Fakulteta za elektrotehniko
Univerza v Ljubljani

Digitalne komunikacije
Podiplomski študij

Mehanizmi za zagotavljanje varnosti v UMTS

Mentor: prof.dr. Sašo Tomažič, univ. dipl. inž el.
Avtor: Iztok Humar, univ. dipl. inž el.

Ljubljana, 8.2.2002

Kazalo

1. Uvod

Brezžične komunikacije omogočajo enostaven dostop do komunikacijskega medija tako komunicirajočim entitetam kot tudi vsem potencialnim prisluškovalcem. Spričo tega dejstva je varnost v brezžičnih komunikacijah vedno bila in tudi bo pereč in relativno dobro obdelan problem. Zavedati pa se je potrebno, da pojem varnosti obsega široko področje in zahteva prisotnost in doslednost na vseh nivojih »mobilnega poslovanja«.
V seminarski nalogi si bomo problematiko varnosti v omrežju UMTS ogledali tako s stališča ponudnika storitve, kot tudi z vidika uporabnika.

Prva generacija mobilne telefonije (1G) – analogno omrežje mobilne telefonije – ni imela vgrajenih veliko mehanizmov za zagotavljanje varnosti. V obdobju njenega razmaha ponujene storitve niso potrebovale varnostnih mehanizmov; uporabniki niso imeli razlogov za izvedbo varne povezave.

Radijsko dostopovno pot mobilnega omrežja, ki je najbolj nezavarovan del sistema, lahko zavarujemo zelo učinkovito, kar pa prinese s seboj pozitivne in negativne posledice. Pri radijski povezavi, izvedeni med dvema točkama, lahko uporabimo poljuben varnostni mehanizem za zagotavljanje varnosti. Takšen način zagotavljanja varnosti je pogosto uporabljen pri vojaških zvezah. V javnih celičnih omrežjih pa se zveza vzpostavlja med eno točko (na eni strani) in različnimi ciljnimi točkami, na drugi strani. Ker oddani signal sprejemajo različne ciljne naprave je izbor poljubnega mehanizma za zagotavljanje varnosti na radijski poti nesprejemljiv; potrebno je uporabiti **standardizirane** varnostne mehanizme.

V drugi generaciji mobilne telefonije (2G) – GSM omrežju – je zagotavljanje varnosti osredotočeno na radijsko dostopovno omrežje, oziroma točneje – na varovanje dostopa do omrežja.

V tretji generaciji mobilne telefonije (3G) – UMTS omrežju – pa je varnostni problem mnogo bolj razdelan. Podobno kot v 2G se tudi v 3G varuje dostop do omrežja; izvedeni pa so tudi drugi vidiki. Današnji poslovni modeli namreč pogosto privedejo v situacijo, kjer je potreben prenos zelo občutljivih informacij med različnimi odjemalci in omrežji. Geografske meje pri prenosu varovanih podatkov in overjanju uporabnikov ne smejo predstavljati ločnic. UMTS nadaljuje z integracijo telekomunikacij in podatkovnih komunikacij, katero pa nadgrajuje s stališča varnosti. V IP svetu je problematika v zvezi z varnostjo komunikacije prisotna že dolgo časa, napravljeno je bilo veliko poskusov vpeljave mehanizmov za zagotavljanje varne komunikacije, ki so se v zadnjem času nenehno razvijali.

Seminarsko nalogo začnem s pregledom obstoječih sistemov, določitvijo pomanjkljivosti in vodil, ki so bila temelj snovanja mehanizmov za zagotavljanje varnosti v sistemi 3G. Ogledamo si vloge v sistemih 3G, grožnje, ki pretijo tako uporabnikom kot ponudnikom storitev, ter pregledamo zahteve, ki so jih standardizatorji izpeljali iz groženj.

V tretjem poglavju je napravljen pregled varnostne arhitekture.

Sledijo poglavja, ki napravijo pregled varnostnih mehanizmov.

Četrto poglavje obdela mehanizme, ki zagotavljajo varovanje dostopa do omrežja. To vključuje varen dostop uporabnika do omrežja UMTS in varno izvedbo povezave na nivoju dostopovnga omrežja. Varnost dostopa do omrežja UMTS temelji na modelu varnosti dostopa do GSM omrežja, kateremu so dodane razširitve.

V petem poglavju sem želel predstaviti razvito rešitev uporabe infrastrukture javnih ključev za overjanje v UMTS omrežju. Zavedam se, da poglavje s svojo specifičnostjo kvari splošnost seminarske naloge, vendar se mi je zdel primer izvedbe zanimiv in sem se odločil, da ga uvrstim »na spored«. V kolikor se bralcu zdi prezahteven ali vsebinsko neskladen, ga naj izpusti.

Komunikacijo pa moramo razumeti kot celoto. Za zaščito podatkov ni dovolj zaščita na najnižjem nivoju ter overovitev uporabnika. Videli bomo, se uporabniški podatki preko omrežja v določenih primerih še vedno prenašajo popolnoma nezaščiteni. Zato v šestem poglavju napravimo rezime sistemskemu in omrežnemu nivoju. Ker na tem nivoju deluje IP, je problematika distancirana od UMTS omrežja. S poglavjema (6, 7), katerim ekvivalente najdemo v večini knjig, ki se ukvarjajo s problematiko varne komunikacije v sistemu UMTS želim zaključiti celoto, zavedam pa se, da je ta problematika precej bolj podrobno obdelana v literaturi, ki govori o IP omrežjih in drugih sorodnih področjih. Sedmo poglavje napravi hiter pregled nivoja aplikacij in storitev. Zavedati pa se je treba, da je se posebej to področje izjemno dinamično, nestandardizirano in bo prav ob uveljavitvi omrežja UMTS doseglo nov razmah. Zato je odločanje o tem, kaj opisati in kaj ne, zelo nehvaležno delo. Problemi teh mehanizmov višjih nivojev – nivojev ponudnikov storitev in vsebin so večinoma neodvisni od strukture samega UMTS omrežja, a nenazadnje igrajo pomembno vlogo v varnosti sistema na splošno. V tem delu se dotaknemo varovanja dostopa v IP multimedijskih sistemih znotraj UMTS omrežja.

Pomembno področje je tudi področje pravne regulative, ki predstavljajo dodaten pogled na težave pri zagotavljanju varnosti na področju mobilnih komunikacij, ki so v zadnjem času postale del moderne družbe.

Ob koncu na enem mestu zberemo identificirane pomanjkljivosti pri zaščiti podatkov v UMTS. Te se večinoma nanašajo na pomanjkljivosti iz četrtega poglavja, ker je v tem področju standardizacija UMTS najbolj dejavna. Ostali nivoji so napisani precej splošno in posvajajo že razvite tehnologije.

2. Splošno o varnosti sistemov 3G

Način radijskega dostopa se bo v omrežju 3G spremenil iz TDMA v WCDMA. Kljub tej spremembi se zahteve po varovanju dostopa do omrežja ne bodo nič spremenile.

Tudi v sistemu UMTS bodo morali biti vsi končni uporabniki *overjeni* (authenticated), kar pomeni, da se identiteta vsakega naročnika preveri. Nihče namreč ne želi plačevati račune za storitve, ki jih napravijo nepooblaščene osebe.

Zaupnost (confidentiality) glasovnih klicev in prenašanih podatkov je varovana na nivoju radijskega dostopovnega omrežja. To pomeni, da ima uporabnik možnost nadzora nad tem, s kom želi komunicirati. Uporabnik prav tako mora vedeti, ali so mehanizmi za zagotavljanje varnosti dejansko vključeni: *vidnost* (visibility) vključenih varnostnih algoritmov. Uporabniki si želijo tudi *zasebnosti* (privacy). Večine povprečnih uporabnikov ne moti dejstvo, da je mogoče izslediti njihovo lokacijo. Zelo moteče pa bi bilo, če bi nekdo trajno beležil njihovo gibanje. Informacija o lokaciji pa bi bila zelo dobrodošla roparjem, ki bi med vlamljanjem lahko nadzorovali gibanje lastnika avtomobila. Zasebnost uporabniških podatkov je kritičnega pomena kadar se podatki prenašajo preko omrežja.

Razpoložljivost (availability) UMTS sistema je ključnega pomena za uporabnike, ker le ti plačujejo to storitev. Operaterji omrežja krmilijo omrežje in s tem skrbijo za *zanesljivost* (reliability) delovanja. *Celovitost* (integrity) omrežja zagotavlja signalizacija med overjenimi omrežnimi elementi. V splošnem celovitost preprečuje manipulacijo sporočil, kot je brisanje, vrivanje ali zamenjava le-teh.

Glavno orodje za zagotavljanje varnosti operaterjem omrežij in naročnikom je *šifriranje* (cryptography).

2.1. Dediščina iz omrežij prejšnjih generacij (1G, 2G)

Prehod iz sistemov 1G na digitalne sisteme 2G je, poleg mnogih drugih sprememb, omogočil uporabo razširjenih kriptografskih metod. Vsi osnovni varnostni mehanizmi 2G mobilnih sistemov so bili ohranjeni in po potrebi razširjeni:

- overovitev naročnika
- šifriranje na radijskem vmesniku
- zagotavljanje identitete naročnika6
- uporaba izmenljivega naročniškega modula
- varen kanal na aplikacijskem nivoju med uporabniškim modulom in domačim omrežjem
- transparentnost varnostnih mehanizmov
- minimalno potrebo po zaupanju med HE in SN

Uspeh GSM in preostalih 2G sistemov je potrdil ustreznost osnovnih varnostnih mehanizmov, vgrajenih v sisteme druge generacije. V sistemih 3G so uporabljene vse dobre lastnosti sistemov 2G.

