CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost mobilnih mreža

NCERT-PUBDOC-2010-06-303

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Mobilni uređaji i mreže dio su današnje svakodnevice. Veliki napredak u bežičnim tehnologijama i rastuća potražnja za mobilnošću tokom telefoniranja i pristupa Internetu rezultirali su potrebom za izgradnjom boljih mobilnih mreža. Telekomunikacijska industrija znatno se razvila od izuma telefona i napredovala u mobilnu mrežu. Tokom razvoja, nastale su četiri generacije mobilnih mreža. Treća i četvrta generacija pružaju značajna poboljšanja u sve traženijem prijenosu podataka i multimedijskih sadržaja. Korisnicima se nudi poboljšana funkcionalnost mobilnih uređaja, kao što je neometano pretraživanje web sadržaja, gledanje televizije, pristup elektroničkoj pošti i navigaciji (GPS). Kako su 3G i 4G usluge nadograđene na 2G usluge, još uvijek se koriste sustavi GSM (eng. *Global System for Mobile Communications*, izvorno fr. *Groupe Spécial Mobile*), GPRS (eng. General Packet Radio Service) i UMTS (eng. *Universal Mobile Telecommunications System*).

Obzirom da je sve popularnije pristupati Internetu preko mobilnih uređaja, javljaju se i opasnosti koje uvijek vrebaju kada se korisnici povezuju na Internet. Uvijek postoje sigurnosni rizici i prijetnje od zlonamjernih napadača. Zato je potrebno pravilno zaštititi sve komunikacijske kanale. Uz to, vrlo su česte prijevare preko telefona i zlouporabe prijenosa govora.

U dokumentu je dan pregled razvoja mobilnih mreža, od 1G sve do 4G sustava. Uz to opisani su standardi koji se koriste (GSM, GPRS, UMTS) te je dan pregled njihove sigurnosti. Također, opisane su i prijetnje koje korisnik može susresti kada koristi mobilni uređaj za komunikaciju te neka od mogućih rješenja sigurnosnih problema.

2. Mobilne mreže

Mobilne mreže su sastavni dio svakodnevice gotovo svih ljudi u razvijenim državama. Ljudi ih koriste kada telefoniraju mobilnim telefonom ili pristupaju Internetu upotrebom mobilnog uređaja (to može biti mobilni telefon koji podržava pristup Internetu ili prijenosno računalo s odgovarajućom opremom).

2.1. Povijesni razvoj mobilnih uređaja i mreža

U današnjem svijetu velika većina ljudi komunicira upotrebom mobilnih telefona. Teško je povjerovati da je mobitel prije petnaest godina bio rijetkost. Povijest mobitela počinje s razvojem radio tehnologije i dvosmjernih radio uređaja u vozilima te se nastavlja pojavom modernih mobitela i usluga vezanih uz njih.

Telefoni temeljeni na radio tehnologiji imaju dugu povijest i datiraju još od izuma Reginalda Fessendena, koji je omogućio komunikaciju broda s obalom korištenjem radio telefonije. Tokom Drugog svjetskog rata vojska je koristila mobilne radijske uređaje za komunikaciju. U pedesetim godinama 20. stoljeća ista se tehnologija prilagodila civilnoj upotrebi (npr. policija, taxi vozila i slično). 1973. godine Martin Cooper je izumio prvi moderni prijenosni telefonski uređaj. Povijest mobilnih uređaja i mreža se obično dijeli na generacije (prva, druga, treća itd.) kako bi se označili ključni koraci u promjenama mogućnosti i tehnologija kojom se ostvaruju te mogućnosti tokom godina.

Slika 1. Mobilni telefon za automobil i M. Cooper sa prvim mobilnim telefonom
Izvor: Wikipedia

2.1.1. Pojava mobilnih uređaja i telefona

Dvosmjerni radio uređaji koristili su se u vozilima kao što su taxi, policijska vozila i kola hitne pomoći, no to nisu bili mobilni telefoni jer nisu bili uključeni u telefonsku mrežu. Točnije, korisnici nisu mogli nazvati telefonski broj iz svojeg vozila već je sve funkcioniralo kao zasebna komunikacijska mreža.

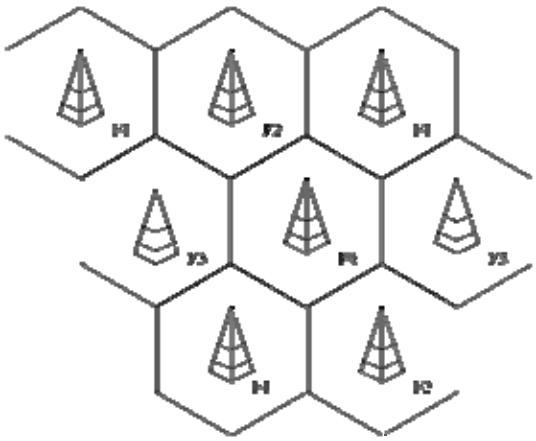
1946. godine ruski inženjeri G. Shapiro i I. Zaharachenko uspješno su testirali svoju inačicu radio mobilnog telefona ugrađenog u automobil. Uređaj se mogao povezati na lokalnu telefonsku mrežu u krugu od 20 kilometara.

U prosincu 1947. godine Douglas H. Ring i W. Rae Young, inženjeri tvrtke Bell Labs, predložili su upotrebu heksagonalne ćelije za mobilne telefone u vozilima. Philip T. Porter, također iz tvrtke Bell Labs, predložio je da odašiljač za svaku ćeliju bude u kutu heksagona, radije nego u centru i da ima usmjerene antene koje bi primale i odašiljale u tri smjera prema tri susjedne ćelije. Tehnologija za ostvarenje ideje tada još nije postojala, a nisu bile određene niti frekvencije koje bi se koristile. Tehnologija ćelija je bila nerazvijena do 60-tih godina 20. stoljeća, kada su Richard H. Frenkiel i Joel S. Engel iz tvrtke Bell Labs razvili potrebne elektroničke uređaje.

1957. godine mladi ruski inženjer Leonid Kupriyanovich iz Moskve stvorio je prijenosni telefonski uređaj i nazvao ga LK-1 ili radiofon. Spomenuti uređaj sastojao se od malih slušalica opremljenih antenom i kolutom za biranje brojeva te je komunicirao s baznom stanicom. Radiofon je težio 3 kilograma i radio je u radijusu od 20 do 30 kilometara te je imao bateriju koja je trajala 20 do 30 sati. Temeljna stanica LK-1 (nazvana ATR, eng. Automated Telephone Radiostation) mogla se povezati na lokalnu telefonsku mrežu i posluživati nekoliko korisnika. 1958. Kupriyanovich je smanjio veličinu radiofona i napravio „džepnu" inačicu koja je težila 500 grama.

U 60-tim godinama 20. stoljeća u Švedskoj je izumljen prvi djelomično automatski telefonski sustav za automobile pod nazivom Mobile System A (MTA). Upotrebom MTA korisnici su mogli komunicirati s korisnicima javne telefonske mreže. Telefonski se broj birao pulsno (kolutom za biranje brojeva).

Koncept ponovne upotrebe frekvencije i predaje poziva iz jedne ćelije drugoj, kao i mnogo drugih koncepata koji čine temelj moderne komunikacije mobilnim telefonima opisani su u 70.-tim godinama 20. stoljeća. 1970. godine Amos E. Joel iz tvrtke Bell Labs smislio je sustav automatske predaje poziva kako bi se omogućila mobilnost telefona kroz područje koje se proteže preko nekoliko ćelija bez gubitka komunikacije tokom poziva. U prosincu 1971. tvrtka AT&T podnijela je zahtjev za stvaranjem ćelija za mobilne telefone federalnoj komisiji za komunikacije (eng. Federal Communications Commission - FCC). Prijedlog je odobren 1982. godine i stvoren je AMPS (eng. Advanced Mobile Phone System) te je odabran pojas frekvencija 824–894 MHz. Analogni AMPS je zamijenjen digitalnim (eng. Digital AMPS) 1990. godine.



Slika 2. Shema ćelija s odašiljačima i ponovna iskoristivost frekcvencija
Izvor: Wikipedia

Jedna od prvih uspješnih javnih komercijalnih mobilnih mreža bila je ARP mreža u Finskoj, pokrenuta 1971. godine. 1973. godine Motorola je izumila prvi mobilni telefon koji je komercijaliziran kao Motorola DynaTAC 8000X. Martin Cooper, istraživač tvrtke Motorola, izumio je spomenuti mobilni telefon i prema tome se smatra i izumiteljem modernog mobilnog telefona. Potrebno je napomenuti kako je postojala duga utrka između Motorole i Bell Labsa tko će prvi izumiti moderni mobilni telefon. Cooper je uputio prvi poziv upotrebom mobitela svojem suparniku Joelu S. Engelu u Bell Labsu.

