SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
ZAVOD ZA ELEKTRONIČKE SUSTAVE I OBRADBU INFORMACIJA

Ksenija Herak
0036385272, INE

UMTS Security

— seminar iz SPVP-a —

Zagreb, lipanj 2004.

Sadržaj

1. Uvod

Treća generacija mobilnih sustava donosi širok izbor telekomunikacijskih usluga, uključujući govor, video, prijenos podataka i kompleksne multimedijske usluge. Digitalne mreže donose korisnicima istovremeno mogućnost upotrebe dodatnih usluga vezanih sa sigurnošću, koje se temelje na upotrebi USIM-a (***U**MTS **S**ubscriber **I**dentity **M**odule*) – pametne kartice. Kartica identificira korisnika u mreži. Sigurnosni sustavi u UMTS-u moraju osiguravati odobravanje (*verifying)*, šifriranje, integritet (cjelovitost) i druge sigurnosne usluge.

2. Prijetnje sigurnosti u mobilnim mrežama

U ovom poglavlju biti će nabrojane i definirane potencijalne opasnosti, koje prijete sigurnosti u 3G sustavima. Biti će navedeno gdje se u sustavu pojavljuju i tko su njihovi nosioci. Te opasnosti moguće je podijeliti na nekoliko načina. Standardno ih se dijeli u sljedeće kategorije:

a) Neovlašten pristup osjetljivim informacijama – kršenje povjerljivosti (violation of confidentiality)

- Prisluškivanje (eavesdropping): Uljez presreće poruke.
- Pretvaranje (masquerading): Uljez prevari korisnika predstavljajući se da je legitiman element sustava i na taj način od njega dobije povjerljivu informaciju. Na taj način uljez sad prevari legitiman sustav da je on odobren korisnik te na taj način dođe do informacija do kojih inače ne bi imao pristupa.
- Prometna analiza (Traffic analysis): Uljez nadzire vrijeme, učestalost, dužinu, izvor i odredište poruka te na taj način utvrdi uporabnu lokaciju ili kada je došlo do pozamašnih transakcija.
- Pregledavanje (Browsing): Uljez potraži osjetljive informacije među spremljenim podacima.
- Propuštanje (Leakage): Uljez dobije informacije pomoću procesa koji ima legitiman pristup informacijama.
- Zaključivanje (Inference): Uljez motri reakcije na slanje signala u sustav. Uljez lako, na primjer, pokušavajući uspostaviti aktivnu komunikaciju te pomoću promatranja vremena, učestalosti, dužine, izvora i odredišta poruke dobije informacije o radio odašiljačima sustava.

b) Neovlašteno mijenjanje osjetljivih podataka – povreda integriteta (violation of integrity)

- Mijenjanje poruka (Manipulation of messages): Uljez namjerno promjeni, ubaci, ponovi ili izbriše poruku.

c) Ometanje ili zlouporaba mrežnih usluga (što vodi ka smanjivanju dostupnosti ili čak ka nedostupnosti usluga)

- Intervencija (Intervention): Uljez sprječava upotrebu usluga odobrenome korisniku s ometanjem prometa, signalizacije ili upravljanih informacija.

- Blokada izvora (Resource Exhaustion): Uljez spriječi pristupanje odobrenog korisnika usluzi tako da promjeni uslugu.
- Zloupotreba usluga (Abuse of services): Uljez zlorabi posebne usluge da bi dobio prednost ili uzrokovao prekid mreže.
- Nijekanje (Repudiation): Korisnik ili mreža zaniječe događaje koji su se dogodili.

d) Neovlašten pristup uslugama

- Pretvaranje (masquerading): Uljez pristupa uslugama pretvarajući se da je korisnik ili mrežni entitet.
- Zlouporaba povlastica (Misuse of privileges): Korisnik ili servisna mreža mogu zlouporabiti svoje povlastice za neovlašten pristup uslugama ili informacijama.

Prijetnje navedene u gornjim kategorijama mogu se podijeliti prema točkama napada:

- Radio odašiljač;
- Terminali i UICC/USIM;
- Preostali dijelovi sustava.

3. Sigurnosni zahtjevi

Iz analize gore navedenih opasnosti, koje prijete sigurnosti sustava treće generacije, izvedeni su sigurnosni zahtjevi.

3.1. Zahtjevi za siguran pristup uslugama

Uvjet potreban da bi korisnik pristupio 3G usluzi je važeći USIM. Zahtjevi predviđaju sposobnost sprečavanja pristupa 3G uslugama uljezima koji se pretvaraju da su ovlašteni korisnici. Isto tako mora biti moguće provjeriti da li je servisnoj mreži odobreno nuditi 3G usluge u korisnikovom domaćem okružju (***H**ome **E**nviroment - HE*) kako na početku, tako i tokom upotrebe ponuđenih usluga.