Popularna tehnologija pa je vedno privlačna za goljufe. Lastnosti sistema GSM, ki so bile najbolj kritizirane, so naslednje:

- aktivni napadi napram omrežju so v principu mogoči. Nekdo, ki ima na razpolago primerno orodje, se lahko predstavlja kot legalnen omrežni element in/ali legalen terminal
- občutljive krmilne informacije, kot so ključi za kriptiranje na radijskem vmesniku, se prenaša v druga omrežja brez kodiranja
- nekateri postopki/deli varnostne arhitekture niso javni, ampak so poslovna skrivnost (kot denimo kriptografski algoritmi). Skrivanje tovrstnih informacij povzroča nezaupanje javnosti.
- ključi, uporabljeni z šifriranje radijskega vmesnika lahko postanejo ranljivi, če se odkrivanja loti večja skupina z metodo neposrednega preizkušanja vseh kombinacij (brute force).

Zgoraj naštete omejitve so v GSM sistemu ostale zavestno. Grožnje, jo vnašajo v sistem, se je razvijalcem zdela zanemarljiva naprav dodatnim stroškom, ki bi nastali ob odpravljanju le-teh. Tehnološki napedek, vedno spretnejši napadalci in vedno boljša orodja, uporabljena za vdore, pa so v obdobju, ko se je začel razvijati sistem 3G premaknila jeziček na tehtnici. Zaradi novih oziroma hujših groženj so se odločili zagotoviti bolj fleksibilne varnostne algoritme, kot so bili načrtovani v GSM omrežju. Odprava pomanjkljivosti sistemov 2G torej predstavlja drugo vodilo pri razvoju sistemov 3G:

- medsebojno overjanje naročnika **in omrežja**
- uporaba začasnih identitet
- šifriranje na radijskega dostopovnega omrežja
- zaščita integritete signalizacije znotraj UTRANa

Podrobneje si bomo vodila za razvoj varnostnih mehanizmov ogledali v nadaljevanju.

Šifrirni algoritmi, ki so uporabljeni v sistemih 3G za šifriranje in zaščito integritete, so javno dostopni. Algoritmi, ki se uporabljajo za medsebojno overjanje so prepuščeni v izbiro operaterju.

2.2. Namen varnostnih mehanizmov v sistemih 3G

Varnostni mehanizmi so v sistemih 3G implementirani z naslednjim namenom:

- zagotoviti, da so informacije, ki jih generirajo uporabniki ali pa uporabnikom pripadajo, dovolj zaščitene pred zlorabo ali nepravilnostmi
- zagotoviti, da so sredstva in storitve, ki jih ponuja omrežje storitev in domače okolje dovolj zaščitena pred zlorabo in nepravilnostmi
- zagotoviti, da so varnostni mehanizmi standardizirani in združljivi preko celotnega sveta (to pomeni, da mora biti s standardi zagotovljen vsaj en tak šifrirni algoritem, ki ga je možno izvažati in uvažati po celem svetu)
- zagotoviti, da so varnostni mehanizmi dovolj dobro standardizirani, da zagotavljajo medsebojno delovanje in gostovanje med različnimi strežnimi omrežji.

- uporabnikom in ponudnikom storitev zagotoviti boljšo stopnjo zaščite, kot jo ponujajo današnja fiksna in mobilna omrežja
- zagotoviti nadgradnjo in razširljivost varnostnih mehanizmov sistemov 3G v skladu z razvojem groženj in storitev

Glavno vodilo pri razvoju varnostnih mehanizmov predstavljajo uporaba takšnih storitev, ki jim je mogoče zagotoviti pravno podlago za njihovo izvršbo. Ovira, ki se pojavlja je neenotnost zakonodaje na različnih področjih, posledice česar si bomo ogledali ob koncu seminarske naloge.

2.3. Vloge v sistemih 3G

V sistemih tretje generacije med seboj sodeluje več udeležencev. V tem razdelku napravimo njihovo razdelitev iz varnostne perspektive ter opisali njihove vloge. Na ta način lažje identificiramo grožnje in ugotavljamo varnostne mehanizme, potrebne za odpravo ugotovljenih groženj. Sodelujoči udeleženci sovpadajo z logičnimi entitetami; ne pomenijo delitve na komercialne entitete, ljudi ali druge entitete iz fizičnega sveta, marveč so elementi iz navedenih skupin zaradi skupnih lastnosti pogosto združene v isto skupino ali obratno, en element iz fizičnega sveta lahko pripada več varnostnim entitetam. Tako, na primer, lahko podjetje predstavlja domače okolje (home environment), kot tudi omrežje storitev (serving network). Človek lahko predstavlja naročnika (subscriber) in uporabnika (user).

3G varnostni mehanizmi temeljijo na uporabi fizične naprave za zaščito, ki se imenuje UICC (UMTS Integrated Circuit Card). Le to je možno vstaviti in odstraniti iz terminala. Kartica vsebuje eno ali več aplikacij, od katerih mora vsaj ena biti USIM (User Services Identity Module).

2.3.1. Domena uporabnikov (User domain)

Naročnik (Subscriber): je oseba ali druga entiteta, ki je povezana z domačim okoljem in je odgovorna za plačilo stroškov v tem domačem okolju (kateri lahko nastanejo pred ali pa po uporabi določene storitve)

Uporabnik (User): oseba ali druga entiteta, ki je avtorizirana za uporabo 3G storitev s strani naročnika. Njegova uporaba je omejena in definirana v njegovem uporabniško storitvenem profilu. Uporabnik ima lahko omejen dostop do svojega uporabniškega profila, v katerem lahko določa parametrom posameznim storitvam.

Tretja oseba (Other Party): telekomunikacijski uporabnik, ki je bodisi v kličoč 3G uporabnika ali klican od 3G uporabnika. Tovrstna stranka ni nujno 3G uporabnik, a vendar lahko obstajajo pravni okviri, ki določajo stopnjo zaščite takšnim uporabnikom.

2.3.2. Domena infrastrukture (Infrastructure domain)

Domače okolje (Home Environment): je glavni nosilec odgovornosti pri zagotavljanju storitev uporabnikom, ki so pooblaščeni s strani naročnikov.

Domače okolje svojim naročnikom zagotavlja naslednje:

- zagotavlja, dodeljuje in upravlja z naročniškimi računi, uporabniško identiteto, uporabniškimi številkami in zaračunavanjem
- zagotavlja in vzdržuje uporabniške profile in omogoča uporabnikom pooblaščen dostop do njih
- pogajanje z operaterji omrežij za združljivost potrebno za zagotavljanje 3G storitev ter zagotavljanje pravilne identifikacije uporabnikov, njihove lokacije, overovitve in avtorizacije, preden se jim ponudi posamezne storitve.

Strežno omrežje (Serving Network): zagotavlja radijske zmogljivosti, upravljanje mobilnosti in preklapljanje (switching) ter usmerjanje (routing). Omrežje ponuja svoje zmožnosti domačim okoljem.

Odgovornosti strežnih omrežij se delijo v štiri področja:

- zagotavljanje in upravljanje radijskih zmogljivosti, vključno s šifriranjem nosilcev za zagotavljanje zaupnosti uporabniškega prometa
- zagotavljanje in upravljanje fiksnih zmogljivosti, prenosnih zmogljivosti, povezav in usmerjanja
- zbiranje podatkov, potrebnih za obračunavanje storitev in posredovanje le teh domačim okoljem in ostalim operaterjem omrežij
- domačim omrežjem s svojimi storitvami omogoča identifikacijo, overovitev, avtorizacijo in lokacijo uporabnikov.

Ponudniki storitev z dodano vrednostjo (Value added Service Provider - VASP): Naročnik se lahko naroči na storitve ponudnikov storitev z dodano vrednostjo, ki so popolnoma neodvisne od domačega okolja in jih z njim veže le to, da so storitve domačega okolja uporabljene za dostop do storitev VASP ponudnikov.

2.3.3. Domena Ne-3G infrastrukture (Non-3G infrastructure domain)

Ne-3G omrežni operaterji: ponujajo storitve, ki ne spadajo v razred 3G storitev. Varnost v 3G omrežjih ne sme biti odvisna od tovrstnih operaterjev (če se varnostni parametre prenašajo iz enega omrežja 3G v drugo omrežje 3G preko vmesnega omrežja, ne pričakujemo, da nam bo integriteto ali zaupnost zagotavljalo to vmesno omrežje).

2.3.4. Zunanji udeleženci (Off-line parties)

Regulatorji (Regulators): so organi, ki so pooblaščeni za pisanje zakonov in izdajo priporočil z zvezi z zagotavljanjem in uporabo 3G storitev, terminalov in omrežne opreme. Primer tovrstnih organizacij so državne vlade in njihove agencije (nacionalna agencija za varnost, uprave za telekomunikacije, ipd.)