2.1.2. Prva generacija

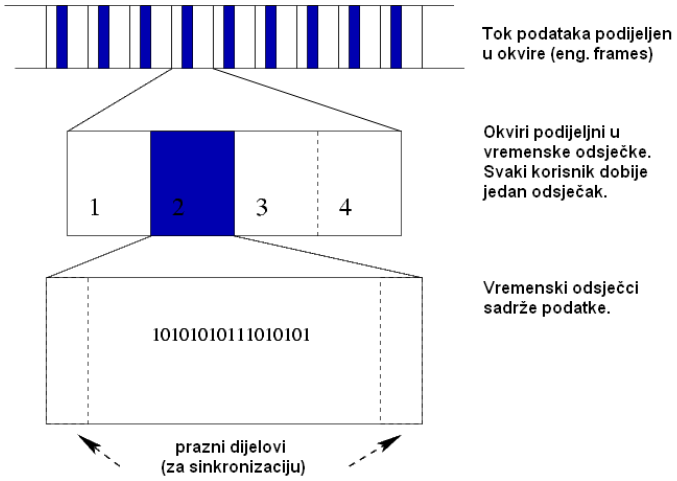
Značajni tehnološki razvoj koji razlikuje prvu generaciju mobilnih telefona od prethodnih generacija je upotreba višestrukih ćelija i mogućnost prijenosa poziva iz jedne ćelije u drugu ako korisnik putuje u području pokrivenom s nekoliko ćelija tokom razgovora. Prvu komercijalnu automatiziranu mrežu ćelija (1G generacija) ostvarila je tvrtka NTT (eng. *Nippon Telegraph and Telephone Corporation*) u Japanu 1979. godine. U početku je mreža pokrivala područje grada Tokia u kojem je živjelo preko 20 milijuna stanovnika i bila je sačinjena od 23 temeljne stanice. U toku 5 godina NTT mreža se proširila i pokrivala je cijelu populaciju Japana te postala prva nacionalna 1G mreža.

2.1.3. Druga generacija

Devedesetih godina 20. stoljeća pojavila se druga generacija (2G) sustava mobilnih telefona koja je koristila GSM standard. 2G telefonski sustavi su se razlikovali od prethodnih generacija u tome što su koristili digitalni prijenos podataka (umjesto analognog) te su uveli napredno i brzo *telefon-prema-mreži* (eng. *phone-to-network*) signaliziranje. Porast upotrebe mobilnih telefona bio je eksplozivan. U ovom su se razdoblju počeli koristiti pretplaćeni mobilni telefoni (eng. prepaid mobile phone). Pretplaćeni mobilni telefon je mobitel za kojeg se kupuju bonovi koje će korisnik trošiti svaki puta kada nekome uputi poziv.

1991. godine osnovana je prva GSM mreža (u Finskoj) pod nazivom *Radiolinja*. Frekvencije koje koriste 2G sustavi u Europi su općenito više nego one u Americi. Na primjer, frekvenciju od 900 MHz su koristile 1G i 2G sustavi u Europi. U Americi su frekvencije bile niže uz nešto preklapanja s Europskim. Uvođenjem 2G sustava mobilni su uređaji postali manji i lakši (100 – 200 grama) te su zamijenili popularne „cigle". Ovu (pozitivnu) promjenu u vidu težine su omogućili napredak u tehnologiji, kao i naprednije baterije, učinkovitija elektronika te uvođenje više ćelija i odašiljača. 2G sustavi koriste CDMA (eng. *Code division multiple access*) i TDMA metode pristupa komunikacijskim kanalima. CDMA je metoda pristupa kanalima koju koriste različite tehnologije za komunikaciju preko radio signala. Jedan od osnovnih koncepata u prijenosu podataka je upotreba nekoliko odašiljača za slanje podataka. Odašiljači šalju podatke istovremeno preko jednog komunikacijskog kanala. Na taj način nekoliko korisnika dijele isti pojas frekvencija (ova metoda naziva se *multipleksiranje*). CDMA koristi široki spektar frekvencija i posebnu shemu kodiranja u kojoj se svakom odašiljaču dodjeljuje određena oznaka kako bi više korisnika moglo komunicirati upotrebom istog fizičkog kanala. Dakle, upotrebom tehnike CDMA više mobilnih uređaja mogu koristiti iste frekvencije te svi mobilni uređaji mogu biti stalno aktivni jer kapacitet mreže ne ograničava broj aktivnih uređaja. CDMA je standard koji se počeo koristiti kao dio 2G GSM sustava.

TDMA (*eng. Time division multiple access*) metoda pristupa kanalu ne koristi multipleksiranje kao CDMA već koristi podjelu vremena. TDMA tehnika omogućuje da nekoliko korisnika koriste isti frekvencijski kanal podjelom u vremenske odsječke (eng. *time slots*). Koriste ju GSM sustavi i tipična je za 2G sustave. Sljedeća slika prikazuje TDMA metodu.



Slika 3. TDMA metoda

Druga generacija je uvela i novu vrstu komunikacije - slanje poruka putem SMS-a (eng. *Short Message Service*), u početku samo preko GSM mreža, a kasnije i preko svih digitalnih mreža. Prva SMS poruka između dvije osobe poslana je u Finskoj 1993. godine. 2G tehnologija je također uvela mogućnost pristupa multimedijalnom sadržaju na mobilnim telefonima, kada je Radiolinja (danas Elisa) u Finskoj uvela prijenos pozivnog tona na mobilni uređaj kao sadržaj koji se plaća. Finska je također prva država u kojoj se na mobilnim telefonima pojavilo oglašavanje, i to u trenutku kada je pokrenuta besplatna usluga slanja dnevnih vijesti u obliku SMS poruka (2000. godine). Prve usluge prijenosa podataka na mobilnim telefonima počele su slanjem SMS poruka, a prva Internet usluga uvedena je u Japanu 1999. godine. Sljedeća slika prikazuje mobilne uređaje proizvedene između 1997. godine i 2003. godine.

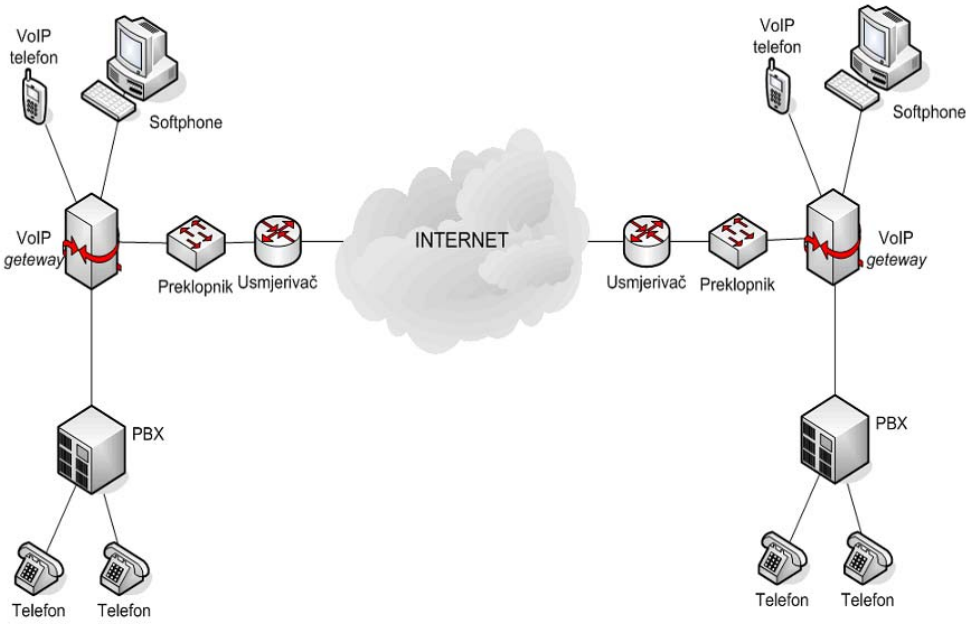
Slika 4. Mobilni uređaji iz Japana proizvedeni između 1997. i 2003.
Izvor: Wikipedia

2.1.4. Treća generacija

Kako je upotreba 2G telefona postala sve raširenija i ljudi su počeli koristiti mobilne telefone u svakodnevnom životu, postalo je jasno da će potražnja za uslugama prijenosa podataka (kao što je Internet) postati sve veća. Također, pojavila se potreba za sve većim brzinama prijenosa podataka. 2G tehnologije nisu pružale spomenute mogućnosti u dovoljnoj mjeri te je počeo rad na stvaranju sljedeće generacije poznate kao 3G (treća generacija). Glavna tehnološka razlika kojom se 3G tehnologija ističe je upotreba preusmjeravanja paketa za prijenos podataka. Uz to, standardizacija je usredotočena više na potrebe nego na tehnologiju (u smislu povećanja brzine i količine prijenosa podataka), što je neizbježno dovelo do nastanka mnogo konkurentskih standarda. 3G sustavi koriste inačice CDMA standarda koje su nadograđene kako bi podržavale 3G tehnologije. CdmaOne ili IS-95 (eng Interim Standard 95) je prvi standard temeljen na CDMA za digitalnu mobilnu komunikaciju. CdmaOne je 2G standard za slanje korisničkih podataka, govora te podataka o pozivima (npr. broj mobilnog telefona) između mobitela i odašiljača.

CDMA2000 (još poznat kao IMT-MC – eng. IMT-Multi-Carrier) je standard koji pripada obitelji 3G standarda mobilne tehnologije. Također se temelji na CDMA metodi pristupa komunikacijskom kanalu za slanje govora, podataka i podataka o pozivima. CDMA2000 uključuje skup standarda: CDMA2000 1X, CDMA2000 EV-DO Rev0, CDMA2000 EV-DO Rev. A i CDMA2000 EV-DO Rev. B. Svi su kompatibilni sa cdmaOne standardom.

Standardi za komunikaciju mobilnih tehnologija treće generacije omogućili su ostvarenje VoIP (eng. *Voice over Internet Protocol*) tehnologije. VoIP je proces digitaliziranja i slanja glasovnih podataka preko Interneta i drugih podatkovnih mreža. Korištenjem VoIP tehnologije, organizacije više ne moraju koristiti samo tradicionalnu telefonsku mrežu, što rezultira smanjivanjem troškova telefoniranja i većom fleksibilnosti rada. IP telefonija je proces prijenosa glasa (govora) preko paketno preklapanih IP mreža nasuprot prijenosu zasnovanom na javnim telefonskim mrežama. Digitaliziranje zvuka u mrežne pakete te njihov prijenos preko Interneta i drugih podatkovnih mreža (intranet i sl.) naziva se VoIP protokolom. VoIP omogućava obavljanje telefonskog razgovora upotrebom postojećih mrežnih konekcija te predstavlja zamjenu za standardnu telefoniju, kako u lokalnom i međugradskom prometu, tako i u međunarodnom. Velika prednost VoIP tehnologije je i mogućnost pozivanja mobilnih i fiksnih pretplatnika te ostvarivanje međunarodnih poziva po izuzetno povoljnim cijenama. Sljedeća slika prikazuje VoIP arhitekturu.



