SIM kartica

Seminarska naloga pri predmetu Kriptografija in teorija kodiranja 2

Neli Blagus, 63050181

18. november 2009

Kazalo

Slike

1 UVOD

V nekaj letih so pametne kartice postale del našega vsakodnevnega življenja, uporabljajo se na veliko področjih - dvigovanje denarja, plačevanje, shranjevanje podatkov na zdravstvenih karticah, komuniciranje z avtomati ter, za ta projekt najpomembnejše, v GSM telefoniji. Mobilni telefon brez (pametne) SIM kartice si težko zamislimo. Kaj šele to, da bi morali ob okvari in menjavi mobitela vsakokrat zamenjati telefonsko številko in na novo zbirati številke vseh prijateljev. Prednosti te majhne kartice, ki jo namestimo v telefon ter nanjo skoraj pozabimo, je veliko. Po drugi strani pa se kdaj vprašamo, ali je PIN koda, ki jo vtipkamo ob vklopu mobitela, zadostna za zagotavljanje varnosti. Naših SMS sporočil res ne bi mogel prebrati vsak? Mogoče kdo telefonira na naše stroške? Nam kdo prisluškuje pri zaupnem telefonskem pogovoru? Je sploh varno govoriti skrivnosti po telefonu?

V projektu bom predstavila SIM kartico in njeno varnost. Na začetku je seveda potreben kratek opis, kaj so pametne kartice na splošno, kakšen pomen imajo v telefoniji in GSM sistemu. Podrobneje so lastnosti, zgradba in funkcije SIM kartice predstavljene v 3. poglavju. Poglavje 4 opisuje varnostne algoritme ter avtentikacijo SIM kartice v omrežje, v 5. poglavju pa sta opisana dva napada, ki lahko ogrozita varnost SIM kartice. V 6. poglavju sta na kratko predstavljeni dve novejši tehnologiji v mobinih omrežjih. Seminarska naloga se zaključi s kratkim orisom trenutnega stanja varnosti SIM kartice.

2 OSNOVNI POJMI (PAMETNE KARTICE IN TELEFONIJA)

2.1 Na kratko o pametnih karticah

Pametna kartica (angleško smart card, chip card, integrated circuit card) je kartica za vsak žep, pravzaprav kar računalnik v malem. Vsebuje integrirano vezje (čip), ki lahko procesira podatke (sprejme vhod, ga procesira in vrne izhod). Osnovni nalogi pametne kartice sta varno shranjevanje podatkov (certifikatov, ključev) ter identifikacija, tudi avtentikacija lastnika kartice, da se prepreči uporaba komurkoli.

Kartice s čipom sicer delimo na več vrst:

- pomnilniške kartice: imajo spominske komponente, lahko tudi nekaj specifične varnostne logike, nimajo pa lastnega procesorja;
- mikroprocesorske kartice (pametne kartice): poleg pomnilnika imajo lastni procesor (zaradi česar jim rečemo "pametne"), lahko dinamično obdelujejo po-

datke, zmožne so šifriranja podatkov, generiranja in preverjanja digitalnih podpisov, podatke imajo organizirane v datotečnem sistemu, do katerega s kartičnim operacijskim sistemom dostopa izključno procesor.

V sedemdesetih letih je Francoz Moreno patentiral prvi koncept spominske kartice, ki je tudi že bila zavarovana z osebnimi geslom (PIN koda). Čez približno deset let pa so se pametne kartice prvič začele uporabljati masovno kot pomnilniške telefonske kartice v Franciji. Od teh začetkov so že tri desetletja, kartice pa uporabljamo na širšem vsakodnevnem področju:

- bančništvo: elektronske denarnice (glej [13]),
- zdravstvo: kartice vsebujejo osebne, zdravstvene in ostale medicinske podatke (na primer krvna skupina, dializa, kronične bolezni) o lastniku, po novem pa se uvajajo tudi kartice, ki ne bodo vsebovale nobenih podatkov o zavarovancu, ampak bodo služile le kot ključ do podatkov, shranjenih v zdravstvenem informacijskem sistemu (več v [12])
- transport: brezkontaktne pametne kartice nadomeščajo papirnate vozovnice, uporabljajo se pri cestninjenju (brezkontaktne kartice, s katerimi se poveča pretok vozil),
- telekomunikacije.

Slika 1: Primeri uporabe pametne kartice na različnih področjih

2.2 Uporaba pametnih kartic v mobilni telefoniji

V digitalni mobilni telefoniji so pametne kartice prisotne že od vsega začetka. Prvotno so se uporabljale za identifikacijo lastnika, a je prihajalo do čedalje pogostejših zlorab (prisluškovanje ter klicanje na tuj račun). Zato je bil pri uvajanju standarda GSM poudarek na varnosti komunikacije, ki jo zagotavlja SIM kartica.

Današnji mobilni (GSM) sistem je sestavljen iz dveh delov - uporabniški sistem in sistem mobilnega operaterja, ki uporabnikom omogoča storitve. Komunikacija med njima poteka preko SIM kartice in je podrobneje opisana v poglavju 4.2.

