HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni nedostaci u GSM mrežama

CCERT-PUBDOC-2005-07-128

CARNet CERT u suradnji s LS&S

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

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

CARNet 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

Danas je uporaba mobilnih uređaji vrlo raširena, svakodnevno ih koriste stotine milijuna ljudi. Štoviše, uporaba mobilnih uređaja ima i dalje trend rasta, tako da bi uskoro broj mobilnih uređaja trebao i prestići broj fiksnih telefonskih linija. Za razliku od fiksne telefonije gdje postoji određena razina fizičke sigurnosti (potreban je fizički pristup telefonskoj žici) u mobilnoj telefoniji svatko s radio prijemnikom može osluškivati eter. Zbog toga je bilo potrebno u GSM sustavu osigurati zavidnu razinu sigurnosti mobilnih uređaja, odnosno prijenosa govora i podataka, pogotovo nakon propusta koji su bili uočeni kod starijih mobilnih tehnologija.
Iako GSM tehnologija osigurava zadovoljavajuću razinu sigurnosti, ona ipak u sebi ima i određene sigurnosne nedostatke koji su mogli biti iskorišteni za kompromitiranje korisnika. Ti nedostaci su najčešće bili posljedica štednje na sigurnosnim implementacijama i neznanju odgovornih ljudi. Najnovije tehnologije, kao što su GPRS i UMTS ispravljaju i te nedostatke.
Ovaj dokument opisuje sigurnost GSM tehnologije, uključujući i njene nedostatke te metode ispravljanja tih nedostataka.

2. GSM mreža

Za ostvarivanje pokretljivosti u javnoj mreži najvažniji je današnji opći pokretni komunikacijski sustav GSM (*engl. Global System for Mobile Comunications*), njegovo proširenje općim paketnim radijskim uslugama GPRS (*engl. General Packet Radio Services*), te općim pokretnim telekomunikacijskim sustavom UMTS (*engl. Universal Mobile Telecomunication System*) koji je ujedno i predstavnik treće generacije pokretnih mreža.
GSM mreža pokriva područje radijskim signalom na principu ćelija (*engl. cellular).* Ćelija je područje koje pokriva jedna bazna stanica. Ovakva struktura je pogodna jer omogućuje dobru iskoristivost raspoloživih frekvencija, pa se u susjednim ćelijama koriste različite frekvencije, a u udaljenim ćelijama moguće je koristiti iste frekvencije. GSM je digitalni sustav u kojem se višestruki pristup ostvaruje u vremenskoj podjeli tako da je na svakoj od 124 frekvencija raspoloživo 8 kanala, što daje ukupno 992 kanala.
GSM mreža se može podijeliti u 4 osnovna dijela:

- korisnički terminal koji se uobičajeno naziva mobilni uređaj (*engl. MS – Mobile Station*),
- sustav baznih stanica (*engl. BSS – base station system*),
- mrežni i komutacijski sustav (*engl. NSS – network and switching system*) i
- operacijski sustav i sustav podrške *(engl. OSS – operation and support system*).

2.1. Mobilni uređaj

Mobilni uređaj, tj. korisnički terminal, se sastoji od komunikacijske pokretne opreme i inteligentne kartice (*engl. smartcard*) nazvane SIM (*engl. Subscriber Identity Module*). Svaki mobilni uređaj posjeduje jedinstveni identifikacijski broj poznat pod nazivom IMEI (*engl. International Mobile Equipment Identity*) koji se sastoji od 15 znamenki i služi za identifikaciju mobilnog uređaja unutar mobilne mreže. Osim toga, svaka SIM kartica posjeduje identifikacijski broj od 15 znamenki koja identificira pojedinog pretplatnika unutar pojedine mobilne mreže, IMSI (*engl. international mobile subscriber identity*).

2.2. Sustav baznih stanica

Sve funkcije za radio prijenos obavljaju se unutar BSS-a koji se sastoji od kontrolnih baznih stanica (*engl. BSC – base station controllers*) i primopredajnih baznih stanica (*engl. BTS – base transceiver stations, BTS*). BSC je preklopnik visokog kapaciteta koji pruža sve kontrolne funkcije i fizički povezuje MSC (*engl. mobile services switching center*) i BTS. Jedan MSC poslužuje više BSC-a. BTS upravlja radio sučeljem prema mobilnom uređaju. Sadrži radio opremu (primopredajnici i antene) potrebnu za posluživanje svih ćelija u mobilnoj mreži. BSC kontrolira grupu BTS-a.

2.3. Mrežni i komutacijski sustav

Komutacijski sustav služi za procesiranje poziva i pretplatničkih usluga te se sastoji od (Slika 1: GSM mreža):

- Domaći lokacijski registar (*engl. HLR – home location register*) je baza podataka koja sadrži podatke o pretplatnicima, pretplatničkim uslugama, informacije o lokaciji pretplatnika i aktivacijski statusa mobilnog uređaja. U jednoj GSM mreži postoji samo jedan HLR.
- Komutacijski centar mobilnih usluga (*engl. MSC – mobile services switching center*) je komutacijski sustav koji upravlja pozivima prema/od drugih telefona ili podatkovnih sustava, naplaćivanjem, povezivanjem različitih mobilnih mreža i signalizacijom .
- Gostujući lokacijski registar (*engl. VLR – visitor location register*) je baza podataka koja sadrži privremene informacije o gostujućim pretplatnicima potrebne MSC-u. Kada se pretplatnik nađe u lokacijskom području određenog MSC-a, VLR povezan s dotičnim MSC-om zatražit će informacije o pretplatniku od njegovog HLR-a i na taj način omogućiti pozive bez da se svaki put mora kontaktirati HLR.
- Centar za autentikaciju (*engl. AUC – authentication center*) sadrži autentikacijske i enkripcijske parametre kojim se provjerava identitet pretplatnika i osigurava sigurnu komunikaciju.
- Registar identifikacijske opreme (*engl. EIR – equipment identity register*) je baza podataka koji sadrži podatke o identitetu mobilnih uređaja na osnovu njihova jedinstvenog broja IMEI.

2.4. Operacijski sustav i sustav podrške

Operacijski sustav i sustav podrške spojen je na svu opremu u komutacijskom sustavu i na BSC te omogućuje GSM operateru usluge centralizacijskog, regionalnog i lokalnog nadzora nad GSM sustavom.