Slika 5. VoIP arhitektura
Izvor: CERT

Prvu nekomercijalnu 3G mrežu pokrenula je tvrtka NTT DoCoMo u Japanu na području Tokija (2001. godine). Tijekom razvoja 3G sustava, sustavi kao 2.5G i GPRS razvijeni su kao produžeci postojećih 2G mreža. Oni pružaju iste usluge kao 3G bez brzog prijenosa podataka i potpune multimedijalne usluge. Kao poboljšanje GPRS tehnologije javlja se EGDE (eng. *Enhanced Data Rates for GSM Evolution*) tehnologija za prijenos podataka preko GSM mobilne mreže. EDGE pruža do tri puta veći kapacitet prijenosa podataka od GPRS tehnologije. EDGE koristi TDMA metodu pristupa kanalu čime se nadograđuje izravno na GSM mrežu. 3G sustavi kombiniraju CDMA i TDMA standarde kako bi bili kompatibilni sa 2G sustavima.

Velike brzine spajanja koje pruža 3G tehnologija omogućile su po prvi puta prijenos toka podataka, odnosno multimedijalnog sadržaja (kao što su radio i televizija) na mobilne uređaje. Nakon 2000. godine počela je evolucija 3G tehnologija i pojavio se protokol HSDPA (eng. *High-Speed Downlink Packet Access*), poboljšani protokol za komunikaciju iz obitelji HSPA (eng. *High-Speed Packet Access*). Spomenuti se protokol još naziva 3.5G, 3G+ ili turbo 3G, a koriste ga mreže temeljene na sustavu UMTS. UMTS pruža veće brzine prijenosa i veći kapacitet za prijenos podataka. Trenutni HSDPA protokoli podržavaju prijenos brzinama 1.8, 3.6, 7.2 i 14 Mbit/s. Veće brzine omogućuje HSPA+, koji pruža brzine do 42 Mbit/s i 84 Mbit/s. U Japanu i Južnoj Koreji na tržištu više ne postoje mobiteli koji ne podržavaju 3G tehnologiju. Sljedeća slika prikazuje vrlo popularan mobilni uređaj ove generacije - iPhone.

Slika 6. iPhone
Izvor: Google

2.1.5. Četvrta generacija

Iako su mobilni telefoni imali pristup podatkovnim mrežama kao što je Internet, pristupanje Internetu putem mobitela nije postala navika sve dok se nisu pojavile 3G mreže i specijalizirani uređaji za pristup mobilnom Internetu. Prvi takvi uređaji su bili poznati kao „*dongles*“ (u prijevodu sklopovski ključ, odnosno uređaj koji se spaja na računalo kako bi se autenticirao programski paket) i priključivali su se izravno na računalo preko USB priključka. Nova vrsta uređaja je bila i tzv. kompaktni bežični usmjerivač (eng. *compact wireless router*), kao što je Novatel MiFi, koji pruža uslugu spajanja više računala odjednom preko WiFi mreže na 3G Internet. Spomenuti uređaji postali su popularni za upotrebu s prijenosnim računalima. Kao posljedica toga proizvođači računala su počeli ugrađivati funkcionalnosti za mobilne mreže i prijenos podataka preko mobilnih mreža u računala, tako da „*dongle*“ ili MiFi nisu više bili potrebni. Umjesto toga SIM kartica se mogla izravno umetnuti u samo računalo te je tako korisnik mogao pristupiti uslugama mobilnog prijenosa podataka. Spomenuta prijenosna računala dobila su naziv „*netbook*“. Do početka 2010. godine korisnicima su postali dostupni različiti uređaji s ugrađenim bežičnim Internetom. Neki od njih su *E-reader*, *Amazon Kindle* i *Nook.* Pojava spomenutih uređaja potaknula je razvoj četvrte generacije mobilne tehnologije. Do 2009. godine postalo je jasno da će 3G mreže postati preopterećene brojem korisnika i upotrebom aplikacija kojima je potreban širokopojasni kanal za prijenos podataka (kao što je na primjer prijenos multimedijskog toka podataka). Počeo je razvoj tehnologija koje su optimizirane za prijenos podataka i koje trebaju omogućiti prijenos podataka velikim brzinama (oko 10 puta brže nego 3G). Prve dvije komercijalne tehnologije bili su standard WiMAX (ponuđen u USA) i standard LTE (ponuđen u Skandinavskim državama). Ono što razlikuje 4G tehnologije od 3G je uklanjanje uspostave kruga (ili kanala) između čvorova i terminala prije uspostave komunikacije među korisnicima. Umjesto toga koristi se IP (eng. Internet Protocol) mreža. Na sljedećoj slici je prikazan mobilni uređaj koji podržava 4G.

Slika 7. HTC
Izvor: Google

2.2. GSM

GSM je najpopularniji standard za sustave mobilne telefonije u svijetu. Njegova sveprisutnost omogućuje međunarodne *„roaming"* ugovore između pružatelja usluga mobilnih telefona te pruža neprekidnu uslugu upotrebe mobilnog telefona u mnogim dijelovima svijeta. GSM je ćelijska mreža, što znači da se mobilni telefoni na nju povezuju traženjem ćelija u neposrednoj blizini uređaja. Postoji pet različitih veličina GSM mreža:

- **makro ćelije** – ćelije u kojima se nalazi antena temeljne postaje, obično je postavljena na vrh visoke zgrade ako se nalazi na području grada,
- **mikro ćelije** – antena se nalazi ispod prosječne visine krovova, obično se nalazi u urbanim područjima,
- **piko ćelije** – pokrivaju nekoliko desetaka metara, koriste se u zgradama,
- **femto ćelije** – koriste se u poslovnom okruženju i povezuju mrežu pružatelja usluga na Internet,
- **ćelije kišobran** – koriste se za pokrivanje rupa između ćelija.

Najveći radijus koji podržava GSM specifikacija u praktičnoj upotrebi je 35 kilometara.

Mreža se sastoji od sljedećih komponenti:

- *Podsustav bazne stanice* (eng. *Base Station Subsystem*) - temeljna stanica i njihovi upravitelji.
- *Podsustav za mrežu i prebacivanje* (eng. *Network and Switching Subsystem*) – dio mreže koji je najsličniji fiksnoj mreži.
- *GPRS jezgrena mreža* (eng. *GPRS Core Network*) – neobavezni dio koji omogućuje povezivanje na Internet temeljeno na paketima.
- *Potporni sustav operacija* (eng. *Operations support system – OSS*) – podsustav koji se koristi za održavanje mreže.

Jedna od ključnih značajki GSM mreže je SIM (eng. *Subscriber Identity Module*) modul. SIM je pametna kartica koja sadrži podatke o korisnikovoj pretplati i telefonski imenik. Ona omogućuje korisnicima da zadrže svoje podatke nakon promjene mobilnog uređaja. Dakle, SIM kartica je neovisna o mobilnom uređaju. Osim toga, korisnici mogu promijeniti pružatelja mobilnih usluga mijenjanjem SIM kartice i zadržavanjem istog mobilnog uređaja. Neki pružatelji usluga postavljaju blokade tako da telefon može koristiti samo SIM kartice koje su oni izdali. To se naziva zaključavanje SIM kartica i ilegalno je u nekim državama (u Hrvatskoj je dozvoljeno).

2.2.1. Sigurnost GSM usluge

GSM je dizajniran tako da podržava umjerenu razinu sigurnosti usluge i pruža mnogo bolju sigurnost od analognih sustava prve generacije. GSM sustav koristi algoritam za kriptiranje govora, GMSK digitalnu modulaciju (eng. *Gaussian Minimum Shift Keying*), sporo preskakanje frekvencija i TDMA arhitekturu. Za presretanje i rekonstrukciju signala potrebno je posjedovati posebnu opremu, skuplju od policijskog skenera.

Sigurnost GSM sustava je orijentirana na sljedeće aspekte zaštite:

- autentikacija identiteta pretplatnika,
- povjerljivost identiteta pretplatnika,
- povjerljivost podataka vezanih uz pozive i
- povjerljivost korisničkih podataka.

Sigurnosni mehanizmi GSM sustava postoje u tri različite komponente sustava:

- SIM (eng. *Subscriber Identity Module*) kartica,
- GSM uređaj, odnosno mobilni telefon te
- GSM mreža.

SIM kartica sadrži:

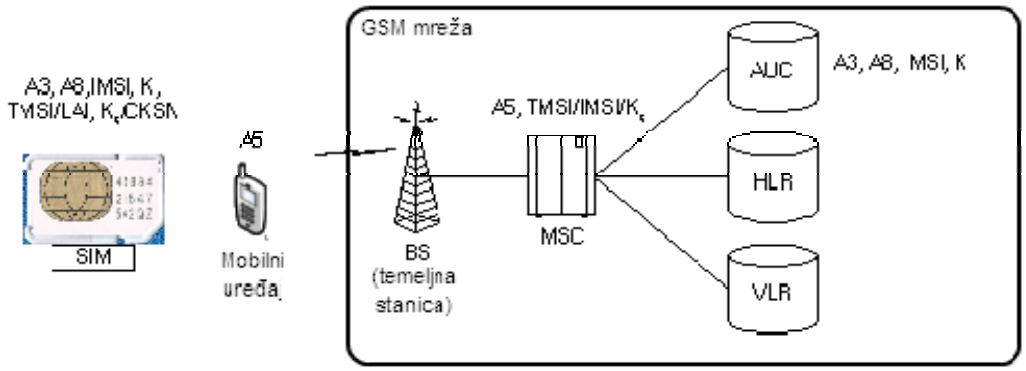
- IMSI (eng. *International Mobile Subscriber Identity*) broj,
- jedinstveni autentikacijski ključ pretplatnika (Ki),
- algoritam za stvaranje kriptografskog ključa (algoritam A8) i
- PIN (eng. *Personal Identification Number*) broj.

