Sigurnost pokretnih komunikacijskih sustava

Milić, Dean

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Dean Milić

SIGURNOST POKRETNIH KOMUNIKACIJSKIH SUSTAVA

ZAVRŠNI RAD

ZAGREB,2015.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

SIGURNOST POKRETNIH KOMUNIKACIJSKIH SUSTAVA

Security of Mobile Communication Systems

Mentor: Ivan Forenbacher, dipl.ing.

Student: Dean Milić ,0135185047

Zagreb, rujan.2015.

SAŽETAK

Sigurnost prometa u javnom pokretnom tekomunikacijskom prometu je jako važna stavka u pružanju telekomunikacijskih usluga. Da bi se zaštitila povjerljivost i pružila sigurnost, mrežni operateri su morali poduzeti razne mjere sigurnosti kako bi se zaštitili davatelji usluga i korisnici od raznih zlonamjernih napada. Međutim, evolucijom javne pokretne mreže, povećao se broj dostupnih usluga i zlonamjernih napada. Mrežni operateri morali su implementirati različite nove sigurnosne mjere kako bi osigurali pouzdano i sigurno korištenje suvremenih mobilnih usluga. Fokus ovoga rada je pružiti uvid u nove prijetnje i sigurnosne mehanizme za javne pokretne telekomunikacijske mreže.

KLJUČNE RIJEČI: sigurnost ; zaštita ; napad ; mjere sigurnosti ; povjerljivost

SUMMARY

Security of public land mobile network traffic is a very important factor in the provisioning of telecommunication services. Mobile providers need to implement security measures in order to ensure confidentiality and protection from various malicious attacks, both to service providers and end-users alike. Evolution of mobile network has increased both the number of services offered and malicious attacks. Therefore, providers had to deploy diverse new security mesaures to ensure reliable and safe use of modern mobile servies. The focus of present work is to discuss emerging threats and defense mechanism for mobile networks. .

KEYWORDS: security ; protection ; attack ; security measures ; confidentiality

SADRŽAJ

1. UVOD 1
2. ARHITEKTURA 3G POKRETNIH KOMUNIKACIJSKIH SUSTAVA 3
2.1. Mobilna stanica – MS 3
2.2. Podsustav baznih stanica BSS 5
2.2.1. Bazna stanica – BTS 5
2.2.2. Upravitelj bazne stanice – BSC 7
2.3. Mrežni komutacijski podsustav – NSS 7
2.3.1. Prospojni centar mobilnih usluga – MSC 8
2.3.2. Registar domaćih pretplatnika – HLR 9
2.3.3. Registar gostujućih pretplatnika – VLR 10
2.3.4. Centar za autentifikaciju – AUC 10
2.3.5. Registar za identifikaciju mobilne opreme – EIR 11
2.4. Podsustav operacijske podrške - OSS 11
3. SIGURNOSNE PRIJETNJE POKRETNOM KOMUNIKACIJSKOM SUSTAVU 12
3.1. Sigurnosne prijetnje kod mobilnih uređaja 12
3.1.1. Tekstualne poruke 12
3.1.2. Kontakti i adresar 15
3.1.3. Video sadržaj 15
3.1.4. Prijepisi telefonskih razgovora 16
3.1.5. Povijest poziva 16
3.1.6. Dokumentacija 16
3.1.7. Upotreba međuspremnika 16
3.2. Sigurnosne prijetnje u GSM/GPRS/UMTS mrežama 17
4. NAPADI NA 3G MREŽE 20
4.1. Odbijanje usluge 21
4.2. Napad preusmjeravanjem 22
4.3. Napad preuzimanjem identiteta 23
5. MJERE SIGURNOSTI 24

5.1. Provjera autentičnosti i ključni sporazum 24
5.1.1. Internacionalni mobilni identitet pretplatnika 25
5.1.2. Privremeni identitet mobilne stanice 25
5.1.3. Provjera autentičnosti i procedura ključnih dogovora 26
5.1.4. Autentikacijski vektori 27
5.1.5. Tajni ključ u AKA mehanizmu 28
5.2. Povjerljivost 29
5.2.1. Povjerljivost korisničkog identiteta 29
5.2.2. Povjerljivost podataka 29
5.2.3. Funkcija povjerljivosti 29
5.3. Podatkovni integritet 30
5.3.1. Funkcija zaštite cjelovitosti podataka 30
5.4. Kasumi algoritam 31
5.5. Sigurnost ključeva u UMTS mreži 32
6. ZAKLJUČAK 34
Popis literature 35
Popis kratica 36
Popis slika 40
Popis tablica 41

1. UVOD

Sigurnost je jako bitan aspekt u ljudskom životu, kako u privatnom životu , tako i u poslovnom, te je jedna od najvažnijih stavki u životu čovjeka prema kojoj donosimo određene odluke, zaključke. U mobilnim mrežama sigurnosni su problemi vezani uz zaštitu razgovora, pozivnih podataka i sprečavanje prijevara putem mobilnih terminalnih uređaja. U starijim analognim sustavima bilo je jednostavno presresti i prisluškivati telefonske razgovore samo uz pomoć policijskog skenera. Sve moderniji (kompleksniji) mobilni uređaji omogućuju korisniku da sa sobom nosi pravo osobno računalo. Iako je korisniku vrlo koristan takav uređaj, uz njega se javljaju isti sigurnosni problemi kao i kod osobnih računala (npr. krađa identiteta, uskraćivanje usluga, neovlaštena uporaba, podmetanje zlođudnih programa i drugo). Unatoč rješavanju nekih sigurnosnih problema, sigurnosne prijetnje još uvijek postoje i napadači stalno smišljaju nove načine napada. Uspješni napadi na mobilnu mrežu uključuju prisluškivanje i/ili lažno predstavljanje, oponašanje mreže, preuzimanje kontrole nad dijelom sustava, ugroženim mrežnim čvorom ili vezom i izmjena, brisanje ili slanje lažnih signala te krađa korisničkih podataka.

Cilj rada je prikazati strukturu 3G pokretne mreže, način njenog rada, prijetnje i napade na pokretne mreže, mjere sigurnosti koje se koriste. Materija je izložena u šest poglavlja:

1. Uvod
2. Arhitektura 3G pokretnih komunikacijskih sustava
3. Sigurnosne prijetnje pokretnom komunikacijskom sustavu
4. Napadi na 3G mreže
5. Mjere sigurnosti
6. Zaključak

U drugom poglavlju, radi boljeg poznavanja problematike pokretnih mreža, ukratko su opisani njeni bitni elementi (mobilna stanica, podsustav bazne stane, mrežni sigurnosni servis i podsustav podrške za upravljanje) princip njihova rada i zadaće u sustavu u kojem djeluju. Također ukratko prezentiran rad registara domaćih i gostujućih pretplatnika, centra za autentikaciju, registra za identikaciju mobilne opreme, prospojnog centra mobilnih usluga i podsustava operacijske podrške.

U trećem se poglavlju govori o sigurnosnim prijetnjama, ovisno da li su usmjereni prema mobilnim uređajima ili mrežama. Pod prijetnjama kod mobilni uređaja pripadaju prijetnje na : tekstualne poruke, kontakte i adresar, video, prijepise telefonskih razgovora, povijest poziva, dokumentaciju i prijetnje upotrebi međuspremnika.

U četvrtom poglavlju su opisani napadi koji se koriste u 3G mrežama, kao što su čovjek u sredini, odbijanje usluge, napad preusmjeravanjem i napad krađe identiteta.

U petom poglavlju su opisane razne mjere sigurnosti koje se koriste u mobilnoj zaštiti, kao što su : provjera autentičnosti i ključni sporazum, povjerljivost, podatkovni integritet, Kasumi algoritam, te sigurnost ključeva u UMTS mreži.

2. ARHITEKTURA 3G POKRETNIH KOMUNIKACIJSKIH SUSTAVA

2.1. Mobilna stanica – MS

Mobilna stanica (engl. *mobile subscriber* ili *mobile station MS*) je korisnikov mobilni terminalni uređaj ili popularno nazvan mobitel. Vlasnik MS-a može biti pretplatnik te mreže u kojoj komunicira ili je pretplatnik kod drugoga operatera. MS je svima poznati uređaj sa kojim smo našu komunikativnost značajno unaprijedili. MS se sastoji od uređaja ME (engl. *mobile equipement*) i SIM (engl. *subscriber identity module*) kartice koja mu daje dio identiteta.

Kad je uključena, MS osluškuje mrežne signale koje odašilja BTS (engl. *base transciever station*) njene ćelije i okolnih ćelija te ih mjeri. BTS je dio mrežne opreme koji povezuje bežičnu komunikaciju između korisničke opreme i mreže, u principu to je antena koja emitira i prima radio valove i tako povezuje mrežu i korisničku opremu. Mjerenja koja poduzima MS se odnose na kvalitetu i jačinu signala. Na osnovu tih podataka MS odlučuje o prelasku pod okrilje susjedne BTS-e (engl. *handover*).

Mjerenja se provode u stanju rada i stanju pripravnosti (engl. *idle*) stanju. Mjerenja u stanju pripravnosti počinju prilikom uključenja MS-a. Nakon uključenja MS traži najjači signal u svim GSM frekventnim područjima[1], te analizira da li je to tzv. BCCH (eng. *Broadcast Control Channel*) nosioc. BCCH je jednosmjerni (*downlink*) kanal od točke prema više točaka i koristi se u Um sučelju kod GSM mobilnog standarda. BCCH nosi ponavljajući uzorak poruka informacija sustava koje opisuju identitet, konfiguraciju i dostupne mogučnosti BTS-a. MS čita BCCH informacije iz kojih doznaje npr. da li je BTS aktivna itd. Alternativno MS može na osnovu pohranjenih lista u svojoj memoriji potražiti frekventne nosioce za PLMN (eng. *Public Land Mobile Network*) u kojem se nalazi. Ukoliko ne nađe BCCH svoga operatera nego nekog drugog operatera, uključiti će se u tu mrežu pod uvjetom da njen domaći operater ima ugovore sa tim stranim operaterom. Ako ih nema registriranje i spajanje na mrežu nije moguće pa MS javlja da su mogući samo pozivi u slučaju opasnosti (engl. *emergency calls only*). Ako ni stranog BCCH nema, javiti će da nema mreže (engl. *no network*).

[1] Definirano je 14 frekventnih područja u ,a ona su :
T-GSM-380, T-GSM-410, GSM-450, GSM-480, GSM-710, GSM-750, T-GSM-810, GSM-850, P-GSM-900, E-GSM-900, R-GSM-900, T-GSM-900, DCS-1800, PCS-1900

Kada je jedanput taj proces prošao, MS je informirana o "svojoj" BTS-i ali i o tome koje nosioce rabe susjedne BTS-e tako da ona pozorno mjeri i njihove signale i u razdoblju kada se ne vodi nikakav razgovor.

Za vrijeme razgovora MS kontinuirano javlja preko signalnog SACCH kanala(*eng.slow associated control channel*) sustavu o snazi i kvaliteti primljenog osnovnog signala koji prima od BTS-e svoje ćelije ali i snazi primljenih signala od drugih BTS-a susjednih ćelija. Na osnovu toga BSC odlučuje kada će mobilnu stanicu predati drugoj BTS-i.[1]

Mobilni terminalni uređaj ili mobitel prijenosni je elektronički uređaj za komuniciranje na veće ili velike udaljenosti. Glavna komunikacijska funkcija je prijenos glasa, no u novije vrijeme dodane su funkcije kao: kratke tekstualne poruke (engl. *Short Message Service, SMS*), elektronička pošta, internet, registracija kontakta, korištenje kalkulatora, sata, alarma i sličnih funkcija te slike i video, multimedijalne poruke (eng. *Multimedia Messaging Service, MMS*), ali i popularni sadržaj su igre. Mobilni terminalni uređaji se razlikuju od prijenosnih telefona, po tome što imaju veći domet i nisu vezani uz jednu baznu stanicu. Osnovni koncepti za mobilnu telefoniju izumljeni su u Bell Labs 1947. [2]

SIM kartica

Modul identiteta pretplatnika ili identifikacijski modul pretplatnika je integrirani krug koji sigurno pohranjuje međunarodno označavanje pokretnih pretplatnika (eng. *International mobile Subscriber Identity, IMSI*) i povezni ključ koji se koristi za identifikaciju i autentifikaciju pretplatnika na mobilne telefonije uređaja (kao što su mobilni terminalni uređaji i računala).