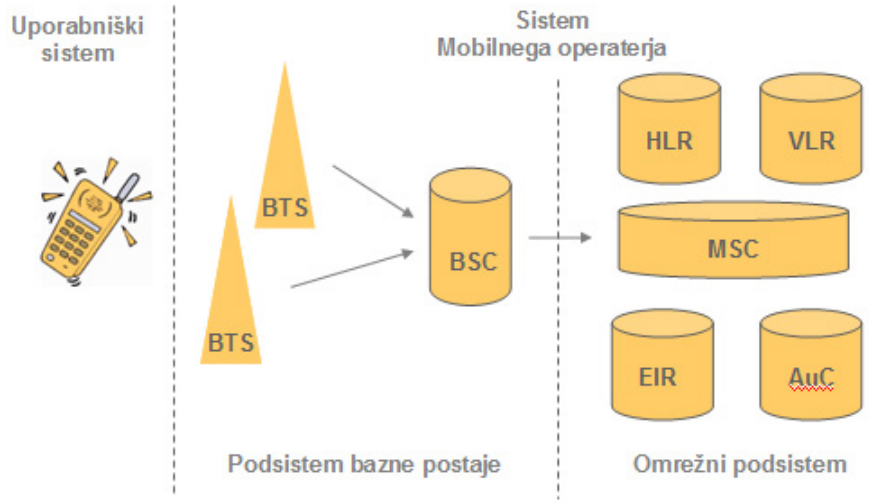
Slika 2: Različne SIM kartice

GSM sistem

Za lažje razumevanje avtentikacije SIM kartice v omrežje bi na kratko omenila še strukturo sistema mobilnega operaterja. Setavljen je iz dveh delov (glej sliko 3):

- Podsistem bazne postaje (kontrolira radijsko povezavo z mobilno napravo):
  - bazna postaja (BTS - Base Transceiver Station): skrbi za radijsko povezavo z mobilnimi napravami v svoji celici (celica predstavlja geografsko območje, kako pogosto so razporejene bazne postaje je odvisno na primer od poselitve),
  - kontroler bazne postaje (BSC - Base Station Controller): upravlja z radijskimi viri ene ali več postaj ter povezuje bazno napravo s preklopnim centrom omrežnega podsistema.
- Omrežni podsistem:
  - MSC (Mobile Switching Center): glavna komponenta podsistema je preklopni center, ki vodi registracije, avtentikacije, usmerjanje klicev, osveževanje lokacij in podobno. MSC predstavlja tudi povezavo z ostalimi fiksnimi telefonskimi omrežji, kot sta PSTN ali ISDN.

- HLR (Home Location Register): vsebuje administrativne informacije (IMSI, trenutna lokacija, omogočene storitve ipd.) registriranih naročnikov tega operaterja,
- VLR (Visitor Location Register): vsebuje informacije o vseh naročnikih obiskovalcih, ki se trenutno nahajajo na območju tega omrežja,
- EIR (Equipment Identity Register): predstavlja bazo vse mobilnih naprav,
- AuC (Authentication Center): zavarovana baza, ki vsebuje kopije ključev K_i vseh naročnikov, algoritme šifriranja in generator naključnih števil (več o generatorju v poglavju 4.2.1).



Slika 3: Sestava GSM sistema

3 SIM KARTICA

SIM (Subscrieber Identity Module) kartica je pametna kartica, ki se uporablja v mobilni telefoniji. Njeni primarni nalogi sta hranjenje identifikacije lastnika (informacije o podpisu, IMSI) in varna avtentikacija mobilnega telefona v omrežje. Poleg tega pa je na SIM kartico možno shraniti še vpise v telefonskem imeniku, tekstovna sporočila, informacije o trenutni lokaciji in razne dodatne storitve ter aplikacije, ki jih določa posamezni mobilni operater. Zelo pomembno je, da so te funkcije in podatki na SIM kartico vpisani na način, ki preprečuje nepooblaščeno branje in spreminjanje podatkov.

3.1 Podatkovni elementi

Pomembnejši podatkovni elementi v zvezi s SIM kartico, so:

- sheme za kodiranje alfanumeričnih znakov,
- SST (SIM Service Table): storitve, ki jih SIM podpira in so omogočene poleg samega prenašanja zvoka (npr. SMS sporočila),
- FDN (Fixed Dialing Number): seznam številk, ki se jih lahko kliče iz mobilnega telefona, ko so ostale blokirane,
- ICCID (Integrated Circuit Card ID): 19 ali 20 številčna serijska številka SIM kartice, sestavljena iz številke izdajatelja in individualnega računa,
- IMEI (International mobile Equipment Identity): enolična označba mobilne naprave, običajno sestavljena iz 15 številk, ki predstavljajo potrditveno kodo, kodo proizvajalca, serijsko številko ter kontrolno številko (pri kraji se mobilna naprava lahko blokira preko IMEI številke),
- IMSI (International Mobile Subscriber Identity): enolična mednarodna identiteta naročnika, sestavljena iz kode države, kode mobilnega omrežja in identifikacijske številke mobilne postaje. Prek omrežja se zaradi varnosti prenese le, ko je to nujno potrebno, na primer ob vklopu mobilnega telefona.
- LAI (Location Area Information): enolična informacija o položaju mobilne naprave. Uporablja se v kombinaciji s TMSI (glej naslednjo alinejo) za generiranje enolične identitete naročnika. Sestavljena je iz kode države, omrežja in lokacije.
- TMSI (Temporary Mobile Subscriber Identity): enolična začasna identiteta naročnika, izračunana iz IMSI. Po uspešni avtentikaciji se uporablja namesto IMSI, spremeni se ob spremembi lokacije mobilne naprave. Za razliko od IMSI, ki velja po vseh GSM omrežjih na svetu, TMSI velja v delu omrežja in je enolična skupaj s LAI.
- ADN (Abbreviated Dialing Numbers): seznam shranjenih telefonskih številk s pripadajočimi podrobnostmi (npr. ime, priimek),
- SMS (Short Message Service): storitev, ki omogoča pošiljanje sporočil iz alfanumeričnih znakov po omrežju preko signalizacijskega kanala. Namenjena je prenosu sporočil naročnika ter prenosu podatkov do mobilnega telefona.

- MSISDN (Mobile Station ISDN Number): številka mobilne naprave (odvisna je od IMSI),
- K_c: 64-bitni sejni ključ za šifriranje prometa med mobilno postajo in omrežjem, generira se med avtentikacijo, spremeni se za vsako sejo (klic),
- K_i: 128-bitno število, ki se uporablja pri avtentikaciji SIM kartice v omrežje. Shranjeno je na kartici ter v avtentikacijskem centru mobilnega operaterja. Nikoli se ne prenaša nikamor, saj na njem temelji varnost avtentikacije.