GSM uređaj sadrži algoritam kriptiranja (algoritme obitelji A5). Enkripcijski algoritmi (A3, A5 i A8) su prisutni u GSM mreži. Autentikacijsko središte (eng. *Authentication Center – AUC*), dio podsustava za upravljanje i održavanje (eng. *Operation and Maintenance Subsystem – OMS*) GSM mreže sadrži bazu podataka sa identifikacijskim i autentikacijskim podacima pretplatnika. Podaci u spomenutoj bazi podataka su :

- IMSI broj,
- TMSI (eng. *Temporary Mobile Subscriber Identity*) broj – pomoću njega se mobitel identificira, dodjeljuje ga mreža i može se mijenjati u određenim vremenskim razmacima,
- LAI (eng. *Location Area Identity*) broj i
- jedinstveni autentikacijski ključ pretplatnika (Ki) za svakog korisnika na mreži.

Ovakva podijeljenost sigurnosnih elemenata i enkripcijskih algoritama pruža dodatnu mjeru sigurnosti osiguravajući privatnost telefonskih razgovora i sprečavajući prijevare putem telefona.

Sljedeća slika prikazuje podijeljenost sigurnosnih elemenata između tri komponente sustava, SIM kartice, mobilnog uređaja i GSM mreže. U GSM mreži sigurnosni se podaci dijele između autentikacijskog središta (AUC), HLR (eng. *home location register*) popisa i VLR (eng *visitor location register*) popisa. HLR je baza podataka koja sadrži detalje o svakom pretplatniku mobilnog telefona koji je autoriziran za korištenje GSM mreže. VLR je baza podataka koja čuva podatke o svim mobitelima koji su pod ovlasti mobilnog preklopnog središta (eng. *Mobile Switching Center – MSC*), MSC je čvor GSM mreže odgovoran za usmjeravanje glasovnih poziva, SMS poruka i ostalih usluga (npr. konferencijski pozivi). AUC je odgovoran za stvaranje brojeva potrebnih kod autentikacije i u postupku kriptiranja koji se spremaju u HLR i VLR.



Slika 8. Podjela sigurnosnih elemenata u GSM sustavu.

GSM sustav autenticira pretplatnika upotrebom dijeljenog ključa i odgovora na temelju izazova (eng. *challenge-response*). Komunikacija između pretplatnika i temeljne bazne stanice može biti kriptirana. Razvoj UMTS-a uvodi neobavezno modul USIM (eng. *Universal Subscriber Identity Module*) koji koristi duži autentikacijski ključ u svrhu pružanja bolje sigurnosti, kao i uzajamnog autenticiranja mreže i korisnika. GSM autenticira samo korisnika prema mreži, obratno ne. Sigurnosni model pruža povjerljivost i autentikaciju, ali ima ograničene mogućnosti autorizacije.

GSM koristi nekoliko kriptografskih algoritama za sigurnost. A5/1 i A5/2 su kriptoalgoritmi koji se koriste kako bi osigurali privatnost razgovora. A5/1 je prvi algoritam koji je razvijen i bolji je od A5/2. Koristi se u Europi i SAD-u. A5/2 je slabiji i koristi se u ostalim državama. Otkrivene su ozbiljne slabosti kod oba algoritma. A5/2 je moguće probiti u realnom vremenu upotrebom napada s kriptiranim tekstom. U veljači 2008. godine tvrtka Pico Computing, Inc otkrila je planove za komercijalizaciju integriranog kruga FPGA (eng. *field-programmable gate array)* koji koristi *rainbow* tablicu [11] za probijanje A5/1 algoritma. GSM sustav podržava različite algoritme tako da je moguće zamijeniti postojeće kriptoalgoritme jačima.

U prosincu 2009. godine njemački inženjer računarstva Karsten Nohl je objavio da je probio A5/1 algoritam. Razvio je niz brojčanih *rainbow* tablica (statične vrijednosti koje smanjuju vrijeme izvođenja napada) i stvorio nove izvorne kodove za napade s poznatim jasnim tekstom. Također, utvrdio je da je moguće izgraditi GSM presretač, no takva aplikacija nikad nije ostvarena jer je ilegalna.

2010. godine je na web stranici *threatpost.com* objavljeno da je skupina kriptografa razvila novi način napada koji je probio Kasumi, kriptografski algoritam koji se koristi za zaštitu prometa na 3G GSM bežičnim mrežama. Korištenom tehnikom moguće je pribaviti potpuni ključ upotrebom taktike poznate kao napad srodnim ključem (eng. *related-key attack*). Kasumi je naziv za A5/3 algoritam koji se koristi za zaštitu većine 3G prometa.

Iako postoje sigurnosni problemi za GSM, upotreba novijih standarda i algoritama može to promijeniti. Upotreba autentikacije , kriptiranja komunikacije i privremenih identifikacijskih brojeva osigurava privatnost i anonimnost korisnika sustava. Čak su GSM sustavi bez enkripcije sigurniji od analognih sustava zbog upotrebe digitalne modulacije i TDMA metode pristupa komunikacijskom kanalu. Unatoč primjeni opisanih sigurnosnih mjera, niti jedan sustav neće biti u potpunosti zaštićen od zlouporabe. Napadači će uvijek smisliti neki način zlouporabe sigurnosnih nedostataka GSM sustava. Upotrebom nekih metoda napadač može prisluškivati i neovlašteno preuzeti audio ulaz i izlaz. Iako postoji rizik od prisluškivanja, opasnost je umanjena činjenicom da za uspješno prisluškivanje napadač mora podmetnuti trojanskog konja, zloćudni program ili virus. Zloćudne programe može otkriti antivirusni program, no mnogi korisnici mobilnih telefona nemaju na svojem uređaju instaliran takav program. Kako bi se što bolje zaštitili, preporuča se povremeno pokretanje antivirusnih programa na mobilnim uređajima.

2.3. GPRS

GPRS je paketno orijentirana mobilna usluga za prijenos podataka dostupna korisnicima 2G i 3G komunikacijskih sustava. U 2G sustavima GPRS pruža brzine prijenosa od 56 – 114 kbit/s. 2G mreže koje podržavaju GPRS se često nazivaju 2.5G mreže. Usluga pruža umjerenu brzinu prijenosa podataka upotrebom TDMA kanala nad GSM sustavom. GPRS nadograđuje GSM usluge i omogućuje sljedeće usluge:

- stalan pristup Internetu,
- MMS (eng. Multimedia Messaging Service),
- PTT (eng. Push to talk) preko ćelija (Poc/PTT) – metoda komunikacije na kanalu koji podržava obostranu, ali neistovremenu (half-duplex), komunikaciju upotrebom tipke za prebacivanje s primanja poruka na slanje poruka,
- IM (eng. Instant messaging),
- podrška za aplikacije za pregledavanje Internet stranica namijenjene pametnim uređajima (eng. *smart devices*) preko protokola WAP (eng. *Wireless Application Protocol*) i
- P2P (eng. *Point-to-point*) spajanje na Internet.

Ako se koristi SMS preko GPRS-a moguće je postići brzinu prijenosa od oko 30 poruka u minuti. To je mnogo brže od prijenosa poruka putem GSM-a gdje je brzina prijenosa između 6 i 10 poruka u minuti.

GPRS podržava sljedeće protokole:

- IP,
- PPP (eng. *point-to-point protocol*) – ovaj način rada često ne podržava pružatelj usluge, ali ukoliko se koristi, mobitel se spaja na modem koji je povezan na računalo te se mobitelu dodjeljuje IP adresa,
- X.25 veze – obično se koristi za aplikacije kao što su bežični terminali za plaćanje.

Kada se koristi TCP/IP, svaki telefon može imati dodijeljenu IP adresu. GPRS će spremati i prosljeđivati IP pakete telefonu tokom putovanja kroz ćelije. TCP protokol upravlja mogućim gubitkom paketa.