SIM kartica je zamjenjiva plastična kartica koja se može prenositi između različitih mobilnih terminalnih uređaja. U početku su se SIM kartice radile u istoj veličini kao kreditne kartice (85, 60 mm x 53, 98 mm x 0, 76 mm). Razvojem fizički manjih mobilnih terminalnih uređaja potaknut je razvoj manjih SIM kartica, mini SIM kartica. Mini SIM kartice imaju istu debljinu kao *full-size* kartice, ali njihova dužina i širina su smanjene za 25 mm × 15 mm.

SIM kartica sadrži svoj jedinstveni serijski broj (eng. *Integrated Circuit Card Identifier, ICCID*) , međunarodni identitet mobilnog pretplatnika (eng. *International Mobile Subscriber Identity, IMSI*), sigurnost autentifikaciju i šifriranje informacije, privremene informacije vezane za lokalnu mrežu, popis usluga kojima korisnik ima pristup i dvije lozinke:

osobni identifikacijski broj (eng. *personal identification number, PIN*) za obično korištenja i osobne deblokade koda (eng. *personal unblocking code, PUK*) za otključavanje PIN-a.[3]

2.2. Podsustav baznih stanica BSS

Base station subsystem (BSS) je fizička oprema koja omogućuje radio pokrivenost na zadana geografska područja, poznat i kao ćelije. Sadrži opremu potrebnu za komunikaciju s MS-om. Funkcionalno, BSS sastoji od kontrole funkcije koju provodi BSC i predajne funkcije u izvedbi BTS-a.

BTS je radio-prijenosna oprema i pokriva svaku ćeliju. BSS može posluživati nekoliko ćelija, jer može nadzirati više BTS-ova.

BTS sadrži adaptivnu jedinicu za generiranje kodiranja (eng. *Transcoder and Rate Adaptation Unit, TRAU*) . U TRAU, se vrši kodiranje i dekodiranje GSM-ova specifična govora, kao i funkcija adaptacije sinkronizacije za prijenos podataka.

U određenim situacijama TRAU se nalazi u MSC-u da stekne prednost više komprimiranih prijenosa između BTS i MSC.[2]

2.2.1. Bazna stanica – BTS

Baza primopredajnik, ili BTS, sadrži opremu za slanje i prijem radio signala (primopredajnici) , antene i opremu za šifriranje i dešifriranje komunikacije s kontrolerom bazne stanice (eng. *base station controller, BSC*) . BTS obično za sve osim za piko ćelije ima po nekoliko primopredajnika koji omogućuju da poslužuje nekoliko različitih frekvencija i različitih sektora ćelija (u slučaju sektornih baznih stanica).

BTS je kontroliran od strane nadređenog BSC putem "funkcije kontrole bazne stanice" (eng. *base control function, BCF*). BCF je implementiran kao zasebna cjelina ili čak ugrađen u TRX (*enl.transciever*) kao kompaktna bazna stanica. BCF pruža usluge operacija i održavanje (O&M) veze sa sustavom za upravljanje mrežom (eng. *network management system, NMS*), i upravlja operativnim stanjima svakog TRX, kao i softverskim rukovanjem i alarmnom zbirkom.

Funkcije BTS-a variraju ovisno o korištenoj mobilnoj tehnologiji i davatelju telefonskih usluga. Postoje dobavljači u kojima je BTS običan primopredajnik koji prima informacije od MS-a (pokretne postaje) preko Um zračnog sučelja, a zatim ga pretvara u TDM (eng. *pulse code modulation, PCM*) bazno sučelje- Abis sučelje, i prosljeđuje ga prema BSC-u. Postoje dobavljači koji grade svoje BTS-ove tako da se informacije obrađuju, napravljena je lista odredišnih ćelija, pa se čak i unutar ćelijski *handover* (eng. *handover, HO*) može u potpunosti kontrolirati. Prednost u ovom slučaju je manje opterećenje na Abisovo sučelje.

BTS-ovi su opremljeni radijima koji su u mogućnosti modulirati prvi sloj Um sučelja; za GSM 2G + modulacijski tip je Gaussova minimalna-modulacija (eng. *Gaussian minimum shift keying, GMSK*), dok EDGE-mrežu omogućuje GMSK i 8-PSK (engl. *8-phase shift keying*) modulacija. Ova modulacija je vrsta konstantne promjene fazno-frekvencijske modulacije. U GMSK, da se signal može modulirati na val nosioc, prvo se izgladi sa Gaussovim niskopropusnim filtrom prije negoli se proslijedi frekvencijskom modulatoru, što uvelike smanjuje smetnje između susjednih kanala. Upravljači (kombinatori) antena rade tako da koriste istu antenu za nekoliko TRX-ova, što se više TRX-a koristi (kombinira) , biti će manje upravljača. U mikro [2]i piko [3]ćelijama je omjer TRX-a i upravljača samo 8:1.

Skokovita promjena nosive frekvencije se često koristi kako bi se povećala ukupna učinkovitost BTS-a, a to uključuje brzu promjenu govornog prometa između TRX-ova u sektoru. Slijed promjene frekvencije prate TRX-ovi i uređaji koji koriste sektor. Dostupno je nekoliko različitih sekvenca promjene frekvencije, a sekvenca koja je u uporabi za određen sektor (ćeliju) se konstantno odašilje od strane same ćelije, tako da bude poznata uređajima koji se nalaze u njoj.

TRX odašilje i prima prema načelu GSM standarda, koji predviđaju osam TDMA vremenskih odsječaka po frekvenciji. TRX može izgubiti neke od svojih kapaciteta ako neke informacije potražuju da se odašilju na uređaj u području koji poslužuje BTS. Ova informacija omogućuje uređaju da identificira mrežu i dobi pristup na nju. Ta signalizacija koristi kanal poznat pod nazivom „kanal za kontrolu odašiljanja“.[3]

[2] Micro- je prefiks u SI sustavu jedinica koji označava faktor od 10^{-6}
[3] Piko- je prefiks u SI sustavu jedinica koji označava faktor od 10^{-12}

2.2.2. Upravitelj bazne stanice – BSC

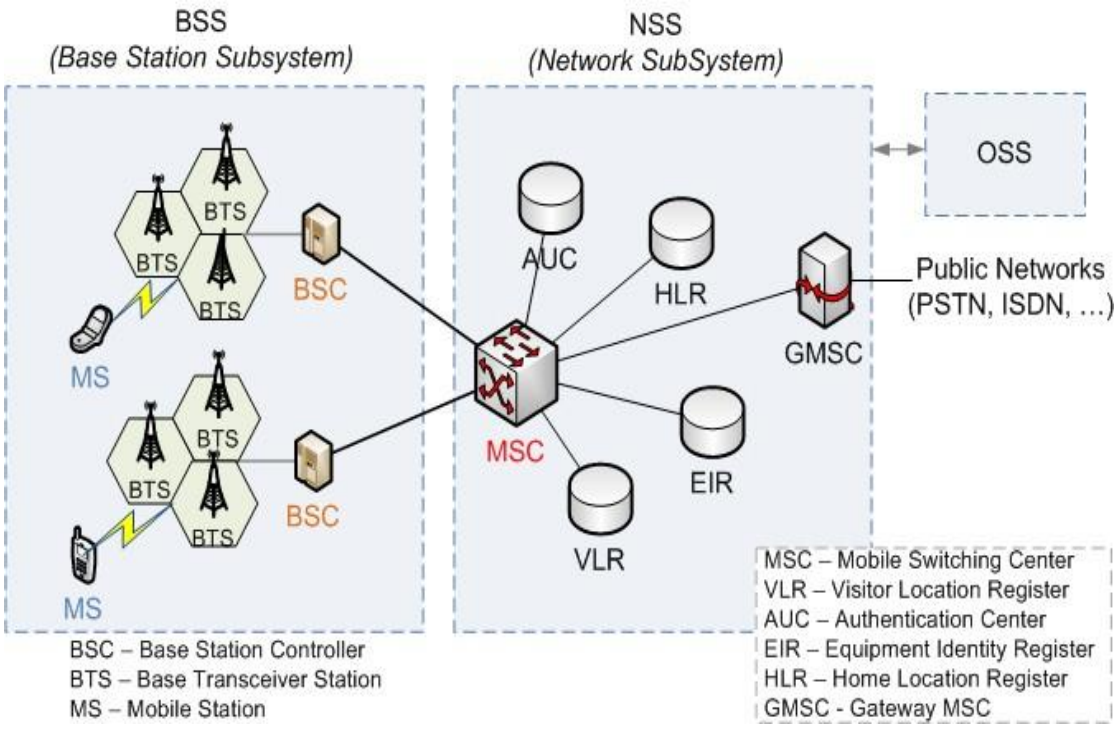
Upravitelj bazne stanice omogućuje, inteligenciju koja stoji iza BTS-a. Obično BSC ima desetke ili čak stotine BTS-a pod svojom kontrolom. BSC rukovodi raspodjelom radio kanala, dobiva mjerenja od mobilnih terminalnih uređaja, i kontrolira proces handovera između BTS-a (osim u slučaju handovera unutar BSCa, u tom slučaju kontrola je dio odgovornosti MSCa). Glavna funkcija BSC je da radi kao koncentrator gdje se puno različitih veza malih kapaciteta s BTS-ovima (relativno male iskorištenosti) smanjuje na manji broj veza prema prospojnoj centrali (MSC s visokim stupnjem iskorištenja). To znači da su mreže često su projektirane da imaju mnogo BSC-a raspoređenih u područjima u blizini njihovih BTS-ova koji su tada spojeni na velike centralizirane MSC stanice.

BSC je nesumnjivo najrobusniji element u BSS. Često se bazira na distribuiranoj računalnoj arhitekturi, sa zalihošću namijenjenoj jedinicama neophodne funkcionalnosti kako bi se osigurala dostupnost i u slučaju kvara. Zalihost se često proteže preko BSC-ove same opreme i obično se koristi u zalihama napajanja u opremi za transmisiju omogućujući A-ter sučelje za PCU (*engl.packet control unit*).

Baze podataka za sve stranice, uključujući informacije kao što su frekvencije nosioca, liste promjene skokovite frekvencije, razine smanjenje snage, dobivene razine za izračun graničnih ćelija, pohranjuju se u BSC-u. Ovaj podatak se dobiva izravno iz inženjerstva radio planiranja koji uključuje modeliranje širenja signala, kao i prometne projekcije.[3]

2.3. Mrežni komutacijski podsustav – NSS

Mrežni komutacijski podsustav (eng. *Network Security Service,* NSS) je sastavni dio mrežnog sustava koji obavlja prospajanje poziva i mobilne upravljačke funkcije za mobilne telefone priključene na mrežu baznih stanica. NSS je u vlasništvu operatera mobilne telefonije te omogućuje mobilnim terminalnim uređajima da komuniciraju kako sa mobilnim tako i sa fiksnim telefonima u široj javnoj telefonskoj mreži (eng. *public switched telephone network,* PSTN) . Arhitektura sadrži konkretne značajke i funkcije koje su potrebne jer telefoni nisu fiksirani na jednom mjestu te je prikazana na slici 1.



Slika 1.Arhitektura mrežnog komutacijskog podsustava.Slika preuzeta od [7]

NSS se izvorno sastoji od prospojne jezgrene mreže, koja se koristi za tradicionalne GSM usluge kao što su glasovni pozivi, SMS i prospajani podatkovni pozivi. Proširena je sa arhitekturom koja pruža paketno orijentirane podatkovne usluge poznate kao GPRS jezgrena mreža. Ona omogućuje mobilnim terminalnim uređajima da imaju pristup uslugama kao što su WAP, MMS i internet.[2]

2.3.1. Prospojni centar mobilnih usluga – MSC

Komutacijski čvor pokretne mreže (eng. *mobile switching centre, MSC*) je primarni čvor pružanje usluga za GSM/CDMA, odgovoran za usmjeravanje glasovnih poziva i SMS-a, kao i ostalih usluga (kao što su konferencijski pozivi, faks i podatkovni promet). MSC započinje i prekida veze sa kraja-na kraj, upravlja mobilnošću i handover potrebama tijekom poziva i vodi brigu o naplati prometa.