Kot bo vidno pri opisu avtentikacije v naslednjem poglavju, varnost temelji na ključu K_i. Pri tem se postavlja vprašanje, kako lahko zagotovimo, da je ključ res varno shranjen tako na SIM kartici kot v avtentikacijskem centru. Vdor v SIM kartico bi lahko naredil škodo le lastniku, medtem ko je varnost avtentikacijskega centra še pomembnejša, saj so tam shranjeni ključi vseh uporabnikov. SIM kartica je pred fizičnim vdorom zaščitena tako, da se uniči (angleško 'tamper resistance'). Avtentikacijski center pa vsebuje strojni varnostni modul (HSM - Hardware Security Module), kjer so shranjeni ključi (več v [14]), in imajo do njega dostop le določeni uslužbenci mobilnega operaterja.

3.2 Zgradba in oblika

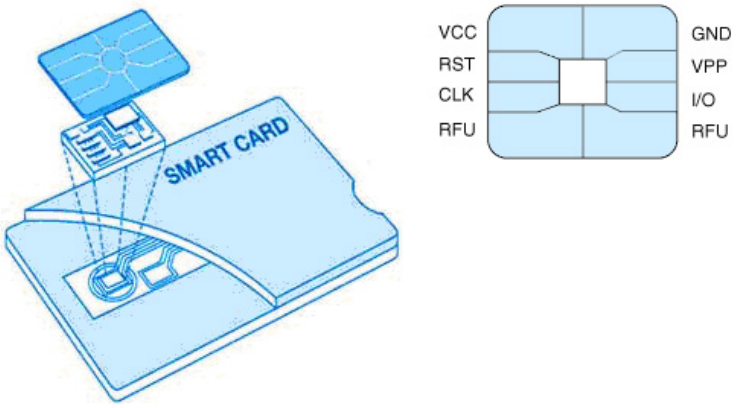
SIM kartice obstajajo v dveh oblikah. Večja oblika je kot navadna kreditna kartica, dimenzij $85,60 \times 53,98 \times 0,76$ milimetrov (ID-1 format). Namenjena je predvsem večkratnemu menjavanju, ko na primer več uporabnikov uporablja isti telefon, vsak s svojo kartico. Miniaturna, vsem bolj znana oblika pa je velikosti 25×15 milimetrov (ID-000 format). Uporablja se v mobilnih telefonih, ko pogostejša menjava ni potrebna. Edina razlika med obema je fizična velikost nosilca (plastike), sicer pa oba formata kartice vsebujeta enako notranjo logiko in komponente. Okoli leta 1995 je dostopnost mobilnih telefonov vplivalo na vse večjo uporabo kartic manjšega formata, ki so izpodrinile večjo obliko.

Glede na dimenzije ima kartica zanimivo zgradbo, je kot pravi računalnik v malem. Sestavljena je iz vodila in nanj priključenih modulov:

- pomnilnik, ki je razdeljen na tri dele: bralni (ROM), trajno bralni (EPROM) in delovni (SRAM)),
- centralna procesna enota, ki zagotavlja ustrezno varnost,
- vhodno-izhodne enote, ki berejo in pišejo podatke v pomnilniku s pomočjo CPE,

- modul za zaščito,
- signal za uro,
- signal za reset.

Na sami kontaktni površini ima kartica še napajanje in ozemljitev, dva kontakta pa sta rezervirana za prihodnjo uporabo.



Slika 4: Zgradba SIM kartice

3.3 PIN koda

SIM kartica je pred nezaželenimi uporabniki mobilnega telefona varovana s tako imenovano PIN (Personal Identification Number) kodo - geslo dolžine od štiri do osem znakov, ki se vnese ob vklopu mobilnega telefona. Služi kot avtentikacija uporabnika v nek sistem, v našem primeru v mobilni telefon (naročnik se predstavi SIM kartici) in posledično omrežje. Brez poznavanja PIN kode je dostop uporabnika do SIM kartice onemogočen, brez vpisanega gesla PIN je možen le klic na številko 112.

Glede na dolžino gesla PIN je očitno, da bi bilo možno kodo uganiti v največ 10^8 poskusih (največja možna dolžina je 8). Vendar ima SIM kartica varovalo tudi za napad s poskušanjem vseh možnosti. Po trikratnem napačnem vnesenem geslu PIN se SIM kartica zaklene. Za nadaljnjo uporabo jo je možno odkleniti z vnosom PUK (Personal Unblocking Key) kode, ki je zaradi varnosti običajno daljša kot PIN. Če napadalec nato še desetkrat napačno vnese PUK geslo, se SIM kartica trajno blokira in postane neuporabna. Zaradi te blokade se potrebuje oziroma proizvede več SIM kartic, kot bi bilo potrebno, če bi se PUK koda lahko spreminjala ali če se SIM

kartica ne bi trajno blokirala. Razlog, da se to kljub temu uporablja, je skrit v varnosti. Če se SIM ne bi blokirala in bi lahko napadalec v nedogled vpisoval PUK geslo, bi ga ugotovil s poskušanjem vseh možnosti.

4 VARNOST

GSM sistem za prenašanje podatkov med naročniki uporablja radjske zveze, ki so še posebej občutljive na zlorabo. Napadalci uporabljajo lažne mobilne postaje, lažne bazne postaje za prisluškovanje ter se izdajajo za druge naročnike (glej poglavje 5 o napadih). Zato mora imeti omrežni sistem GSM varnostne mehanizme za:

- varovanje dostopa do mobilnih storitev,
- avtentikacijo naročnika v omrežje,
- varovanje podatkov, ki se prenašajo po radijski poti (šifriranje podatkov),
- zagotovljanje zasebnost naročnikov,
- varno shranjevanje zasebnih ključev.