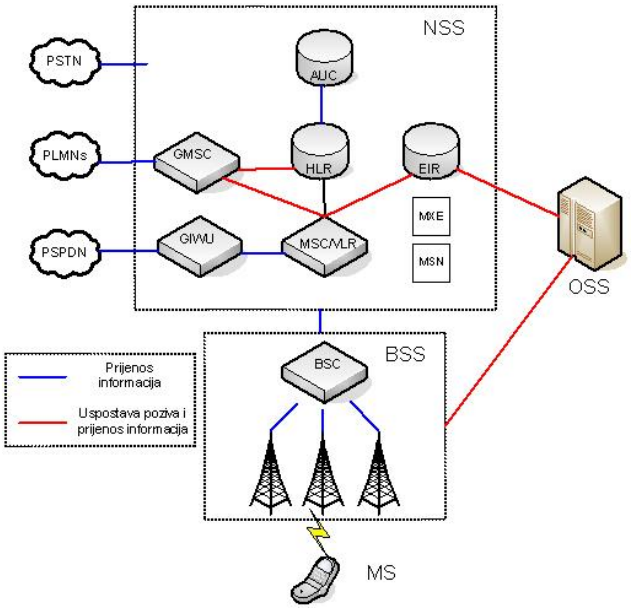
2.5. Dodatni funkcionalni elementi

Ostali funkcionalni elementi prikazani na *Slika 1:* GSM mreža su:

- Centar za poruke (*engl. MXE – message center*). U centru za poruke integrirane su usluge glasovnih poruka, faksa i podatkovnih poruka. Točnije, centar za poruke upravlja SMS porukama, govornom poštom, faks porukama i porukama elektroničke pošte.
- Čvor za mobilne usluge (*engl. MSN – mobile service node*) upravlja inteligentnim mobilnim uslugama.
- Usmjernik mobilnih usluga komutacijskog centra (*engl. GMSC – gateway mobile services switching center*) povezuje dvije različite mobilne mreže. Najčešće je implementiran unutar komutacijskog centra, MSC-a.
- GSM jedinica za međusobno djelovanje (*engl. GIWU – GSM interworking unit*) se sastoji od hardvera i softvera koji pružaju sučelje za razne mrežne i podatkovne komunikacije. Preko GIWU-a korisnik može mijenjati između govora i prijenosa podataka za vrijeme jednog poziva. Hardver je implementiran unutar MSC/VLR-a.

2.6. Uspostava poziva u GSM mreži

Na slici (**Slika 1**) je prikazana osnovna struktura GSM mreže.



Slika 1: *GSM mreža*

Odlazni poziv se u koracima ostvaruje na sljedeći način:

- mobilni uređaj traži kanal,
- provjerava se autentičnosti (u AUC-u) i identitet mobilnog uređaja (u EIR-u),
- poziv se prospaja: BTS – BSC – MSC – GMSC – druga mreža,
- osigurava se kriptografska zaštita tijekom prijenosa.

Kod dolaznog poziva procesi koji se odvijaju su sljedeći:

- GMSC od HLR-a traži lokacijsku informaciju (MSC/BSC) za mobilni uređaj,
- HLR i VLR izmjenjuju podatke o pozvanom mobilnom uređaju,
- MSC prenosi svim BSC (BTS) zahtjev za pozivanjem dotičnog mobilnog uređaja,
- provjerava se autentičnosti (u AUC-u) i identitet mobilnog uređaja (u EIR-u),
- vrši se prospajanje i osigurava kriptografska zaštita tijekom prijenosa.

3. Sigurnosne značajke GSM mreža

GSM specifikacija identificira 3 sigurnosna područja značajna za GSM komunikaciju:

- autentikacija korisnika – sposobnost mobilnog uređaja da dokaže da ima dozvolu korištenja određenog pretplatničkog računa kod GSM operatora,
- povjerljivost podataka i signalizacijskih paketa – svi podaci (govor i tekstualne poruke) i signalizacijski paketi moraju biti kriptirani,
- anonimnost korisnika – u trenutku autentikacije pretplatnika, jedinstveni IMSI mora biti kriptiran.

Detaljniji opis sigurnosnih nedostataka u navedenim područjima dan je u nastavku dokumenta.

3.1. Autentikacija

Autentikacijom se sprečava prijava neovlaštenih korisnika, te neovlašteno korištenje korisničkih računa ovlaštenih korisnika/pretplatnika. U suprotnom, neovlašteni korisnik bi mogao "oteti" tuđi pretplatnički račun i koristiti ga, dok bi računi stizali na naplatu oštećenom pretplatniku. Da bi se riješio taj problem bilo je potrebno uvesti tip provjere kojom bi se testirao sam mobilni uređaj.

3.1.1. IMEI

IMEI je 15-znamenkasti jedinstveni broj koji se koristi za identificiranje mobilnog uređaja u mobilnoj mreži. Otisnut je na unutrašnjoj strani mobilnog uređaja (kod baterije), a moguće ga je i očitati pozivom na *#06#. Sastoji se od tri polja: identifikacija proizvođača, serijski broj uređaja i kontrolni broj. Format IMEI- a je 11111111-222222-3 i prikazan je u Tablica 1.

Tablica 1: *Format IMEI-a*

TAC								SNR						CD
D14	D13	D12	D11	D10	D09	D08	D07	D06	D05	D04	D03	D02	D01	

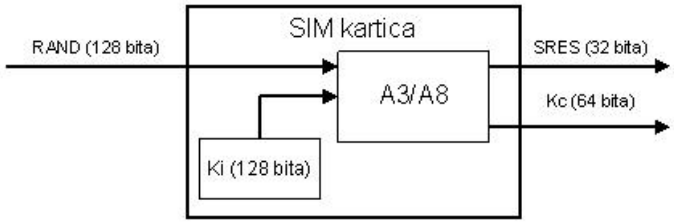
- TAC (*engl. type allocation code*) – je 8-znamenkasti broj koji određuje zemlju podrijetla mobilnog uređaja i proizvođača,
- SNR (*engl. serial number*) – je 6-znamenkasti jedinstveni broj koji se dodjeljuje određenom tipu mobilnog uređaja,
- CD (*engl. check digit*) – koristi se za provjeru vjerodostojnosti IMEI-a kod različitih tipova mobilnih uređaja.

U slučaju krađe mobilnog uređaja vlasnik uređaja koji zna IMEI broj svog uređaja može prijaviti krađu svom operateru koji će onemogućiti korištenje tog mobilnog uređaja u svojoj mreži. Operater će tu informaciju proslijediti ostalim operaterima koji bi trebali učiniti isto (onemogućiti korištenje mobilnog uređaja je moguće kod onih koji podržavaju tu mogućnost). Svi bi operateri trebali biti spojeni na bazu podataka CEIR (*engl. central EIR*) u kojoj se nalaze svi IMEI brojevi svih mobilnih uređaja na svijetu, što u praksi ipak nije slučaj.

3.1.2. SIM kartica

SIM kartica,koja se stavlja u mobilni uređaj osigurava funkcionalnost mobilnog uređaja. Sam za sebe, mobilni uređaj nije povezan niti s jednom mobilnom mrežom, pa SIM kartica služi kao veza između određene mobilne mreže i mobilnog uređaja (pretplatnika). SIM kartica sadrži sve podatke potrebne za uspostavljanje pristupa određenom pretplatničkom računu. Ustvari, sve što je potrebno su 2 informacije:

- IMSI – jedinstveni broj dodijeljen svakom korisniku mobilnog uređaja (svakom pretplatniku) na svijetu. Sadrži informacije o domaćoj mreži pretplatnika i zemlji u kojoj se nalazi ta mreža. Ova informacija se može dobiti samo lokalnim pristupom mobilnom uređaju, tj. SIM kartici, a najčešće je zaštićena samo PIN (*engl. Personal Identification Number*) brojem. IMSI sadrži do 15 znamenaka, prvih 5 ili 6 specificira mrežu i zemlju operatera.
- Ključ K_i – korijenski enkripcijski ključ. To je slučajno generiran 128 bitni broj dodijeljen svakom pretplatniku koji predstavlja početni ključ za generiranje svih ostalih ključeva i provjera tokom GSM komunikacije. Ključ K_i je visoko zaštićen i poznat je samo SIM kartici i mrežnom autentikacijskom centru, AUC (*engl. Authentication Centre*). Mobilni uređaj ne zna vrijednost ključa K_i, te SIM kartici samo daje informacije potrebne za autentikaciju i generiranje ključeva za kriptiranje. SIM kartica sadrži mikroprocesor, te se autentikacija i generiranje ključeva se odvijaju unutar nje, Slika 2.