2.3.5. Vsiljivci (Intruders):

Vsiljivci (Intruders): so tisti, ki želijo ogroziti, uničiti ali na kakršen koli drug način zlorabiti zaupnost, integriteto ali dostopnost 3G omrežij ali ogoljufati uporabnike, domače okolje ali strežno omrežje. Nevšečnosti, ki jih povzročajo vsiljivci so opisane v nadaljevanju.

2.4. Grožnje varni komunikaciji v mobilnih omrežjih

V tem poglavju bomo našteli potencialne grožnje, ki pretijo varnosti v 3G sistemih, jih definirali, navedli, kje v sistemu se pojavljajo in kdo so njihovi nosilci.

Grožnje je mogoče razdeliti v več različnih pogledih. Standardizacija jih deli v naslednje kategorije:

Nepooblaščen dostop do občutljivih informacij – kršitev zaupnosti (violation of confidentiality)

- **Prisluškovanje (eavesdropping):** Vsiljivec prestreza sporočila.
- **Pretvarjanje (masquerading):** Vsiljivec pretenta avtoriziranega uporabnika, da je legitimen element sistema in na ta način od njega pridobi zaupno informacijo. Prav tako lahko vsiljivec pretenta legitimen sistem, da je avtoriziran uporabnik in se na ta način dokoplje do storitev ali zaupnih informacij, do katerih bi sicer ne imel dostopa.
- **Prometna analiza (Trafic analysis):** Vsiljivec nadzoruje čas, pogostost, dolžino, izvor in ponor sporočil ter na ta način določa uporabniško lokacijo ali pa določa, kdaj je prišlo do posameznih transakcij.
- **Pregledovanje (Browsing):** Vsiljivec preišče občutljive informacije med shranjenimi podatki.
- **Uhajanje (Leakage):** Vsiljivec pridobi informacije s pomočjo procesa, ki ima legitimen dostop do informacij.
- **Sklepanje (Inference):** Vsiljivec opazuje reakcijo na pošiljanje poizvedb ali signalov v sistem. Vsiljivec lahko, na primer, s poskusom aktivne vzpostavitve komunikacijske seje in s pomočjo opazovanja časa, pogostosti, dolžine, izvora in ponora sporočil pridobi informacije o radijskih vmesnikih sistema.

Nepooblaščeno spreminjanje občutljivih podatkov - kršitev integritete (violation of integrity)

- **Spreminjanje sporočil (Manipulation of messages):** Vsiljivec lahko namerno spremeni, vrine ponovi ali izbriše sporočilo

Motenje ali zloraba mrežnih storitev (ki vodijo v zmanjšano dostopnost ali nedostopnost storitev)

- **Poseganje (Intervention):** Vsiljivec prepreči uporabo storitev avtoriziranemu uporabniku z motenjem prometa, signalizacije ali krmilnih informacij.
- **Izraba virov (Resource Exhaustion):** Vsiljivec prepreči avtoriziranemu uporabniku dostop do storitve s preobremenitvijo storitve.
- **Zloraba privilegijev (Misuse of privileges):** Uporabnik ali strežno omrežje lahko zlorabi svoje privilegije za dostop do neavtoriziranih storitev ali informacij.
- **Zloraba storitev (Abuse of services):** Vsiljivec lahko zlorabi posebne storitve ali pripomočke za pridobitev prednosti ali povzročitev prekinitve omrežja

Zavračanje (Repudiation): Uporabnik ali omrežje zanika dogodke, ki so se zgodili.

Nepooblaščen dostop do storitev:

- Vsiljivec dostopa do storitev s pretvarjanjem kot uporabnik al omrežna entiteta
- Uporabnik ali omrežna entiteta pridobi neavtorziran dostop do storitev z zlorabo svojih dostopnih pravic

Grožnje, navedene v zgoraj naštetih kategorijah se lahko razdelijo glede na nivo v katerem pride do napada:

- Radijski vmesnik
- Preostali deli sistema
- Terminali in UICC/USIM

2.4.1. Grožnje, povezane z napadi na radijski vmesnik

Radijski vmesnik med terminalsko opremo in strežnim omrežjem predstavlja precej izpostavljeno točko pred napadi v sistemih 3G. Grožnje, povezane z napadi na radijski vmesnik lahko razvrstimo v naslednje tri kategorije:

- Nepooblaščen dostop do podatkov
    - Prisluškovanje podatkom
    - Prisluškovanje signalizaciji in krmilnim informacijam
    - Pretvarjanje za komunikacijsko entiteto
    - Pasivna analiza prometa
    - Aktivna analiza prometa
- Grožnje integriteti
    - Spreminjanje uporabniškega prometa
    - Spreminjanje signalizacije in krmilnih informacij
- Nedostopnost storitev (denial of service)
    - Fizično poseganje
    - Protokolno onemogočanje
    - Nedostopnost storitev zaradi pretvarjanja komunikacijskih entitet
- Nepooblaščen dostop do storitev
    - Pretvarjanje kot drug uporabnik

2.4.2. Grožnje, povezane z napadi na preostale dele sistema

Čeprav napadi na radijski del predstavljajo glavno nevarnost, so prav tako lahko prizadejani tudi napadi na preostale dele sistema. To vključuje napade na preostale brezžične vmesnike, na ožičene vmesnike in napade, ki jih ne moremo omejiti na en sam vmesnik ali točko. Grožnje, povezane z napadi na preostale dele sistema so podobne grožnjam na radijskem vmesniku, le da se dogajajo na drugih nivojih sistema in jih prav tako lahko razdelimo v naslednje kategorije:

- Nepooblaščen dostop do podatkov
    - Prisluškovanje podatkom
    - Prisluškovanje signalizaciji in krmilnim informacijam
    - Pretvarjanje za predvidenega sprejemnika podatkov
    - Pasivna analiza prometa
    - Nepooblaščen dostop do podatkov, shranjenih v sistemu
    - Zbiranje podatkov o lokacijah uporabnikov
- Grožnje integriteti
    - Spreminjanje uporabniškega prometa
    - Spreminjanje signalizacije in krmilnih informacij
    - Spreminjanje s pretvarjanjem kot komunikacijska entiteta
    - Spreminjanje z aplikacijami in podatki, naloženimi na terminal ali USIM
    - Spreminjanje obnašanja terminala s pomočjo pretvarjanja kot avtor (upravljalec) aplikacij
    - Spreminjanje podatkov, ki jih shranjujejo sistemske entitete
- Nedostopnost storitev (denial of service)
    - Fizično poseganje
    - Protokolno onemogočanje
    - Nedostopnost storitev zaradi pretvarjanja komunikacijskih entitet
    - Zloraba storitev namenjenih za uporabo v sili (USIM-less)
- Zavračanje
    - Zanikanje plačila
    - Zanikanje oddajanja prometa
    - Zanikanje prejemanja prometa
- Nepooblaščen dostop storitev
    - Pretvarjanje kot drug uporabnik
    - Pretvarjanje kot strežno omrežje
    - Pretvarjanje kot domače okolje
    - Zloraba uporabniških pravic
    - Zloraba pravic strežnega omrežja

2.4.3. Grožnje, povezane z napadi na terminale in UICC/USIM

- Uporaba ukradenih terminalov in UICC
- Uporaba izposojenih terminalov in UICC
- Uporaba ukradenih terminalov
- Spreminjanje identitete ukradenim terminalom
- Kršitev integritete podatkov na terminalih
- Kršitev integritete podatkov na USIM
- Prisluškovanje UICC-terminalskem vmesniku
- Pretvarjanje za predvidenega prejemnika podatkov na UICC-terminalskem vmesniku
- Zaupnost overovitvenih podatkov na UICC/USIM
- Zaupnost specifičnih podatkov v teminalu ali na UICC/USIM

Med najhujše grožnje sodijo prisluškovanja in pasivne analize prometa in signalizacije, pretvarjanje za komunikacijsko entiteto, uporabnika ali strežno omrežje ter uporaba ukradenih terminalov in UICC. Tako lahko, glede na dosedanje izkušnje iz mobilnih omrežij, večino znatnejših groženj razvrstimo v le naslednje skupine:

Pretvarjanje – kot drug uporabnik za pridobitev neavtoriziran dostop
Prisluškovanje – omogoča vdor v zaupne uporabniške podatke
Naročniške prevare – vsiljivci zlorabijo storitve brez namena poravnati nastale stroške

Napadi postajajo vse bolj kompliciran. Vse pogostejši so aktivni napadi, ki uporabljajo tehniki prisluškovanja in pretvarjanja. Napadalci spreminjajo in oddajajo lažno signalizacijo (promet na radijskem vmesniku) ter se pretvarjajo kot bazna postaja.

2.5. Zahteve za varno komunikacijo

Oglejmo si zahtev za varno komunikacijo, ki so krojile razvoj sistemov 3G. Bile so razvite na podlagi analize v prejšnjem poglavju navedenih groženj. Vsaka izmed groženj namreč postavlja varnostne zahteve, s katerimi onemogočimo njeno izvedbo.

2.5.1. Zahteve za varnost 3G storitev

2.5.1.1. Zahteve za varen dostop do storitev

- Za dostop do 3G storitev je potrebno imeti veljaven USIM. Izjema so nujni klici, katere naj bi omrežje omogočalo tudi brez uporabe USIM modula.
- Sposobnost preprečevanja vsiljivcem, da pridobijo nepooblaščen dostop do 3G storitev s pretvarjanjem kot pooblaščeni uporabniki.
- Zmožnost, da uporabniki preverijo, ali je strežno omrežje avtorizirano za ponujanje 3G storitev za uporabnikovo domače okolje in sicer na začetku in med uporabo ponujene storitve.