4.1 Varnostni algoritmi

Za zagotavljanje varnosti v GSM komunikaciji se uporabljajo trije algoritmi: A3, A5 in A8. Spodaj sledijo krajši opisi algoritmov, podrobnejši opisi so v viru [3].

A3

A3 je avtentikacijski algoritem (avtentikacija je tipa izziv-odgovor), ki ga vsebuje SIM kartica ter HLR del omrežnega podsistema mobilnega operaterja. Glavna naloga algoritma je avtentikacija identitete lastnika mobilnega telefona. Implementacija samega algoritma ni določena in je odvisna od omrežja.

Pomembno pri algoritmu A3 je, da izhod ne daje nobene informacije o vhodu (iz izhoda se ne da izračunati ali uganiti vhoda), običajno je tipa enosmerna hash funkcija. Algoritem iz 128-bitnih K_i in RAND generira 32-bitni ključ $SRES_1$ na strani SIM kartice oziroma $SRES_2$ v avtentikacijskem centru.

V praksi največ operaterjev za implementacijo A3 algoritma uporablja eno izmed verzij algoritma COMP128.

A5

A5 je algoritem za šifriranje in odšifriranje. Algoritem je standardiziran, specifikacije pa niso javno dostopne. Implementacija je skupna za vse operaterje, kar omogoča komunikacijo brez zapletov v vseh omrežjih (med seboj se morata razumeti SIM kartica enega in bazna postaja drugega operaterja).

A5 algoritem se nahaja na mobilni napravi v SIM kartici ter na kontrolerju baznih postaj. Namenjen je šifriranju podatkov in klicev, ki se pošiljajo med mobilno in bazno postajo. Algoritem je sestavljen iz treh vzporedno delujočih pomičnih registrov z linearnim odzivom (tokovna šifra LFSR) različnih dolžin (19, 22 in 23 bitov) ter šifrira vsak okvir (en okvir predstavlja 228-bitov podatkov), ki se prenese med mobilno in bazno postajo, z drugim tokom šifer.

Obstaja več različic algoritma A5:

- A5/0: ne uporablja enkripcije (podatki se ne šifrirajo), operaterji ga redko vklopijo, največkrat ob kakšnih tehničnih težavah v omrežju,
- A5/1: osnovna različica, uporablja 64-bitni ključ, uporablja se predvsem v Evropi,
- A5/2: uporablja krajši kjluč,
- A5/3: različica z močnejšo zaščito kot A5/1, uporablja se v tretji generaciji mobilnih naprav.

A8

Algoritem A8 je namenjen generiranju kodirnega ključa K_c. Podobno kot A3 algoritem se nahaja na SIM kartici ter na HLR delu omrežnega podsistema operaterja. Implementacija je odvisna od posameznega operaterja, večina mobilnih operaterjev pa uporablja kar predlagano implementacijo - okvirni algoritem COMP128.

A8 generira 64-bitni ključ K_c za vsako sejo posebej. Generira ga iz izziva RAND, odgovora SRES in ključa K_i. Ključ K_c se uporabi za kriptiranje podatkov in zvoka pri algoritmu A5. SIM kartica K_c izračuna sama, bazna postaja pa ga prejme od preklopnega centra. Nato se s ključem K_c kriptira promet med njima.

COMP128

Algoritem, imenovan COMP128, je največkrat uporabljen za implementacijo A3 in A8 algoritmov. Uporablja se za avtentikacijo mobilne postaje bazni postaji ter za inicializacijo šifrirnega algoritma A5. Do leta 1998 ni bil javno objavljen, nato pa je del specifikacij postal znan in so algoritem razbili (ugotovili njegovo delovanje).

Slika 5: Vhod in izhod algoritmma COMP128

Od takrat se uporabljata izboljšani verziji COMP128-2 in COMP128-3, ki še nista javno objavljeni.
Vhod algoritma:

- 128-bitno število RAND (izziv),
- 128-bitni zasebni ključ K_i.

Iz zgornjega vhoda algoritem generira izhod, dolg 128 bitov, dejansko pa se uporabi le 86 bitov izhoda:

- 32 bitov predstavlja SRES za avtentikacijo,
- 54 bitov se uporabi za inicializacijo LFSR toka za A5 algoritem (ki sicer potrebuje 64 bitov, zato se zadnjih 10 nastavi na 0).

Potek algoritma:

- vhoda RAND in K_i se s konketinacijo zdruzita v vhod x,
- vhod x se z zgoščevalno funkcijo zgosti 8-krat, da postane dolg 128-bitov,
- za vsakim zgoščevanjem, razen v zadnjem krogu, se vrednost x permutira,
- po osmih krogih se zgoščena vrednost uporabi kot izhod algoritma.

Zgoščevalna funkcija je sestavljena iz 5 nivojev, v vsakem je za substitucijo uporabljena druga S-škatla. Osnovni princip funkcije je metuljčna struktura (butterfly structure, tj. pozicija po dveh vrednosti v tabeli se zamenja). 16 parov po 16 bitov vhoda (skupaj 256 bitov) se skozi substitucije zreducira na 16 parov po 4 bite (skupaj 128 bitov).

4.2 Avtentikacija

GSM avtentikacija poteka med mobilno postajo, bazno postajo in omrežnim podsistemom mobilnega operaterja. Avtentikacija je tipa izziv - odgovor in se izvede v več korakih (glej sliko 6):

1. Mobilna postaja se želi prijaviti v omrežje (običajno po vklopu in vpisani PIN kodi), zato pošlje prošnjo za avtentikacijo (authentication request) s svojo IMSI (oziroma TMSI skupaj z LAI, razlika je opisana v poglavju 3.1) številko najbližji bazni postaji. Ta posreduje podatke preklopnemu centru, MSC pa jih pošlje naprej omrežnemu podsistemu, natančneje v HLR. Če se mobilna postaja nahaja v tujem omrežju, se trojka iz naslednjega koraka pošlje še do VLR.