Slika 2: *Koncept autentikacije u SIM kartici*

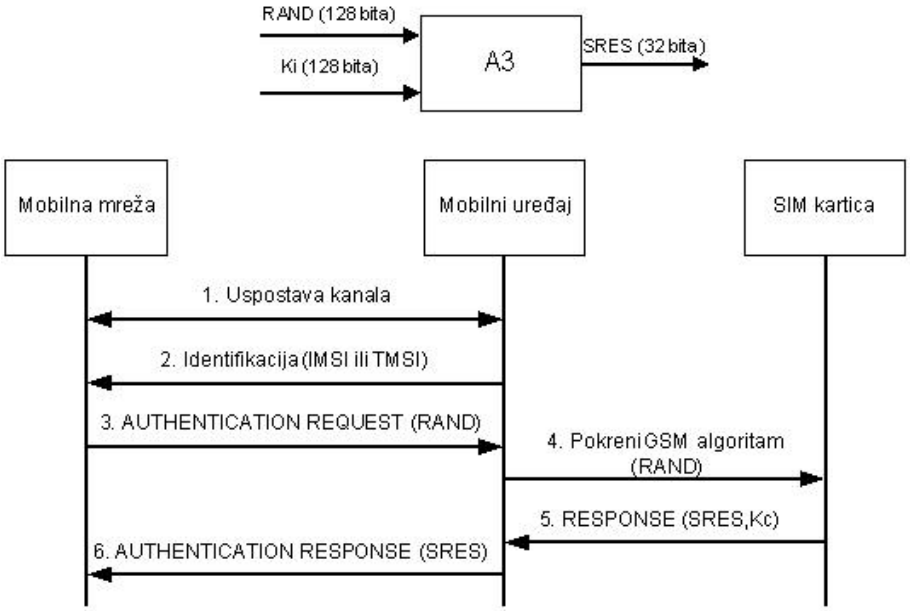
3.1.3. Dodatna lokalna zaštita SIM kartice

SIM kartica je opcionalno zaštićena PIN brojem i to na sličan način kako je bankovna kartica zaštićena bankovnim PIN-om. PIN se unosi preko tipkovnice na mobitelu, te se prosljeđuje SIM kartici na verifikaciju. Ako uneseni PIN ne odgovara PIN-u spremljenom na SIM kartici, SIM kartica upozorava korisnika (porukom na zaslonu mobitela) na neispravnost PIN-a, te odbija provesti autentikaciju sve dok se ne unese ispravan PIN. Da bi se ostvario viši stupanj sigurnosti SIM kartica zaključa mobilni uređaj nakon što se nekoliko puta unese neispravan PIN (najčešće 3 puta). Nakon toga da bi se mobilni uređaj mogao otključati potrebno je unesti PUK (*engl. PIN Unlock*) koji je dodijeljen od strane

operatora. Ako se i PUK nekoliko puta pogrešno unese (najčešće 10 puta) SIM kartica se trajno zaključava onemogućavajući pristup podacima i autentikaciju.

3.1.4. A3 algoritam i procedure autentikacije

Najjednostavniji način autentikacije bio bi slanje ključa K_i mobilnoj mreži kad ga mobilna mreža zatraži, ali to bi bilo jako nesigurno, jer bi ključ u tom slučaju bio ranjiviv na presretanje (i otkrivanje). Umjesto toga mobilna mreža generira 128 bitni slučajni broj, poznat kao RAND, kojeg iskoristi (u A3 algoritmu) za matematičko generiranje tokena poznatog kao SRES. Tada mobilne mreža šalje RAND mobilnom uređaju koji izvrši istu proceduru. SIM kartica generira 32 bitni SRES koji se šalje mobilnoj mreži na usporedbu. Ako SRES koji je generirao mobilni uređaj, odgovara prethodno izračunatom SRES-u koji je generirala mreža na temelju predstavljanja korisnika (korištenjem IMSI ili TMSI) tada i ključevi K_i moraju biti isti. Time je mobilni uređaj dokazao da zna koji je ključ K_i, te je time autenticiran. RAND svaki puta mora biti drukčiji, inače bi se napadač mogao predstaviti kao pretplatnik slanjem istog SRES-a.



Slika 3: *Procedura autentikacije*

Procedura prikazana na Slika 3 može se podijeliti u slijedeće korake (mobilna mreže prije komunikacije generira slučajan broj RAND i izračunava SRES za svakog pojedinog pretplatnika):

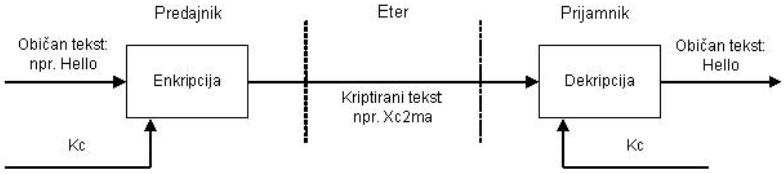
1. Početak komunikacije između mobilnog uređaja i mobilne mreže.
2. Mobilni uređaj se predstavlja (šalje svoj identitet). Sve poruke na početku komunikacije sadrže polje za identifikaciju. Kad god je moguće mobilni uređaj ne šalje svoj IMSI u običnom tekstualnom obliku (da bi se spriječilo zlonamjerne korisnike u "prisluškivanju" i dohvaćanju jedinstvenog IMSI broja) nego šalje privremeni IMSI (*engl. TMSI, Temporary Mobile Subscriber Identity*).
3. Nakon potvrde TMSI-a, mobilna mreža šalje poruku *AUTHENTICATION REQUEST* koja sadrži generirani slučajan broj (*engl. RAND*).
4. Mobilni uređaj prima RAND i prosljeđuje ga SIM kartici unutar naredbe *RUN GSM ALGORITHM*.
5. SIM kartica izvršava algoritam A3, te prosljeđuje mobilnom uređaju SRES.
6. Mobilni uređaj šalje SRES mobilnoj mreži u poruci *AUTHENTICATION RESPONSE*.
7. Mobilna mreža uspoređuje SRES kojeg je generirao mobilni uređaj s SRES-om kojeg je prethodno izračunala i ako su isti mobilna mreža daje dozvolu za komunikaciju. U drugom slučaju (ako nisu isti) mreža ponavlja postupak sa IMSI brojem ili vraća poruku *AUTHENTICATION REJECT*. To se smatra neuspjelom autentikacijom.