U mobilnom sustavu, za razliku od ranijih analognih usluga, fax i podatkovne informacije se šalju direktno u digitalnom kodu na MSC. MSC vrši re-kodiranje u "analogni" signal. Pristupni MSC (eng. gateway mobile switching centre, G-MSC) je MSC koji razaznaje u kojem se MSC-u nalazi korisnik kojeg se zove. Također surađuje sa PSTN-om. Svi pozivi unutar

mobilne mreže ili prema fiksnoj mreži se preusmjeruju kroz G-MSC. Posjećeni MSC (eng. *visited MSC, V-MSC*) je onaj MSC gdje se korisnik trenutno nalazi. VLR povezan s tim MSC će imati podatke o pretplatniku u njemu. Početni MSC je MSC iz kojeg je prospajanje počelo. Završni MSC je MSC prema kojem se vrši prospajanje. Server komutacijskog čvora pokretne mreže je dio redizajniranog MSC koncepta.[2]

2.3.2. Registar domaćih pretplatnika – HLR

Registar domaćih pretplatnika (eng. *home location register, HLR*) je središnja baza podataka koja sadrži podatke o svakom mobilnom pretplatniku koji je ovlašten za korištenje jezgre mobilnog sustava. Mogu biti razni logički, fizički, HLR-ovi po javnoj kopnenoj pokretnoj mreži , ali je samo jedan međunarodni mobilni identitet pretplatnika koji se može povezati samo sa jednim logičkim HLR-om (koji se može obuhvatiti nekoliko fizičkih čvorova) u isto vrijeme. HLR sprema pojedinosti o svakoj SIM kartici izdanoj od strane operatera mobilne telefonije. Svaki SIM ima jedinstveni identifikator koji se zove IMSI što je primarni ključ za svaki HLR zapis.

Još jedna važna stavka podatka vezane za SIM je MSISDN (eng.*Mobile Subscriber International Subscriber Directory Number*), to su telefonski brojevi koje koriste mobiteli da bi uspostavili i primili pozive. Primarni MSISDN je broj koji se koristi uspostavu i primanje glasovnih poziva i SMS-a, ali je moguće da SIM ima i drugi MSISDN broj koji služi za fax i podatkovni poziv. Svaki MSISDN je također primarni ključ za HLR zapis. HLR podaci se pohranjuju sve dok je pretplatnik kod operatera mobilne telefonije. Primjeri ostalih podataka pohranjenih u HLR:

1. Mobilna usluga koju je pretplatnik je zatražio ili dobio
2. Postavke GPRS-a kako bi se pretplatniku omogućio pristup paketnoj usluzi.
3. Trenutni položaj pretplatnika
4. Postavke skretanja poziva za svaki pridruženi MSISDN.

HLR je sustav koji neposredno prima i obrađuje MAP transakcije i poruke elemenata u GSM mreži, primjerice, poruke ažuriranja adresa dobivenih od mobitela koji putuju uokolo.[2]

2.3.1. Registar gostujućih pretplatnika – VLR

Baza podataka gostujućih pretplatnika je baza podataka od pretplatnika koji su došli pod nadležnost prospojni centar za mobitele (eng. *Mobile Switching Center, MSC*) kojeg poslužuje. Svaka glavna bazna stanica u mreži je poslužena s točno jednim VLR, stoga pretplatnik ne može biti prisutan u više od jednog VLR u isto vrijeme.

Podaci pohranjeni u VLR su dobiveni ili od HLR, ili prikupljeni od MS-a. U praksi, zbog izvedbenih razloga, većina proizvođača integrira VLR izravno na V-MSC, a tamo gdje to nije učinjeno, VLR je vrlo usko povezan sa MSC preko vlasničkog sučelja. Kad MSC otkrije novi MS u svojoj mreži, osim stvaranja novog zapisa u VLR, također ažurira HLR mobilnog pretplatnika, pokazuje informaciju o novoj lokaciji tog MS-a. Ako su VLR podaci oštećeni to može dovesti do ozbiljnih problema sa uslugama slanja SMS poruka i obavljanja telefonskih poziva. Prema [2] pohranjeni podaci su:

1. IMSI (identifikacijski broj pretplatnika)
2. Podaci za autorizaciju
3. MSISDN (broj telefona pretplatnika)
4. GSM usluge kojima pretplatnik ima dozvoljen pristup
5. Pretplatnikova pristupne točke (eng. general packet radio service, GPRS)
6. HLR adresa pretplatnika.

2.3.1. Centar za autentifikaciju – AUC

Središte za provjeru autentičnosti (eng. *authentication centre, AuC*) je funkcija za provjeru svake SIM kartice koja se pokušava spojiti na GSM mrežu. Nakon uspješne autorizacije, HLRu je dopušteno upravljati SIM karticom i gore navedenim uslugama. Također je stvoren ključ za šifriranje koji se potom koristi za šifriranje cijele bežične komunikacije (govor, SMS, itd.) između mobilnog telefona i GSM sustava.

Ako autentifikacija ne uspije, onda nema usluge koje su dostupne sa tom kombinacijom SIM kartice i operatera mobilne telefonije. Pravilna provedba sigurnosti u i oko AuC je ključni dio strategije operatera kako bi se izbjeglo SIM kloniranje.

AUC se ne bavi izravno s procesom provjere autentičnosti, ali umjesto toga generira podatke poznate kao trojke za MSC koji se koriste tijekom postupka. Sigurnost procesa ovisi o

zajedničkoj tajni između AuC i SIM i zove se Ki. Ki je utisnut u SIM tijekom proizvodnje, a također se replicira u AuC. Ki se nikad ne prenosi između AuC i SIM, ali u kombinaciji sa IMSI proizvode tajni ključ pod nazivom Kc, koji se koristi za kriptiranje u bežičnoj komunikaciji.[2]

2.3.2. Registar za identifikaciju mobilne opreme – EIR

Registracijski uređaj za prepoznavanje je često integriran u HLR. EIR čuva popis mobilnih terminalnih uređaja (prepoznaju se po IMEI) koji su se zabranili u mreži ili koji se nadziru. To je osmišljeno kako bi se omogućilo praćenje ukradenih mobitela. U teoriji svi podaci o svim ukradenim mobitelima trebali bi biti distribuirani svim EIR u svijetu kroz središnji EIR. EIR podaci se ne moraju mijenjati u realnom vremenu, što znači da je ova funkcija može biti manja distribuirana od funkcija HLR. EIR je baza podataka koja sadrži podatke o identitetu mobilnih terminalnih uređaja koji sprječava pozive sa ukradenih, neovlaštenih ili neispravnih mobilnih uređaja. [2]

2.4. Podsustav operacijske podrške - OSS

Operativno održavalački centar (eng. *operation maintenance centre, OMC*) je spojen sa svom opremom u prespojnom sustavu, i na BSC. Implementacija OMC se naziva sustav za upravljanje i podršku (eng. *Operation Support Subsystem*, OSS). Neke od funkcija OMC su:

1. Administracija i komercijalna operacija (pretplata, krajnji terminala, naplata i statistike)
2. Sigurnost upravljanja.
3. Konfiguracija mreže, upravljanje rukovođenjem i izvođenjem
4. Održavanje.

Funkcije rukovođenja i održavanja se temelje na konceptima upravljanja telekomunikacijskom mrežom (eng. *telecommunication network, TMN*). OSS je funkcionalna cjelina, preko koje mrežni operater prati i kontrolira sustav. Svrha OSS-a je ponuditi kupcima isplativu podršku za centralizirane, regionalne i lokalne operativne i održavalačke aktivnosti koje su potrebne u GSM mreži. Važna funkcija OSS-a je pružiti pregled mreže i podršku za održavanje aktivnosti različitih organizacija rada i održavanja.[4]

3. SIGURNOSNE PRIJETNJE POKRETNOM KOMUNIKACIJSKOM SUSTAVU

3.1. Sigurnosne prijetnje kod mobilnih terminalnih uređaja

U mobilnim mrežama sigurnosni su problemi vezani uz zaštitu razgovora, pozivnih podataka i sprečavanje prijevara putem mobilnih terminalnih uređaja. U starijim analognim sustavima bilo je jednostavno presresti i prisluškivati telefonske razgovore samo uz pomoć policijskog skenera.

Također, sigurnosni su problemi tzv. „kloniranje mobilnih uređaja“, odnosno krađa identiteta i lažno predstavljanje. Postupak kojim mobilni uređaj registrira svoju poziciju mobilnoj mreži ranjiv je na presretanje. U slučaju da napadač presretne i sazna poziciju mobitela, saznao je i korisnikovu poziciju čiju promjenu može iskoristiti kada mobitel nije u upotrebi.

Sve moderniji (kompleksniji) mobilni uređaji omogućuju korisniku da sa sobom nosi pravo osobno računalo. Iako je korisniku vrlo koristan takav uređaj, uz njega se javljaju isti sigurnosni problemi kao i kod osobnih računala (npr. krađa identiteta, uskraćivanje usluga, neovlaštena uporaba, podmetanje zlođudnih programa i drugo).

Jedan takav uređaj je „smart phone“ koji kombinira funkcije osobnog digitalnog asistenta i mobilnog telefona. Takvi telefoni, no i malo slabiji modeli, posjeduju kamere, omogućavaju pristup Internetu, koriste virtualne tipkovnice, sadrže module za reprodukciju multimedijalnih sadržaja i ostale tipične funkcionalnosti koje imaju osobna računala.

Međutim, upravo kao što su osobna računala ranjiva na sigurnosne propuste, upravo tako su i mobilni terminalni uređaji. Zanimljivo je da povećanjem funkcionalnosti koje mobitel nudi, kod njega se javljaju isti sigurnosni problemi kao i kod prijenosnih ili osobnih računala.[4]

3.1.1. Tekstualne poruke

Gotovo svi mobilni uređaji korisniku pružaju mogućnost slanja i blokiranja poruka. Napadači mogu korisniku poslati posebno oblikovane poruke sa zlođudnim programskim kodom koji mogu iskoristiti za krađu osobnih podataka i ostalih podataka koji se nalaze na mobilnom telefonu. Osim opisanih poruka, napadač može korisniku poslati poruku u kojoj ga navodi na

otkrivanje osjetljivih podataka. Takav oblik napada se naziva *SMiShing*, prema već poznatom obliku napada na osobnim računalima *phishingu*.

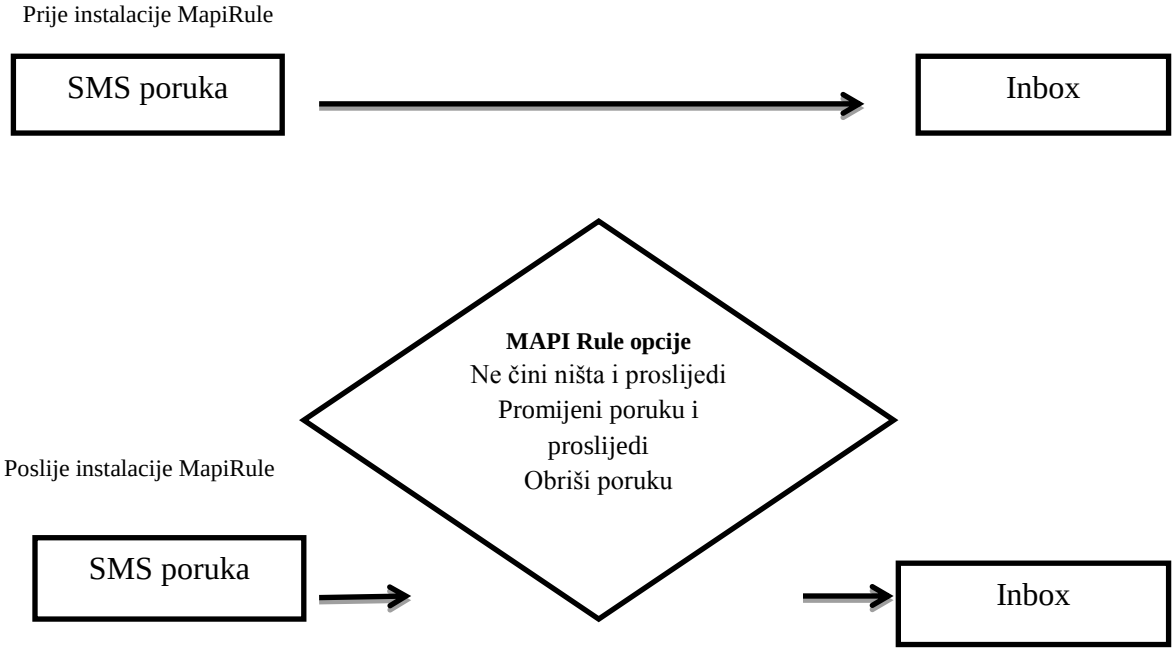
Primjer zloćudnog programa kojeg napadač može podmetnuti korisniku je tekstualna poruka koja koristi funkcije za upravljanje SMS porukama za slanje lažnih poruka ljudima koji se nalaze u adresaru. Ova metoda napada je slična napadu korištenjem poruka elektroničke pošte na osobnim računalima, no napad upotrebom SMS poruka ima veću mogućnost uspjeha jer žrtva obično nije svjesna da postoji takva sigurnosna prijetnja. Korisnici uglavnom vjeruju u autentičnost dolaznih SMS porukama na temelju broja s kojeg su poslane. No ako je napadač ukrao identitet osobe koju spomenuti korisnik ima u svojem adresaru, i može se lažno predstavljati kao korisnikov prijatelj, može mu također slati lažne SMS poruke. Običan će korisnik vrlo teško otkriti jesu li dobivene SMS poruke zloćudne.