2. Ko HLR prejme IMSI mobilne postaje, generira naključno 128-bitno število RAND (glej poglavje 4.2.1), ki predstavlja izziv za mobilno postajo. Nato AuC s pomočjo K_i ter algoritma A3 generira $SRES_1$, 32-bitni ključ (signed response, zakriptiran RAND) in z algoritmom A8 šifrirni ključ K_c. Trojko (RAND, $SRES_1$, K_c) HLR pošlje preklopnemu centru.

   Ko se mobilna naprava prvič prijavi v neko omrežje, avtentikacijski center pravzaprav generira pet različnih trojk (RAND, SRES, K_c). Vsaka izmed njih se porabi pri eni avtentikaciji te mobilne naprave v omrežje. Ko trojk zmanjka, se generirajo nove in se spet posredujejo preklopnemu centru.

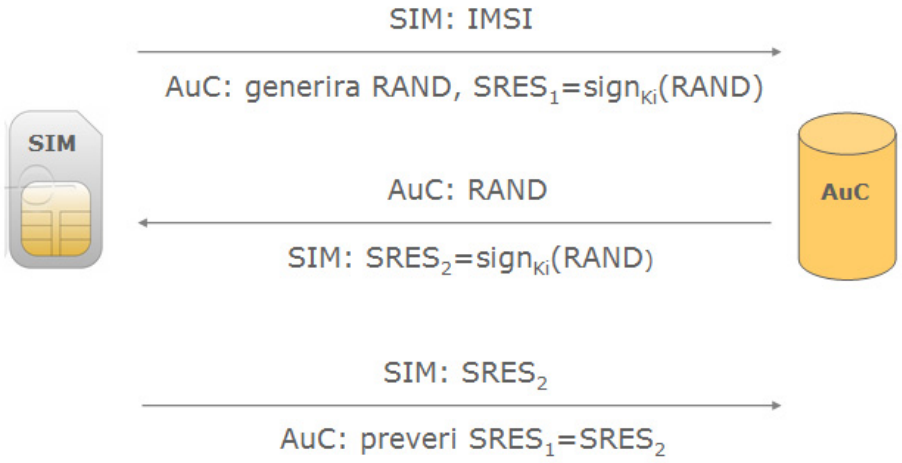
3. SIM kartica dobi izziv RAND in na enak način kot AuC izračuna $SRES_2$ (z algoritmom A3 in ključem K_i zakodiran RAND). $SRES_2$ pošlje nazaj prek bazne postaje do MSC.

4. Preklopni center preveri, ali se $SRES_1$ in $SRES_2$ ujemata. Če se, je avtentikacija uspela in mobilna postaja lahko uporablja storitve omrežja. SIM kartica ob prvi avtentikaciji prejme še začasno številko TMSI.

5. Po uspešni avtentikaciji dobi podsistem bazne postaje sejni ključ K_c, SIM kartica ga izračuna sama. Z njim se kriptira nadaljnji promet med bazno in mobilno postajo.

4.2.1 Generiranje naključnih števil

Avtentikacijski center vsebuje psevdo-naključni generator števil, ki generira naključna 128-bitna števila RAND v postopku avtentikacije. Število RAND se generira za



Slika 6: Poenostavljen potek avtentikacije SIM kartice v omrežje

vsako avtentikacijo posebej. Kakšen naj bo generator naključnih števil, v specifikacijah GSM sistema ni predpisano. Veljati pa mora:

1. vrednost RAND se za določenega uporabnika ne sme nikoli ponoviti, kar se doseže s tem, da algoritem generira dolge cikle brez ponavljanja. Matematično pa je zaradi paradoksa rojstnih dni težko zagotoviti, da se števila ne bodo ponovila, lahko se zagotovi le, da se bodo ponovila z majhno verjetnostjo.

2. vrednosti RAND naj ne bo mogoče napovedati - napoved je težka že zaradi velikosti prostora, ker je število 128-bitno in je vseh možnosti 2^{128}.

Več v [14] (poglavje 3.2.2).

4.2.2 Pomankljivosti avtentikacije

V postopku avtentikacija je že na prvi pogled opaznih nekaj pomanjkljivosti:

- SIM kartica se avtenticira avtentikacijskemu centru in omrežju, medtem ko obratne avtentikacije ni; AuC je lahko kdorkoli, ki pozna ključ K_i. Uporabnik mobilne naprave ne more biti siguren, da je povezan v pravo ali v ponarejeno omrežje. Varnost avtentikacije tako temelji le na skrivnem ključu K_i.

- Isti ključ K_c se uporablja toliko časa, dokler se mobilna postaja na novo ne avtenticira preklopnemu centru, kar lahko traja tudi nekaj dni. Ključ K_c se tako ne spreminja med posameznimi klici. Promet med bazno in mobilno postajo se lahko odšifrira s poznavanjem ključa K_c in velikosti okvirjev.

- Preneseni podatki in govorni signali so kriptirani le na radijski poti med mobilno in bazno postajo, drugje se pojavljajo v odprti obliki in so zaščiteni le s fizično zaščito dostopa.
- Zaradi napredka računalniške tehnologije, načina šifriranja podatkov ter dolžine ključev, je nivo zaščite v nekaj letih zelo upadel.
- Zaradi tehničnih razlogov mora mobilna naprava posredovati svojo trenutno lokacijo bazni postaji vsake toliko časa. Taki podatki se lahko uporabijo za izsledite gibanja naročnika mobilne naprave (kar posega v zasebnost posameznika, zato lahko podatke v večini državah pridobijo le uradni organi, na primer policija za iskanje pogrešanih ljudi).

Zgornje varnostne luknje omogočajo kar nekaj različnih napadov, ki so podrobneje opisani v naslednjem poglavju.