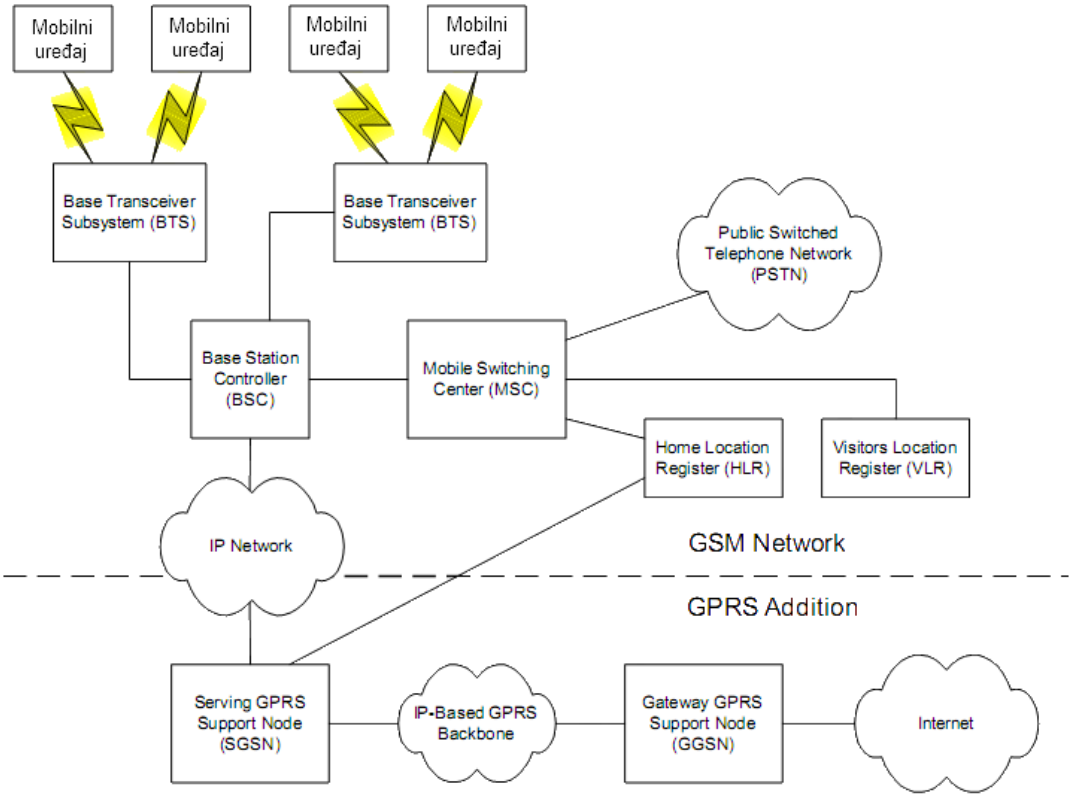
GPRS veza se uspostavlja referencom na ime točke pristupa (eng. *Access point name – APN*). APN definira usluge kao što su WAP pristup, SMS, MMS te pristup elektroničkoj pošti i Internetu. Za uspostavljanje GPRS veze na bežični modem korisnik mora odrediti APN, korisničko ime i lozinku (opcionalno) te rijetko IP adresu. Sve navedeno korisniku dodjeljuje pružatelj usluge.

GPRS optimizira upotrebu mreže i radio resursa. Postoji stroga odvojenost između radio podsustava i mrežnog podsustava. Elementi GPRS mreže su:

- SGSN (eng. *Serving GPRS Support Node*) – služi za dostavu podatkovnih paketa prema i od mobilnog uređaja (mobilne stanice – MS). Zadaće koje obavlja uključuju usmjeravanje i prijenos paketa, , upravljanje logičkim poveznicama, autentikacija i naplaćivanje usluga te komunikaciju s GGSN čvorom.
- GGSN (eng. *Gateway GPRS Support Node*) – glavni element mreže, odgovoran za mrežnu suradnju GPRS mreže i vanjskih mreža s usmjerivanjem paketa. Može se smatrati usmjerivačem za podmrežu. Zapravo skriva unutarnju građu GPRS mreže prema vanjskim mrežama.
- BG (eng. *Border Gateway*) – protokol za usmjerivanje paketa na Internetu
- *Backbone* mreža (intra-PLMN i inter-PLMN (eng. *PLMN - public land mobile network*))– mreža koja povezuje njezine različite dijelove pružajući put za izmjenu podataka između različitih mreža i podmreža.
- HLR (eng. *Home location register*)- središnja baza podataka koja sadrži detalje o svakom pretplatniku mobilnog telefona koji je autoriziran za korištenje GSM mreže.
- MSC/VLR (eng. *Mobile Switching Center - Visitor Location Register*) – odgovoran je za prebacivanje glasovnih poziva i praćenje točnog položaja područja u kojem se nalazi korisnik mobitela.
- SMS-GMSC (eng. *SMS gateway Mobile Switching Centre (MSC)*) – točka mobilne mreže za kontakt s drugim mrežama.

- BTS (eng. *Base Transceiver Subsystem*) – primopredajnik koji omogućuje bežičnu komunikaciju između korisnikovog uređaja i mreže.
- BSC (eng. *Base Station Controller*) – odgovoran je za dodjeljivanje frekvencija mobilnom uređaju, administraciju frekvencija i predaju veze između BTS-ova.

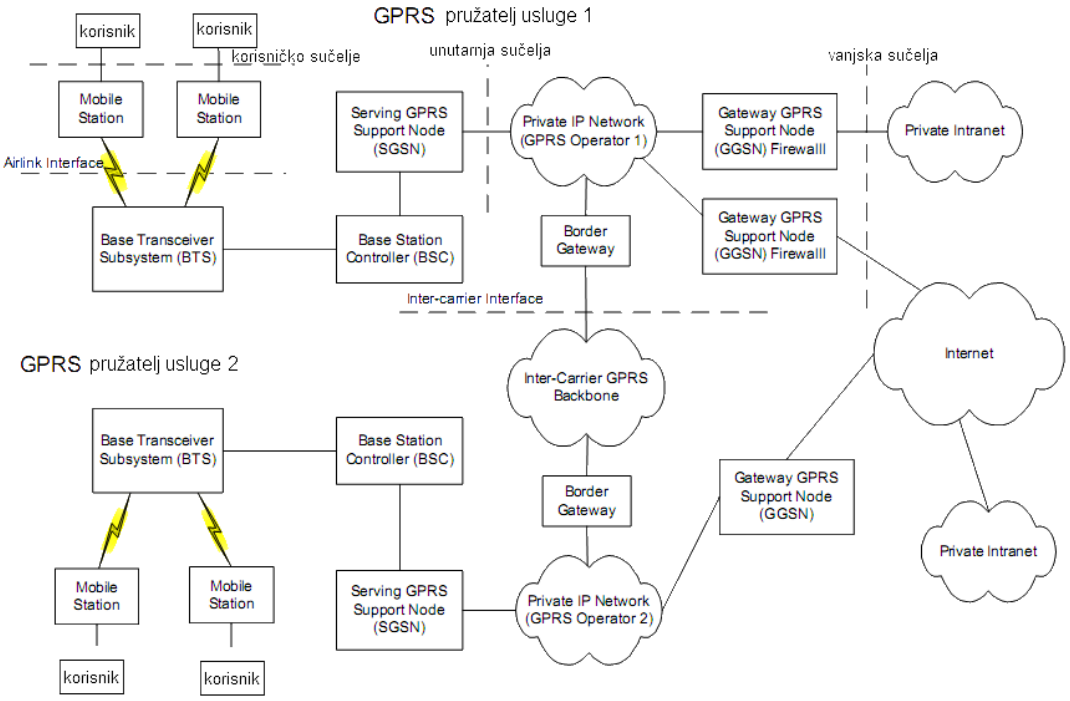
Sljedeća slika prikazuje arhitekturu GPRS mreže:



Slika 9. GPRS mreža.

GPRS koristi postojeću strukturu ćelija i dodaje novu potpornu IP mrežu (eng. *IP backbone network*) koja uključuje dva nova čvora, SGSN i GGSN. Elementi postojeće mreže su BTS i BSC. Dodatni uređaj je PCU (eng. *Packet Control Unit*) koji treba biti postavljen na BSC kako bi upravljao kanalima i radio vezom te pružio standardno sučelje za SGSN. Između mobilnog uređaja i BTS-a postoje tzv. „zračna sučelja". Svaki je BTS povezan na BSC. BSC upravlja prometom odjeljujući glasovni promet od podatkovnog. Glasovni promet se usmjeruje prema MSC-u, a podatkovni prema SGSN-u. MSC povezuje PTSN, HLR i VLR te tako upotpunjuje usmjeravanje glasovnog prometa.

Paketi koji putuju prema i od mobilne stanice moraju proći kroz nekoliko mrežnih komponenti tokom prijenosa. Kako bi se olakšao prijenos podataka kada prolaze GPRS/GSM mrežom, svaka mrežna komponenta koristi mrežno sučelje za interakciju s ostalim mrežnim komponentama. Sljedeći dijagram prikazuje dva GPRS operatora i mrežna sučelja koja pokreću komunikaciju između mrežnih komponenti:



Slika 10. Komunikacija između dva korisnika upotrebom GPRS-a.

2.3.1. Sigurnost GSM/GPRS mreže

Osnovna funkcija GSM/GPRS mreže je pružiti potporu i olakšati prijenos informacija (glasovnih i podatkovnih). Obzirom da se radi o prijenosu informacija, postoje sigurnosni rizici pa je potrebno poduzeti određene sigurnosne mjere kako bi se zaštitila komunikacija. Tipovi informacija koji se trebaju zaštititi na GSM/GPRS mreži uključuju sljedeće:

- **Korisnički podaci** – glasovne ili podatkovne informacije poslane ili primljene preko GSM/GPRS mreže.
- **Naplaćivanje informacija** – informacije koje prikupe SGSN i GGSN koriste se za naplaćivanje usluga.
- **Informacije o pretplatniku** – pohranjene su u mobilnom uređaju te u HLR-u i VLR-u.
- **Tehničke informacije o GSM/GPRS mreži** – opisuju arhitekturu i konfiguraciju mreže.

Pružatelji mobilnih usluga su odgovorni za postavljanje sigurnosti na svojoj GSM/GPRS mreži. Neki uređaji koji se koriste u mreži već imaju u sebi sigurnosne funkcionalnosti, kao što su kriptiranje podataka i autentikacija korisnika. Uz to, pružatelj usluga može dodati funkcionalnosti koje poboljšavaju sigurnost mreža. Neke od njih su vatrozidovi (eng. *firewall*) i VPN veze preko GPRS mreže.

Standardne sigurnosne usluge koje nude GSM/GPRS mreže su:

- anonimnost,
- autentikacija,
- zaštita slanja signala te
- zaštita korisničkih podataka.