Zloćudni programi koje podmetnu napadači mogu koristiti funkcije za upravljanje SMS porukama za naplaćivanje usluga mobilnih terminalnih uređaja preko SMS poruka. Na primjer, u mobilnim terminalnim uređajima koji koriste programski jezik Javu otkriveni su takvi napadi. Ukoliko napadač uspješno podmetne trojanskog konja koji šalje posebne tekstualne poruke pružatelju usluga, napadač može otkriti koliko korisnik plaća usluge korištenja mobilne mreže pružatelja usluga te zlouporabiti te podatke za svoju financijsku korist.

Na primjer, upotrebom programskog paketa *Windows Mobile Software Development Kit*, alata za razvoj aplikacija namijenjenih operacijskom sustavu *Windows Mobile*, napadač može stvoriti posebno oblikovani programski kod samo upotrebom primjera programskog koda naziva MapiRule. MAPI Rule klijent je COM (eng. *Component object model*) objekt koji implementira *IMailRuleClient* sučelje. MAPI Rule klijenta pokreće aplikacija koja prima elektroničku poštu i tekstualne poruke u dolazni sandučić. Dolazne SMS poruke se predaju MAPI Rule klijentu kako bi on odlučio koje će akcije biti obavljene nakon primitka poruke. Razlika između toka poruka s postavljenim MAPI Rule klijentom i bez njega je prikazana na slici 2.

Napadač može podmetnuti MAPI Rule program i ometati rad s tekstualnim porukama. Stvaranje zlonamjernog koda je vrlo jednostavno. Nakon što je napadač podmetnuo programski kod, on postaje filtar između kratkih poruka i programa za elektroničku poštu *tmail.exe*. Napadač može ometati uporabu slanja tekstualnih poruka brisanjem, izmjenom i/ili prosljeđivanjem poruka. Osim toga, napadač može podmetnuti zloćudni program kao dodatak porukama koje

prosljeđuje. Ukoliko korisnik koristi svoj mobitel za komunikaciju u svojoj tvrtci ili za izmjenu službenih podataka, napadač može opisanim načinom učinkovito presretati korporacijski tok podataka.



Slika 2 Primjer toka poruka sa postavljenim MAPI Rule klijentom i bez njega [4]

Ovakav napad predstavlja opasnost korisnicima, nema potrebe za panikom. MAPI Rule tehnologija za blokiranje SMS poruka koristi točno određena vrata (eng. *port*) koje je predodredio proizvođač. Prema tome, korisnici lako mogu utvrditi imaju li na svojem uređaju program kojemu tu nije mjesto. Za instalaciju na predviđeni priključak (eng. port) zloćudni se program mora registrirati kao DLL (eng. *Dynamic-link library*) modul za filtriranje i imati dodani CLSID ključ. CLSID ključ je jedinstvena oznaka koja identificira objekt COM klase (razreda). On izgleda na primjer ovako:

"{3AB4C10E-673C-494c-98A2-CC2E91A48115}"=dword:1

CLSID ključ se treba dodati u direktorij:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules]

Međutim nije svaki program koji je identificiran na opisani način na mobilnom uređaju zloćudan. Ukoliko korisnik ukloni pogrešan ključ, neki važni programi mogu prestati raditi. Kada korisnik otkrije sličan ključ koji je dan u primjeru prilikom donošenja odluke treba se pouzdati u antivirusni program (radije nego da sam uklanja problem).[4]

3.1.2. Kontakti i adresar

U korporacijskom okruženju adresar je jedna od najvažnijih aplikacija na mobilnom uređaju. Krađa kontaktnih podataka može imati kobne posljedice za zaposlenike i tvrtku. Napadač može, ukoliko uspješno podmetne zlonamjerni program, ukrasti podatke s mobilnog uređaja, među njima i kontaktne podatke osoba u adresaru.

Napadač tada može osobama čije je kontakte ukrao slati poruke sa zlonamjernim programima u privitku, poruke koje sadrže poveznicu na web stranicu koja sadrži zloćudne programe i/ili poslati poruku u kojoj navodi korisnika na otkrivanje povjerljivih podataka. Napadač može iskoristiti ugrađene alate za stvaranje sigurnosne preslike (eng. *backup*) adresara, kao što su *IPOutlook, ItemCollection, IFolder* i *IContact* te izmijeniti podatke u adresaru i poslati takve podatke nekome drugome.[4]

3.1.3. Video sadržaj

Većina mobilnih terminalnih uređaja u današnje vrijeme ima kameru kojom se mogu snimati fotografije i video sadržaj. Napadač može podmetnuti posebno oblikovani programski kod kojim preuzima upravljanje kamerom na mobilnom uređaju. No kako korisnici uglavnom čuvaju svoje mobilne uređaje u džepu ili torbici, mjestima s kojih nije korisno slikati ili snimiti video sadržaj, vjerojatnost takve zlouporabe je vrlo mala. Veći sigurnosni problem je ukoliko napadač preuzme upravljanje nad mobilnim terminalnim uređajemi sadržajem koji je pohranjen u direktoriju kamere.

Na mobilnim terminalnim uređajima je uobičajeno da postoji poseban direktorij za pohranu multimedijskog sadržaja kojem se može pristupiti putem kamere. U slučaju uspješnog napada, napadač može ugroziti sigurnost fotografija i video snimaka koje se nalaze na mobitelu. Napadač može postaviti posebno oblikovani program da pošalje sve slikovne datoteke njemu ili na neku adresu elektroničke pošte kojom upravlja.[4]

3.1.4. Prijepisi telefonskih razgovora

Mnogi mobilni terminalni uređaji imaju aplikacije koje mogu snimati telefonske razgovore. Na primjer, na operacijskom sustavu *Windows Mobile* moguće je instalirati aplikaciju „*Waveform Audio Functions*“ za snimanje i reprodukciju audio datoteka. Aplikacija je vrlo slična i temelji se na onima koje se koriste na osobnom računalu, tako da napadač može iskoristiti sigurnosne propuste tih aplikacija i prilagoditi ih programima namijenjenim mobitelima. Audio sadržaj snimljen modernim mobilnim terminalnim uređajima visoke je kvalitete, čak i ako je sadržaj snimljen dok se uređaj nalazio u korisnikovom džepu.

Mobilni uređaji imaju ograničen prostor za pohranu podataka i datoteka tako da se sadržaj ne može snimati neograničeno dugo. Ukoliko napadač podmetne posebno oblikovani program i preuzme upravljanje nad snimanjem zvuka, može snimati proizvoljno dugo i poslati si datoteku u poruci elektroničke pošte ili multimedijalne poruke. Ako napadač koristi metode spomenute u poglavlju 3.1.1., podmetnuti zlćudni program može zlouporabiti SMS poruke za pokretanje i zaustavljanje snimanja.[4]

3.1.5. Povijest poziva

Zapisi o pozivima mogu koristiti napadaču i on može podmetnuti posebno oblikovani program kako bi pročitao podatke o prijašnjim pozivima. Korisnici bi u svrhu zaštite trebali pratiti zapise o pozivima i povremeno ih obrisati.[4]

3.1.6. Dokumentacija

Mnogi korisnici mobilnih terminalnih uređaja čitaju i spremaju dokumente tipa Word, Excel ili PDF na svoje mobitele. Napadač može podmetnuti zlćudni program kojim će ukrasti takve datoteke. Datoteke sa ekstenzijama *.doc, *.xls i *.pdf su popularne mete napadača, zato jer te ekstenzije sadrže često povjerljive informacije do kojih napadači žele doći. Preporuča se da korisnici mobilnih terminalnih uređaja ne spremaju važne i povjerljive dokumente na svoje uređaje.[4]

3.1.7. Upotreba međuspremnika

Sigurnosni propusti vezani uz međuspremnike (eng. *buffer*) su neki od najčešćih programskih propusta. U slučaju postojanja programskog propusta vezanog uz međuspremnik,

napadač ga može iskoristiti za prepisivanje spremnika. Ukoliko se to dogodi, napadač može podmetnuti proizvoljni programski kod. Operacijski sustavi mobilnih terminalnih uređaja vrlo su slični operacijskim sustavima osobnih računala i upotreba međuspremnika je uobičajena.[4]

3.2. Sigurnosne prijetnje u GSM/GPRS/UMTS mrežama

Prije pojave GPRS i UMTS protokola, GSM mreže su korisnicima pružale dovoljnu sigurnosnu zaštitu. Pojavom GPRS i UMTS tehnologija koje su se ili nadograđivale ili su osmišljene tako da budu kompatibilne sa GSM sustavom, povećale su se brzine prijenosa i kapacitet komunikacijskih kanala. Također, povećao se broj usluga koji se nudi korisnicima, kao što je prijenos multimedijalnog sadržaja. Pri nadogradnji GSM sustava na tehnologije treće generacije ispravljeni su neki sigurnosni propusti GSM mreža, kao što su postojanje prijetnje napada upotrebom lažne temeljne postaje i nezaštićeni prijenos kriptografskih ključeva i autentikacijskih podataka u samoj mreži.

Unatoč rješavanju nekih sigurnosnih problema, sigurnosne prijetnje još uvijek postoje i napadači stalno smišljaju nove načine napada. Uspješni napadi na mobilnu mrežu uključuju prisluškivanje i/ili lažno predstavljanje, oponašanje mreže, preuzimanje kontrole nad dijelom sustava, ugroženim mrežnim čvorom ili vezom i izmjena, brisanje ili slanje lažnih signala te krađa korisničkih podataka.

Uspješan napad podrazumijeva da napadač posjeduje posebno prilagođen mobilni uređaj i/ili baznu stanicu (odašiljač).

Napadač može izvesti napad uskraćivanja usluga slanjem posebno oblikovanih zahtjeva za odjavom ili obnovom položaja mobilnog uređaja iz područja u kojem se korisnik ne nalazi. Ukoliko izvodi napad s čovjekom u sredini, napadač se upotrebom prilagođenog mobitela ili bazne postaje ubaci između mreže i korisnika.

Mobilni korisnici se identificiraju upotrebom privremenih identiteta, no postoje slučajevi kada mreža traži korisnika da pošalje svoj pravi identitet u obliku jasnog teksta. Napadi koje napadač može izvesti u ovoj situaciji su:

1. pasivna krađa identiteta – napadač ima prilagođeni mobilni uređaj i pasivno čeka pojavu nove registracije ili rušenje baze podataka jer se u tim slučajevima od korisnika traži da pošalje svoje podatke u čistom tekstu.
2. aktivna krađa identiteta – napadač ima prilagođenu temeljnu stanicu te potiče korisnika da se priključi na njegovu postaju. Zatim ga traži da mu pošalje IMSI.

3. Napadač se može maskirati i pretvarati da je prava mobilna mreža. To može učiniti na sljedeće načine:
    1) Ukidanjem enkripcije između korisnika i napadača – napadač s prilagođenom baznom stanicom potiče korisnika na prijavu na njegovu lažnu postaju i kada korisnik koristi usluge postaje, opcija kriptiranja nije uključena.
    2) Ukidanjem enkripcije između korisnika i prave mreže – u ovom slučaju tokom uspostave poziva mogućnosti kriptiranja mobilnog uređaja su promijenjene i mreži se čini kao da postoji razlika između algoritma kriptiranja i autentikacije. Nakon toga mreža može odlučiti uspostaviti nekriptiranu vezu. Napadač prekida vezu i lažno se predstavlja mreži kao korisnik.