4.2.3 Dobre strani avtentikacije

Kljub vsem slabim luknjam pri poteku avtentikacije, je nekaj stvari tudi dobro rešenih:

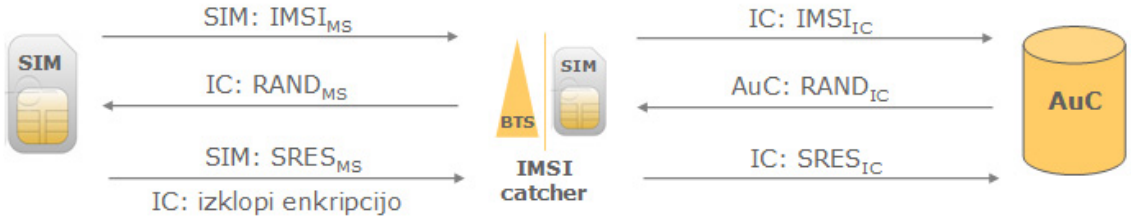
- Skrit ključ K_i poznata SIM kartica in avtentikacijski center, zato ni potrebe, da bi se kakorkoli prenašal brezžično.
- Če se mobilna naprava nahaja v tujem omrežju, dobi VLR trojke od domačega avtentikacijskega centra in tujemu ni treba poznati algoritmov A3 in A5. Tako ima lahko vsako omrežje svojo implementacijo obeh algoritmov, brez da bi to predstavljajo kakšno oviro.

5 NAPADI

5.1 Virtualna bazna postaja

Napad v obliki predstavljanja kot bazna postaja (IMSI catcher) izkorišča prvo izmed zgoraj naštetih pomankljivosti avtentikacija, ki pravi, da se SIM kartica avtenticira bazni postaji, le-ta pa se ne avtenticira nazaj. Virtualna bazna postaja je naprava za identificiranje IMSI-jev bližnjih mobilnih naprav, s katero lahko napadalec prestreže in posluša klice napadenega. Mobilni napravi se predstavi kot bazna postaja, bazni postaji pa kot mobilna naprava (s SIM kartico).

Namišljena bazna postaja prisili mobilno napravo, da se poveže nanjo in pri enkripciji uporablja algoritem A5/0 (ki pravzaprav ne uporablja nobene enkripcije).



Slika 7: Poenostavljen potek avtentikacije z uporabo virtualne bazne postaje

Tako lahko IMSI catcher prestreže podatke, ki bi se sicer prenašali med mobilno in pravo bazno postajo - virtualna bazna postaja izvede napad imenovan 'man-in-the-middle-attack'. Uporaba takšne virtualne postaje je v večini držav z zakonom prepovedana.

Vsaka mobilna naprava je narejena tako, da optimizira sprejem, zato se prijavi na bazno postajo, katere sprejem je na danem mestu najboljši. Virtualna bazna postaja z dobrim sprejemom povzroči, da se v okviru nekega radija vse mobilne naprave priklopijo nanjo. S posebno prošnjo o identitei (identity request) zahteva od mobilnega telefona, da ji sporoči IMSI številko. Pri tem lahko napadalec naleti na kar nekaj problemov, če želi pridobiti IMSI točno določene mobilne naprave:

- mobilna naprava napadenega mora biti prižgana in priklopljena v omrežje,
- med vsemi IMSI-ji, ki jih prestreže, mora najti pravega,
- naenkrat se lahko poveže le na eno SIM kartico in prestrega le njene klice, dohodnih klicev pa sploh ne more spremljati,
- blizu prave bazne postaje ima le-ta dovolj dober signal, da se bo mobilna naprava povezala nanjo, ne na virtualno,
- nekatere mobilne naprave ob ne-uporabi enkripcije o tem obvestijo lastnika z opozorilnim znakom na zaslonu.

5.2 Kloniranje SIM kartice

Pri napadu s kloniranjem SIM kartice gre za to, da napadalec prevzame identiteto napadenega in uporablja storitve na njegov račun. S tem lahko naredi velike stroške napadenemu ali celo operaterju omrežja. Osnovna ideja pri kloniranju je zajemanje in snemanje signalov ter odšifriranje kodirnih algoritmov, ki se uporabljajo pri pošiljanju in sprejemanju informacij z mobilno napravo. Prvotno so bile te vrste zlorab le telefonski klici, z razvojem na primer m-bančništva pa je problem postal bolj pereč.

Varnost GSM sistema temelji na skrivnem zasebnem ključu K_i. Če napadalec odkrije ta ključ, lahko ne le posluša naročnikove klice, temveč lahko tudi kliče na račun napadenega. GSM sistem sicer ima rešitev pred slednjim problemom: ko omrežje zazna, da sta aktivni dve mobilni napravi z enakim ID-jem naenkrat na različnih lokacijah, avtomatsko blokira naročniški račun. Tako se hitro prepreči klicanje na račun napadenega, ne ustavi pa poslušanja klicev. Pri tem napadalec ostane skrit, neaktiven in neviden omrežju.

Ključ K_i je možno pridobiti na dva načina: s fizičnim dostopom do SIM kartice, prav tako pa so že odkrili način, kako K_i odkriti na daleč, brez fizičnega kontakta s kartico. V prvem primeru se kartica SIM preko čitalca kartic priključi na računalnik. Nato se ji pošlje veliko (na primer 150.000) izzivov, da SIM generira odgovor SRES in sejni ključ K_c. K_c temelji na izzivu in skrivnem ključu K_i ter se ga da izračunati iz odgovora (SRES) kartice. Identično kopijo kartice je možno narediti v nekaj urah. Pri tem je potrebno omeniti še, da je možno s fizičnim dostopom klonirati SIM kartice, ki uporabljajo prej omenjeni algoritem COPM 128. Novejše verzije algoritma pa zaenkrat tak napad preprečujejo - COMP128-3 generira daljši, 64-bitni ključ K_c, namesto 54-bitnega, ki ima dodanih 10 ničel. Sicer pa sta implementaciji novejših algoritmov COMP128 verzije 2 in 3 še v tajnosti.