3.2. Zahtjevi za sigurno izvršavanje usluga

Zahtjevi te skupine predviđaju mogućnost da onaj koji nudi uslugu odobri korisnika na početku i tokom upotrebe usluge te na taj način onemogući uljezima neovlašten pristup ponuđenim uslugama. Mora postojati mogućnost prepoznavanja i uklanjanja neovlaštene uporabe usluga te alarmiranja ponuđača usluga o zlouporabi. Predviđeno je i zabilježavanje poruka o događajima. U primjeru zloupotreba se predviđa mogućnost sprečavanja pristupa pojedinačnim USIM do pojedinačnih ili svih 3G usluga. Servisne mreže moraju imati sposobnost provjere izvora korisničkog prometa, signalizacije podataka i upravljanih podataka na radio odašiljačima te onemogućavanja da uljezi ograničavaju dostup usluga korisnicima. Osigurana mora biti sigurna infrastruktura između mrežnih operatera. To treba biti ostvareno tako da su potrebe HE u vezi povjerenja u servisnu mrežu po pitanju sigurnosti minimalne.

3.3. Zahtjevi za osiguravanje sustavne cjelovitosti

Zahtjevi te skupine osiguravaju zaštitu od neovlaštenih promjena korisničkog prometa, signalnih i upravljanih informacija, posebno na radio odašiljačima, zaštitu od neovlaštenih promjena korisničkih podataka, nakupljenih i sačuvanih u terminalu ili USIM-u, zaštitu od neovlaštenih promjena korisničkih podataka, obrađenih i sačuvanih kod ponuđača usluga. Osiguravaju podatke o izvoru i cjelovitosti aplikacija i podataka, sakupljenih na terminalu i UICC-u. Isto tako potrebno je osigurati njihovu povjerljivost. Trebaju biti poznati podaci o izvoru i cjelovitosti pristupnih podataka, posebno ključa za šifriranje (cipher key) na radio odašiljaču. Mora postojati mogućnost komunikacije među operatorima preko sigurne infrastrukture.

3.4. Zahtjevi za zaštitu osobnih informacija

- **Sigurnost korisničkih podataka koji se prenose preko mreže**

  Zahtjevima za osiguravanje korisničkih podataka koji se prenose preko mreže pripadaju: mogućnost osiguravanja povjerljivosti korisničkih podataka, signalnih i upravljanih podataka, posebno na radio odašiljaču, povjerljivost podataka o identitetu i lokaciji korisnika. Korisnik mora moći provjeriti da li su njegovi podaci i s njim povezane informacije zaštićene tokom prijenosa. Ovakvo provjeravanje mora zahtijevati minimalne napore, dakle mora biti što jednostavnije.

- **Sigurnost korisničkih podataka koji su pohranjeni u sustavu**

  Ponuđač mora biti sposoban osigurati povjerljivost korisničkih podataka koje pohranjuje ili obrađuje. Isto tako mora biti osigurana povjerljivost korisničkih podataka pohranjenih na korisničkom terminalu ili USIM-u.

3.5. Zahtjevi na terminal i USIM

- **Sigurnost vezana uz terminal**

Terminal mora posjedovati osobine odvraćanja od krađe. Mora biti osigurana nemogućnost pristupa 3G uslugama na pojedinačnim terminalima. Također mora biti onemogućena promjena identiteta terminala, s namjerom zaobilaženja zabrane pristupa uslugama.

- **Sigurnost vezana uz USIM**

Kao i kod terminala, i kod USIM-a je moguće ograničavati pristup. S USIM karticom omogućen je pristup 3G uslugama samo korisnicima koji su eksplicitno odobreni sa strane naručitelja. Moguće je ograničiti i pristup podacima spremljenim na USIM. Neki su podaci, na primjer, dostupni samo odobrenom HE, dok su drugi namijenjeni upotrebi unutar samoga USIM-a (ključevi za šifriranje i algoritmi).