Napadač može izvesti napad lažno se predstavljajući kao običan korisnik:

1. Upotrebom ugroženog autentikacijskog vektora – napadač s prilagođenim mobilnim uređajem i ugroženim autentikacijskim vektorom oponaša korisnika prema mreži i ostalim korisnicima.
2. Prisluškivanjem postupka autentikacije – napadač s prilagođenim mobilnim uređajem koristi podatke koje je dobio prisluškivanjem.
3. Krađa odlaznih poziva u mrežama s isključenom enkripcijom.
4. Krađa dolaznih poziva kod kojih je isključena enkripcija.

Krađom mobilnog uređaja na kojem nije postavljen mehanizam zaključavanja, kao što je zaštita lozinkom, neovlašteni korisnik može takvim mobitelom zatražiti usluge na GPRS mreži pretvarajući se da je izvorni korisnik.

Pretplatnici koriste GPRS usluge uz pretpostavku da se podaci šalju sa i prema njihovom mobitelu zaštićeni te da je ostvarena povjerljivost podataka. Zbog toga je osiguravanje povjerljivosti odgovornost pružatelja usluga. GPRS standardi nude algoritme za stvaranje jedinstvenih sjedničkih kriptografskih ključeva u svrhu izmjene i sakrivanja poretka podatkovnih paketa koji se šalju radio putovima između mobitela i SGSN-a (*engl. Serving GPRS suport node*). Svaki puta kada se autorizirani GPRS mobilni uređaj registrira na mrežu, uspostavlja se jedinstveni sjednički ključ koji se koristi za kriptiranje svih podataka koji se prenose između mobitela i SGSN-a.

Zaštita mobilnih mreža uključuje zaštitu sljedećih elemenata mobilne mreže:

1. base transceiver station
2. base station controller
3. mobile switching centre
4. home location register
5. visitor location register

U početku su se nabrojani elementi koristili isključivo za bežični prijenos glasovnih poruka, ali uvođenjem usluga razmjene neglasovnih podataka, kao što je pristup Internetu, spomenute su komponente izmijenjene tako da podržavaju i takve usluge. Nadogradnja dostupnih usluga povećala je broj vrsta usluga na mobilnoj mreži. Samim time, povećao se rizik od zlouporabe. Ukoliko napadač neovlašteno pristupi elementima GSM/GPRS mreže, može umetnuti nevažeće i izmišljene pretplatnike u HLR i/ili VLR ili izvesti napad uskraćivanja usluga (eng. *Denial of Service*).

Prema tome, osiguravanje fizičkih položaja elemenata GSM/GPRS mreže je također važno. Jednako je važno znati tko sve ima pristup spomenutim elementima mreže. Pristupni popisi i zapisi se trebaju provjeravati, potrebno je postaviti i video nadzor te provjeriti prošlost zaposlenika koji rade za mobilne operatere.[4]

4. NAPADI NA 3G MREŽE

Zbog rasprostranjene arhitekture mobilne mreže, postoji lista napada kojima je mobilna infrastruktura izložena. Prema [1] neki od najzastupljenijih su:

A. Uskraćivanje usluge (eng. *denial of service, DOS*) : vjerojatno i najkompetentniji napad koji može srušiti cijelu mrežnu infrastrukturu. Nastaje slanjem nepotrebnih podataka u mrežu, više no što ona može podnijeti, rezultirajući da korisnici ne mogu pristupiti mrežnim resursima.
B. Distributivno uskraćivanje usluge (eng. *distributive denial of service, DDOS*) : jednom domaćinu bi bilo teško pokrenuti DOS napad velikih razmjera, pa se koristi više domaćina.
C. Ometanje kanala: to je tehnika kojom napadači ometaju kanal i tako legitimnim korisnicima onemogućavaju pristup mreži.
D. Neovlašten pristup: ako nije korištena valjana metoda autentifikacije, tada napadač može dobiti besplatan pristup mreži i može koristiti usluge za koje nije ovlašten.
E. Prisluškivanje: ako promet na bežičnoj liniji nije kriptiran, tada napadač može prisluškivati i presresti osjetljivu komunikaciju kao što je privatan poziv, povjerljivi dokumenti i ostalo.
F. Krivotvorenje poruke: ako komunikacijski kanal nije osiguran tada napadač može presresti poruku iz oba smjera i promijeniti joj sadržaj, a da korisnici niti ne znaju.
G. Ponovna poruka: ako je komunikacijski kanal i osiguran, napadač može presresti kriptiranu poruku i onda je ponovno poslati kasnije, a da korisnik niti ne zna da paket kojeg je primio nije originalan.
H. Napad čovjeka između: napadač se postavi između korisnika i bazne stanice i presreće poruke između njih i mijenja ih.
I. Krađa sesija: zlonamjerni korisnik može oteti već uspostavljenu sesiju i predstavljati se kao legitimna bazna stanica.

Kao što se može vidjeti, s jedne strane je vrlo jednostavno presresti UMTS sustav jer radi na bežičnom sučelju. S druge strane, UMTS zaštita nije jednostavna. 3GPP mreža je identificirala razne prijetnje UMTS sustavu koje su prikazane u Tablici 1.

Tablica 1. Napadi na sigurnost UMTS mreža

	UMTS Attacks	A	C	D1	Risk
1	Replay Attack	Da	Ne	Da	Nizak
2	Man-In-The-Middle (MiM) Attack	Da	Da	Da	Visok
3	Brute Force Attack	Da	Ne	Ne	Srednji
4	Eavesdropping Attack	Ne	Da	Ne	Nizak
5	Impersonation of The User Attack	Da	Ne	Ne	Visok
6	Dictionary Attack	Da	Ne	Ne	Nizak
7	Impersonation of The Network Attack	Da	Ne	Ne	Nizak
8	Compromising AV In The Network Attack	Da	Ne	Ne	Nizak
9	Denial of Service (DoS) Attack	Da	Da	Da	Visok
10	Identity Catching Attack	Da	Da	Da	Visok
11	Redirection Attack	Da	Da	Da	Visok
12	Sequence Number DepletionAttack	Da	Ne	Ne	Nizak
13	Roaming Attack	Da	Da	Da	Visok
14	Bidding Down Attack	Ne	Da	Da	Srednji
15	Guessing Attack	Da	Da	Ne	Srednji
16	Substituion Attack	Da	Da	Da	Visok
17	Disclosure Of User Identity (IMSI) Attack	Da	Ne	Ne	Nizak
18	Packets Injection Attack	Ne	Ne	Da	Nizak
19	Content Modification Attack	Ne	Ne	Da	Nizak
20	Secret Key Exposure Attack	Da	Da	Da	Visok

Izvor: http://www.pearsonhighered.com/samplechapter/0139491244.pdf [6]

Kao što tablica pokazuje neki napadi prijete samo jednom faktoru dok drugi mogu ugroziti dva ili sva tri faktora. Dakle, napadi su razvrstani u tri razine opasnosti, malu , srednju i veliku. Iz tablice smo odabrali četiri napada sa velikom razinom opasnosti o kojima ćemo nešto više govoriti. Ti napadi mogu iskoristiti slabosti sustava i orijentirati se na AKA (eng. *authentication and key agreement*) mehanizam. U nastavku se analizira svaki od njih.[2]

4.1. Uskraćivanje usluge

Napade uskraćivanjem usluge (DoS napadi) u UMTS mreži je teško pokrenuti jer cjelovita zaštita kritičnih signalnih poruka izbjegava DoS napade koristeći lažne korisnikove

zahtjeve za ponovnom registracijom, lažne zahtjeve za ažuriranjem lokacije i zadržavanje (kampiranje) na lažnom BS/MS. Nezaštićene poruke prije obaveznog načina zaštite su se mogle koristiti za pokretanje DoS napada. Slijedeći primjeri pokazuju djelomični ili cjeloviti DoS prema korisniku.

1) Lažni zahtjev za ponovnom registracijom:

Ako mrežna strana ne može provjeriti autentičnost poruke, tada napadač (sa modificiranom MS) može poslati zahtjev za ponovnom registracijom mreži, koji je sastavljen od strane mreže i istovremeno šalje podatkovne instrukcije HLR-u da napravi isto. Tako da je cjelovita zaštita kritičnih signalnih poruka obavezna SN provjerava cjelovitost zahtjeva za ponovnom registracijom i odgovara.

2) Lažni zahtjev za ažuriranjem lokacije:

Umjesto slanja zahtjeva za ponovnom registracijom, napadač šalje zahtjev za ažuriranje lokacije sa drugog dijela SN (ili druge mreže) u kojem je korisnik trenutno prisutan. Kao rezultat korisnik je pozvan u drugo područje. Zahtjev za ažuriranjem lokacije je uvijek zaštićeno od ponavljanja i modifikacije.

3) Kampiranje na lažnom BS/MS:

Napadač sa modificiranim MS/BS zauzima mjesto između SN-a i korisnika-žrtve. Cjelovitost zaštite kritičnih signalnih poruka štite od DoS napada u jednom dijelu, tako da napadač ne može mijenjati signalne poruke. Međutim, sistem ne sprečava napadača i hakera da prosljeđuje ili ignorira neke od poruka (ali ne sve) između mreže i korisnika.[2]

4.2. Napad preusmjeravanjem

Napad preusmjeravanjem je jedan od mogućih napada većeg broja kućnih mobilnih mreža. U ovom napadu, napadač posjeduje uređaj koji istovremeno može raditi i imitirati baznu stanicu (eng. *base station, BS*) i mobilnu stanicu. Da prevari MS žrtve, napadač se predstavlja kao legitimna bazna stanica, tako d odašilje lažni BSS ID (*engl. Basic service set identification*). Također se predstavlja kao i žrtvin MS da zavara BSS. Napadač se spaja na drugu legalnu stanu mrežu na štetu legitimnog MS-a i kreira čist tunel za slanje poruka između autorizirane strane

mreže i žrtvinog MS-a. Budući da su AUTN, RAND i tajni ključevi uspješno dogovoreni, žrtvin MS će tada biti ovjeren od strane mreže.

Napad preusmjeravanjem uzrokuje poteškoće žrtvi sa računom mobilnog operatera za mobilne usluge. Napad djeluje tako da prisiljava žrtvin MS na njegovom HN da bude naplaćen roming u stranoj domeni koju vodi drugi davatelj usluga. U ovom slučaju niti HN niti žrtva ne mogu primijetiti napad preusmjeravanjem.

Također je moguće da napadač preusmjeri žrtvin MS na nesigurnu mrežu sa slabom ili nikakvom zaštitom. Tada napadač može prisluškivati komunikaciju.[2]

4.3. Napad preuzimanjem identiteta

Nažalost UMTS nudi slabu zaštitu protiv krađe identiteta. Iako se IMSI zamjenjuje sa TMSI (eng. *temporary MSI,* TMSI) nakon prvog zahtjeva za konekcijom, IMSI je jasno poslan tijekom inicijalnog zahtjeva za konekcijom i također u prilikama kada dođe do kraha VLR baze podataka dolazi do nemoćnosti VLR da identificira TMSI. Napadač se predstavlja kao UMTS VLR/SGSN. Tijekom zahtjeva za ponovno uspostavljanje konekcije žrtva može koristiti TMSI. Ako se TMSI ne može razaznati, mreža može zatražiti provjeru identiteta. U tom slučaju ME mora poslati svoj IMSI čist u cijelosti. Nakon dobivanja IMSI, napadač se isključuje. Taj napad klasificiramo kao:

1) Pasivna krađa identiteta:

Napadač sa modificiranim MS čeka neaktivan do nove registracije ili kraha baze podataka jer u tom slučaju je korisnik primoran poslati svoj identitet u jasnom tekstu (nešifriranom obliku) . Korištenjem privremenih identiteta sprječava pasivnu krađu identiteta jer napadač mora čekati novu registraciju ili neusklađenost u SN bazi podataka da bi ulovio korisnikov trajni identitet u izvornom obliku.

2) Aktivna krađa identiteta:

U ovom slučaju napadač sa modificiranim BS-om potiče korisnika da kampira na njegovom BS i tada ga traži da mu pošalje svoj IMSI. U ovom slučaju 3G mreža ne pruža adekvatnu zaštitu protiv ove vrste napada.[2]

5. MJERE SIGURNOSTI

UMTS sigurnosna arhitektura definira pet zasebnih sigurnosnih domena, u svrhu otkrivanja pojedinih prijetnji radi postavljanja određenog sigurnosnog mehanizma:

1. Sigurnost pristupne mreže:

U ovoj domeni su bitna pitanja poput:uzajamne autentikacije, povjerljivosti korisničkog identiteta i povjerljivosti prijenosnih podataka, zaštita integriteta važnih podataka.