Raziskovalci SDA in ISAAC so prepričani, da so odkrili napad kloniranja SIM kartice tudi po brezžičnem kanalu, a svojih trditev ne morejo preveriti, saj je uporaba takšne opreme v ZDA nelegalna. Napad temelji na dejstvu, da se bo mobilna naprava odzvala vsakemu izzivu GSM omrežja. Podobno kot pri napadu z virtualno bazno postajo je potrebno tudi v tem primeru narediti virtualno bazno postajo, ki mobilni napravi neprestano pošilja izzive. Iz odgovorov lahko nato napadalec rekonstruira ključ K_i. V času pošiljanja izzivov mora biti mobilna naprava ves čas v dosegu virtualne bazne postaje, mogoče pa je napadati v območjih brez signala ter vsak dan po malem (ne naenkrat).

Na novejših SIM karticah se že uporablja preprečevanje napada s pošiljanjem velikega števila izzivov. Kartica je zavarovana tako, da se po prejetem velikem številu (na primer 2^{16}) izzivov zaklene.

Podobno kot iz SIM kartice je teoretično možno pridobiti ključ K_i tudi od avtentikacijskega centra omrežja. AuC mora, kot SIM kartica, odgovoriti na vse izzive, in vrne avtentikacijske trojke. Razlika z napadom na SIM kartico je v tem, da avtentikacijski center stvari izračuna veliko hitreje ter da ga je zaradi varnostnih mehanizmov težje napasti.

6 NOVEJŠE TEHNOLOGIJE

Zaradi zahtev po večji varnosti v GSM sistemu ter uvajanju dodatnih storitev (na primer certifikati na SIM kartici) so se razvili novi sistemi. Spodaj sta na kratko opisana dva, UMTS , kot predstavnik tretje generacije mobilnih tehnologij, ter WPKI, ki omogoča uporabljanje certifikatov v mobilnem sistemu.

6.1 UMTS

Pri UMTS (Universal Mobile Telecommunications System) sistemu je v primerjavi z GSM sistemom odpravljenih kar nekaj varnostnih lukenj:

- dvosmerna avtentikacija: poleg tega, da se mobilna naprava avtenticira omrežju, se tudi omrežje avtenticira mobilni napravi, s čimer se preprečijo napadi z virtualno bazno postajo,
- integriteta podatkov: postaja, ki prejema (mobilna ali bazna), preveri avtentičnost vsakega prejetega podatka, kar je spet obramba pred napadom z virtualno bazno postajo,
- varna komunikacija znotraj omrežja in med omrežji (uporaba IPsec-a),
- širše varnostno območje: namesto baznih postaj so radijski omrežni kontrolerji (RNC - Radio Network Controller),
- večja fleksibilnost: varnostne storitve se lahko širijo,
- varnejše aplikacije (USIM kartica),
- uporabniki vidijo kakšen nivo varnosti uporabljajo in ga lahko spreminjajo,
- daljši ključi: dolžina ključa je 128 bitov, namesto 64, kot v v GSM sistemu.

Več o UMTS sistemu v [17], [18] (poglavje 4) in [19].

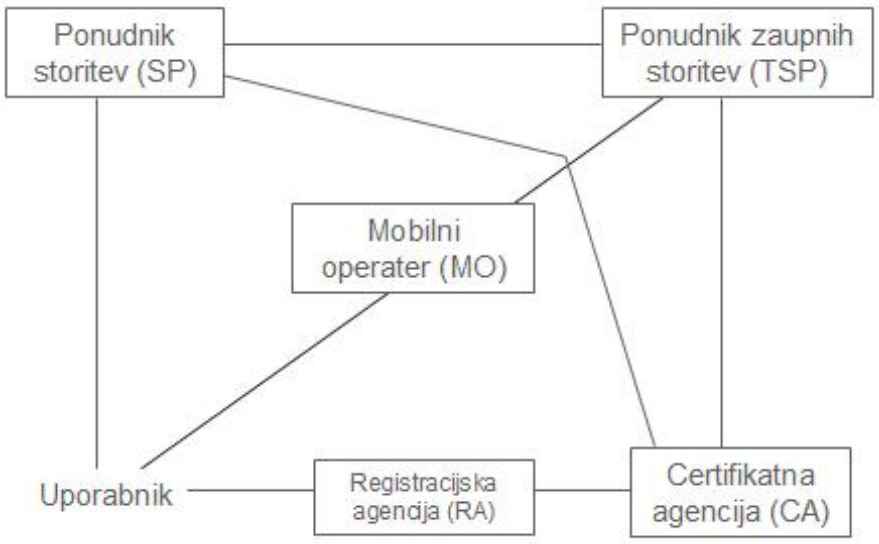
6.2 WPKI

WPKI (Wireless Public Key Infrastructure) je infrastruktura javnih ključev, namenjena varni interakciji v ne varnem okolju (na primer internet) na mobilnih napravah. Vlogo nosilca certifikata namesto pametne kartice ali trdega diska prevzeme kartica SIM.

PKI SIM kartica je navadna SIM kartica, dopolnjena s funkcijo PKI. Dodan je procesor, ki skrbi za dešifriranje in identifikacijo s privatnim ključem. PKI SIM kartica vsebuje poseben prostor za shranjevanje privatnih ključev za digitalno podpisovanje. S tem uporabniku omogoča avtentikacijo in generiranje digitalnih podpisov.