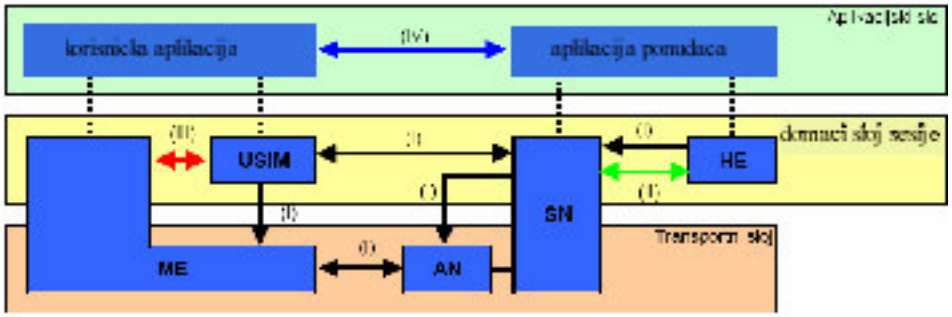
3.6. Vanjski zahtjevi - pravno/regulacijski zahtjevi

Agencije koje djeluju pod pravnim nadzorom moraju imati mogućnost nadzora i presretanja svakog poziva (ili čak želje poziva) te ostalih usluga i korisničkih namjera, u

skladu s državnim zakonodavstvom i regulativama.

4. Pregled sigurnosne arhitekture

Na slici 1 imamo pregled cjelokupne 3G sigurnosne arhitekture.



Slika 1. Pregled sigurnosne arhitekture

Definirano je pet sigurnosnih skupina. Svaka među njima rješava probleme određene skupine opasnosti i podupire određene sigurnosne zahtjeve:

- **Siguran pristup mreži - I (Network access security)**

Skupina sigurnosnih osobitosti koje osiguravaju korisniku siguran pristup 3G uslugama i štite ga od napada na radio sučelju.

- **Sigurnost mrežne domene - II (Network domain security)**

Skupina sigurnosnih osobitosti koje omogućavaju čvorištima domene ponuđača da međusobno sigurno izmjenjuju signalizacijske podatke i štite od prodora u bežičnu mrežu.

- **Sigurnost korisničke domene - III (User domain security)**

Skupina sigurnosnih osobitosti koje štite pristup mobilnim stanicama.

- **Sigurnost aplikacijske domene - IV (Application domain secutiy)**

Skupina sigurnosnih osobitosti koje omogućavaju aplikacijama iz korisnikove i domene ponuđača sigurnu izmjenu poruka.

- **Vidljivost i konfigurabilnost sigurnosti - V (Visibility & Configurability of Security)**

Skupina sigurnosnih osobitosti koje omogućavaju korisniku da provjeri upotrebu sigurnosnih mogućnosti i da li se upotreba usluga temelji na mehanizmima sigurnog prijenosa.

Za neke od skupina standardizacija još nije napravljena. Skupine sadrže mehanizme koji provode njihovu namjenu. U 5. poglavlju će biti prikazan kratak pregled mehanizama za zaštitu pristupa mreži.

4.1. Osobine sigurnog pristupa mreži

Osobine sigurnog pristupa mreži mogu se podijeliti u sljedeće kategorije: vjerodostojnost entiteta (*entity authentication*), povjerljivost (confidentiality) i cjelovitost podataka (*data*

integrity). Slijedi opis sigurnosnih osobina koje pripadaju prvoj skupini:

- **Vjerodostojnost korisnika (*User authentication*)**: Svojstvo servisne mreže da ima mogućnost potvrditi korisnika;
- **Vjerodostojnost mreže (*Network authentication*)**: Svojstvo koje omogućava korisniku da potvrdi da je povezan na servisnu mrežu kojoj je njegova domaća mreža (*home network*) odobrila pružanje usluga. Ovo uključuje i jamstvo da autorizacija nije zastarjela.

Sljedeća svojstva tiču se povjerljivosti podataka na mrežnoj pristupnoj liniji:

- **Dogovor o algoritmu za šifriranje** *(Cipher algorithm agreement)*: Svojstvo koje omogućava da mobilna stanica i servisna mreža mogu sigurno pregovarati o algoritmu koji će koristiti;
- **Dogovor o ključu za šifriranje** *(Cipher key agreement):* Svojstvo koje omogućava mobilnoj stanici i servisnoj mreži dogovor o ključu koji će upotrebljavati za šifriranje;
- **Povjerljivost korisničkih podataka** *(Confidentiality of user data):* Svojstvo koje uklanja mogućnost prisluškivanja korisničkih podataka na radio sučelju;
- **Povjerljivost signalnih podataka** *(Confidentiality of signaling dana):* Svojstvo koje uklanja mogućnost prisluškivanja signalnih podataka na radio sučelju;

Osobine koje osiguravaju cjelovitost podatak na pristupnoj vezi mreži su sljedeće:

- **Dogovor o algoritmu cjelovitosti** *(Integrity algorithm agreement)*: Svojstvo koje omogućava da mobilna stanica i servisna mreža mogu sigurno pregovarati o algoritmu koji će koristiti;
- **Dogovor o ključu cjelovitosti** *(Integrity key agreement):* Svojstvo koje omogućava mobilnoj stanici i servisnoj mreži dogovor o ključu koji će upotrebljavati;
- **Cjelovitost podataka i zaštita izvora signalnih podataka** *(Data integrity and origin authentication of signaling data):* Svojstvo koje omogućava entitetu koji prima podatke (mobilna stanica ili servisna mreža) da provjeri da li je signaliziranje ispravno ili je promijenjeno od neautorizirane osobe od trenutka kada je podatak poslao entitet koji šalje podatke (mobilna stanica ili servisna mreža). Također daje mogućnost provjere da li je izvor signalnih podataka uistinu onaj za kojeg se tvrdi.