A3 algoritam ne predstavlja jedan jedini algoritam nego se tako naziva algoritam kojeg mobilni operator koristi u implementaciji za autentikaciju. Najčešće implementacije A3 algoritma su COMP128v1 i COMP128v2. Oba algoritma obavljaju funkciju i A3 i A8 algoritma (algoritam za

generiranje ključa, objašnjen kasnije u dokumentu) u istoj fazi. U trenutku kad SIM kartica računa SRES računa i novi K_c (*engl. ciphering key*) koji će se koristiti za kriptiranje komunikacije, tako da se procedura autentikacije ne koristi samo pri autentikaciji korisnika, nego i kad mobilna mreža zahtjeva promjenu ključeva.

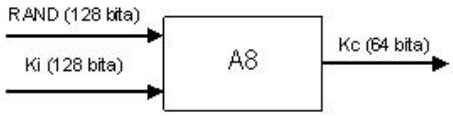
3.2. Kriptiranje (*engl. ciphering*)

Kriptiranje je jako važan dio GSM sustava, jer štiti podatke i signalizacijske poruke od presretanja. GSM sustav koristi simetričnu kriptografiju, podaci se kriptiraju algoritmima koji za kriptiranje koriste ključ K_c. Obzirom da se radi o simetričnoj kriptografiji, isti K_c koristi se i za dekriptiranje podataka, Slika 4. Ideja je ta, da je taj ključ poznat samo mobilnom uređaju i mobilnoj mreži, pa svakom tko presretne poruku kriptiranu na taj način poruka ništa neće značiti bez znanja tog ključa.



Slika 4: *Enkripcija i dekripcija*

Ključ K_c bi se također morao neprestano mijenjati, u slučaju da je otkriven. Metoda distribucije ključa K_c mobilnom uređaju povezana je s procedurom autentikacije. Svaki put kad se pokrene algoritam A3 (za generiranje SRES-a), pokreće se i A8 algoritam (u SIM kartici oba algoritma se izvršavaju u isto vrijeme). Algoritam A8 koristi slučajan broj RAND i ključ K_i kao ulaze za generiranje 64 bitnog ključa, ključa K_c, koji se pohranjuje u SIM karticu, Slika 5. Mobilna mreža također generira ključ K_c kojeg šalje baznoj stanici (*engl. base station*) koja sudjeluje u komunikaciji.



Slika 3.4

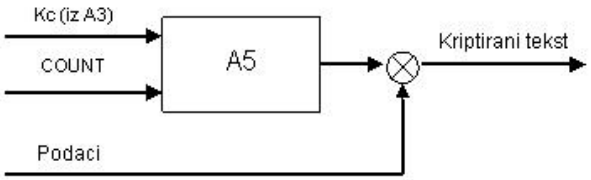
Slika 5: *Algoritam A8*

Iako dizajn GSM sustava dozvoljava uporabu bilo kojeg algoritma za A3 i A8, većina operatera se odlučuje za COMP128 (razvijan u potpunoj tajnosti). COMP128 je na kraju završio u javnosti (putem raznih dokumenata koji su procurili u javnost), te je otkriveno da sadrži ozbiljne sigurnosne propuste. Većina operatera se odmah prebacila na noviju inačicu algoritma, COMP128-2. Iako algoritam povećava sigurnost u odnosu na prijašnju inačicu i za njega su otkriveni neki sigurnosni propusti. Također, postoji i COMP128-3 inačica algoritma koja koristi svih 64 bita za generiranje ključa K_c, u odnosu na COMP128-2 koji je oslabljen za 10 bitova koji su postavljeni u 0.

3.2.1. Algoritmi za kriptiranje komunikacije

Mobilna mreža može koristiti do 7 različitih algoritama za kriptiranje (ili niti jedan), ali smije koristiti samo one algoritme koje pojedini mobilni uređaj podržava. Trenutno su definirana 3 algoritma: A5/1, A5/2 i A5/3. A5/1 i A5/2 su izvorni algoritmi definirani GSM standardom i bazirani su na jednostavnom LFSR-u (*engl. linear feedback shift registers*). A5/2 je namjerno oslabljena inačica algoritma koja se koristi u određenim regijama (manje razvijenim), dok se A5/1 koristi u SAD-u, Velikoj Britaniji i Australiji. A5/3 je dodan 2002 i bazira se na otvorenom Kasumi algoritmu definiranom od strane 3GPP-a.

U bilo kojem trenutku, mobilna mreža može započeti kriptiranje podataka (nakon autentikacije) koristeći generirani K_c. Mreža može izabrati bilo koji algoritam kojeg podržava i mobilni uređaj (algoritme kriptiranja koje podržava mobilni uređaj šalju se mobilnoj mreži porukom *classmark* koja specificira mogućnosti mobilnog uređaja). Algoritam radi na način da generira blok binarnih brojeva (kriptirani blok) koji se modulo 2 aritmetikom ("ekskluzivno ili", XOR) dodaje korisničkim podacima koji se prenose eterom, Slika 6. Podaci se dekriptiraju ponovo operacijom XOR nad kriptiranim blokom, koji bi trebao biti isti.

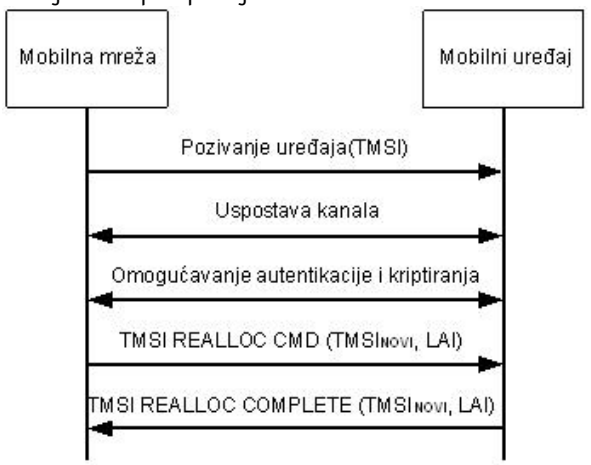


Slika 6: *Algoritam A5*

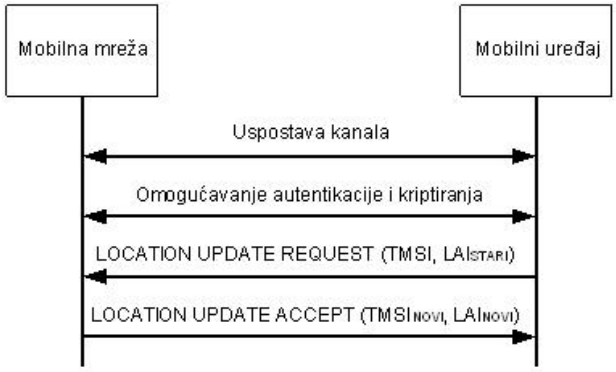
U algoritmu A5 koristi se varijabla COUNT, temeljena na TDMA broju okvira, koje se sekvencijalno dodaje svakom GSM okviru (GSM okvir se generira svakih 4.615 ms). Uvijek se korist isti korijenski K_c čija se vrijednost mijenja operacijom XOR između 32-34 bita K_c i jednog od brojeva između 0 i 7 (*timeslot number*).