2.5.1.2. Zahteve za varno zagotavljanje storitev

- Zmožnost, da ponudniki storitev overijo uporabnika na začetku in med uporabo storitev ter na ta način onemogočijo vsiljivcem nepooblaščen dostop do ponujenih storitev
- Zmožnost zaznavanja in odpravljanja sleparske uporabe storitev. Z alarmom je potrebno opozoriti ponudnika storitev. Potrebno je beležiti poročila o dogodkih.
- Zmožnost preprečevanja dostopa posameznim USIM do 3G storitev.
- Zmožnost takojšnega odklopa vseh storitev, ki jih domače okolje ponuja določenim uporabnikom, tudi tistih, ki jih ponujajo strežna omrežja.
- Sposobnost strežnih omrežij, da preverjajo izvor uporabniškega prometa, signalizacijo podatkov in krmilne podatke na radijskih vmesnikih.

- Sposobnost preprečevanja, da vsiljivci omejujejo dostopnost storitev uporabnikom.
- Zagotovljena mora biti varna infrastruktura med omrežnim operaterjem, načrtovana tako, da so potrebe domačega okolja glede zaupanja v strežno omrežje glede varnosti minimalne.

2.5.2. Zahteve za zagotavljanje sistemske integritete

- Zagotavljanje zaščite pred neavtoriziranimi spremembami uporabniškega prometa.
- Zagotavljanje zaščite pred neavtoriziranimi spremembami signalnih in krmilnih informacij, posebno na radijskih vmesnikih
- Zagotavljanje zaščite pred neavtoriziranimi spremembami uporabniških podatkov, naloženih in shranjenih v terminalu ali USIM
- Zagotavljanje zaščite pred neavtoriziranimi spremembami uporabniških podatkov, obdelanih in shranjenih pri ponudniku storitev
- Zagotavljanje podatka o viru in integriteti aplikacij in podatkov, naloženih na terminal in UICC ter zmožnost preverjanja le-teh. Prav tako je potrebno zagotoviti njihovo zaupnost.
- Zagotavljanje izvora, integritete overovitvenih podatkov, posebej šifrirnega ključa (chiper key), na radijskem vmesniku.
- Zagotavljanje varne infrastrukture med operatorji

2.5.3. Zahteve za zaščito osebnih informacij

2.5.3.1. Varnost uporabniških podatkov, ki se prenašajo prek omrežja

- Zmožnost zagotavljanja zaupnosti uporabniškim podatkom, posebno na radijskem vmesniku.
- Zmožnost zagotavljanja zaupnosti signalnim in krmilnim podatkom, posebno na radijskem vmesniku.
- Zmožnost zagotavljanja zaupnosti podatkov o identiteti uporabnikov, posebno na radijskem vmesniku.
- Zmožnost zagotavljanja zaupnosti podatkov o lokaciji uporabnikov, posebno na radijskem vmesniku.
- Sposobnost, da uporabnik preveri, ali so njegovi podatki in z njim povezane informacije med prenosom zaščitene. Preverjanje mora zahtevati minimalen napor s strani uporabnika.

2.5.3.2. Varnost uporabniških podatkov, ki so shranjeni v sistemu

- Zmožnost zagotavljanja zaupnosti uporabniškim podatkom, ki jih shranjuje ali procesira ponudnik.
- Zmožnost zagotavljanja zaupnosti uporabniškim podatkom, shranjenih na uporabniškem terminalu ali USIM.

2.5.4. Zahteve za terminal in USIM

2.5.4.1. Varnost terminala

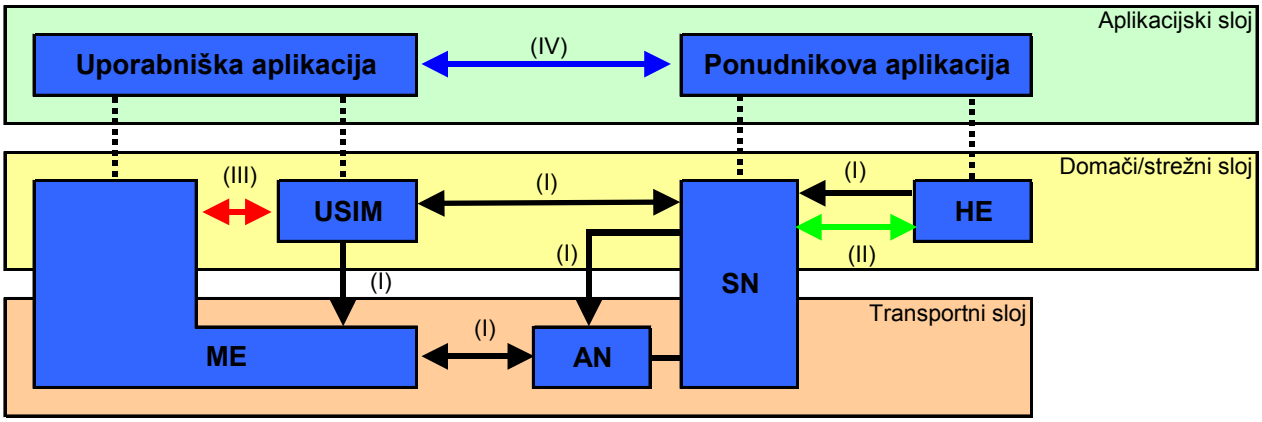
- Terminal mora odvračati od kraje.
- Zmožnost onemogočanja dostopa do 3G storitev na posameznih terminalih.
- Onemogočeno spreminjanje identitete terminalov z namenom, da bi zaobšli prepoved dostopa do storitev iz določenih terminalov.

2.5.4.2. Varnost USIM

- Zmožnost omejevanja dostopa do USIM. Na ta način je z USIM kartico omogočen dostop do 3G storitev samo tistim uporabnikom, ki so eksplicitno avtorizirani s strani naročnika.
- Zmožnost omejevanja dostopa do podatkov, shranjenih na USIM. Nekateri podatki, na primer, so dostopni samo avtoriziranemu domačemu okolju.
- Nezmožnost dostopa do podatkov, shranjenih na USIM, ki so namenjeni uporabi znotraj samega USIM, kot so šifrirni ključi in algoritmi

3. Pregled varnostne arhitekture

Slika 3.1 nam prikazuje pregled 3G varnostne arhitekture.



Slika 3.1: Pregled varnostne arhitekture v 3G (vir [2])

Definiranih je pet varnostnih skupin. Vsaka izmed njih rešuje probleme določene skupine groženj in podpira pripadajoče varnostne zahteve:

- **Varen dostop do omrežja – I (Network access security)**

Skupina varnostnih lastnosti, ki zagotavlja uporabnikom varen dostop do 3G storitev in jih ščiti pred napadi na radijskem (dostopovnem) nivoju.

- **Varnost omrežne domene – II (Network domain security)**

Skupina varnostnih lastnosti, ki omogočajo vozliščem domene ponudnika, da med seboj varno izmenjujejo signalizacijske podatke in ščitijo pred vdorom v brezžično omrežje.

- **Varnost uporabniške domene – III (User domain secutiy)**

Skupina varnostnih lastnosti, ki ščitijo dostop do mobilnih postaj.

- **Varnost aplikacijske domene – IV (Application domain secutiy)**

Skupina varnostnih lastnosti, ki omogoča aplikacijam iz uporabniške in ponudnikove domene varno izmenjavo sporočil.

- **Vidnost in nastavljivost varnosti – V (Visibility & Configurability of Security)**

Skupina varnostnih lastnosti, ki omogoča uporabnikom, da preverijo katere varnostne lastnosti uporabljajo.

3.1. Varnostne lastnosti

3.1.1. Varen dostop do omrežja – I (Network access security)

3.1.1.1. Zaupnost identitete uporabnika

V povezavi z zagotavljanjem zaupnosti identitete uporabnika so razvite naslednje varnostne lastnosti:

- **Zaupnost identitete uporabnika (user identity confidentiality)**

Zagotavlja, da s prisluškovanjem radijskim povezavam ni mogoče odkriti podatkov o stalni identiteti uporabnika (permanent user identity – IMSI)

- **Zaupnost lokacije uporabnika (user location confidentiality)**

Zagotavlja, da s prisluškovanjem radijskim povezavam ni mogoče odkriti prisotnosti ali prihoda uporabnika na določeno fizično področje.

- **Neizsledljivost uporabnika (user untraceability)**

Zagotavlja, da s prisluškovanjem radijskim povezavam ni mogoče odkriti, ali so posamezne storitve namenjene določenim uporabnikom.

Da bi dosegli zgoraj navedene cilje, moramo uporabnika identificirati z začasno identiteto, s katero ga prepozna obiskano strežno omrežje. V izogib sledljivosti, ki lahko pripelje do razkritja uporabniške identitete, uporabnik ne sme predolgo uporabljati iste začasne identitete. Prav tako je, za doseganje zgoraj navedenih ciljev, nujno potrebno, da so vsi prenosi uporabniških podatkov in signalizacije, ki bi lahko razkrili uporabniško identiteto šifrirani na nivoju radijskega dostopa.