5. Mehanizmi za zaštitu pristupa mreži

5.1. Identifikacija pomoću privremenog identiteta

Mehanizam omogućava identifikaciju korisnika na temelju upotrebe privremenog mobilnog pretplatničkog identiteta (***T**emporary **M**obile **S**ubscriber **I**dentity - TMSI*). TMSI je lokalni parametar, koji se upotrebljava samo u području gdje je korisnik registriran. Izvan tog područja upotrebljava se uz pratnju pripadajućeg identifikatora lokalnog područja (***L**ocation **A**rea **I**dentification - LAI*) ili identifikatora usmjeravajućeg područja *(**R**outing **A**rea **I**dentifier - RAI*), da se izbjegnu zabune. Preslikavanje među stalnim i privremenim identitetom zapisano je u VLR-u (***V**isited **L**ocation **R**egister/**S**erving **G**PRS **S**upport **N**ode (VLR/SGSN)*), u kojem je korisnik registriran.

TMSI se upotrebljava kod zahtjeva za spajanjem na mrežu, zahtjeva za uslugama, osvježavanjima lokacija, zahtjevima za ponovnom uspostavom veze, zahtjevima za iskapčanje itd. Postupci su slični mehanizmima upotrijebljenim u GSM sustavima.

Postupak određivanja TMSI

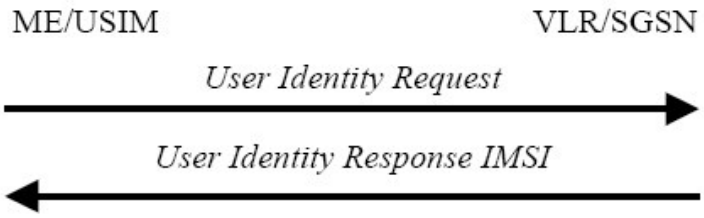
Postupak se izvodi odmah po uspostavi šifriranja. VLR izračuna novi privremeni identitet (TMSIn) i pohrani ga zajedno sa stalnim identitetom IMSI u bazu podataka. TMSI mora biti nepredvidljiv. VLR pošalje korisniku novi TMSIn i (ako je potrebno) također i lokacijski identifikator (LAIn).

Slika 2. Postupak određivanja TMSI

Po primitku TMSIn-a korisnik ga pohrani te automatski ukloni stari TMSIo. Korisnik zatim pošalje potvrdu o primitku VLR-u. Nakon što primi potvrdu VLR također ukloni stari TMSIo i IMSI iz baze podataka.

5.2. Identifikacija pomoću stalnog identiteta

Mehanizam omogućava identifikaciju korisnika na vezi na radio sučelje upotrebom stalnog korisničkog identiteta (***P**ermanent **S**ubscriber identity - IMSI*). Aktivira ga servisna mreža u slučaju kada korisnika nije moguće identificirati upotrebom mehanizma identifikacije privremenim identitetom. To se događa, npr., kada se korisnik prvi put prijavljuje u mrežu ili kada mreža ne može iz TMSI-a zaključiti s kojim se IMSI korisnik želi identificirati.