GSM/GPRS mreže koriste TBMI (eng. *Temporary Mobile Subscriber Identities*) funkcionalnost kako bi osigurali da identitet pretplatnika ostane zaštićen na mobilnoj mreži. Identitet pretplatnika se utvrđuje u kratkom vremenskom razmaku kada se mobilni uređaj priključuje na mrežu. Kada mobilni uređaj uspostavi vezu s mrežom, mora pružiti svoj IMSI (eng. *International Mobile Subscriber Identity*). IMSI sadrži osobni broj pretplatnika, njegovo ime i mrežu te kod države u kojoj je ugovorio pretplatu. Kada je mreža završila s upotrebom informacija za identifikaciju pretplatnika, mobilnom uređaju se dodjeljuje TMBI. Nakon toga se održava anonimnost korisnika.

GSM/GPRS mreže koriste mehanizam „izazov-odgovor“ (eng. challenge-response) kako bi osigurali da samo autorizirani korisnici imaju pristup mreži. Za GSM glasovne usluge autentikaciju obavlja MSC, a za GPRS SGSN. SGSN dodjeljuje slučajno odabrane 128 bitne brojeve mobilnom uređaju. Mobilni uređaj upotrebom privatnog autentikacijskog ključa jedinstvenog za svakog pretplatnika (pohranjenom u SIM kartici) i GSM autentikacijskog algoritma A3 stvara 32 bitni broj kao odgovor 128 bitnom broju kojeg je poslao SGSN. SGSN prima odgovor na izazov i obavlja isti računski postupak kao i mobilni uređaj. Ako su rezultati jednaki, mobilni uređaj se uspješno autenticirao na GPRS mreži i može koristiti njezine usluge. Tokom opisane interakcije pretplatnikov privatni ključ se ne prenosi preko radio sučelja (kako bi se zaštitio).

Slanje signala i korisničkih podataka preko GPRS-IP potporne mreže i preko radio veze zaštićeno je od presretanja i prisluškivanja kriptografskim algoritmima. SGSN i mobilni uređaj koriste 128 bitni broj korišten u procesu autentikacije i privatni ključ pretplatnika (također spremljen u HLR-u) te u kombinaciji sa algoritmom za stvaranje ključeva A8 stvaraju kriptografski ključ. Podaci koji se prenose između mobilnog uređaja i GPRS mreže se mogu kriptirati upotrebom algoritma GPRS-A5 (prilagođene inačice A5 algoritma koji se koristi za kriptiranje glasovne komunikacije preko GSM mreža).

2.4. EDGE

EDGE je tehnologija koja pruža poboljšane brzine prijenosa podataka mobilnim mrežama te je produžetak GSM standarda. EDGE se smatra 3G tehnologijom i prvi put je uveden kao dodatak GSM mrežama 2003. godine u SAD-u. EDGE je standardizirao 3GPP i dio je GSM obitelji te pruža bolje mogućnosti nego GSM/GPRS mreže. Uvode se bolje metode kodiranja i prijenosa podataka. EDGE se može koristiti s bilo kojom aplikacijom koja prebacuje pakete (eng. *packet switching*), kao što je na primjer aplikacija za povezivanje na Internet.

„*Evolved* EDGE“ je standard koji pruža smanjenu latenciju i dvostruko bolje performanse. Pruža prijenos brzinama 1Mbit/s za primanje podataka te 400 kbit/s za slanje podataka. Kako bi se ugradila podrška za EDGE, potrebno je postaviti primopredajnik na podsustav temeljne postaje. Uz uporabu EDGE standarda korisnici će moći iskusiti brzine pristupa Internetu, odnosno prijenosa podataka koje odgovaraju ADSL (eng. *Asymmetric Digital Subscriber Line*) usluzi (u prosjeku brzne su oko 500 kbit/s).

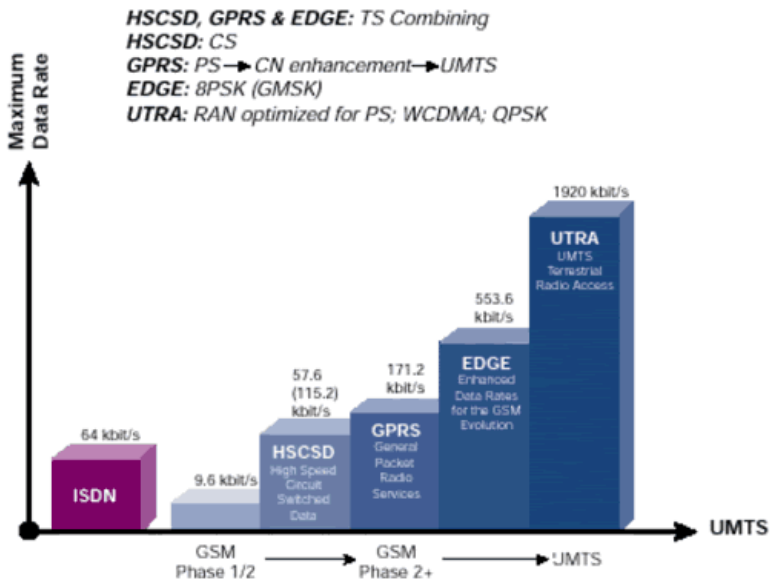
2.5. UMTS

UMTS je jedna od tehnologija treće generacije. Najuobičajeniji oblik UMTS-a koristi W-CDMA (eng. *Wideband Code Division Multiple Access*) kao sučelje za prijenos podataka bežičnim putem, koje također pokriva TD-CDMA (eng. *Time-division Code Division Multiple Access*) i TD-SCDMA (eng. T*ime Division Synchronous Code Division Multiple Access*) pristup. CDMA (eng. *Code division multiple access*) je metoda za pristup kanalu kojeg koriste različite radio komunikacijske tehnologije. Jedan od osnovnih koncepata u komunikaciji prijenosom podataka je ideja da nekoliko odašiljača šalje podatke istovremeno preko jednog komunikacijskog kanala.

UMTS je potpun mrežni sustav te prema tome pokriva radio pristup mreži (eng. *UMTS Terrestrial Radio Access Network – UTRAN*) i jezgrenu mrežu (eng. *Mobile Application Part – MAP*) te podržava autentikaciju upotrebom USIM (eng. *Universal Subscriber Identity Module*) kartica. Za ostvarenje UMTS-a bilo je potrebno postaviti nove bazne postaje i odrediti nove frekvencije. UMTS je srodan GSM/EDGE tehnologiji i izgrađen je na konceptu koji je započeo GSM. Zbog toga većina mobilnih uređaja također podržava i GSM, što omogućuje dvostruki način korištenja samih uređaja. Ovo dualno korištenje istog uređaja rezultira hibridnom mrežom - 3GSM, čime se naglašava povezanost UMTS-a s GSM tehnologijom. Od 2006. godine u mnogim državama se odvija proces nadogradnje UMTS mreža HSDPA tehnologijom (poznatom još kao 3.5G). Velike brzine prijenosa koje pruža UMTS se uglavnom koriste za pristup Internetu. Iskustva u Japanu pokazuju da korisnici ne obavljaju mnogo video poziva te da ljudi više koriste tehnologiju za pristup Internetu izravno putem mobitela ili preko mobitela povezanog na računalo putem WiFi, Bluetooth, Infrared ili USB tehnologija. UMTS koristi dva različita sučelja za bežičnu komunikaciju:

- MAP – jezgru GSM-a i
- skupinu pretvarača govora (GSM obitelji) u digitalni signal i obratno uz komprimiranje signala.

UTRAN se sastoji od višestrukih temeljnih postaja koje koriste različite standarde sučelja i frekvencijske pojaseve. U Europi i Sjevernoj Americi se za UMTS koristi frekvencija od 2100 MHz. Frekvencija 1900 MHz se koristi za 2G usluge, a 2100 MHz se koristi za satelitsku komunikaciju. Sljedeća slika daje usporedbu brzina prijenosa različitih standarda i njihov odnos prema UMTS tehnologiji. Može se uočiti da je UMTS standard za vrlo brzi prijenos podataka u odnosu na svoje prethodnike.



Slika 11. Usporedba brzina postojećih standarda. Izvor: Web ProForums

Telefoni koji podržavaju UMTS dizajnirani su tako da se jednostavno prebacuju s mobilne mreže jedne države na mobilnu mrežu druge države (*roaming* usluga). Uz to, gotovo svaki mobilni uređaj nudi dvostruki način rada (UMTS i GSM) tako da, ako se korisnik sa mobitelom nađe u području koje ne pokriva UMTS mreža, se može transparentno prebaciti na drugu GSM mrežu. *Roaming* usluga je obično skuplja za korisnike ako koriste UMTS. UMTS telefoni mogu koristiti USIM kartice, kao i obične GSM SIM kartice. USIM i SIM su globalni standardi i omogućuju mreži da identificira i autenticira karticu u telefonu. Zanimljivo je da je Japan prva država koja je primijenila 3G tehnologije te da nije prije koristila GSM tehnologije. Prije pojave 3G u Japanu se koristila PDC (eng. Personal Digital Cellular) mreža. Prema tome, mobilni uređaji u Japanu nemaju potrebu za ugradnjom modula koji bi im omogućio rad s GSM tehnologijom. Zbog toga su njihovi uređaji već u početku bili manje veličine od ostalih u svijetu.

2.5.1. Sigurnost UMTS usluge

Nove usluge koje je uvela UMTS tehnologija zahtijevaju nove sigurnosne značajke kako bi se te usluge zaštitile. Uz to, uočeno je da postoje nedostaci kod sigurnosti GSM-koji se trebaju ispraviti (prvenstveno kod UMTS sustava).