Celotna infrastruktura WPKI je sestavljena iz:

- certifikatne agencije (CA - Certification Authority) - skrbi za izdajo ter preklic certifikatov,
- registracijske agencije (RA - Registration Authority) - zbirka podatkov o naročnikih, ki skrbi za preverjanje istovetnosti uporabnikov ter zamenjavo navadne SIM kartice za PKI SIM kartico,
- ponudnik zaupnih storitev (TSP - Trusted Service Provider) - omogoča PKI storitve za ponudnike storitev, povezan je z omrežjem ostalimi entitetami infrastrukture, da zagotavlja osnovne stvari, kot sta avtentikacijo uporabnika in podpisovanje e-dokumentov,
- mobilnega operaterja (MO) - omogoča in skrbi za dostop do kriptografskih storitev na SIM kartici za vse ponudnike zaupnih storitev,
- ponudnika storitev (SP) - kreira e-storitve, ki temeljijo na WKPI.



Slika 8: Infrastruktura WPKI

V WPKI so pomembni štirje procesi: priprava SIM kartice, aktivacija, uporaba in prenehanje certifikata.

Priprava SIM kartice

SIM kartica se pripravi tako, da bodo na njej lahko kvalificirani certifikati:

- registracijska agencija vzpostavi identiteto uporabnika in mu dostavi SIM kartico (osebno),
- certifikat naprave na kartici postane aktiven in dosegljiv TSP-jem,
- uporabnik dobi aktivacijsko kodo za kvalificiran certifikat.

Aktivacija certifikata

Namen je generiranje in aktivacija certifikata:

- uporabnik poda zahtevo za aktivacijo certifikata,
- RA sproži zahtevo za podpis (signing request) osebnih podatkov na mobilni napravi,
- uporabnik preveri podatke in jih podpiše z vpisom aktivacijske kode,
- RA sprejme podpisane podatke, doda še dodatne podatke (med drugim certifikat naprave) in pošlje prošnjo za certifikat certifikatni agenciji,
- CA generira in aktivira kvalificiran certifikat ter ga objavi.

Uporaba certifikata

Uporaba storitve z avtentikacijo poteka v 5 korakih (postopek med SP in TSP, ko želi uporabnik dostopati do neke storitve):

- SP od TSP zahteva identiteto uporabnika (osebna ID koda ali telefonska številka),
- TSP generira zahtevo za podpis in jo pošlje uporabniku,
- uporabnik podpiše zahtevo z vpisom gesla,
- TSP prejme podpisane podatke, preveri njihovo veljavnost in veljavnost certifikata pri certifikatni agenciji,
- TSP pošlje ponudniku storitev podatke o identiteti uporabnika.

Preklic certifikata

Uporabnik se lahko odloči, da storitev PKI več ne bo uporabljal:

- registracijska agencija obvesti CA o preklicu certifikata,
- CA takoj prekliče certifikat in osveži listo preklicanih certifikatov (CLR),
- če se je uporabnik odločil, da storitev ne bo uporabljal zaradi izgubljene ali poškodovane SIM kartice, se prekliče še certifikat naprave pri vseh TSP-jih.

7 ZAKLJUČEK

V okviru izdelave seminarske naloge sem med drugim poskušala odgovoriti na vprašanje varnih pogovorov, prisluškovanj in vlogo SIM kartice pri tem. Osredotočila sem se predvsem na GSM sistem, novejše sisteme sem omenila le na kratko. Ugotovila sem, da ima GSM sistem luknje v varnosti, ki jih uspešno popravljajo, prav tako uspešno pa napadalci spet in spet odkrivajo nove. A vseeno se je SIM kartica obdržala in omogoča dokaj varen način komunikacije, varnost SIM kartice kljubuje raznim napadom. S spreminjanjem in posodabljanjem funkcij, kartica ohranja stik s časom in napadalci (PKI SIM kartica, USIM). Če vzamem na primer problem enosmerne avtentikacije, je rešen že pri novejšem sistemu UMTS, kjer je avtentikacija dvosmerna. Je pa najbrž le vprašanje časa, kdaj bodo tudi pri tem odkrili napake. Zato bi v primeru strogo zaupnih stvari raje priporočala star način pogovora na štiri oči. A seveda le v primeru, da prisluškovalcev ni kje blizu...

Literatura

[1] W. Rankl, W. Effing: Smart Card Handbook, third edition, Wiley, 2003, strani 735-789

[2] D. Strobel: IMSI-catcher, Ruhr-University of Bochum, 2007

[3] T. Zupančič: Pregled varnosti pri komunikaciji z GSM, Ljubljana, 2006

[4] A. Alazeib: An Ontology for Generic Wireless Authentication, Stuttgart, 2005

[5] L. Šolc: Varnost v mobilnem telefonskem omrežju tretje generacije, delavnica VITEL 2003

[6] Enciklopedija Wikipedia: http://en.wikipedia.org

[7] Y. Li, Y. Chen, T. Ma: Security in GSM

[8] A. Jurišić, J. Tonejc: Napadi in obrambe: velike skrivnosti malih kartic, Monitor 11/9 (september 2001), strani 44-51

[9] C. J. Mitchell: The security of the GSM air interface protocol, University of London, 2001

[10] L. Pesonen: GSM Interception, Helsinki University of Technology, 1999

[11] S. He: SIM Card Security, Ruhr-University of Bochum, 2007

[12] Zavod za zdravstevno zavarovanje Slovenije, http://www.zzzs.si/zzzs/internet/zzzs.nsf/o/065D1D9A6605B629C1256E8B002FBC61

[13] B. Clark: Electronic Wallets: Past, Present, and Future, GPayments

[14] Philipp Suedmeyer: COMP128, Ruhr-University Bochum, Germany, 2006

[15] G. M. Koien: Entity Authentication and Personal Privacy in Future Cellular Systems, 2009

[16] E3PWork Group: WPKI specification, 2007

[17] V. Prajapati, V. Sevani, O. Pal, S. Rana: GSM and UMTS Security, Indian Institute of Technology, Bombay, 2007

[18] K. Mayers, K. Markantonakis: Smart Cards, TOkens, Security and Applications, Springer, 2008

[19] M. Gupta: 3G Security Principles, 2001