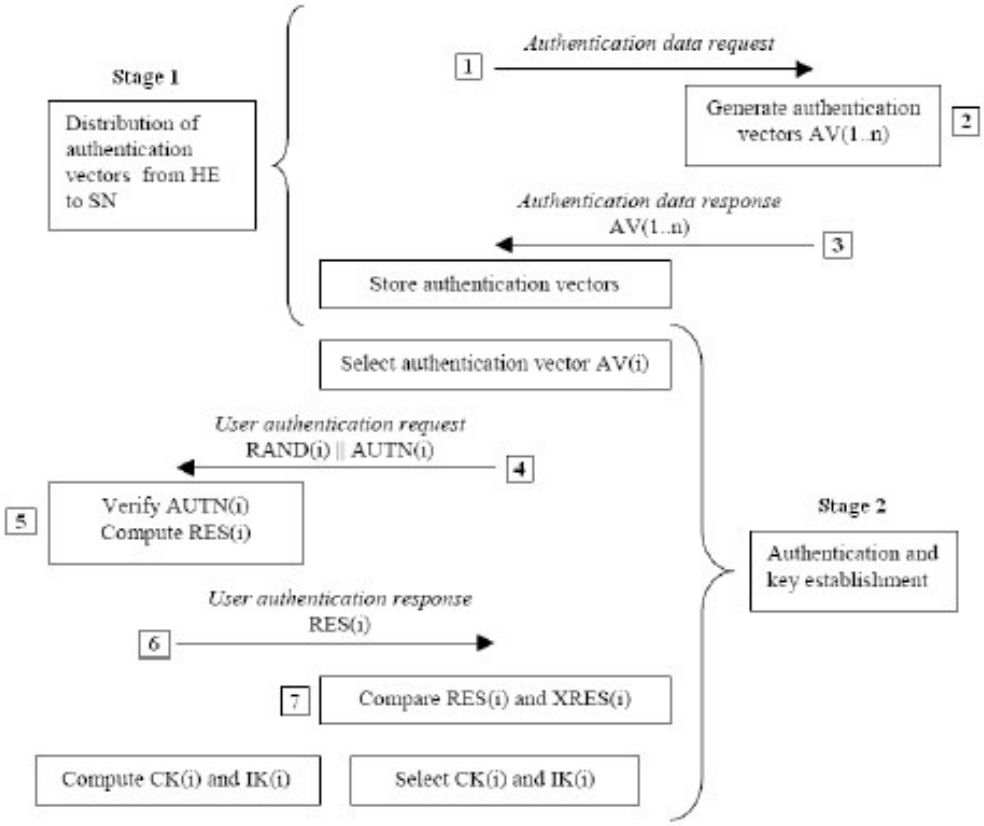


Slika 3. Identifikacija pomoću stalnog identiteta

VLR/SGSN od korisnika zahtijeva stalni identitet IMSI, korisnik se odazove sa IMSI u nešifriranom tekstu (cleartext). To predstavlja 'rupu' u tajnosti korisničkog identiteta. Iz tog je razloga ovakvo predstavljanje mreži smisleno upotrebljavati samo u nuždi.

5.3. Zaštita i dogovor o ključevima
(UMTS AKA – *UMTS Authentication and Key Agreement*)

Navedeni mehanizam osigurava međusobno odobravanje među korisnikom i mrežom. Obje strane moraju poznavati tajni ključ sesije K koji je dostupan samo USIM-u i u AuC-u (***A**uthentication **C**enter*) u korisnikovom HE.



Slika 4. Odobravanje i izmjena ključeva

Taj mehanizam bio je izabran da bi se osigurala povezanost s postojećom GSM arhitekturom te time pospješio prijelaz s GSM na UMTS sustav. Mehanizam se temelji na protokolu zahtjeva/odziva (*challenge/response*), koji je identičan odobravanju GSM korisnika i sporazumijevanju o ključevima, združenim s protokolom koji se temelji na sekvencijalnom brojanju jednokratnih prolaza za mrežno odobravanje, izvedenim iz ISO standarda. VLR/SGSN pošalje zahtjev za odobravanje. HE/AuC se odazove s uređenim poljem AVs-a (***A**uthentication **V**ectors*), razvrstanih po sekvencijalnim brojevima koje vrati VLR/SGSN.

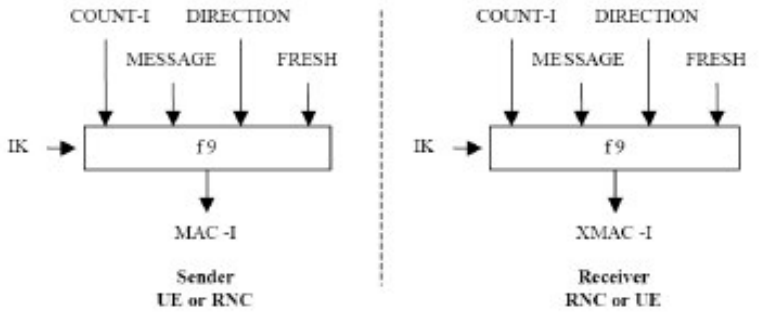
Svaki AV sadrži sljedeće komponente:

- Slučajni broj RAND (*Random challenge*);
- Očekivani odziv na slučajni broj XRES (*Expected response*);
- Ključ za šifriranje CK (*Cipher key*) i integritetni ključ IK (*Integrity key*);
- Žeton za odobravanje AUTN (*Authentication token*).

