||T)$.
- SEED, $D_t\ in\ P_t$ bi še vedno ostali skrivni. Ker je SEED napadalcu neznan ne more izračunati D_{t+1}. Torej se ne more avtenticirati, ker ne zna izračunati $H(P_{t+1}) \oplus H(D_{t+1})$.

6.2 Zaščita pred napadom s prenosom

V razdelku 6.1 smo videli primer varnostne sheme, ki onemogoči napad s ponavljanjem posnete seje. Napad s ponavljanjem lahko preprečimo z enkratnim geslom, časovnim žigom ali protokolom izziv-odgovor. Prednost časovnega žiga je, da ne potrebujemo izvora naključnosti. Vendar pa je za zaščito pred napadom s ponavljanjem najbolje uporabiti kombinacijo več mehanizmov. Kot smo videli, sta bila v zgornji shemi uporabljena časovni žig in enkratno geslo. Lahko bi rekli, da je bil uporabljen tudi protokol izziv-odgovor. Protokol izziv odgovor je v splošnem vsaka komunikacija kjer ena stran drugo preveri tako, da ji pošlje neko informacijo (ponavadi naključno število) in od nje pričakuje odgovor, ki ga lahko generira le s pomočjo deljene skrivnosti (oziroma tajnega ključa v primeru PKI). Za uporabo protokola izziv odgovor in splošno kakršnegakoli avtentikacijskega protokola potrebujemo generator pravih naključnih števil. To dandanes na brezkontaktnih pametnih karticah ni več problem saj imajo sodobni čipi že integriran TRNG (True Random Number Generator). Čip predstavljen v [13] vsebuje TRNG razreda AIS31 tipa P2. Tak generator naključnih števil je dovolj dober tudi za implementacijo EMV [14] standardov.

Žal pa ti varnostni mehanizmi niso dovolj za preprečitev napada s prenosom signala. Pri napadu s prenosom časovni žig ne prepreči ničesar saj se napad dogaja v realnem času, signali se le prenašajo med terminalom in kartico. Torej tudi izzivi in odgovori potujejo med terminala in kartico nedotaknjeni. Do sedaj omenjeni mehanizmi ne prepečijo napada. Bistvena razlika med pravo komunikacijo in napadom s prenosom je v poti, ki jo mora opraviti signal. Pot je namreč zaradi večje razdalje daljša. Torej bi lahko napad preprečili z ustreznim zmanjšanjem dovoljene latence. Ta rešitev bi le omejila maksimalno razdaljo napada, ne bi ga pa povsem preprečila.

Druga možnost je že omenjena kartica s stikalom. Če bi kartica delovala le ko mi to želimo, torej ko pritisnemo na gumb, bi bil napad s prenosom, medtem ko imamo kartico v žepu onemogočen. Enak učinek bi imel tudi protokol, ki bi pri vsaki transakciji zahteval vnos PIN kode. Vendar pa take metode bistevno omejijo priročnost in hitrost brezkontaktnih pametnih kartic.

Obetavna rešitev je opisana v [15]. Avtorji so jo poimenovali »Distance Bounding Protocol«. Protokol izkorišča dejstvo, da nobena informacija ne more potovati hitreje kot svetloba. Tako s pomočjo meritev časov prenosa določi maksimalno možno oddaljenost kartice od terminala. Če je razdalja prevelika komunikacijo prekine. Protokol je skiciran na sliki 5.

6.2.1 Opis »Distance Bounding« protokola

Najprej terminal pošlje brezkontaktni pametni kartici naključno zaporedje bitov N_V.

$$V \rightarrow P : N_V$$

Terminal in kartica nato uporabita psevdo-naključno funkcijo *h* in skrivni ključ *K* za izračun dveh zaporedij $R^0 in\ R^1$:

$$R_1^0 R_2^0 R_3^0 \dots R_n^0 || R_1^1 R_2^1 R_3^1 \dots R_n^1 := h(K, N_V)$$

Nato se po vnaprej določenem številu urinih ciklov po prenosu N_V začne sekvenca n enobitnih izmenjav izzivov in odgovorov. Terminal v i-tem koraku pošlje naključni C_i kartici, kartica pa vsakič ustrezno odgovori z $R_i^{C_i}$.

$$V \rightarrow P : C_i \in \{0,1\}$$

$$P \rightarrow V : R_i^{C_i} \in \{0,1\}$$

Ker je tudi terminal izracunal vrednosti R, lahko seveda preveri odgovore kartice. Odgovori morajo biti pravilni in prejeti v dovolj kratkem času.