3.3. Anonimnost

Jedan od važnijih ciljeva u GSM sigurnosti bilo je izbjegavanje slanja IMSI-a (*engl. International Mobile Subscriber Identity*) u običnom tekstualnom obliku preko etera i time onemogućiti zlonamjerne korisnike u prisluškivanju korisnika (u kojem se području korisnik nalazi i koje usluge koristi). To je izbjegnuto korištenjem 32 bitnog TMSI-a (*engl. Temporary Mobile Subscriber Identity*), koji je valjan u samo jednom lokacijskom području (*engl. LA – Location Area*). Pomoću tog 32 bitnog TMSI-a pretplatnik se predstavlja ili ga se poziva. TMSI se obnavlja najmanje za vrijeme svake promjena lokacijskog područja ili unutar unaprijed određenog vremenskog razdoblja. Također, mobilna mreža može promijeniti TMSI kad god poželi. Promijenjeni TMSI se uvijek šalje kriptiran tako da napadač ne može znati kada je nastupila promjena.



Slika 7: *Alokacija novog TMSI-a (u slučaju kad nema promjene lokacijskog područja)*



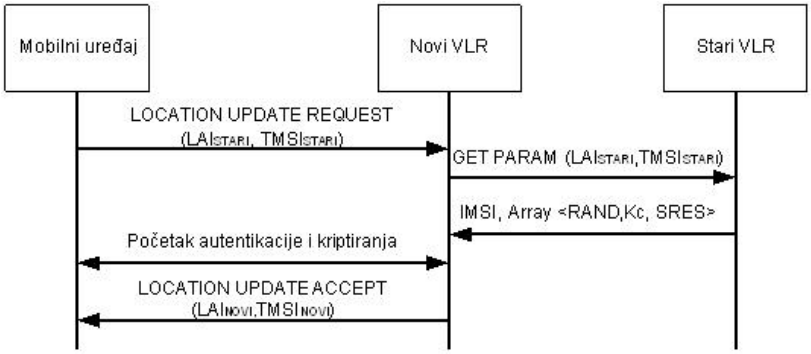
Slika 8: *Alokacija novog TMSI-a (u slučaju promjene lokacijskog područja)*

Mobilni uređaj mora pohraniti TMSI u "stalnu" memoriju (mora ostati sačuvan i nakon isključivanja mobilnog uređaja). Najčešće je pohranjen na SIM kartici. Inicijalno (odmah nakon proizvodnje) mobilnom uređaju nije dodijeljen TMSI, ima samo IMSI. U prvom postupku kriptiranja (pri prvom

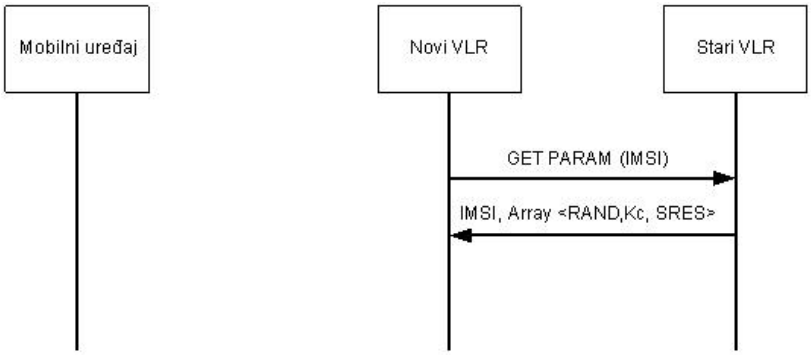
uključivanju) dodjeljuje se TMSI. VLR koji kontrolira LA u kojem je TMSI valjan održava vezu između TMSI-a i IMSI-a na taj način da u slučaju kad mobilni uređaj uđe područje drugog VLR-a stari mu VLR može dojaviti kome pripada TMSI (koji nije pravovaljan u području drugog VLR-a).

3.4. Distribucija informacija autentikacije i kritiranja preko mreže

Kao što je i prije rečeno korijenski ključ za generiranje svih ostalih ključeva za kriptiranje i autentikaciju je ključ K_i koji je spremljen u SIM kartici i u mrežnom AUC-u (smatra se da je AUC dio HLR-a). Uslijed toga, kad određeni VLR, koji nadgleda jednog ili više MSC-a (*engl. Mobile Switching Centre*) i upravlja mobilnom komunikacijom u svom području, treba autenticirati korisnika mora preuzeti informacije od HLR-a. Distribuiranje K_i-a VLR-u predstavlja sigurnosni rizik, osobito ako se pretplatnik nalazi u *roamingu* (strana mreža će saznati vrijednost K_i). Također, stalno preispitivanje HLR-a za signalizacijskim informacijama (Slika 9), svaki put kad je potrebna autentikacija, bi ga ubrzo preopteretilo, pa se umjesto signalizacijskih poruka koriste autentikacijski vektori koji sadrže SRES, K_c i RAND za svaki traženi IMSI, Slika 10. Uobičajeno, VLR-u se šalje više različitih setova vektora. Na taj način se smanjuje količina prenesenih informacija, te K_i ostaje tajan. Također, pri prijelazu iz jednog VLR-a u drugi šalju se autentikacijski vektori, a ne cijele poruke.



Slika 9: *Slanje informacija o autentikaciji između VLR-a*

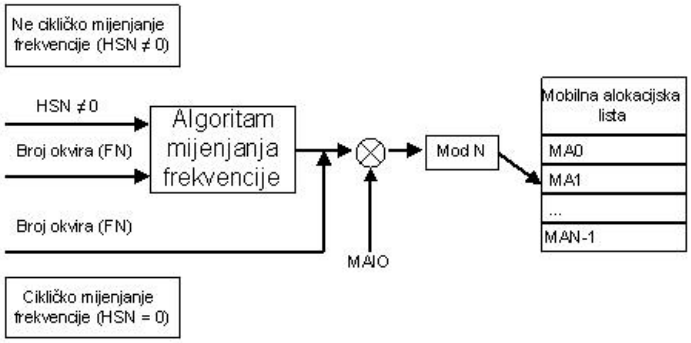


Slika 10: *Slanje autentikacijskih vektora između VLR-a*

3.5. Promjena frekvencije

U GSM sustavu se koristi promjena frekvencije, gdje se svakih 4.615ms ili 217 puta u sekundi mijenja frekvencija nosioca signala. Sekvencijalna promjena frekvencije određena je s dva parametra: HSN (*engl. Hopping Sequence Number*) i MAIO (*engl. Mobile Allocation Index Offset*). Postoje dva načina mijenjanja frekvencija: cikličko i necikličko, Slika 11. U oba načina, MAIO odlučuje u kojoj će se fazi mijenjanja frekvencije koristiti. Ako je HSN jednak 0, koristi se cikličko mijenjanje frekvencije gdje mobilni uređaj jednostavno promjeni bilo koji niz frekvencija. U necikličkom mijenjanju frekvencija koristi se brojčani okvir za povećanje složenosti mijenjanja frekvencija. U oba slučaja mijenjanje frekvencije utječe na povećanje sigurnosti. Ako bi napadač pokušao prisluškivati kanal u svrhu pribavljanja podataka morao bi osluškivati cijeli spektar frekvencija dok ne bi pronašao onu koja se trenutno koristi, što bi morao ponavljati svaki put kad dođe do promjene frekvencije. U obje

implementacije GSM-a; GSM900 i GSM1800 frekvencijski spektri su veličine nekoliko desetaka MHz (u slučaju da je poznata lokacijska frekvencija operatora te spektre je moguća smanjiti).