2. Sigurnost domene mreže:

Omogućuje različite čvorove u mrežnoj domeni radi sigurne razmjene podataka i štiti od napadača na žičanoj liniji mreže.

3. Sigurnost domene korisnika:

Osigurava samo autorizirani pristup Univerzalnom pretplatničkom identifikacijskom modulu

4. Sigurnost domene aplikacije:

Omogućuje aplikacijama u domeni korisnika i pružatelja usluga da razmjenjuju osjetljive poruke.

5. Vidljivost i konfigurabilnost sigurnosti:

Obavještava korisnika ukoliko je sigurnosna značajka uključena i da li korištenje i pružanje usluge bitno utječe na sigurnost.

UMTS sigurnost ima pet domena. Mi usredotočujemo naš trud prema sigurnosti pristupne mreže, jer je to najosjetljiviji i najvažniji dio u UMTS arhitekturi. Ostale domene koriste dobro uhodani sigurnosni protokol – Ipsec.[4]

5.1. Provjera autentičnosti i ključni sporazum

Sigurnosni mehanizam pristupne mreže koji se zove AKA mehanizam (eng. *Authentication & Key Agreement*) , baziran je na sigurnosnom ključu K koji je raspodijeljen između domaće mreže i USIM-a. Glavne promjene u odnosu na GSM provjeru autentičnosti i protokola ključnih dogovora su:

1. Prvi izazov je zaštita od napada ponavljanjem i to rednim brojevima, tako da se i oni „potpisuju“. To znači da podaci autentikacije presretani od strane napadača ne mogu biti ponovno upotrijebljeni.

2. AKA generira IK kao dodatak za CK. Taj ključ se koristi da bi se zaštitio integritet signalizacijskih podataka između mobilne stanice i radijskog mrežnog kontrolera (eng. *radio network controller, RNC*) . AKA protokol je izabran na način da se ostvari najveća moguća kompatibilnost sa trenutnom GSM sigurnosnom arhitekturom. AKA mehanizam izvršava zajedničku autentikaciju korisnika i mreže koristeći simetrični ključ K i proizvodi novu šifru i integritet ključeva. Tri su ključne cjeline uključene u ovaj proces. Prva je kućno okruženje korisnika (eng. *Home Location Register/Authetication centre, HLR/AuC*), koji koriste tajni ključ K da bi kreirali Autentikacijske Vektore (eng. *authentication vectors, AV*) Slijedeća ključna cjelina je uslužna mreža (poslužuje GPRS čvor za podršku/gostujući registar pretplatnika (SGSN/VLR), u kojoj su korisnici smješteni, tada zaprima i upošljava AV za provjeru autentičnosti. Posljednja ključna cjelina je korisnička oprema koja koristi svoj tajni ključ za autentikaciju i sigurnosnu uspostavu veze sa mrežom. [4]

5.1.1. Međunarodni mobilni identitet pretplatnika

Osnovna zamisao autentikacije je da entiteti imaju predefinirane univerzalne identitete. Primarni korisnikov identitet je Internacionalni pretplatnički mobilni identitet (IMSI) -broj.

On nije dobro nam poznat pretplatnički broj (zvan MSISDN broj). MSISDN broj (ili brojevi) je telefonski broj sa punim međunarodnim prefiksom i pridruženim IMSI brojem iz važeće baze podataka. MSISDN brojevi su (općenito) javno dostupni, dok IMSI broj je kreiran radi namjere unutarnjeg usmjeravanja i identifikacije u sustavu. [4]

5.1.2. Privremeni identitet mobilne stanice

Prikaz identiteta mora prethoditi provjeri identiteta, budući da autentikacijska procedura generira sesiju ključeva za enkripciju. Imamo situaciju gdje će trajni identitet biti vidljiv na zračnom sučelju. To nije sigurno s obzirom da omogućava praćenje lokacije pretplatnika. Da bi se riješio taj problem uslužna mreža (eng. *service network,* SN) može izdati lokalni privremeni identitet zvan Privremeni Identitet Mobilne Stanice koji se koristi za dodatnu identifikaciju. Tako da normalna procedura je da se UE predstavi sa svojim IMSI brojem po prvi puta. Onda ulazi u novo područje usluge (SGSN ili VLR). Nakon toga je započela enkripcija, SN šalje TMSI broj UE-u. Ovaj identitet se zove međunarodni identitet mobilne opreme (eng. *Internacional Mobile*

Equipment Identity, IMEI) i to je jedinstven identitet. IMEI broj će redovito provjeravati ponovo u bazi podataka koja se zove Registar Identiteta Opreme (eng. *equipment identity register*, EIR).[4]

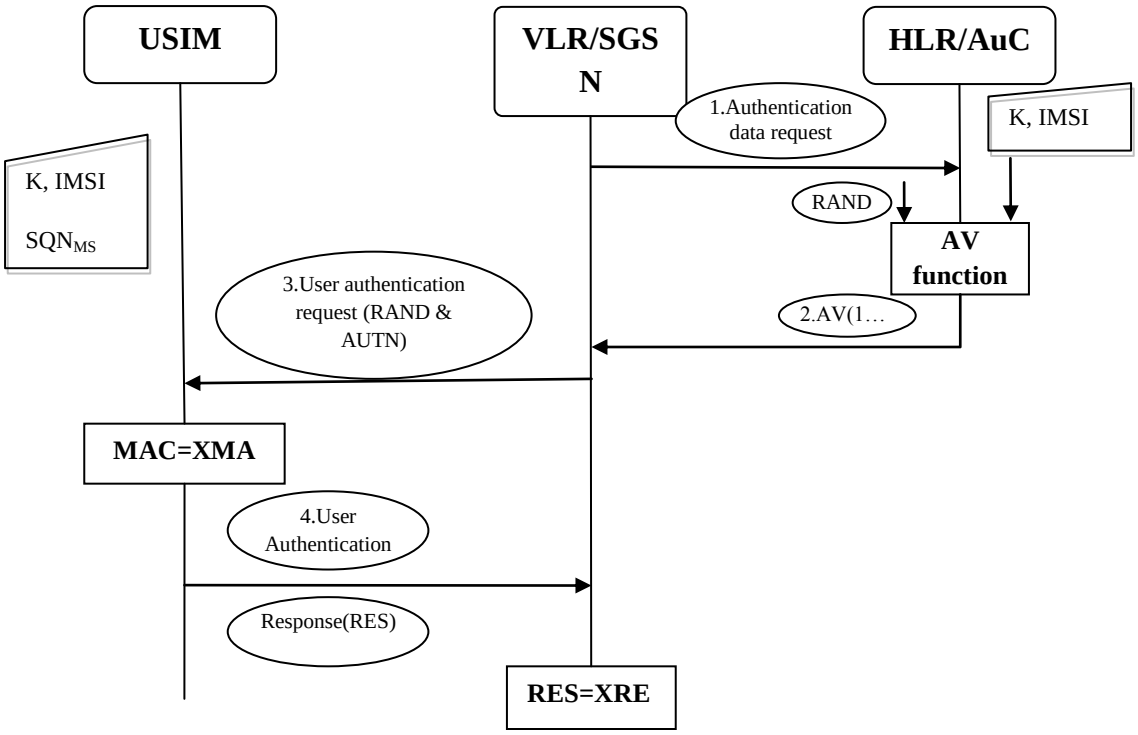
5.1.3. Provjera autentičnosti i procedura ključnih dogovora

Kada je mobilna oprema (eng. *mobile equipment*, ME) UMTS-a uključena, ona skenira dostupan čvor- baznu stanicu i pokušava se povezati sa onom od koje ima najveću snagu signala. U početku se procedura ažuriranja lokacije provodi sa nečim što bi moglo biti dodatak IMSI broju, Normalno Ažuriranje Lokacije (eng. *normal location updater*, NLU) ili Periodičnim Ažuriranjem Lokacije (eng. *periodic location update*, PLU). Ažuriranje lokacije počinje sa zahtjevom za spajanje radijskom kontrolom izvora (eng. *radio resource control, RRC*), koji šalje mobilna oprema baznoj stanici. Kako još niti jedan kanal nije dodijeljen, tako se prva poruka šalje kroz zajednički upravljački kanal koji je smješten na slučajnom pristupnom kanalu za slanje podataka. Poslije ovog koraka, provodi se AKA procedura. [4]

AKA procedura omogućava autentikaciju u oba smjera. Autenticira mobilnu opremu (ME) i uslužnu mrežu (eng. *service network,* SN) u isto vrijeme. Ova procedura počinje sa zahtjevom za podatkovnu autentikaciju od strane VLR/SGSN-a. Oni prosljeđuju IMSI ili USIM prema HLR/AuC-u. Taj zahtjev se prikazuje kao poruka 1 na slici 3.IMSI broj i K broj su razmijenjeni između USIM-a i HLR-a. Na temelju IMSI broja, K broja i slučajnog broja (eng. random number, RAND), HLR proizvodi pet autentikacijskih vektora (eng. *authentication vectors*, AV) i prosljeđuje ih VLR/SGSN-u, što je prikazano kao poruka 2 na slici 3.VLR/SGSN odabiru RAND i autentikacijski token (eng. *authentication token*, AUTN) koji odgovara jednom od AV-a i prosljeđuje ga ME kao što je prikazano kao poruka 3 . Sada ME izračunava očekivanu poruku autentikacijskog koda X-MAC i uspoređuje ju sa MAC dobivenom od AUTN.

Ako su obje iste i SQN je u važećem rasponu tada je mreža autenticirana. Posljedica obostrane autentikacije je da tada USIM postaje aktivni entitet. U UMTS mreži USIM pokušava autenticirati mrežu, pa tako postoji mogućnost da će USIM odbiti mrežu. Dok u GSM-u korisnik nije mogao autenticirati mrežu, tako da mobilni uređaj je nije niti mogao odbiti. Sada ME kalkulira vrijeme odziva (eng. *response*, RES) i šalje ga VLR/SGSN-u kako je prikazano na

poruci 4 slika 3.VLR/SGSN uspoređuje RES sa očekivanim vremenom odgovara (eng. *Expected response*, *X-RES*) . Ako se obje stavke poklapaju, korisnik je autenticiran.



Slika 3. Provjera autentičnosti i procedura ključnih dogovora [6]

VLR/SGSN sada šalje CK i IK prema RNC-u. Poslije ovog koraka i RNC i ME imaju svoj odgovarajući ključ za enkripciju i zaštitu integriteta. Poruke od broja 1 do 4 nisu niti šifrirane niti imaju zaštitu, jer se šalju prije dogovora o tajnom ključu. Te poruke se šalju bežično na sučelja između ME i BS i zato su osjetljive na presretanje i premodifikaciju. Njihova modifikacija od strane uljeza može uzrokovati posebne napade kao što je odbijanje usluge (eng. *denial of service*, DoS) ili čovjek u sredini (eng. *man in the middle*, MiM) . [4]

5.1.4. Autentikacijski vektori

Av-ovi (eng. *Authentication Vectors*) sadrže osjetljive i važne podatke kao što su podaci autentikacije na zahtjev i kriptografski ključevi. Iz toga je jasno da prijenos AV-a između HLR/AuC i SGSN/VLR-a zahtijeva siguran prijenos zaštićen od prisluškivanja i napada

presretanjem i modificiranjem. Stvarni mehanizam prijenosa za AV je SS7 –baziran na mobilnom aplikacijskom protokolu (eng. mobile *application protocol, MAP*). MAP protokol ustvari ne uključuje nikakvu sigurnosnu funkcionalnost, ali sigurnosna ekstenzija MAP-a zvana MAPec je proizvedena u suradnji sa projektom 3G (eng. *3rd Generation Partnership Project, 3GPP*). MAPec protokol pripada području sigurnosti mrežne domene u UMTS sigurnosnoj arhitekturi. Ono uključuje i MAPec specifičnost i specifičnost kako zaštititi veze internet protokola na upravljačkoj ravnini UMTS jezgrene mreže. AV ima pet komponenata proizvedenih koristeći pet sigurnosnih funkcija (f1, f2, f3, f4 i f5). Opisi funkcija autentifikacijskog vektora su opisani u tablici 2. [4]

Tablica 2. Opis funkcija autentifikacijskog vektora. Podaci od [6].