Svaki AV upotrebljiv je samo za jedno odobravanje i dogovaranje o ključevima između VLR/SGSN i USIM-a. Kad VLR/SGSN započne odobravanje i dogovaranje o ključevima izabere sljedeći vektor uređenog polja i pošalje parametre RAND i AUTN korisniku. Vektori se upotrebljavaju po FIFO (*First In First Out*) metodi. USIM provjeri da li može primiti AUTN podatak i ako može, odazove se na RAND podatke s RES odgovorom, kojeg pošalje VLR/SGSN. USIM izračuna još i ključeve CK i IK. VLR/SGSN uspoređuje primljeni RES podatak s podatkom XRES i ako se slažu to znači da je odobravanje uspjelo. USIM i VLR/SGSN dostave ključeve CK i IK entitetima koji žele osiguravati šifriranje i integritet.
Pomoću izračunatih CK i IK VLR/SGSN lako omogućava sigurne usluge i kada HE/AuC nije dostupan. Odobravanje se u tom slučaju obavlja pomoću IK koji osiguravaju zaštitu integriteta signalizacijskim porukama.

5.4. Algoritmi za cjelovitost i povjerljivost (*Integrity and Confidentiality Algorithms*)

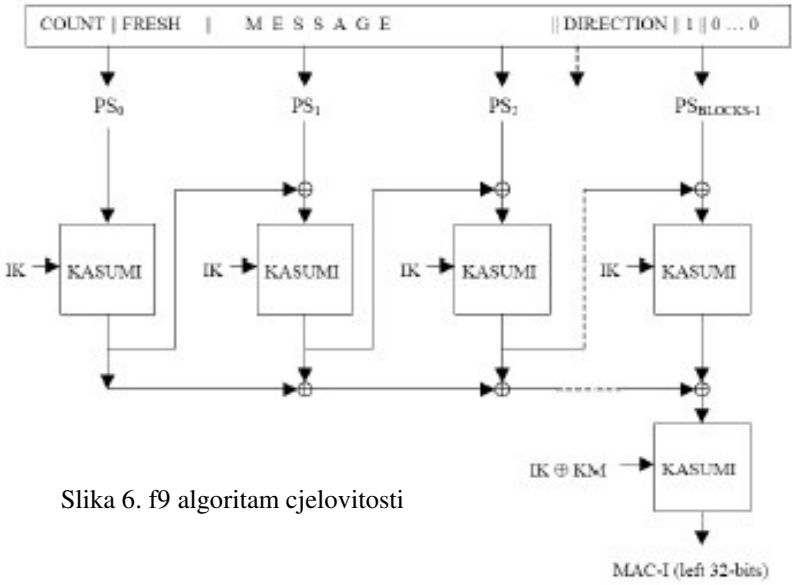
Kontrolne signalne informacije koje se prenose između mobilne stanice i mreže bitne su i vrlo osjetljive. Zato je potrebno zaštititi njihovu cjelovitost. Mehanizam, koji to ostvaruje temelji se na UMTS algoritmu cjelovitosti (***UMTS Integrity Algorithm – UIA***) implementiranom kako u mobilnu stanicu tako i u UTRAN (***UMTS Terrestrial Radio Access Network***) modul bliži jezgri mreže (npr. u RNC – ***Radio Network Controller***).
UIA je f9 algoritam, objašnjen na slici 5.



Slika 5. Izvođenje MAC-I iz signalnih podataka putem f9 algoritma

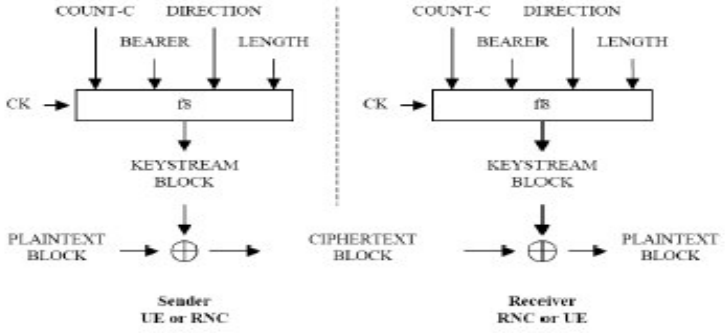
Postupak određivanja cjelovitosti podataka izvodi se na sljedeći način: prvo f9 algoritam u korisničkoj opremi izračuna 32-bitni MAC-I (***Message Authentication Code***) za cjelovitost podataka temeljen na ulaznim parametrima, koji uključuju signalne podatke (poruka). Zatim se MAC-I pripaja signalnoj informaciji i šalje preko radio sučelja sa korisničke opreme do RNC-a. Kada RNC primi informaciju i pripojeni MAC-I, izračuna XMAC-I za signalne podatke na isti način kako je mobilna stanica izračunala MAC-I. Cjelovitost informacije odredi se uspoređivanjem MAC-I i XMAC-I.
Slika 6 prikazuje unutarnju strukturu f9 algoritma, koja dijeli IK i temelji se na lancu

blokova šifri implementirajući tako KASUMI algoritam. Izlazi blokova dugi su 64 bita, ali je izlaz iz cijelog algoritma dug 32 bita.