Slika 11: *Mijenjanje frekvencije*

Ako se informacije prenose u običnom tekstualnom obliku, kao što se i prenose prilikom uspostave konekcije, vrlo je lako napadaču nastaviti sekvencu (napadač bi znao koja je slijedeća frekvencija.). Ali inače, pri postavljanju kanala za podatke ili govor, alociran je dodatni kanal slanjem poruka po inicijalnom kanalu u trenutku kad je taj kanal kriptiran, čime je napadaču znatno smanjenja mogućnost lakog pogađanja sekvence. Glavni sigurnosni problem u mijenjanju frekvencija je taj da su parametri sekvenci u baznim stanicama uglavnom statični. Ako bi napadač imao pristup mobilnoj mreži vrlo bi lako mogao saznati tipične parametre sekvenci. Općenito, mijenjanje frekvencije ne pridonosi mnogo podizanju razine sigurnosti, iako istovremeno povećava složenost cijelog sustava.

4. Nedostatci u postojećim metodama

4.1. Mreža se ne autenticira mobilnom uređaju

Najveći nedostataka u implementaciji GSM sustava jest nekorištenje dvosmjerne autentikacije. Autentikacija je jednosmjerna, tj. mobilna mreža se ne mora autenticirati korisniku. To omogućava napadaču da postavi lažnu baznu stanicu sa identičnim kodom mobilne mreže (*engl. Mobile Network Code*) pretplatnikove mreže. Zbog toga što mreža odlučuje o trenutku autentikacije, lažna mreža jednostavno može poslati RAND i ignorirati odgovor mobilnog uređaja ili uopće ne autenticirati. Također ne mora ni pokrenuti kriptiranje. Napadač čak može postaviti parametre lažne mreže tako da privlači pretplatnike (velika vrijednost parametra *CELL_RESELECT_OFFSET*). Pretplatnik bi tada bez znanja mogao obavljati razgovore i slati poruke preko te lažne bazne stanice omogućavajući napadaču da ih presreće, tzv. *man-in-the-middle* napad.

4.2. Nedostatci u implementaciji algoritama A3 i A8

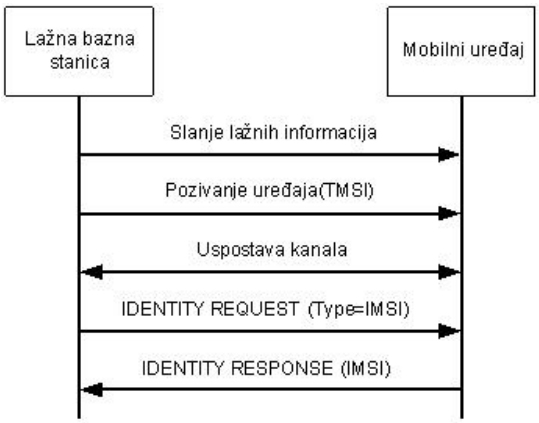
Najčešće implementacije A3 i A8 algoritma su implementirane unutar jednog algoritma, COMP128, koji generira 64 bitni ključ K_c i 32 bitni SRES iz 128 bitnog RAND i 128 bitnog ulaznog ključa K_i. Ovaj algoritma ima jednu veliku manu, ne generira potpuno slučajnu vrijednost RAND, što napadaču može bitno olakšati razbijanje ključa. Propust se javlja u drugom prolasku algoritma (2R napadi) gdje nastaje usko grlo. Pojedinačni okteti u izoliranim grupama od 4 okteta na izlazu drugog prolaska ovise samo o jedinstvenim grupama od 4 okteta sa ulaza (2 okteta ključa K_i i 2 otketa RAND-a) što omogućuje provedbu *collision* napada. Raniji 2R napadi su mogli srušiti SIM karticu za oko 2^{17} RAND-a. Tim napadom ključ K_i može biti razbijen u roku sat vremena (ovisno o brzini SIM kartice – čija frekvencija rada se može povisiti na čak 10 MHz). Iako se taj tip napada, među korisnicima, ne smatra ozbiljnim propustom, jer napadač mora biti fizički prisutan za vrijeme postupka, u slučaju krađe mobilnog uređaja može dovesti do kloniranja SIM kartice što može prouzročiti velike probleme (materijalne) za vlasnika kartice.

Osnovna implementacija A3 i A8 algoritma ima još jedan nedostatak, namjerno oslabljivanje algoritma. U trenutku generiranja 64 bitnog ključa K_c uvijek se zadnjih 10 bitova postavlja u 0. Taj postupak efektivno smanjuje snagu kriptiranja podataka na 54 bita (smanjenje za faktor 1024), bez

obzira koji se algoritam koristi. Ovo namjerno oslabljivanje algoritma prisutno je i u algoritmu COMP128-2.

4.3. Ranjivost u mehanizmu identifikacije korisnika

Mreža kontaktira korisnike preko njegova TMSI-a i održava bazu povezanosti TMSI-a sa IMSI-ma u VLR-u. Ako mreža u nekom trenutku izgubi podatke o korisnikovom TMSI-u, pa zbog toga ne može identificirati korisnika, mora od korisnika zatražiti njegov IMSI koristeći IDENTITY REQUEST i IDENTITY RESPONSE poruke. To znači da konekcija ne može biti kriptirana, jer VLR ne zna tko je korisnik, te se IMSI prenosi u običnom tekstualnom obliku.

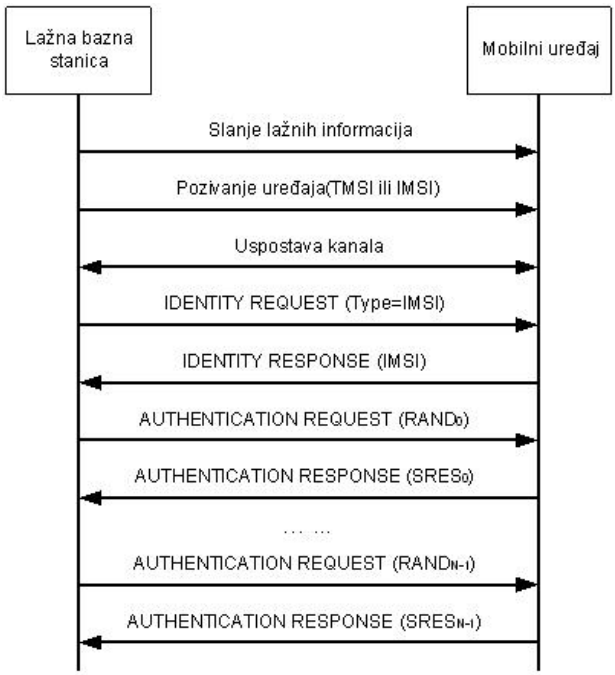


Slika 12: *Upotreba lažnih baznih stanica*

Kombinirajući prethodno spomenuti propust u autentikacijskoj proceduri, napadač može povezati TMSI sa njegovim IMSI-om. Lažnim predstavljanjem bazne stanice, ostvarivanjem konekcije i slanjem IDENTITY REQUEST poruke (*Identity Type* = IMSI) napadač može potaknuti mobilni uređaj na slanje IMSI-a, Slika 12.