V nadaljevanju si bomo ogledali mehanizme, ki omogočajo uporabniku identifikacijo preko radijske poti z uporabo začasne identitete, s katero se identificira obiskanemu strežnemu omrežju. Mehanizem je običajno uporabljen za identifikacijo uporabnika na nivoju radijske zveze v zahtevah za osvežitev podatka o lokaciji, zahtevah za storitev, zahtevah za ločitev, zahtevah za ponovno vzpostavitev, itd.

3.1.1.2. Overovitev entitete

V povezavi z overjanjem entitete so razvite naslednje varnostne lastnosti:

- **Overjanje uporabnika (user authentication)**

Lastnost, s katero strežno omrežje potrdi uporabniško identiteto uporabnika

- **Overjanje omrežja (network authentication)**

Lastnost, s katero uporabnik potrdi, da je priključen na strežno omrežje, ki je overjeno s strani uporabnikovega domačega okolja za zagotavljanje storitev.

Da dosežemo zgoraj navedena cilja je potrebno izvesti overoverovitev slehernikrat, ko vzpostavljamo zvezo med uporabnikom in omrežjem. Uporabljena sta dva mehanizma: overovitveni mehanizem z uporabo overovitvenega vektorja, dodeljenega s strani uporabniškega HE strežnemu omrežju in overovitveni mehanizem, ki uporablja integritetni ključ, pridobljen od uporabnika in strežnega omrežja med prejšnjo izvedbo overovitve in proceduro pridobivanja ključa. Mehanizme si bomo podrobneje ogledali v nadaljevanju.

3.1.1.3. Zaupnost

Ob overjanjem entitete se izvedejo naslednje varnostne lastnosti:

- **Dogovor o šifrirnem algoritmu (chiper algorithm agreement)**

MS in SN se dogovorita o algoritmu, ki ga uporabita za šifriranje informacij.

- **Dogovor o šifrirnem ključu (chiper key agreement)**

MS in SN se dogovorita o šifrirnem ključu, ki ga uporabljata.

- **Zaupnost uporabniških podatkov (confidentiality of user data)**

Uporabniškim podatkom ni mogoče prisluškovati na radijskem vmesniku.

- **Zaupnost signalizacijskih podatkov (confidentiality of signalling data)**

Signalizacijskim podatkom ni mogoče prisluškovati na radijskem vmesniku.

Dogovor o šifrirnem ključu se sprejme med izvajanjem mehanizma za overjanje in dogovarjanje o ključu (AKA). Dogovor o šifrirnem algoritmu je del mehanizma za varen načina posredovanja med uporabnikom in omrežjem. Več o obeh bomo govorili v nadaljevanju.

3.1.1.4. Integriteta podatkov

V povezavi z integriteto podatkov na omrežnem nivoju so razvite naslednje varnostne lastnosti:

- **Dogovor o algoritmu za zagotavljanje integritete (integrity algorithm agreement)**

MS in SN se dogovorita o algoritmu, ki ga uporabita za zagotavljanje integritete.

- **Dogovor o ključu za zagotavljanje integritete (integrity key agreement)**

MS in SN se dogovorita o ključu, ki ga uporabita za zagotavljanje integritete.

- **Podatkovna integriteta in izvorno overjanje signalizacijskih podatkov (data integrity and origin authentication of signaling data)**

Sprejemna entiteta (MS ali SN) je sposobna preveriti, da signalizacijske informacije niso bile nepooblaščeno spremenjene na poti od izvora do ponora in da so podatki o izvoru signalizacijskih informacij ujemajo z dejanskimi.

Tudi ključ za zagotavljanje integritete podatkov se določi med izvajanjem mehanizma za overjanje in dogovarjanje o ključu (AKA). Dogovor o algoritmu za zagotavljanje integritete pa se sprejme med izvajanjem mehanizma za varen načina posredovanja med uporabnikom in omrežjem. Več o obeh bomo govorili v nadaljevanju.

3.1.1.5. Identifikacija mobilne opreme

V določenih primerih lahko SN zahteva od MS, da ji pošlje podatke o identiteti mobilne opreme. Ti podatki se pošljejo po overovitvi SN (izjema so le nujni klici). IMEI je varno shranjen v terminalu. Predstavitev te identitete ni varnostna funkcija in prenos IMEI preko omrežja ni zaščiten.

3.1.2. Varnost omrežne domene – II (Network domain security)

V to skupino spadajo varnostnih lastnosti, ki omogočajo vozliščem domene ponudnika, da med seboj varno izmenjujejo signalizacijske podatke in ščitijo pred vdorom v brezžično omrežje.

Varnostni mehanizmi tega nivoja v časa pisanja seminarske naloge še niso bili določeni.

3.1.3. Varnost uporabniške domene – III (User domain secutiy)

3.1.3.1. Overjanje uporabnika s strani USIM

Lastnost zagotavlja, da je entiteta, ki želi uporabljati USIM, omejena toliko časa, dokler ni USIM ne overi uporabnika. To zagotavlja, da je dostop do SIM omejen le na pooblaščene uporabnike. Za izvedbo overjanja si morata uporabnik in USIM deliti skrivnost (PIN), ki je varno shranjena v USIM. Uporabnik pridobi dostop do USIM samo, če pozna pravi PIN.

3.1.3.2. Povezava med USIM in terminalom

Lastnost zagotavlja, da je dostop do terminala ali druge uporabniške opreme omejen samo na avtoriziran USIM. Za to morata terminal in USIM deliti skrivnost, varno shranjeno v terminalu in USIM. Če USIM ne pozna skrivnosti, ji je dostop do teminala onemogočen.

3.1.4. Varnost aplikacijske domene – IV (Application domain secutiy)

3.1.4.1. Varna sporočila med USIM in omrežjem

Z orodjem USIM Application Toolkit lahko operaterji ali drugi ponudniki izdelajo aplikacije, katere gostujejo na USIM (podobno, kot za sistem GSM obstaja aplikacija SIM Application Toolkit). Pojavlja se potreba po varnem prenosu sporočil, s katerimi prenesemo aplikacije na USIM preko omrežja s stopnjo varnosti, ki jo določi operater omrežja ali ponudnik aplikacij.

3.1.5. Vidnost in nastavljivost varnosti – V (Visibility & Configurability of Security)

3.1.5.1. Vidnost

Čeprav naj bi bile varnostne storitve v splošnem transparentne za uporabnika, je zaradi pomembnosti dogodkov v zvezi z varnostjo potrebno posvetiti večjo pozornost informiranju uporabnika o (ne)uporabi varnostnih storitev. Z varnostjo povezani dogodki so:

- Naznanitev uporabe omrežnega šifriranja – obvešča uporabnika o tem, da je njegovim podatkom zagotovljena zaupnost z izvedbo zaščite na radijskem vmesniku, še posebej takrat, ko je šifriranje izključeno.
- Naznanitev stopnje varnosti – obvešča uporabnika o stopnji varnosti, ki je uporabljena obiskanem strežnem omrežju, še posebej takrat, ko se uporabnik premakne v omrežje z nižjo stopnjo varnosti.

3.1.5.2. Nastavljivost

Uporabnik ima možnost nastavljati, kakšna stopnja varnosti ščiti uporabo storitev. Seveda je uporabnik omejen na nabor storitev, ki jih ponuja omrežje. Predlagane so naslednje zmožnosti nastavljanja:

- Vklop/izklop overjanja uporabnika s strani USIM
- Sprejemanje/zavračanje prihajajočih, nešifriranih klicev
- Vzpostavljanje/ne vzpostavljanje nešifriranih klicev
- Sprejemanje/zavračanje posameznih šifrirnih algoritmov

4. Mehanizmi za zaščito dostopa do omrežja

V mehanizem overjanja so vključeni trije osebki:

- Domače omrežje
- Strežno omrežje
- USIM

Osnovna ideja je da strežno omrežje preveri identiteto naročnika s pozivom in preveri njegov odziv. (Metodo si bomo ogledali v nadaljevanju). Terminal pa preveri, ali je strežno omrežje pooblaščeno s strani domačega omrežja, da lahko preverja njegovo identiteto (Na ta način USIM preveri, ali ji prijavljen v legitimno omrežje). Prav ta, zadnji del postopka, je novost v sistemu UMTS, če ga primerjamo s sistemom GSM.

Protokoli medsebojnega overjanja ne preprečujejo scenarija, podanega na naslovnici seminarske naloge. V kombinaciji z ostalimi mehanizmi pa zagotavljajo, da se aktivni napadalec v dani situaciji ne more okoristiti s podatki. Edina možnost zlorabe, ki še vedno preostane napadalcu, je motenje komunikacije, vendar pa ni nobenega protokola, s katerim bi mu omogočil tudi tovrstni napad, kajti v končni fazi bi napadalec lahko izvedel napad motenja širokega pasu frekvenčnega spektra.

Na začetku si oglejmo postopke idenitfikacije.
Stalna identiteta uporabnika v UMTS omrežju se imenuje IMSI, kot v GSM omrežju. Identifikacija uporabnika v UTRAN se večino časa izvaja z uporabo začasne identitete TMSI. Tovrstni pristop je ubran z željo po zagotavljanju zaupnosti uporabniške identitete. Izjema pa je prva registracija, ker takrat začasna identiteta še ne obstaja.