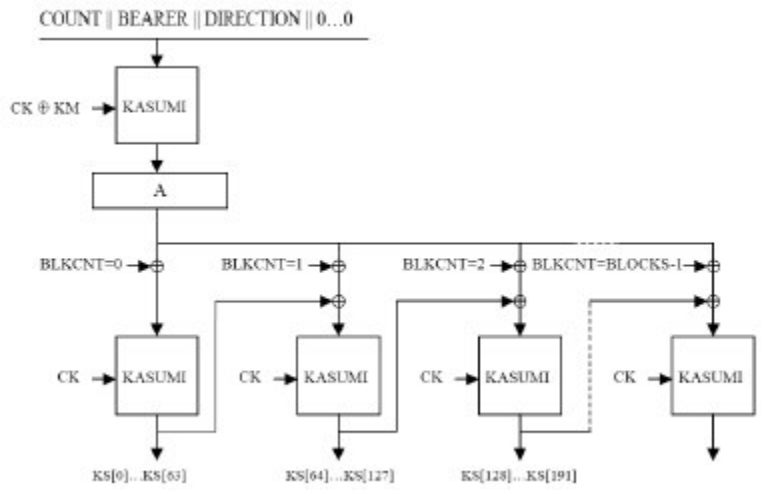
Slika 6. f9 algoritam cjelovitosti

Za razliku od algoritma cjelovitosti, koji vrši operacije samo nad signalnim informacijama, mehanizmi povjerljivosti rade i na signalnim informacijama i na korisničkim podacima. Algoritam koji obavlja ovu vrstu operacija naziva se f8 algoritam i radi na sljedeći način: koristeći ključ za šifriranje (CK) i još neke parametre f8 algoritam u korisničkoj opremi izračuna izlazni slijed bitova. Zatim se, bit po bit, izvrši XOR operacija između ovih bitova i podataka – čistog teksta (*plaintext*), da bi se dobio šifrirani blok podataka (*ciphertext*). Šifrirani tekst šalje se u mrežu kroz radio sučelje. F8 algoritam u RNC-u koristi iste ulaze kao i u korisničkoj opremi, uključujući i CK koji dijele, da bi generirao jednak izlazni slijed bitova kao što ga je generirala korisnička oprema. Konačno, izvrši se XOR operacija između izlaznog slijeda bitova i primljenog šifriranog teksta da bi se dobila početna informacija. Slika 7 prikazuje shemu šifriranja.



Slika 7. Šifriranje signalnih i korisničkih podataka upotrebom f8 algoritma

Na slici 8 prikazana je struktura f8 algoritma. Ponovo se vidi nekoliko KASUMI blokova, s time da su ovaj put povezani u petlji povratne veze. Svaki blok generira 64-bitni izlazni slijed bitova i šalje ih na ulaz sljedećeg bloka.