	DESCRIPTION
RAND	Nasumična vrijednost
SQN	Redni broj izmjenjenen pomoću AK ključa
AMF	Polje za upravljačku autentikaciju je 16 bitno polje koje se koristi za upravljačke svrhe
MAC	Kodna poruka o autentikaciji koja je ovjerena od korisnika
XRES	Odgovor koji mreža očekuje od korisnika
CK	Ključ tajnosti
IK	Ključ integriteta
AUTN	Autentifikcijski token ovjeren od korisnika pomoću kojeg se registrira na mrežu

5.1.5. Tajni ključ u AKA mehanizmu

Slijed autentikacije između SGSN/VLR i USIM-a se temelji na obostranom autentikacijskom programu koristeći unaprijed dogovoreni tajni ključ K (128 bita). Taj glavni ključ je pohranjen samo na univerzalnoj integriranoj strujnog kartici (eng. *Universal Integrated Circuit Card* UICC) ili USIM i u AuC. UICC je pametna kartica pretplatnikova identikacijskog modula otporna na neovlašteno korištenje, a USIM je aplikacija koja se izvodi na UICC-u. Da bi se održala sigurnost neophodno je da se ne otkrije K, jer u suprotnom će biti ugrožen za dani UICC/SGSN tijekom svog vremena. AKA slijed obično inicira VLR/SGSN kada mreža treba provjeriti identitet pretplatnika. Ako SGSN/VLR još ne posjeduje valjani AV za tvrđeni pretplatnikov identitet, mora zatražiti od barem jedan AV od HLR/AuC. AV se izračunava i

pohranjuje u AuC. AV se generira sredstvima specifičnih operatorskih autentikacijskih funkcija.[4]

5.2. Povjerljivost

Mehanizam povjerljivosti se realizira sredstvima šifriranja u mnogim sustavima i uslugama. Šifrirani ključevi kao CK i IK koji se koriste proizvedeni su AKA procedurom. CK je uvijek veličine reda 128 bita, ali samo jedan može kontrolirati značajan broj bitova konfiguriranjem ključeva derivacijom f3 funkcija . Osnovna funkcija MILENAGE f3 je za povjerljivost ključa od 128 značajnih bitova. Povjerljivost možemo klasificirati u dva različita tipa: povjerljivost korisničkog identiteta i povjerljivost podataka. [4]

5.2.1. Povjerljivost korisničkog identiteta

Glavni ciljevi povjerljivosti značajki korisničkog identiteta su da spriječe uljeze od nekih napada kao što su prisluškivanje IMSI-a. Da bi se ostvarila ova svrha, korisnik se identificira sredstvima TMSI-a preko bežičnog sučelja koje ima lokalnu važnost i radi u kombinaciji sa lokalnim područnim identifikatorom (eng. local area identity, LAI) ili područnim identifikatorom usmjeravanja (eng. *regional area identity, RAI*), za analogne i digitalne domene redom. Svaki puta kada UE pokušava pristupiti 3G uslugama, predstavlja se preko sredstava TMSI/LAI ili TMSI/RAI. [4]

5.2.2. Povjerljivost podataka

U sigurnosti UMTS-a, korisnički podatci i neki elementi informacija se smatraju osjetljivima i mogu biti zaštićeni povjerljivošću. Potreba za zaštićenim načinom prijenosa je upotpunjeno sa povjerljivosti f8 funkcije. Ta funkcija šifriranja se primjenjuje na potrebne kanale između ME i RNC-a. Trenutne specifikacije f8 funkcije se baziraju na KASUMIJEVOM algoritmu. [4]

5.2.3. Funkcija povjerljivosti

UMTS-ova f8 funkcija šifriranja je veza sloja simetrično sinkronog toka šifra. Ta funkcija je predodređena da generira prividno-slučajan tok blok ključeva koji je u kombinaciji sa blokom običnog teksta na način da se nad bitovima vrši modul operacija (XOR funkcija) .

Funkcija uzima 128 bitni ključ CK, ali radi fizički na 64 bitnim blokovima. Ta funkcija povjerljivosti za ulaz uzima tajni ključ (CK 128 bita), redni broj (COUNT-C, 32 bita), pokazatelja radio kanala (BEARER, 5bita) i pokazatelj smjera (DIRECTION, 1bit). Uz sve to, dobiva se dužina (LENGHT, 16 bita) od toka bloka ključa. [4]

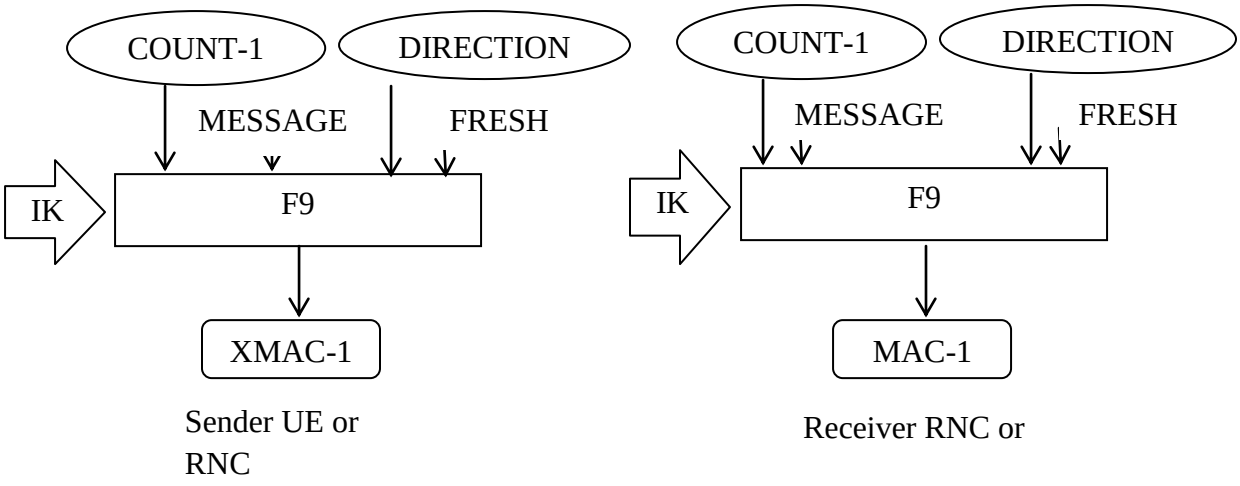
5.3. Podatkovni integritet

Kao što smo napomenuli prije, zaštita integriteta signalnih poruka između ME i RNC-a počinje čim se spozna ključ integriteta i zaštitni algoritam integriteta. IK je uvijek dug 128 bitova, ali ako je sličan CK-u, može se podesiti IK da ima manje značajnijih bitova ako je to potrebno. Zadana MILENAGE f4 funkcija proizvodi IK sa 128 bitnih bitova. MAC funkcija se primjenjuje na svaku specijalnu poruku na RRC sloju skupa protokola UMTS-ovog zemaljskog radijskog pristupa mreži. Zaštita integriteta kritičnih poruka omogućuje zaštitu od mnogih aktivnih prijetnji i napada kao što su MiM napadi.

Djelomična zaštita integriteta korisničkih podataka UMTS-a također ima mehanizam koji sprječava umetanje ili brisanje, ali ne i modifikaciju korisničkih podataka. Ova karakteristika treba spriječiti određene propusnosti napada otmice, dok se izbjegava cijena mehanizma cjelokupne zaštite integriteta korisničkih podataka. Usluga sigurnosti cjelovitosti je obuhvaćena sa sredstvima MAC mehanizma koji omogućuju obostranu autentikaciju poruka i zaštitu cjelovitosti od namjernih modifikacija. [4]

5.3.1. Funkcija zaštite cjelovitosti podataka

UMTS cjelovitost podataka je ograničena u osiguranju poruka između MS i RNC-a. Funkcija integriteta, f9 uzima za ulaz ključ integriteta (IK, 128 bita) , poruku (MESSAGE) koja se štiti, redni broj (COUNT-I, 32 bita), slučajnu vrijednost (FRESH, 32 bita) i vrijednost indikacije smjera (DIRECTION, 1bit). Izračunati MAC-1 se stavlja u signalnu poruku od strane koja ga šalje. Strana koja prima poruku izračunava odgovarajući XMAC-1 za poruku, i smatra se da je cjelovitost podataka potvrđena ako su izračunati XMAC-1 i primljeni MAC-1 identični. Funkcija zaštite cjelovitosti podataka je prikazana na slici 4.



Slika 4. Funkcija zaštite cjelovitosti podataka [6]

U UMTS sustavu signalne poruke su u suštini kratke;stoga dužine glavnih komponenata poruke su razmjerno kratke. Stvarna dužina elementa poruke predstavljene f9 funkciji je duža od poruke poslane bežično budući da je pet bitova korišteno da se označi kanal nosioc i one su izvučene iz konteksta vala nosioca.

Specifikacije proizvoljno ograničuju veličinu f9 ulaznih poruka na red veličina od 5000bitova. Standardna f9 funkcija se bazira na KASUMIJEVOM bloku šifra (kao i f8). Ta funkcija je varijanta slične tehnike izgradnje autentikacijskih kodova lančanog šifriranja blokova poruka (CBC-MAC). Da se koristi običan način CBC-MAC za KASUMI bio bi ograničen na veličinu bloka od 64 bita, ali neobična lančana tehnika omogućava f9 funkciji da podržava 128 bitnu unutarnju situaciju. Završni izlaz od KASUMI-ja koristeći f9 je 64 bitni šifrirani blok, koji je skraćen i postao 32 bitna MAC-ova vrijednost. Slika 6 ilustrira korist cjelovitosti algoritma f9 da autenticira cjelovitost podataka od RRC signalne poruke. [4]

5.4. Kasumi algoritam

Funkcija povjerljivosti f8 se koristi za opskrbu podatkovne enkripcije, dok se funkcija f9 koristi za zaštitu cjelovitosti signalnih standardiziran za korištenje tih algoritama. Funkcija f8 (povjerljivost), funkcija f9 (cjelovitost) i algoritam korišten u tim funkcijama su bili analizirani od različitih znanstvenika i zaključeno da pružaju odgovarajuću i dovoljnu sigurnost. Šifrant blokova KASUMI je modifikacija MISTY1. KASUMI je Feistelov šifrant koji se sastoji od osam

krugova. Radi na 64 bitnom podatkovnom bloku pod kontrolom 128 bitnog ključa. Sigurnosna arhitektura UMTS-a omogućuje 16 različitih enkripcijskih algoritama i 16 različitih algoritama cjelovitosti specificiranih preko UMTS-og identifikatora algoritma šifriranja (eng. *Encryption algorithm, UEA*) i UMTS-ova algoritma cjelovitosti (eng. *Integrity algorithm, UIA*). [4]

5.5. Sigurnost ključeva u UMTS mreži

Kao što je navedeno ranije UMTS sigurnosti koristi tri ključa, K (tajni ključ koji se dijeli između HN i USIM i koristi se tijekom AKA procedure), CK (eng. *Confidelity Key*) i IK (ključ cjelovitosti podataka). Ta tri ključa su izložena na radio vezi na sličan način kriptografskim napadima. Ako napadač želi dobiti CK ili IK mora koristiti podatke poslane između UE i SN kako bi napao funkcije (f8 ili f9). U toj prilici napadač je pristupio samo zaštićenim podatcima;stoga napadač može napasti samo umetanjem šifriranog teksta.

U drugom slučaju ako napadač želi probiti K (ključ) , mora presresti poruke koje se razmjenjuju tijekom AKA procedure i iskoristiti ih da umetne napade protiv sigurnosnih funkcija f1, f2, f3, f4 i f5. Značajnije vrijednosti koje napadač može presresti su AMF, MAC, RES i RAND. Stoga kada napadač pokušava dobiti K, napadač može samo postaviti obostrani šifrirani tekst i poznati otvoreni tekst. U prijašnjem slučaju je napadač pokušavao otkriti CK ili IK, imao je više teksta kojeg je mogao upotrijebiti, ali je mogao napasti samo postavljanjem šifriranog teksta.

Sličnost izloženosti napadima je u razlici ogromne važnosti od uspješnog napada ako napadač sazna IK ili CK, tada je samo ograničeni dio podataka kompromitiran, tj. u drugom slučaju ako se napadač domogne K, onda je cijela sigurnost od prošle i buduće komunikacije kompromitirana. Tako da je K mnogo zanimljiviji i privlačniji napadačima i napadačima od CK i IK ključa. Stoga je zaštita ovog ključa veoma važna i UE i SN-u.

Neki mehanizmi i procedure predlažu da se poveća sigurnost tajnog ključa. Predstavljene su tri metode; napredna procedura identifikacije koja omogućava uspostavljanje privremenog ključa (eng. temporary key, TK), šifriranje autentikacijske poruke koje zaštićuje od napada i povećava veličinu tajnog ključa, K.