4.1. Identifikacija z začasno identiteto

Mehanizem omogoča identifikacijo uporabnika na radijski dostopovni povezavi z uporabo začasne mobilne naročniške identitete (temporary mobile subscriber identity – TMSI). TMSI je lokalen parameter, ki se uporablja le v področju, kjer je uporabnik registriran. Izven tega področja se uporablja v spremstvu pripadajočega indentifikatorja lokalnega področja (Location Area Identification – LAI) ali identifikatorja usmerjevalnega področja (Routing Area Identifier – RAI), da se izognemo zamenjavam. Preslikava med stalnim in začasnim identifikatorjem je zapisana v Visited Location Register (VLR/SGSN), v katerem je uporabnik registriran.

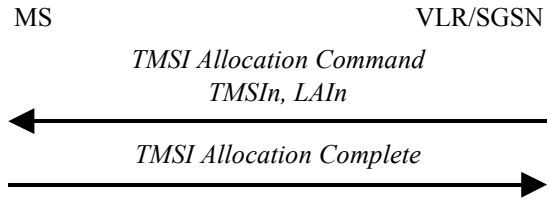
TMSI je, kadar je dosegljiv, običajno uporabljen za identifikacijo uporabnika na radijski dostopovni povezavi, kot denimo pri zahtevi za priklop, zahtevah za storitve, osvežitvah lokacije, zahtevah za ponovno vzpostavitev povezave, zahtevah za izklop, itd.

Postopki so podobni mehanizmom uporabljenih v sistemih GSM.

4.1.1. Postopek realokacije TMSI

Namen uporabe tega mehanizma je določiti par TMSI/LAI par uporabniku, s katerim se bo le-ta v nadaljevanju identificiral na radijski dostopovni povezavi.

Postopek se izvede po inicializaciji šifriranja. Sama izvedba šifriranja komunikacije preko radijske poti je opisano v nadaljevanju.



Slika 4.1: Zahteva za TMSI

Postopek začne VLR, ki generira novo začasno identiteto (TMSIn) in ga shrani skupaj s stalno identiteto IMSI v podatkovno bazo. TMSI mora biti nepredvidljiv. VLR pošlje novo število TMSIn in (če je potrebno) tudi lokacijski identifikator (LAIn) uporabniku.

Po sprejemu, uporabnik shrani TMSIn in avtomatično odstrani stari TMSI. Uporabnik pošlje potrdilo o sprejemu VLR.

Po sprejemu potrdila, tudi VLR odstrani staro TMSIo in IMSI iz podatkovne baze.

4.1.2. Nepotrjen sprejem začasne identitete

Če SN ne prejme potrditve o uspešnem sprejemu začasne identitete TMSI s strani uporabnika, potem mora omrežje voditi povezavo med novo identiteto TMSIn in IMSI ter med staro identiteto TMSIo in IMSI (v kolikor ta obstaja).

Kadar uporabnik predstavlja izvor transkacije, mora omrežje omogočiti uporabniku, da se identificira s staro začasno identiteto TMSIo ali novo začasno identitetno TMSIn. To omogoča omrežju, da ugotovi, katera začasna identiteta je shranjena v mobilni postaji. Omrežje v nadaljevanju izbriše povezavo med preostalo identiteto in IMSI, ter jo na ta način sprosti za ponovno uporabo z naslednjimi uporabniki.

Kadar pa omrežje predstavlja izvor transakcije, mora omrežje identificirati uporabnika z uporabo njegove stalne identitete (IMSI). Po vzpostavitvi radijske zveze omrežje obvesti uporabnika, naj izbriše shranjeni TMSI. Ko omrežje sprejme potrditev od uporabnika, izbriše povezavo med IMSI in vsemi TMSI v bazi; na ta način jih sprosti za ponovno uporabo z naslednjimi uporabniki.

Omrežje lahko kadarkoli zahteva ponovno izmenjavo TMSI podatkov.

4.1.3. Osvežitev lokacijskih podatkov

V primeru, ko se uporabnik identificira z uporabo TMSIo/LAIo para, ki mu je dodelil VLRn, le ta lahko iz baze določi pripadajoč IMSI. V ostalih primerih lahko VLRn zahteva od uporabnika, da se predstavi s stalno identiteto IMSI. Več o tem mehanizmu si bomo ogledali v nadaljevanju.

V primeru, ko se uporabnik identificira z uporabo TMSIo/LAIo para, ki mu ni bil dodeljen VLRn, kjer se uporabnik sedaj nahaja. V tem primeru morata VLRn in prejšnji VLRo izvesti izmenjavo overovitvenih podatkov, poleg tega pa VLRo pošlje VLRn tudi podatke o permanentni identiteti IMSI. Tudi o tem mehanizmu bo govora v nadaljevanju. Mehanizem je del mehanizma za distribucijo overovitvenih podatkov med VLR-ji. V kolikor

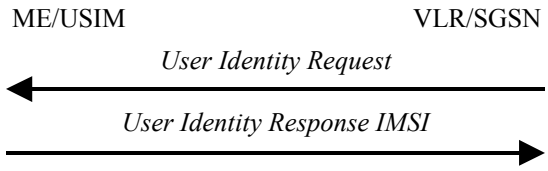
prej obiskanega VLR ni mogoče najti oziroma doseči, oziroma ni mogoče pridobiti podatkov o uporabnikovi identiteti, potem mora VLR za stalno identifikacijo IMSI zaprositi uporabnika samega.

4.2. Identifikacija s stalno identiteto

Ostal nam je še en problem: Kako strežno omrežje prejme IMSI pri prvi povezavi? Ker imajo začasne identitete pomen le lokalno, mora biti začasnim identitetam pripeta oznaka lokalnega področja (LAI), s čimer enolično identificiramo uporabnika. Če pa UE pride v novo področje, se mora TMSI prenesti iz pretekle lokacije. V kolikor to ni mogoče (naslov TMSI ni poznan ali pa se zveze s področjem, kjer se je uporabnik nahaja prej ni mogoče vzpostaviti) se mora uporabnik prijaviti z stalno identiteto – IMSI.

Mehanizem torej omogoča identifikacijo uporabnika na radijski dostopovni povezavi z uporabo stalne naročniške identitete (permanent subscriber identity – IMSI).

Sproži ga strežno omrežje v primeru, ko uporabnika ni mogoče identificirati z uporabo mehanizma za indentifikacijo z začasno identiteto. Tak primer je, denimo, prva prijava v omrežje ali pa, kadar omrežje ne more dobiti IMSI iz TMSI, s katerim se identificira uporabnik.



Slika 4.2: Identifikacija s stalno identiteto

VLR/SGSN od uporabnika zahteva stalno identiteto IMSI, uporabnik pa se odzove z IMSI v nešifriranem tekstu (cleartext). To predstavlja luknjo v zaupnosti uporabniške identitete.

Obstajajo prostori, kjer identifikacija z uporabo IMSI relativno pogosta (denimo letališča, kjer uporabniki prižigajo svoje mobilne terminale po pristanku). Sledenje ljudem na takem mestu bi bilo verjetno lažje na kak drug način (opazovanje potnikov, ki izstopajo iz letala).

Vidimo, da identifikacijski mehanizem ne zagotavlja 100% zaščite, zagotavlja pa relativno visok nivo varnosti. Zavedati se moramo, da tovrstna zaščita proti aktivnemu napadalcu ni uspešna, ker se nam le-ta lahko pretvarja kot novo strežno omrežje, kateremu uporabnik zaupa svojo stalno identiteto. Tudi mehanizem overjanja nam v tem primeru ne pomaga, kajti uporabnik se mora identificirati preden se začne postopek overjanja, opisan v nadaljevanju.

4.3. Overjanje (avtentikacija) in dogovor o ključih (key agreement)

Temeljni kamen overovitvenega mehanizma predstavlja *glavni ključ (master key)* ***K***, ki je zapisan na USIM in hkrati v podatkovni bazi domačega omrežja. Gre za 128 dolg parameter, ki mora biti skrbno varovan in nikoli ne zapusti omenjenih dveh lokacij. Uporabnik ključa ne more prebrati.

Kot bomo videli v nadaljevanju, se v postopku overjanja določita tudi ključa za šifriranje in zagotavljanje integritete. To so začasni ključi dolžine 128 bitov. Izpeljani so iz stalnega ključa ***K*** med vsakim overjanjem. Osnovno vodilo pri šifriranju je čim bolj redka uporaba stalnega ključa; le-to nadomesti uporaba izpeljanih ključev, s katerimi zaščitimo kose podatkov.

Naveden mehanizem zagotavlja medsebojno overovitev med uporabnikom in omrežjem. Oba morata namreč poznati skrivni ključ K, ki je shranjen samo na USIM in v AuC v uporabnikovem HE. Poleg tega imata USIM in HE vgrajena števca: SQN_{MS} in SQN_{HE}. Števca štejeta ločeno, potrebujemo pa ju za overovitev omrežja. Vsak uporabnik ima svoj SQN_{HE} števec, sekvenčna številka SQN_{MS} pa označuje največjo sekvenčno številko, ki jo je USIM sprejel.

Mehanizem je izbran tako, da zagotavlja kar se da veliko združljivosti z obstoječo varnostno arhitekturo GSM sistema ter s tem pospešuje prehod iz GSM na UMTS sistem. Mehanizem temelji na protokolu zahteva/odziv (challenge/response), ki je identičen overjanju GSM uporabnika in sporazumevanju o ključih združenih s protokolom, ki temelji na sekvenčnem štetju enkratnih prehodov za mrežno overjanje.