UMTS pruža uslugu međusobne autentikacije između dva UMTS pretplatnika koju omogućuje USIM. Uz to, mreža provjerava identitet pretplatnika i obratno, pretplatnik provjerava da je povezan na mrežu na koju treba biti. Osim autentikacije obavlja se i provjera besprijekornosti podataka te autentikacija izvornosti. To se obavlja sljedećim funkcionalnostima:

- **Dogovor algoritma provjere integriteta** – mobilna stanica i poslužujuća mreža mogu sigurno pregovarati o algoritmu koji koriste,
- **Dogovor integriteta ključa** – mobitel i mreža se dogovaraju o integritetu ključa koji bi mogli koristiti.

UMTS pruža i povjerljivost korisničkog prometa:

- **algoritam kriptiranja** – mobitel i postaja pregovaraju o upotrebi algoritma kriptiranja,
- **ključ kriptiranja** – dogovara se i ključ kriptiranja,

- **povjerljivost podataka i korisnika** – napadač ne može prisluškivati preko radio sučelja korisničke podatke, kao ni podatke koji se prenose.

UMTS primjenjuje MAPSEC. Osnovna ideja MAPSEC-a je da se MAP (eng. *Mobile Application Part*) poruka kriptira te da se kriptirana poruka pridružuje drugoj MAP poruci. MAP je protokol koji pruža funkcionalnost aplikacijskog sloja u GPRS i UMTS mrežama. Istovremeno se kriptografski zbroj (*eng. checksum*), npr. autentikacijski kod poruke koji pokriva izvornu poruku, uključuje u novu MAP poruku. Za čitanje kriptirane poruke i upotrebu autentikacijskih kodova poruke potrebno je imati ključeve.

3. Sigurnosni problemi u mobilnim mrežama

U mobilnim mrežama sigurnosni su problemi vezani uz zaštitu razgovora, pozivnih podataka i sprečavanje prijevara putem mobilnih telefona. U starijim analognim sustavima bilo je jednostavno presresti i prisluškivati telefonske razgovore samo uz pomoć policijskog skenera. Slučaj koji je bio poznat u medijima uključivao je snimku razgovora Britanske kraljevske obitelji.

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 zlćudnih programa i drugo). Jedan takav uređaj je „smart phone“ ili u doslovnom prijevodu pametni telefon. 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 telefoni. Ironija je da povećanjem funkcionalnosti koje mobitel nudi, kod njega se javljaju isti sigurnosni problemi kao i kod prijenosnih ili osobnih računala.

Slika 12. Velik broj sigurnosnih problema kod mobilnih uređaja. Izvor: Binary Head

Najčešći operacijski sustavi koji se javljaju na mobilnim telefonima i PDA (eng. presonal digital assistants) uređajima su Microsoft Windows Mobile (na njemu se temelje Windows Mobile 2003 i Windows Mobile 6) i Symbian OS (npr. uređaj Nokia S60) te sustavi koje održava i proizvodi tvrtka Symbian (neki uređaji tvrtki Samsung, Panasonic, Siemens, Lenovo). Tvrtka Google je također razvila operacijski sustav za mobilne telefone naziva Android, koji omogućuje programerima da pišu programe za njega u programskom jeziku Java i oblikuju sustav prema svojim potrebama. Konkurentski operacijski sustav Androidu je iOS tvrtke Apple, kojeg koriste mobilni uređaji iPhone. Sustav iOS je dizajniran prema operacijskom sustavu Mac OS X i temelji se na operacijskom sustavu Unix.

Nabrojani operacijski sustavi korisniku koji zna iskoristiti njihove prednosti olakšava rad i nudi mnoge dodatne funkcionalnosti, no postoji i druga strana, a to je da iste prednosti koje omogućuju prilagodljivost operacijskih sustava napadači mogu iskoristiti za zlouporabu i ugroziti sigurnost podataka na mobilnim telefonima korisnika. Na primjer, napadači mogu iskoristiti činjenicu da operacijski sustavi Windows Mobile (inačice 2003 i 6) imaju istu jezgru za pisanje učinkovitih zlođudnih programa koji će nanijeti štetu svim mobilnim uređajima koji koriste sustave Windows Mobile. Korisnici mobilnih telefona čuvaju mnogo privatnih podataka u svojim uređajima. Ukoliko napadač neovlašteno pristupi uređaju i ukrade podatke, može ih iskoristiti za lažno predstavljanje, a ako se među ukradenim podacima nađu i oni o kreditnim karticama, napadač može nanijeti i financijsku štetu korisniku. Razvoj programa za operacijske sustave na mobilnim uređajima vrlo je slično razvoju programskih paketa za operacijske sustave namijenjene osobnim računalima, što napadačima olakšava prilagodbu pisanja zlođudnih programa za mobilne uređaje.

3.1. Sigurnosne prijetnje kod mobilnih uređaja

Najopasnije su sigurnosne prijetnje za mobilne uređaje u sljedećih sedam područja:

- tekstualne poruke,
- kontakti i adresar,
- video,
- prijepisi telefonskih razgovora,
- povijest poziva,
- dokumentacija te
- upotreba međuspremnika.

3.1.1. Tekstualne poruke

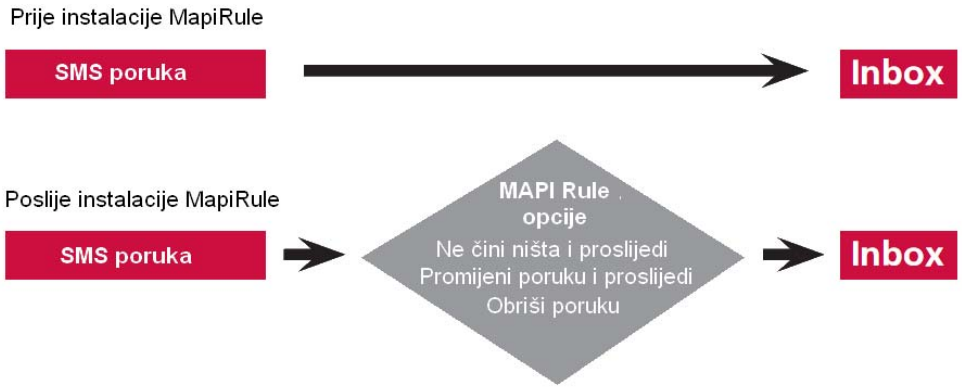
Gotovo svi mobilni uređaji korisniku pružaju mogućnost slanja i blokiranja poruka. Napadači mogu korisniku poslati posebno oblikovane poruke sa zlođudnim programskim kodom koji mogu iskoristiti za krađu osobnih podataka i ostalih podataka koji se nalaze na mobilnom telefonu. Osim opisanih poruka, napadač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

Zlođudni programi koje podmetnu napadači mogu koristiti funkcije za upravljanje SMS porukama za naplaćivanje usluga mobilnih telefona preko SMS poruka. Na primjer, u mobilnim telefonima 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. Napadač može podmetnuti MAPI Rule program i ometati rad s tekstualnim poruka. 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. Sljedeća slika daje primjer toka poruka sa postavljenim MAPI Rule klijentom i bez njega.



Slika 13. Tok poruka sa i bez MAPI Rule klijenta.

Iako 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).

3.1.2. 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 kontakte 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.

3.1.3. Video

Većina mobilnih telefona 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 telefonom i sadržajem koji je pohranjen u direktoriju kamere. Na mobilnim telefonima 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.

3.1.4. Prijepisi telefonskih razgovora

Mnogi mobilni telefoni 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 telefonom 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 zloćudni program može zlouporabiti SMS poruke za pokretanje i zaustavljanje snimanja.

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.

3.1.6. Dokumentacija

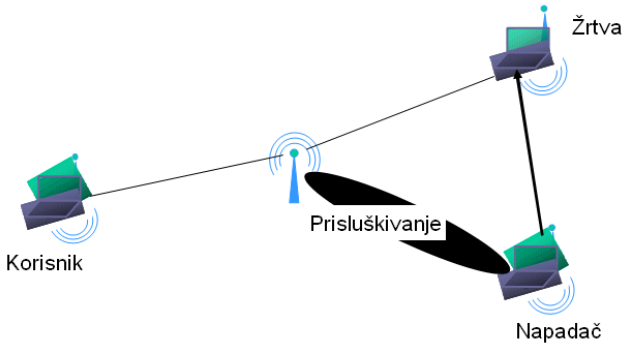
Mnogi korisnici mobilnih telefona čitaju i spremaju dokumente tipa Word, Excel ili PDF na svoje mobitele. Napadač može podmetnuti zloćudni program kojim će ukrasti takve datoteke upotrebom metode opisane u poglavlju 3.1.1. Datoteke sa ekstenzijama *.doc, *.xls i *.pdf su popularne mete napadača. Preporuča se da korisnici mobilnih telefona ne spremaju važne i povjerljive dokumente na svoje uređaje.

3.1.7. Upotreba međuspremnika

Sigurnosni propusti vezani uz međuspremnike 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 telefona vrlo su slični operacijskim sustavima osobnih računala i upotreba međuspremnika je uobičajena.

3.2. Sigurnosne prijetnje u GSM/GPRS/UMTS mrežama

Sigurnost GSM/GPRS mreža je umjerene razine i njezine značajke su opisane u poglavlju 2.2.1. i 2.3.1. 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). Sljedeći dijagram prikazuje napad u kojemu napadač prisluškuje komunikaciju i ometa ju.



Slika 14. Napad s čovjekom u sredini.

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:

- **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.
- **aktivna krađa identiteta** – napadač ima prilagođenu temeljnu stanicu te potiče korisnika da se priključi na njegovu postaju. Zatim ga traži da mu pošalje IMSI.