U prvoj mjeri zaštite možemo koristiti protokol koji je već predložen i možemo ga poboljšati kako bi osigurali adekvatnu zaštitu glavnog ključa. Taj protokol je dodatak mobilnoj sigurnosti i korisničkoj povjerljivosti u UMTS mreži (eng. Enhancement Mobile Security and User Confidentiality for UMTS, EMSUCU) koji je predložen za zaštitu IMSI-ja. Kao što smo već rekli, UMTS sustav ograničuje korištenje IMSI identiteta koliko je god to moguće. Kada je moguće koristi se privremeni identitet, TMSI. Dalje, TMSI se šalje šifriran radijskom vezom. Sukladno tome, predlaže se da se AV proizvede koristeći se TK, umjesto K. Za postavljanje tajnog ključa TK predlaže se prilagodba EMSUCU protokola. Novi TK ključ bi bio proizveden svaki puta kada bi se izvodio napredni EMSUCU protokol. U UMTS-ovom sigurnosnom standardu kada istekne vrijeme šifriranja para ključeva CK, IK onda ME briše njihove vrijednosti. Nakon toga nova AKA procedura će se započeti u svrhu proizvodnje novog para ključeva CK i IK.

Drugi predložak je jednostavniji i prikladniji: kada vrijeme šifriranja CK i IK istekne, ME započinje AKA proceduru prije negoli obriše par ključeva CK i IK. U ovom slučaju ti ključevi će biti upotrjebljeni da bi se zaštitile poruke koje se izmjenjuju tijekom AKA procedure. Bilo bi veoma jednostavno primijeniti ovu metodu, jer uključuje samo male promjene u slijedu događaja u UMTS sigurnosnim protokolima. Kao sa svim ostalim porukama, šifriranje bi vršilo ME na korisnikovoj strani, a RNC na mrežnoj strani, koristeći iste algoritme za sigurnost. Iako je šifriranje AKA poruka dostatno i jednostavno za provođenje, mana mu je što treba set valjanih tajnih ključeva CK i IK. Tako da će biti slučajeva kada neće biti moguće koristiti ih da bi se zaštitile AKA poruke, npr. kada korisnik uključi svoju UE.

Osim gore navedenih mjera, također se predlaže da se poveća veličina tajnog ključa K sa 128 bita na bar 256 bita. Zbog važnosti tajnog ključa K, prijedlog je da mu minimalna dužina bude 256 bita. [4]

6. ZAKLJUČAK

Kako se razvija tehnologija, tako se razvija i mobilna telekomunikacija i „dodaju“ se osnovnom paketu i neke nove usluge koje se mogu pružiti, a da nisu telefonija i SMS,kao npr.:prijenos podataka,usluge lokacije,a samim time i novije aplikacije i mogučnosti u mobilnoj tehnogiji. Time se uvjetuju i novi sigurnosni zahtjevi kojima se korisniku treba omogučiti siguran rad, konstantnu raspoloživost usluga, te sigurnost osobnih informacija i opreme.

U početku kod analognih sustava je relativno jednostavno bilo zaštititi korisnika i vezu, jer se radilo samo o govornim pozivima. Pojavom digitalnog doba i novog načina prijenosa, te novim uslugama, nije samo porastao broj usluga , već i broj potencijalno različitih napada na korisnike, mrežu i usluge. Iako je sigurnosna zaštita relativno dobra i zadovoljavajuča kako AKA sigurnosnim mehanizmom sa generiranjem tajnih ključeva u pristupnoj mreži, te Kasumijevim algoritmom u prijenosnoj mreži, ne može se pobječi od činjenice da ništa nije stoposto sigurno, te da i pored te zaštite postoje propusti-mogučnost za napade na sigurnost.

Ono što se može zaključiti da povečanjem brzina prijenosa se povečava broj novih aplikacija, čime se povečava i broj prijetnji, a time će se povečati i sigurnosni mehanizmi. Znači da bi se veča količina informacija prenijela u što kračem roku, tražit će se i veća brzina, sigurnost prijenosa iste; čime će od ukupne količine podataka koji se prenose sve veći dio otpasti na dio koji nije relevantan-nije informacija, već služi kao zaštita te iste.

U svakom slučaju mobilna tehnologija je najrasprostranjeniji oblik komunikacije na zemlji i kao takva ima mnoštvo prijetnji, ugroza i napada, ali se sa svime odnosi na uspješan način, tako da pokušava zadovoljiti uvjete korisnika, dostupnost usluga, povjerljivost informacija.

POPIS LITERATURE

1. Mobarhan, M. A., Moabarhan M. A., i Shahbahrami A., (2012), *Evaluation of security attacks on UMTS authentication mechanism*, International Jorunal of Network Security & its Applications, Preuzeto u travnju (2015) sa: http://airccse.org/journal/nsa/0712nsa03.pdf

2. Perez A.,(2012), *Mobile Networks Architecture*, preuzeto u travnju (2015) sa: http://www.amazon.com/Mobile-Networks-Architecture-Andre-Perez/dp/1848213336/ref=sr_1_1?ie=UTF8&qid=1428775759&sr=8-1&keywords=mobile+network+architecture

3. Sauter M., (2014), *From GSM to LTE Advanced*, preuzeto u travnju (2015) sa: http://www.amazon.com/GSM-LTE-Advanced-Introduction-Networks-Broadband/dp/1118861957/ref=sr_1_1?ie=UTF8&qid=1428775722&sr=8-1&keywords=from+GSM+to+LtE

4. CARNet Hrvatska akademska i istraživačka mreža, *Sigurnost mobilnih mreža*, preuzeto u travnju (2015) sa:

   http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-303.pdf(16.04.2013)

5. Garg K.V., Wilkes E.J.(1998); *GSM Arhitecture and Interfaces*, PEARSON Principles and Applications of GSM.preuzeto u travnju (2014) sa:

   http://www.pearsonhighered.com/samplechapter/0139491244.pdf(16.4.2013)

6. Tutorialspoint, (2015), *GSM – the operation subsystem (OSS)*, Preuzeto u travnju (2015) sa:

   http://www.tutorialspoint.com/gsm/gsm_operation_support_subsystem.htm(18.04.2013)

7. Vega-Rodriguez M.A,Chaves-Gonzales J.M.;*Multiobjective Frequency Assignment Problem*; preuzeto u lipnju(2015) sa:

   http://mstar.unex.es/index.php?option=com_content&view=article&id=59&Itemid=55

POPIS KRATICA

3GPP – (*3rd Generation Partnership Project*) dogovor telekomunikacijski organizacija o suradnji oko 3G mreže

AKA – (*Authentication and Key Agreement*) sigurnosni protokol

AUC – (*authentication centre*) autentikacijski centar

AUTN – (*authentication token*) autentikacijski token

AV – (*authentication vectors*) autentikacijski vektori

BCCH – (*broadcast control channel*) kontrolni kanal za odašiljanje

BCF – (*base control function*) kontrolna funkcija bazne stanice

BSC – (*base station controller*) upravitelj bazne stanice

BSS – (*base station subsystem*) podsustav bazne stanice

BSSID – (*basic service set identification*) MAC adresa bežićne pristupne točke u podsustavu bazne stanice

BTS or TRX – (*base transceiver station*) primopredajnik bazne stanice

CDMA – (*code division multiple access*) kodni način prijenosa informacija

CK – (*cipher key*) ključ za šifriranje

CLSID – (*class ID*) jedinstvena oznaka koja identificira objekt COM klase

DDOS – (*distributive denial of service*) distributivno odbijanje usluge

DLL – (*dynamic link library*) ekstenzija programima sa aktivnom poveznicom na bazi podataka

DOS – (*denial of service*) odbijanje usluge, vrsta napada

EDGE – (*enhanced data rates for GSM evolution*) poboljšane brzine prijenosa podataka u GSM evoluciji, dodatak 2.5G-u

EIR – (*equipment identity register*) registar mobilne opreme

G-MSC – (*gateway mobile switching centre*) prijelazni mobilni komutacijski centar

GMSK – (*Gaussian minimum shift keying*) vrsta modulacije prijenosnog signala

GPRS - (*general packet radio service*) opća usluga radijskog paketskog prijenosa podataka, 2.5G

GSM – (*global system for mobile communication*) globalni sustav mobilne komunikacije

HLR – (*home location register*) registar vlastitih pretplatnika

HN – (*home network*) domaća mreža

HO – (*handover*) prijelaz sa jedne bazne na drugu

ICCID – (*Integrated Circuit Card Identifier*) integrirana kartica za identifikaciju

IK – (*integrity key*) ključ cjelovitosti

IMEI – (*International Mobile Station Equipment Identity*) međunarodni identitet mobilne opreme

IMSI – (*International mobile Subscriber Identity*) međunarodni identitet mobilnog pretplatnika

LAI – (*local area identity*) područni identitet

MAP – (*mobile application protocol*) protokol mobilne aplikacije

ME – (*mobile equipment*) mobilna oprema

MIM – (*man in the middle*) čovjek u sredini, vrsta napada

MMS – (*Multimedia Messaging Service*) usluga multimedijalne poruke

MS – (*mobile station*) mobilna stanica

MSC – (*mobile switching centre*) prospojni centar za mobitele

MSISDN – (*Mobile Subscriber International Subscriber Directory Number*) ISDN broj mobilnog pretplatnika

NLU – (*normal location updater*) normalno ažuriranje lokacije

NMS – (*network management system*) mrežni operativni sustav

NSS – (*Network Security Service*) mrežni sigurnosni servis

O&M – (*operation and maintenance*) upravljanje i održavanje

OMC – (*operation maintenance centre*) centar za upravljanje i održavanje

OSS – (*Operation Support Subsystem*) podsustav podrške za upravljanje

PCM – (*pulse code modulation*) pulsno kodna modulacija

PCU – (*packet control unit*) jedinica za upravljanje paketima

PDF – (*Portable Document Format*) prijenosni format dokumenta

PIN – (*personal identification number*) osobni identifikacijski broj

PLMN – (*public land mobile network*) javna zemaljska pokretna mreža

PLU – (*periodic location update*) periodično ažuriranje lokacije

PSK - (*phase shift keying*) fazna modulacija signala

PSTN – (*public switched telephone network*) komutirana javna telefonska mreža

PUK – (*personal unblocking code*) osobni kod za deblokadu

RAI – (*regional area identity*) regionalni identitet

RAND – (*random number*) nasumičan broj

RES – (*response*) vrijeme odziva

RNC – (*radio network controller*) upravitelj radijske mreže

RRC – (*radio resource control*) kontrola radijskog resursa

SACCH – (Slow *Associated Control Channel*) pridruženi spori kontrolni kanal

SGSN – (*serving GPRS support node*) čvor za podršku usluživanja GPRS usluge

SIM – (*subscriber identity module*) pretplatnikov identifikacijski modul

SP – (*Smart phone*) pametni telefon

SMS – (*short message service*) usluga kratke poruke

SN – (*service network*) uslužna mreža

SSL – (*Secure Sockets Layer*) sloj osiguranog priključka

TDM – (*time division multiplex*) vremenski podjela kanala, način podjele kanala za prijenos informacija

TK – (*temporary key*) privremeni ključ

TMN – (*telecommunication network*) telekomunikacijska mreža

TMSI – (*temporary MSI*) privremeni identitet mobilnog pretplatnika

TRAU – (*Transcoder and Rate Adaptation Unit*) primopredajna i jedinica stope adaptacije

UMTS – (*universal mobile telecommunication system*) međunarodni mobilni telekomunikacijski sustav

VLR – *(visitor location register*) registar gostujućih pretplatnika

V-MSC – (*visited MSC*) posječeni mobilni prospojni centar

WAP – (*wireless application protocol*) protokol za bežične aplikacije

WI-FI – (*wireless fidelity*) bežična vjernost, vrsta bežičnog prijenosa informacija

POPIS SLIKA

1. SLIKA 1. Arhitektura mrežnog komutacijskog podsustava
2. SLIKA 2. Primjer toka poruka sa postavljenim MAPI RULE klijentom i bez njega
3. SLIKA 3. Provjera autentičnosti i procedura ključnih dogovora
4. SLIKA 4. Funkcija zaštite cjelovitosti podataka

POPIS TABLICA

1. TABLICA 1. Napadi na sigurnost UMTS mreže
2. TABLICA 2. Opis funkcija autentikacijskog vektora