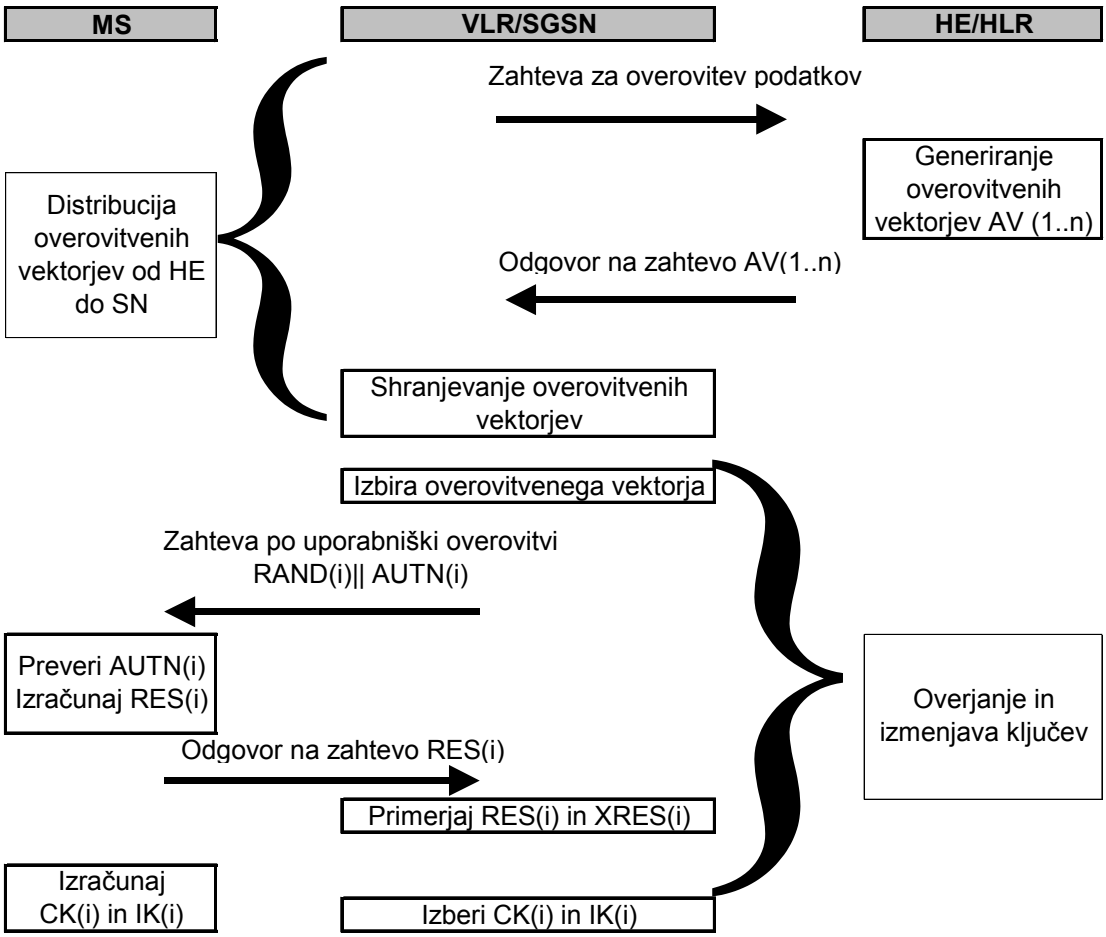
4.3.1. Izvedba

Overovitven postopek se prične, ko je uporabnik identificiran v strežnem omrežju. Identifikacija pomeni, da se TMSI ali IMSI prenese v VLR ali SGSN. VLR oziroma SGSN pošlje zahtevo za overjanje domačemu okolju HE. AuC domačega okolja HE se odzove z urejenim poljem *overovitvenih vektorjev (authentication vectors)*– kvinteti v UMTS sistemu (ekvivalentni "tripletom" v GSM sistemu), razvrščenim po sekvenčnih številkah, ki jih vrne VLR/SGSN v obliki *odziva overovitvenih podatkov (authentiation data response)*. Vsak overitveni vektor vsebuje naslednje komponente:

- Naključno število RAND – 128 bitov
- Pričakovan odziv na naključno število XRES – 32 do 128 bitov
- Šifrirni ključ CK – 128 bitov
- Integritetni ključ IK– 128 bitov
- Overovitveni žeton AUTN

Vsak overovitveni vektor je uporaben le za eno overjanje in dogovarjanje o ključih med VLR/SGSN in USIM.

Proces je razviden na Slika 4.3. Kontrolna sporočila se prenašajo z uporabo MAP protokola.



Slika 4.3: Overjanje in dogovarjanje o ključih (vir [2])

Ko VLR/SGSN začne overjanje in dogovarjanje o ključih, izbere naslednjega izmed vektorjev urejenega polja in pošlje uporabniku zahtevo po uporabniški overovitvi. Ta vsebuje parametra RAND in AUTN. Overovitveni vektorji posameznega vozlišča so uporabljeni po FIFO metodi. USIM preveri, če lahko sprejme AUTN podatek in če ga lahko, potem se na RAND podatke odzove z RES odgovorom, ki ga pošlje VLR/SGSN. USIM izračuna še ključa CK in IK. VLR/SGSN primerja prejet RES podatek s podatkom XRES in če se ujemata, to pomeni uspešen zaključek overjanja. USIM in VLR/SGSN dostavita ključe CK in IK entitetam, ki želijo zagotavljati šifriranje in integriteto.

Z uporabo izračunanih šifrirnih in integritetnih ključev lahko VLR/SGSN zagotavlja varnostne storitve tudi kadar HE/AuC ni dosegljiv. Overjanje se v tem primeru izvaja s pomočjo integritetnih ključev, ki zagotavljajo zaščito podatkovne integritete signalizacijskim sporočilom.

Pri overjanju torej sodelujeta USIM in AuC uporabnikovega domačega okolja (HE/AuC). Mehanizem se izvede po naslednjem postopku:

- Distribucija overovitvenih podatkov od HE/AuC do VLR/SGSN. Ogledali si jo bomo v nadaljevanju. Uporabnikovo domače okolje mora zaupati VLR/SGSN, da bo varovala overovitvene informacije. Prav tako se pričakuje, da so notranje povezave

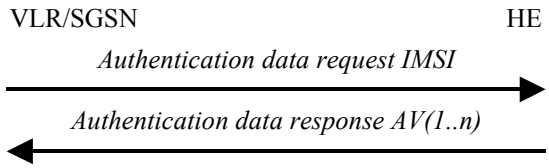
(intra-system links) med VLR/SGSN in HE/AuC primerno varovane. Tudi uporabnik mora zaupati svojemu domačemu okolju HE.

- Medsebojno overjanje in izmenjava novih šifrirnih in integritetnih ključev med VLR/SGSN in MS, prav tako opisana v nadaljevanju.
- Distribucija overovitvenih podatkov od prejšnjega VLR novemu VLR. Zopet so privzete dovolj varne povezave med VLR/SGSN-ji.

Podrobneje si oglejmo posamezne operacije, ki sestavljajo AKA:

4.3.2. Generiranje in distribucija overovitvenih podatkov

Namen postopka je preskrbeti VLR/SGSN s svežimi overovitvnimi vektorji iz uporabnikove HE za izvedbo več uporabniških overjanj.

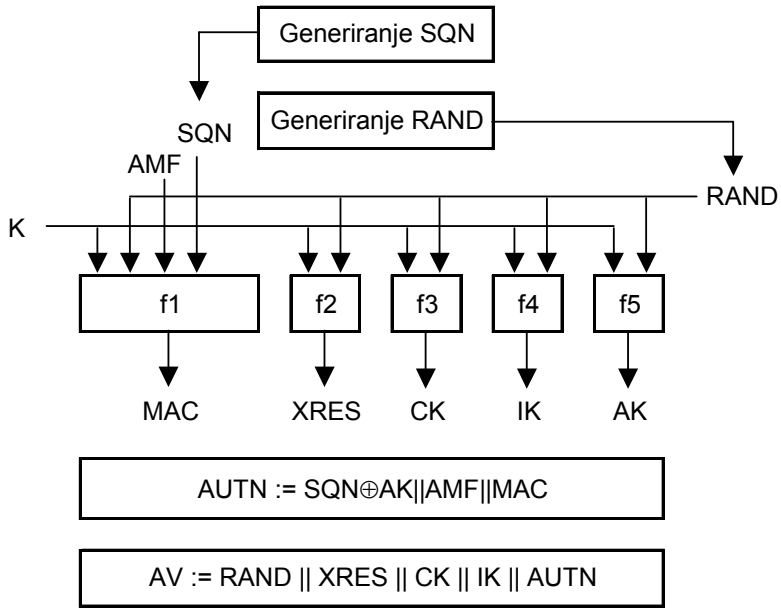


Slika 4.4: Distribucija overovitvenih podatkov med HE in VLR/SGN

VLR/VSGN sproži postopek z zahtevo za overovitvene vektorje, katero pošlje HE/AuC.

Zahtevek za overovitev podatkov vsebuje tudi IMSI.