Napadač se može maskirati i pretvarati da je prava mobilna mreža. To može učiniti na sljedeće načine:

- **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.
- **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:

- Upotrebom ugroženog autentikacijskog vektora – napadač s prilagođenim mobilnim uređajem i ugroženim autentikacijskim vektorom oponaša korisnika prema mreži i ostalim korisnicima.
- Prisluškivanjem postupka autentikacije – napadač s prilagođenim mobilnim uređajem koristi podatke koje je dobio prisluškivanjem.
- Otimanjem odlaznih poziva u mrežama s isključenom enkripcijom.
- Otimanjem 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. 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 GSM mreže:

- BTS
- BSC
- MSC
- HLR
- VLR

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. Zaštita od napada zlućudnim programima

Kao što je opisano u poglavlju 3.1., najveća prijetnja korisnicima mobilnih uređaja su zlućudni programi. Kao mjera zaštite u operacijskom sustavu Windows Mobile primjenjuju se certifikati za programe koji koriste ugrađena programska sučelja (eng. Application programming interface – API). Spomenuta su sučelja najčešća polazna točka napada. Međutim, sustav certifikata pruža djelotvornu zaštitu sve dok korisnik nema želju instalirati program koji nije izvorno proizvela tvrtka Microsoft. Jedan način zaobilaženja sustava certifikata je upotreba alata kao što je program tvrtke Novosec – „SDA_ApplicationUnlock“, koja onemogućuje provjeru certifikata na mobilnom telefonu. Ukoliko korisnik primjeni spomenuti program postoji opasnost da je mobitel postao ranjiv na napade zlućudnim programom. Ukoliko korisnici ne žele riskirati izloženost ovakvim napadima preporuča im se da ne mijenjaju ugrađene mjere zaštite.

Najbolji način zaštite mobilnih uređaja je primjena istih mjera zaštite kao na osobnom računalu. Antivirusni programi su vrlo učinkoviti u prepoznavanju zlućudnih programa, kao i u njihovom uklanjanju i korisnicima se preporuča njihova upotreba na mobilnim uređajima. Nakon što je mobilni uređaj zaražen zlućudnim programom postoji vjerojatnost da ga nije lako ukloniti. Zbog toga je dobro koristiti antivirusne programe posebno namijenjene mobilnim uređajima. Prilikom upotrebe Interneta korisnici trebaju paziti na posjećivanje sumnjivih web stranica i otvaranje sumnjivih poruka elektroničke pošte. Također, preporuča se preuzimanje isključivo programa koji imaju digitalni potpis i certifikat.

Upotrebom programskih paketa za upravljanje procesima iskusniji korisnici mogu pretraživati uređaj za sumnjivim procesima i spriječiti njihovo izvođenje. Mobilni uređaji ne mogu istovremeno izvoditi mnogo procesa zbog sklopovskog ograničenja. Korisnicima se preporuča čuvanje zapisa o svim procesima koji su uobičajeno pokrenuti na mobilnom uređaju. Ako se kasnijim pregledom pokrenutih procesa otkrije neki koji nije bio prije pokrenut postoji mogućnost da je to zlućudni program.

Slika 15. Antivirusni programi na mobilnim uređajima
Izvor: oohooo.com

S svrhu zaštite također se korisnicima preporuča isključivanje Wi-Fi i Bluetooth funkcionalnosti kada nisu u upotrebi. Obje funkcionalnosti napadač može lako iskoristiti za slanje zlućudnih programa korisniku mobilnog telefona. Osim toga, napadač može presresti prijenos podataka kada korisnik za to koristi Wi-Fi ili Bluetooth. Preporuča se da se spomenute funkcionalnosti koriste u sigurnom okruženju.

Svakom korisniku mobilnog telefona najvažniji podaci u mobilnom uređaju su kontakti u adresaru. Ako napadač uspješnim napadom ukrade kontakte ili ih obriše, posljedice mogu biti velike. Uvijek je dobro napraviti sigurnosnu presliku podataka koji se čuvaju u mobilnom uređaju. U tom slučaju, čak i ako je mobilni uređaj ukraden ili se na njemu nalazi zlućudni program, korisnik je sačuvao svoje kontakte.

Većina tvrtki koje proizvode antivirusne programe proizvode i inačice namijenjene mobilnim uređajima. Mnogi pružatelji mobilnih usluga ugrađuju u telefone koje prodaju i antivirusne programe. Ukoliko korisnik nema na svojem mobilnom uređaju postavljen antivirusni program, preporuča se da ga postavi ili da povremeno pregleda svoj uređaj antivirusnim programom spajanjem na osobno računalo. Neki od besplatnih antivirusnih programa za mobitele su:

- NetQin Mobile Antivirus – program kojeg preporuča tvrtka Nokia i podržava ga velika većina dostupnih mobilnih uređaja,

- BitDefender Mobile Antivirus – funkrionira na operacijskom sustavu Windows Mobile Pocket PC, inačica 2002 i novije, Windows Mobile Smartphone, inačice 2002 i novije, Symbian 60 i 80,
- F-Secure - program se izvodi u pozadini i automatski pregledava sve datoteke na uređaju i memorijskoj kartici, namijenjen je uređajima tvrtke Nokia,
- Flexilis Mobile Security,
- Airscanner AntiVirus for Windows Mobile,
- Kaspersky Mobile Security,
- McAfee VirusScan Mobile i drugi.

Korisnicima se ne preporuča spremanje povjerljivih datoteka i/ili važnog multimedijalnog sadržaja na mobilne uređaje. Mobilni telefoni i PDA uređaji nisu dovoljno sigurni za pohranu spomenutog sadržaja.

Mobilni uređaji koji koriste operacijske sustave i pružaju usluge kao i osobno računalo vrlo su popularni. No postoji manjak sigurnosne osviještenosti kod korisnika. Iako većina zloćudnih programa koji se javljaju na mobilnim uređajima ne predstavlja velik rizik korisnicima, to se može promijeniti u (vrlo skoroj) budućnosti. Zbog toga je uvijek dobro biti na oprezu kada je riječ o napadima zloćudnim programima.

5. Zaključak

Jedan od ključnih faktora za uspjeh mobilne tehnologije je mogućnost pružanja poboljšane funkcionalnosti koja se može usporediti s fiksnim mrežama. Uz to, razvijene su napredne i dalekosežne mreže koje omogućuju korisnicima laku dostupnost podataka, brze i efikasne komunikacije te jednostavan pristup Internetu. Standardi koji korisnicima omogućuju spomenute usluge su GSM, GPRS, UMTS i u novije vrijeme WiMAX. Naravno, još uvijek postoji mjesta za razvoj i kako raste potražnja za količinom informacija i njihovom besprijekornom kvalitetom, tako će napredovati i mobilna tehnologija. 3G tehnologije su prisutne već nekoliko godina i uskoro će ih zamijeniti 4G tehnologije.

Usluge 3G mreža nude poboljšanu funkcionalnost mobilnih uređaja i neometan tok podataka. Takve su usluge svakodnevica i moguće je reći sa sigurnošću da će pružatelji usluga nadograditi postojeće strukture tako da podržavaju nove tehnologije. U tom postupku potrebno je paziti na pojavu sigurnosnih nedostataka koji su vezani upravo uz nadogradnju usluga. Postojeća zaštita je dovoljno dobra za stare tehnologije, pa je s nadogradnjom sustava potrebno nadograditi i obnoviti zaštitu mobilnih sustava. Jednake sigurnosne prijetnje koje postoje u fiksnim mrežama, postoje i u bežičnim. Pružatelji usluga moraju prilagoditi sigurnosne mjere razvoju tehnologije te spriječiti napadače od ugrožavanja dostupnosti mreže, besprijekornosti podataka i povjerljivosti informacija. Standardi za 2G i 3G tehnologije sadrže mehanizme za autentikaciju i enkripciju, međutim nije dovoljno oslanjati se isključivo na te sigurnosne standarde.

Iako sigurnost 3G mreža označava velik korak naprijed u odnosu na prošle generacije, još uvijek postoje sigurnosni propusti koje treba riješiti u budućnosti. Mobilni uređaji i mreže su se ponudom usluga približili funkcionalnostima osobnih računala. Korisnici svih mobilnih uređaja, a pogotovo treće i četvrte generacije, trebaju biti svjesni sigurnosnih prijetnji koje se javljaju upotrebom mobilnih tehnologija i primijeniti preporučene mjere zaštite. Iako prijetnja možda nije jednako opasna kao ona kod mreža računala i osobnih računala, uvijek je dobro biti na oprezu.

6. Reference

[1] Cellular network, http://en.wikipedia.org/wiki/Cellular_network, svibanj 2010.

[2] Cell phone history, http://cellphones.org/cell-phone-history.html, 2008.

[3] History of mobile phones, http://en.wikipedia.org/wiki/History_of_mobile_phones, lipanj 2010.

[4] GSM, http://en.wikipedia.org/wiki/GSM, lipanj 2010.

[5] How does SMS work, http://www.logixmobile.com/faq/show.asp?catid=1&faqid=3, lipanj 2010.

[6] Dung Chang, Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services, SANS Institute, siječanj 2002.

[7] A. Bais, W.T. Penzhorn, P. Palensky, Evaluation of UMTS security architecture and services, Proceedings of the Fourth IEEE International Conference on Industrial Informatics, 2006.

[8] C. Peng, GSM and GPRS Security, HUT TML, 2000.

[9] A. Bavosa, GPRS Security Threats and Solution Recommendations, juniper networks, 2004.

[10] Universal Mobile Telecommunications System, http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System, lipanj 2010.

[11] Rainbows tablice, http://www.cert.hr/documents.php?id=340, kolovoz 2008.

[12] Z. Cheng, Mobile Malware: Threats and Prevention, McAfee, 2007.

[13] 15 Killer Antivirus Tools for Mobiles and Smartphones, http://www.aboutonlinetips.com/free-antivirus-for-mobile-or-smartphones/, lipanj 2009.