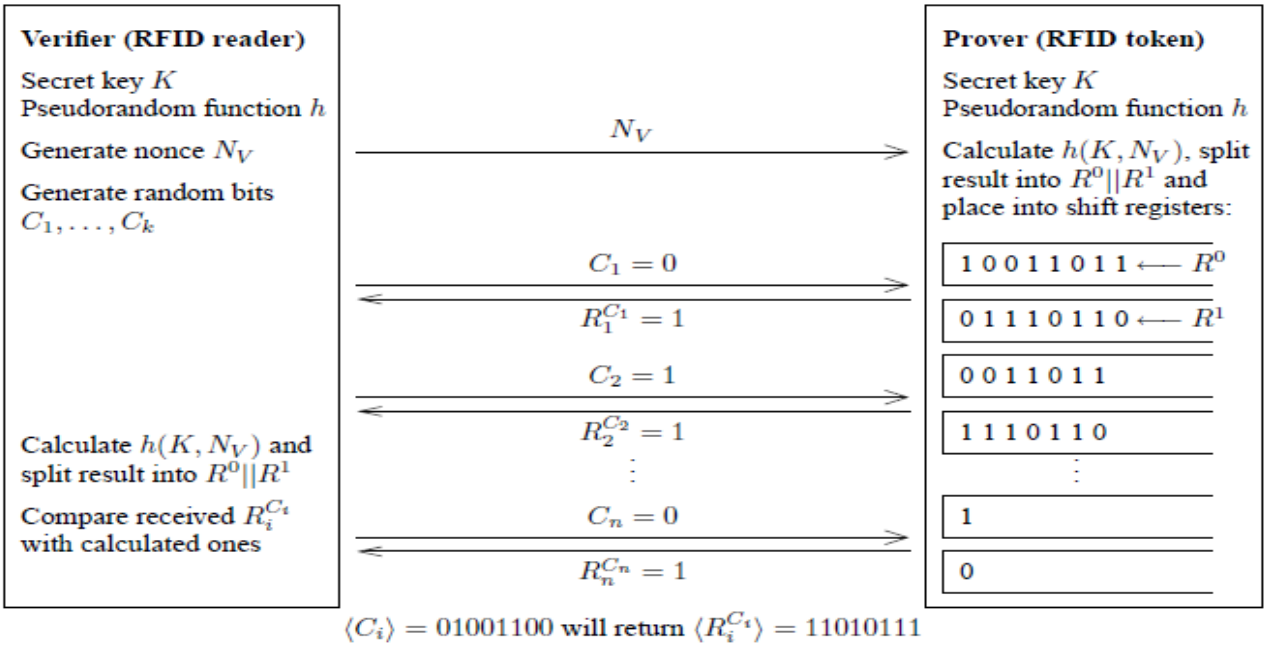
Sedaj lahko terminal izračuna oddaljenost kartice s pomočjo formul

$$t_m = 2 \cdot t_p + t_d$$

$$d = c \cdot \frac{t_m - t_d}{2}$$

kjer je c svetlobna hitrost, t_p hitrost prenosa v eno smer, t_m latenca, ki jo je izmeril terminal in t_d zamik zaradi procesiranja na kartici.

Kot so pokazali v [15] ima napadalec le $\left(\frac{3}{4}\right)^n$ verjetnosti, da bi uspešno prelisičil algoritem, torej poneveril odgovore kartice.



Slika 5: Distance Bounding Protocol

Potrebno je še omeniti, da se omenjeni protokol izvaja na fizični plasti saj so le tako izmerjeni časi dovolj natančni.

7 PRIMERJAVE Z DRUGIMI TEHNOLOGIJAMI

7.1 Primerjava brezkontaktne tehnologije in RFID-a (Radio frequency identification)

Brezkontaktna kartica je pametna kartica, ki uporablja radijske frekvence za komunikacijo s terminalom. Za komunikacijo uporablja vgrajeno anteno. Brezkontaktne kartice imajo čip z mikroprocesorjem, ki podpira različne varnostne protokole vključno s kriptiranjem podatkov. Mednarodni standard dovoljuje brezkontaktnim karticam delovanje na razdalji 0-10 cm od terminala.

RFID etikete so enostavne in poceni. Uporabljajo se za identifikacijo živali, označevanje hrane in zamenjujejo črtne kode v trgovinah. RFID etikete navadno le shranjujejo ID številko. S pomočjo antene se ta številka prenese do terminala. Ko je terminal dovolj blizu RFID etikete dobi etiketa iz radijskih frekvenc energijo za delovanje in prenese svojo ID številko terminalu. Delovanje je torej precej enostavno in ne nudi nobene varnosti. Omogoča le enkripcijo podatkov (ID številke). Tipično se RFID etikete lahko bere iz razdalje do nekaj metrov.

7.2 Primerjava varnosti kartic z magnetnim trakom in brezkontaktnih pametnih kartic

Prednost brezkontaktne pametne kartice je vsekakor v tem, da jo uporabniku nikoli ni potrebno izročiti trgovcu, ki ima lahko zle namene. S tem se izognemo nekaterim napadom ali pa jih vsaj otežimo. Brezkontaktna pametna kartica, za razliko od kartice z magnetnim trakom, za vsako transkacijo uporabi novo kodo in ne statično kodo zapisano na kartici. Slabost brezkontaktnih pametnih kartic pa je v tem, da so vedno aktivne. Torej se nam lahko kadarkoli nekdo pribilža s terminalom in prebere našo kartico, tudi ko mi tega ne želimo ali se tega sploh ne zavedamo. K sreči so novejše kartice že zaščitene proti takim zlorabam. Zaščita temelji predvsem na vzajemni avtentikaciji, ki pogosto temelji na kriptografiji javnih ključev.