Slika 9. algoritam povjerljivosti f8

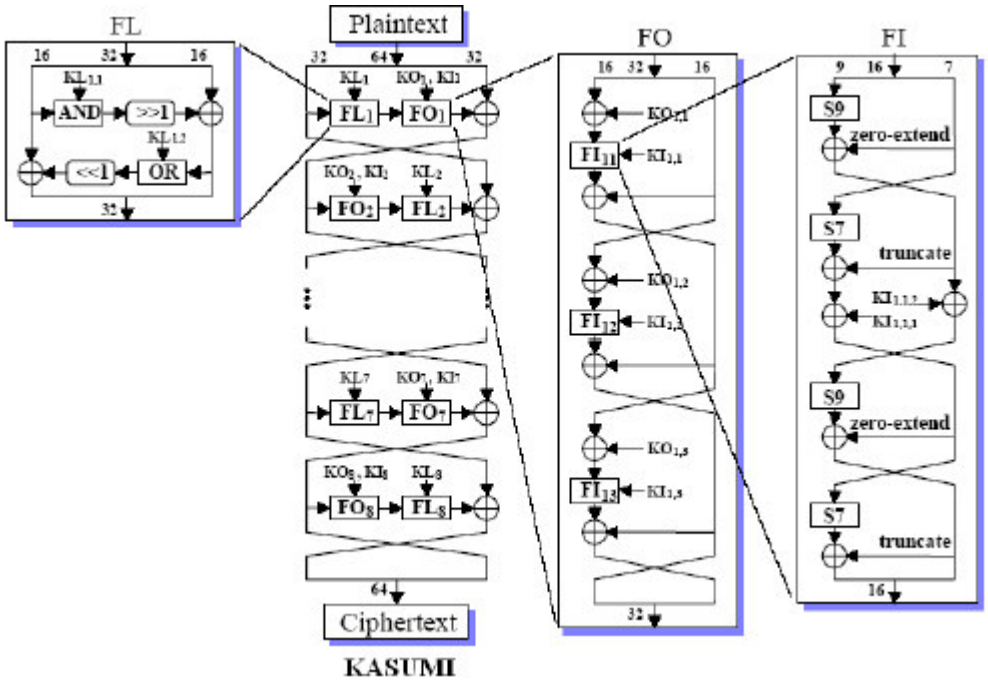
5.5. KASUMI blok za šifriranje

Ovaj blok čini jezgru mehanizama cjelovitosti i integriteta u UMTS mrežama. KASUMI je šifra koja ima Feistel strukturu i vrši operacije nad 64-bitnim blokovima podataka kontroliranim sa 128-bitnim ključem. Uslijed svoje Feistel strukture KASUMI posjeduje sljedeće značajke:

- Temelji se na 8-cikličnoj (*8 round*) obradi;
- Ulazni 'čisti' tekst je ulaz u prvom krugu obrade;
- Šifrirani tekst je izlaz iz posljednjeg kruga obrade;
- Enkripcijski ključ K upotrebljava se da bi se generiralo ključeve za pojedine krugove obrade (KL, KO, KI);
- Svaki krug računa drugu funkciju, dok god su ključevi različiti;
- Isti algoritam koristi se za kriptiranje i dekriptiranje.

Razvoj KASUMI šifre temelji se na prethodnoj šifri zvanoj MISTY1. MISTY1 je bila temelj algoritama šifriranja za 3GPP zbog svoje dokazane sigurnosti protiv najnaprednijih metoda razbijanja šifri. MISTY je bila optimizirana za implementaciju u sklopovlje.

Na slici 10 prikazana je organizacija KASUMI šifre. Vidi se da je funkcija f, izračunata u svakom krugu, sastavljena od dvije podfunkcije, FL i FO. To ovisi o ulaznim parametrima kruga i odgovarajućem setu ključeva. Na slici se vidi i unutarnja struktura svake od dviju podfunkcija. FL funkcija ima jednostavnu strukturu, sastoji se od logičkih operacija i vrši pomicanje (*shift*) ulaza. FO je kompliciranija. Ima Feistel strukturu sastavljenu od tri kruga, od kojih svaki zahtijeva izračunavanje FI podfunkcije, koja je također sastavljena od tri kruga.



Slika 10. Dijelovi KASUMI šifriranja

6. Zaključak

Arhitektura ostvarivanja sigurnosti UMTS-a temelji se na mogućnostima usluga da ostvare jedan ili više zahtjeva, odnosno osobina koje jamče sigurnost (*security features*), kao i procese koji omogućavaju te osobine, tzv. mehanizme za provedbu sigurnosti (*security mechanisms*). Najbitnije osobine su: uzajamna vjerodostojnost (*authentication*), algoritmi za šifriranje i ključevi za šifriranje, povjerljivost korisničkih i signalnih podataka, algoritam cjelovitosti i dogovor o ključu cjelovitosti, te metode koje jamče kako cjelovitost podataka, tako i zaštitu izvornih signalnih podataka. F8 algoritam jamči povjerljivost podataka i signala, dok f9 algoritam služi da bi osigurao cjelovitost signalnih informacija. Oba algoritma temelje se na KASUMI šifriranju, temeljenom na Feistel strukturi.

7. Literatura

1. An Introduction to Access Security in UMTS. Dostupno na URL:
http://wireless.poly.edu/act/files/An%20Introduction%20to%20Access%20Security%20in%20UMTS.ppt

2. Security Architecture in UMTS Third Generation Cellular Networks. Dostupno na URL:
http://ccc.inaoep.mx/Reportes/CCC-04-002.pdf

3. UMTS security. Dostupno na URL:
http://www.crypto.ruhr-uni-bochum.de/Seminare/BeitraegeITS/UMTS%20Security.pdf

4. UMTS security features. Dostupno na URL:
http://www.umtsworld.com/technology/security.htm

5. Varnost v mobilnih sistemih UMTS. Dostupno na URL:
http://www.ltfe.org/pdf/Varnost_v_UMTS.pdf