4.4. Probijanje ključa K_i za vrijeme prenošenja eterom

Kombinacijom svih dosad nabrojanih propusta moguće je provesti neki od ozbiljnijih napada. Lažno predstavljajući legitimnu mobilnu mrežu napadač može iskoristiti autentikacijsku proceduru za iskoristiti ranjivosti COMP128 algoritma. Napadač će kontaktirati mobilni uređaj slanjem njegova TMSI-a uspostavljajući konekciju. Uspostavljanjem konekcije napadač na vrlo lagan način može doći do IMSI-a slanjem *IDENTITY REQUEST* naredbe (na koju je mobilni uređaj obvezan odgovoriti). U nastavku, napadač može nastaviti slati RAND putem *AUTHENTICATION REQUEST* poruka, na što će mu mobilni uređaj odgovorit sa SRES-om, Slika 13. Napadač taj napad može ponoviti nekoliko puta, sve dok ne sakupi dovoljno informacija da iz njih može izvući K_i. Kad napadač pozna K_i i IMSI može se predstaviti kao pretplatnik (onaj kojemu je i uzeo te podatke), te obavljati komunikaciju u njegovo ime (pozivi i SMS). Također, ti podaci se mogu iskoristiti za prisluškivanje te linije (slušanjem RAND poruka legitimne mreže u kombinaciji s poznatim K_i moguće je odrediti K_c koji se koriste za enkripciju). Ovaj tip napada se može provesti na bilo kojem mobilnom uređaju osluškujući eter, a napadač čak i ne mora fizički prisutan (udaljenost mora biti dovoljna za uspostavu konekcije).



Slika 13: *Uporaba lažnih baznih stanica, slanje poruka s RAND-om*

4.5. Kriptiranje se obavlja nakon FEC-a

U GSM-u kao i u ostalim bežičnim komunikacijama koristi se FEC (*engl. forward error correction*) za pomoć u ispravljanju pogrešaka izazvanih šumom ili slabljenjem signala. FEC dodaje redundantne bitove podacima povećavajući ukupnu količinu prenesenih podataka. Problem u GSM- u je taj što se kriptiranje odvija nakon dodavanja FEC bitova, što znači da se i redundantni bitovi dodaju modulo 2 dodaju aritmetikom kriptiranom podatku i time olakšavaju *crypt-analytical* napad, jer su ti redundantni bitovi poznati. Broj mogućih kombinacija ključeva napadač može dodatno smanjiti kombiniranjem znanja o A5 algoritmu.

4.6. Nedostatci u A5/1 i A5/2 algoritmima

A5/1 algoritam je baziran modulo 2 zbrajanjem 3 LFSR-a čiji se sinkronizacijski ulazi kontroliraju većinskom funkcijom određenih bitova u samim LFSR-ima. Alex Biryukov, Adi Shamir i David Wagner su dokazali da se algoritam A5/1 može razbiti u samo jednoj sekundi koristeći PC i određene prije izračunate tablice. Napad iskorištava propust u algoritmu u trenutku spremanja tih tablica spajajući znanje od statističke analize koraka algoritma i iskorištavanja slabe jedno bitne kontrole sinkronizacije LFSR-a. A5/2 je namjerno oslabljena inačica A5/1 algoritma što ga čini još ranjivijim.

5. Unapređenja GSM tehnologije

GSM specifikacije su bile podložne mnogim revizijama od njihova nastanka. Dodane su tehnologije kao što su GSM1800, HSCSD, GPRS i EDGE. Ustvari GSM standard i dan danas evoluira i trenutno je u fazi 3 generacije, 3G (UMTS). Dodana su mnoga poboljšanja u tehnologiji i sigurnosti od kojih su neka prikazana u nastavku dokumenta.

5.1. GSM – nove implementacije algoritma A3,A5 i A8

Kako je već i spomenuto uvedene su nove implementacije algoritama A3 i A8, COMP128-2 i COMP128-3 obje razvijane u velikoj tajnosti. COMP128-2 još uvijek sadrži namjerno 10 bitno oslabljivanje ključa Kc, dok COMP128-3 je isti taj algoritam bez oslabljivanja (64 bitni ključ). Algoritmi COMP128-2 i COMP128-3 su uspjeli ukloniti mogućnost kloniranja SIM kartica, te znatno otežali razbijanje šifre

preko etera (čak i ako ne dostižu punu snagu od 2^{128}). Također, 3GPP je definirao potpuno nove, otvorene, autentikacijske algoritme za uporabu u UMTS mrežama.
GSM podržava 7 različitih algoritama za A5 kriptiranje. Do 2002 korišteni su samo A5/1 i A5/2 kad je uveden novi snažniji algoritam A5/3 temeljen na Kasumiovom algoritmu (glavni enkripcijski algoritam u UMTS-u).

5.2. GPRS – GAE3 kriptiranje

Slično algoritmu A5/3 za GPRS je dodan novi algoritam također temeljen na Kasumiovom algoritmu zvan GEA3.

5.3. GPRS/UMTS – kriptiranje se obavlja prije FEC-a

Kriptiranje u GPRS-u se obavlja na višoj razini protokolnog stoga, u LLC-u (*engl. Logical Link Control*). RLC/MAC poruke se ne kriptiraju, te se FEC dodaje na fizičkom sloju. U UMTS-u kriptiranje se obavlja na RLC/MAC sloju, koji se nalazi odmah iznad fizičkog sloja u kojem se izvodi FEC.

5.4. UTMS – mreža se autenticira mobilnom uređaju

Kod UMTS-a je mogućnost da se napadač predstavi korisniku kao mreža otklonjena korištenjem dvosmjerne autentikacijske procedure. Procedura u kojoj se mobilni uređaj autenticira mobilnoj mreži nije se promijenila u odnosu na GSM, dok se sada i mreža mora autenticirati mobilnom uređaju i to porukom (*engl. Authentication Token*, AUTN) koju prenosi zajedno sa RAND-om. AUTN se sastoji od broja sekvence (SQN) kriptiranog koristeći RAND, korijenskog ključa K i MAC koda slične funkcije kao i SRES. Ako XMAC i MAC (izračunat u SIM-u) nisu identični mobilni uređaj šalje poruku odbijanja autentikacije i time terminira konekciju. Konačno, da bi se spriječilo napadača da jednostavno odgovori mreži na poruku traženja autentikacije, SIM kartica kontrolira brojeve sekvence sprečavajući ponavljanje brojeva sekvenci.

5.5. UMTS – unapređeni algoritmi

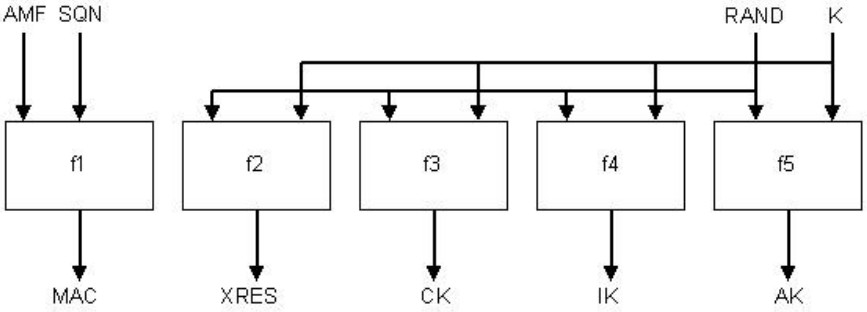
U UMTS-u se koriste potpuno novi kriptografski algoritmi koji ispravljaju nedostatke prijašnjih algoritama, te povećavaju razinu sigurnosti u mobilnoj komunikaciji.