7.3 Primerjava z ostalimi elektronskimi karticami

V Evropi se že nekaj časa uporablja EMV standarde ki temeljijo na kriptografiji javnih ključev. Evropske plačilne kartice uporabljajo DDA (Dynamic Data Authentication), kjer kartica digitalno podpiše naključen izziv terminala. Zaradi razpoložljivosti EMV strojne opreme in njene podpore kriptografiji javnih ključev ni povsem jasno zakaj so se podjetja niso odločila za implementacijo teh tehnologij in s tem dosego višjega nivoja varnosti. Najbrž je k taki odločitvi pripomogla lažja integracija z obstoječim sistemom. Kartice, ki ne podpirajo javne kriptografije so cenejše in omogočajo delovanje na večji oddaljenosti in hitrejše prenose. Brezkontaktne plačilne kartice ki so v uporabi v Ameriki uporabljajo 3-DES simetrično kriptografijo.

Zaključek

Spoznali smo delovanje brezkontaktnih pametnih kartic, njihove prednosti in slabosti. Poglobili smo se v ranljivosti, ki jih prinaša uporaba brezkontaktne RFID tehnologije. Predstavili nekaj v praksi uspešno izvedenih napadov in načine, kako se pred napadi zaščititi. Primerjali smo brezkontaktne pametne kartice z ostalimi karticami in RFID etiketami.

V nalogi smo se osredotočili predvsem na varnost brezkontaktne tehnologije. Sama uporaba brezkontaktne tehnologije prinaša veliko prednosti, a seveda tudi kakšno slabost. Kritike gredo predvsem na račun varnosti. Vendar pa pri varnosti ne gre za nerešljive pomanjkljivosti ali pomanjkanje ustreznih varnostnih mehanizmov. Problem ni v proizvajalcih, problem je v naročnikih. Naročnik je tisti, ki določa kaj želi in koliko je za to pripravljen plačati. Kot smo spoznali na primeru ameriških bank, je včasih lažja in cenejša pot bolj mamljiva, pa čeprav na račun končnih uporabnikov in njihove (ne)zaščite pred zlorabami.

V prihodnosti lahko pričakujemo integracijo brezkontaktnih pametnih kartic z drugimi elektronskimi napravami. Predvsem priročna bi bila integracija z mobilnim telefonom, ki ga ima že skoraj vsak od nas neprestano pri roki. Predstavljajte si SIM kartico, ki bi opravljala še funkcijo potnega lista, osebne izkaznice, vozniškega dovoljenja, različnih kartic ugodnosti in plačilne kartice. Pri taki funkcionalnosti sploh ne bi več potrebovali denarnice. Hkrati pa bi taka integracija zaradi lastnega napajanja mobilnega telefona in večje računske moči omogočala uporaba naprednejših kriptografskih algoritmov in morda celo biometričnih metod. S pritiskom na gumb, ki bi hkrati preveril naš prstni odtis, bi lahko varno in hitro opravljali transakcije, dokazovali našo identiteto in potovali.

Literatura

[1] Flavio D. Garcia, *Dismantling MIFARE Classic,* Radbound University Njimegen, 2008

[2] V.Richardson, *Contactless credit cards spark concerns for data privacy,* http://www.CreditCards.com, 2009

[3] K. Finkenzeller, *RFID Handbook Second Edition,* John Wiley & Sons Ltd, 2003

[4] T. Heydt-Benjamin , D.V. Bailey, K. Fu, A. Juels, T. O'Hare, *Vulnerabilities in First-Generation RFID-enabled Credit Cards, 2006*

[5] Octopus Card, http://en.wikipedia.org/wiki/Octopus_card

[6] H. Handschuh, *Contactless Technology Security Issues,* Gemplus Security Tecnologies Department, 2004

[7] M. Ullmann*, Password Authenticated Key Agreement for Contactless Smart Cards,* RFIDSec08, 2008

[8] *Contactless Smart Card Applications: Design Tool and Privacy Impact Assessment,* ACT Canada, 2007

[9]*Key managment: a vital element to a contactless smart card system* , http://www.xceedid.com/pdf/XceedID-KeyManagement.pdf

[10] *RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities , http://www.hidglobal.com/documents/tagsVsSmartcards_wp_en.pdf*

[11] *Richard Sebastian,* Malaysia's Progress with the Malaysia Microchip Project, http://www.frost.com/prod/servlet/market-insight-top.pag?docid=159367189 , 2009

[12] Y. Chang, C. Chang, J. Kuo, *A secure one-time password authentication scheme using smart cards without limiting login times,* National Chung Cheng University, 2004

[13] Dual contactless smart card with TRNG, *http://www.st.com/stonline/products/literature/bd/15272.pdf*

[14] EMV, http://www.emvco.com/

[15] Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: Proc. of the 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005) (2005) 67–73