5.5.1. Autentikacija i generiranje ključa

Na sličan način kao i kod GSM-a, autentikacija i sva generiranja ključeva obavljaju se u SIM kartici i mrežnom AC-u, ali uz veći stupanj sigurnosti ulaznih parametara. Algoritmi još uvijek rade na principu nepoznatog 128 bitnog glavnog ključa označenog kao K koji je poznat samo SIM kartici i AUC-u. Kriptografski algoritmi (Slika 14) koje koristi UMTS su:

- F1 – se koristi za generiranje autentikacijskog znaka (MAC) koji ima sličnu namjenu kao i SRES u GSM-u, ali se koristi za autentikacije mobilne mreže mobilnom uređaju (mobilni uređaj traži od mobilne mreže znanje glavnog ključa K). Ulazi u algoritam su 128 bitni RAND, 128 bitni K, 48-bitni broj sekvence SQN i AMF (vrijednost koja može biti korištena za specifičnu implementacijsku namjenu).
- F2 – se koristi za generiranje XRES-a sličnog SRES-u samo je dugačak 128 bita. Ulazi u algoritam su ključ K i RAND.
- F3 – se koristi za generiranje 128 bitnog ključa za kriptiranje CK. Ulazi u algoritam su K i RAND.
- F4 – se koristi za generiranje 128 bitnog ključa integriteta IK. Ulazi u algoritam su K i RAND. IK se koristi za digitalni potpis kontrolnih poruka.
- F5 – se koristi za generiranje 128 bitnog autentikacijskog ključa AK, koji se koristi za dekriptiranje (metodom XOR) broja sekvence SQN u trenutku slanja mobilnom uređaju.

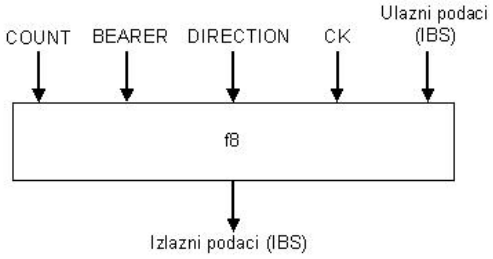
Kao i u GSM-u ovi algoritmi ovise o implementacijama pojedinih operatera koji će najvjerojatnije koristiti samo one najosnovnije. Takva implementacija je već prihvaćena od strane 3GPP i poznata je kao *MILENAGE,* te je u potpunosti dostupna javnosti (bazira se na AES-u).



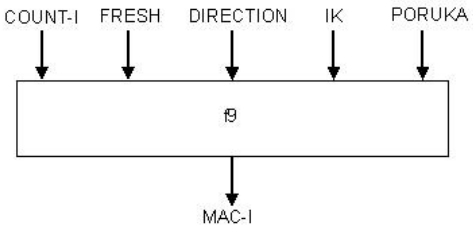
Slika 14: *Autentikacija i generiranje ključeva*

5.5.2. Kriptiranje i integritet

UMTS radio veze se kriptiraju na sličan način kao i u GSM-u. Mobilna mreža može izabrati između predefiniranih algoritama koje podržava pojedini mobilni uređaj. Algoritam za kriptiranje u UMTS mreži poznat je kao F8 (F8 funkcija). Ulazi i izlazi su sličnu kao i u GSM-u na način da je ulaz predstavljen pomoću 128 bitnog ključa za kriptiranje (KC), te kao dodatak parametri DIRECTION (smjer protoka podataka), COUNT-C (broj sekvencije kriptiranja) i BEARER (jedinstvena vrijednost za svaku multipleksiranu radio vezu), Slika 15. Kriptirani okvir podataka se XOR-a s podacima koji se prenose. Trenutno, je definirana samo jedna implementacija F8 i to UEA1 koji je baziran na algoritmu Kasumi. Dodatno, UMTS provjerava integritet RCC (*engl. Radio Resource Control protocol*) signalizacijskih poruka između bazne stanice i mobilnog uređaja. U provjeri integriteta svakoj se poruci dodaje 32 bitni okvir (MAC-I) koji doslovno predstavlja digitalni potpis koji dokazuje da je poruka stigla od određene mobilne stranice. Digitalni potpis se generira kao funkcija F9 128 bitnog ključa integriteta (IK) zajedno i sa DIRECTION, cijelom porukom, COUNT-I i FRESH (jedinstvena vrijednost koja se koristi za vrijeme konekcije koja sprečava korisnika ponovo šalje te iste poruke za vrijeme neke druge konekcije), Slika 16. Obje implementacije F8 i F9 bazirane su na Kasumi algoritmu. Kasumi je 8 bitni kružni model za kriptiranje čiji se S-elementi lako mogu implementirati koristeći logička vrata (lagana hardverska implementacija).



Slika 15: *Ulaz i izlaz funkcije F8*



Slika 16: *Ulaz i izlaz funkcije F9*

6. Zaključak

Iako je u počecima stvaranja GSM-a sigurnost bila jedan od glavnih ciljeva, u praktičnoj implementaciji pokazali su se i određeni nedostaci. Zbog jednostavnosti i ušteda, mnogi mobilni operatori odlučili su se samo na najosnovniju zaštitu. Algoritmi koji su bili definirani od strane GSM konzorcija kao predložak (za daljnje razvijanje) mnogi su iskoristili u izvornom obliku i tako narušili sigurnost svojih sustava. Iako postojeće sigurnosne nedostatke u GSM tehnologiji nije lako iskoristiti da bi se nanijela šteta korisnicima ili operaterima, ipak je moguće utvrditi da GSM komunikacija nije potpuno sigurna.

U stvarnosti nisu dokumentirani ozbiljniji slučajevi povreda sigurnosti korisnika. Nedostatke potencijalno mogu iskoristiti isključivo stručni napadači ili organizacije kao što su vojska i vlada što im može omogućiti presretanje poziva i prisluškivanje.

U novim implementacijama kao što su GPRS i UMTS sigurnosne funkcije su poboljšane iako ni one nisu savršene.

7. Literatura

[1] Racal research LTD.:**GSM System Security Study**, http://jya.com/gsm061088.htm

[2] Javier Gozalvez Sempere: ***An overview of the GSM system***, http://www.comms.eee.strath.ac.uk

[3] Goldberg, Briceno: **GSM Cloning**, http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

[4] Briceno, Goldberg, Wagner: **An implementation of the GSM A3A8 algorithm**, http://www.mirrors.wiretapped.net/security/cryptography/hashes/a3a8/a3a8.c

[5] 3GPP TS 25.202 - **3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; KASUMI Specification (Release 5, 6)**, http://www.3gpp.org/ftp/Specs/archive/35_series/35.202/

[6] 3GPP TS 35.201 - **Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; f8 and f9 Specification (Release 5, 6)**, http://www.3gpp.org/ftp/Specs/archive/35_series/35.201/

[7] GSM 11.11 - **Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11)**, http://www.ttfn.net/techno/smartcards/gsm11-11.pdf