Po sprejetju zahtevka, HE odgovori z željenim številom overovitvenih vektorjev. Le te že lahko ima pripravljene in jih pošlje kar direktno iz HLR, lahko pa jih izračuna na zahtevo.



Slika 4.5: Postopek generiranja ključev

HE/AuC pošlje po sekvenčnih številkah urejeno polje overovitvenih vektorjev AV(1..n).

Center za overjanje (AuC) uporabnikovega domačega okolja začne proces z generiranjem sveže sekvenčne številke SQN (še ne uporabljene pred tem, ločeno jo obravnava za vsakega

uporabnika posebej) in nepredvidljivega števila RAND. Generiranje nepredvidljivega števila je zahtevna naloga.

HE sicer ima nekaj protosti glede uporaljanja s sekvenčnimi števili, izpolnjevati pa mora naslednje pogoje:

- Mehanizem generiranja mora omogočati ponovno sinhronizacijo
- V kolikor SQN identificira lokacijo uporabnika, je potrebno uporabiti AK s katerim se le ta zakrije
- Mehanizem mora imeti vgrajeno zaščito proti obrnitvi števca na USIM modulu.

Za izračun overovitvenega vektorja se uporabljajo t.i. enosmerne funkcije (one-way functions). To so funkcije, katere se relativno hitro izračunajo, vendar pa jih je praktično nemogoče invertirati. Tako z vhodnimi parametri enostavno izračunamo izhodne parametre, če pa poznamo zgolj izhodne parametre pa ne obstaja algoritem, s pomočjo katerega bi se dokopali do vhodnih parametrov. Obstaja nam le »najpreprostejši« algoritem, pri katerem preizkusimo vse vhodne kombinacije in iščemo želeno izhodno vrednost. Glede na dolžino vektorjev pa je ta algoritem, imenovan tudi »brute force attack« neučinkovit.

Za izračun celotnega overovitvenega vektorja uporabljamo pet enosmernih funkcij, opisanih v nadaljevanju. $f1_K$ se od ostalih štirih razlikuje po številu vhodnih parametrov. Ker imajo enako skupno lastnost (enosmernost) so zgrajene okrog ene same glavne (core) funkcije. Med seboj se funkcije fundamentalno razlikujejo. Iz izhodnih podatkov ene funkcije ne moramo sklepati prav nič o tem, kakšni so izhodni podatki preostalih funkcij.

Funkcije izračunajo naslednje parametre overovitvenega vektorja:

- Koda za overjanje sporočila (64 bitov) **MAC**=$f1_K$(SQN||RAND||AMF), kjer f1 predstavlja funkcijo za overjanje sporočil
- Pričakovan odziv (32 do 128 bitov) **XRES**=$f2_K$ (RAND), kjer f2 predstavlja navadno okrnjeno funkcijo za overjanje sporočil
- Šifrirni ključ (128 bitov) **CK**=$f3_K$(RAND), kjer f3 predstavlja funkcijo za generiranje ključa
- Ključ za zagotavljane integritete (128 bitov) **IK**=$f4_K$(RAND), kjer f4 predstavlja funkcijo za generiranje ključa
- Ključ za zagotavljanje anonimnosti (64 bitov) **AK**=$f5_K$(RAND), kjer f5 predstavlja funkcijo za generiranje ključa ali pa je f5≡0.

Na tem mestu napravimo še pregled ostalih parametrov, ki se uporabljajo in njihovih dolžin:

- Glavni overovitveni ključ (128 bitov) ***K***
- Naključni poziv (128 bitov) **RAND**
- Sekvenčna številka (48 bitov) **SQN**
- Polje za upravljanje z overjanjem (16 bitov) **AMF**
- Koda za overjanje sporočila (64 bitov) **MAC in MAC-S**
- Overovitveni žeton (128 bitov) **AUTN**

Iz izračunanih podatkov se zgradi overovitveni žeton AUTN = SQN⊕AK||AMF||MAC.

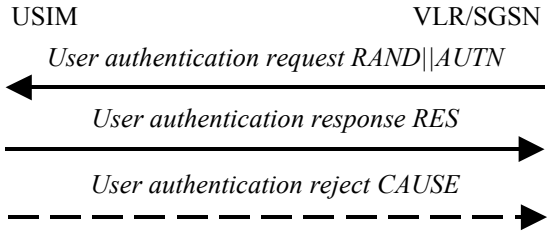
Ključ za zagotavljanje anonimnosti se uporablja za zakrivanje sekvenčne številke, ki bi lahko izdala identiteto ali lokacijo uporabnika. Uporablja se za zaščito pred pasivnimi napadi. Če tovrstna zaščita ni potrebna, potem je f5≡0 oziroma AK=0.

Izbira algoritma za funkcije f1..f5 in sekvenčnih števil

Glede na to, da se algoritem za izvedbo funkcij f1 .. f5 izvaja zgolj v AuC in USIM, je standard pustil operaterjem proste roke in je izbira algoritma odvisna od operaterja. Primer takega algoritma z imenom MILENAGE je opisan v 3GPP specifikaciji [3]. Izbira algoritma za izdelavo sekvenčnih števil SQN prav tako pripada operaterju. V glaven se operaterji oprimejo enega izmed dveh glavnih vodil: vsak uporabnik ima svojo sekvenčno številko ali pa generiranje sekvenčnih števil temelji na globalnem števcu (denimo univerzalnem času). Obstaja tudi možnost kombinacije obeh strategij – glavni del SQN je odvisen od uporabnika, manj pomemben del števila SQN pa od globalnega števca.

4.3.3. Overjanje in izmenjava ključev na strani USIM

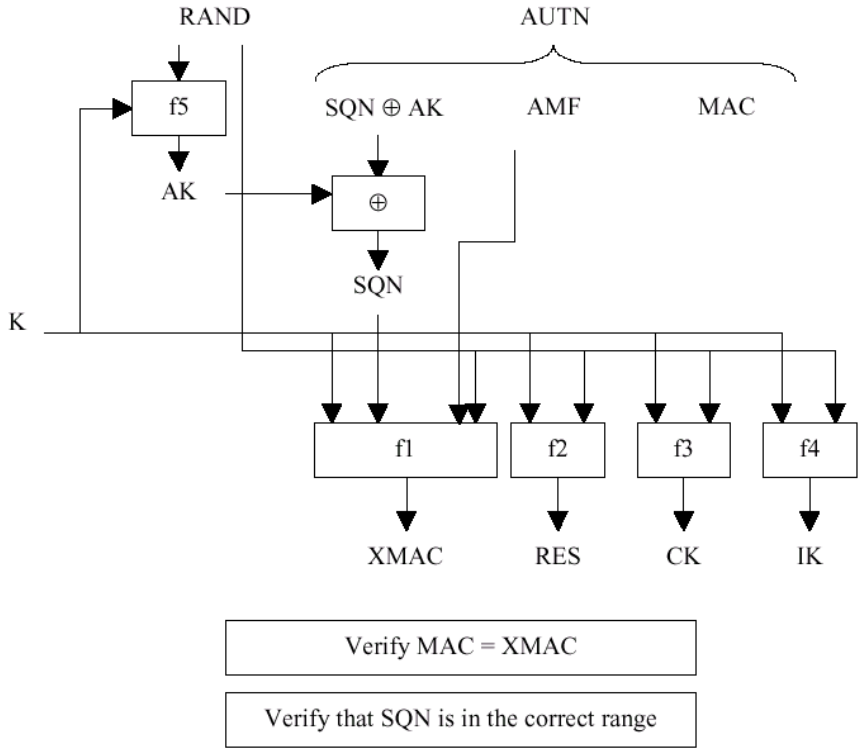
V tem poglavju si podrobneje oglejmo, kako je izvedeno overjanje na strani USIM. Namen procedure je overiti uporabnika in izvesti izmenjavo novega šifrirnega in integritetnega ključa med VLR/SGSN in USIM. Med overjanjem USIM preveri, če so overovitveni vektorji, ki so v uporabi, sveži.



Slika 4.6: Overjanje in izmenjava ključev.

Postopek sproži VLR/SGSN, ki izbere naslednji neuporabljen overovitveni vektor iz urejenega polja vektorjev svoje podatkovne baze. Overovitveni vektorji v posameznih vozliščih so uporabljeni po FIFO principu. VLR/SGSN pošlje USIM-u naključni poziv RAND in overovitveni žeton, za overovitev omrežja AUTN iz izbranega overovitvenega vektorja.

Odziv uporabnika po sprejemu je razviden iz slike. Za izračun parametrov so uporabljene iste funkcije, vendar v nekoliko drugačnem zaporedju. Videli bomo, da se mora funkcija f5 izračunati pred funkcijo f1, ker je f5 potrebna za določitev števila SQN. Zakrivanje je SQN je namreč potrebno, da se napadalec ne more dokopati do uporabniške identite.



Slika 4.7: Funkcije za overjanje uporabnika na USIM

Iz sprejetih parametrov RAND in AUTN, USIM najprej izračuna $AK=f5_K(RAND)$ in s pomočjo njega pridobi sekvenčno število $SQN=(SQN \oplus AK) \oplus AK$. Nadalje USIM izračuna $XMAC=f1_K(SQN||RAND||AMF)$ in ga primerja z MAC, ki je vsebovan v AUTN. Če se vrednosti ne ujemata, potem uporabnik pošlje *user autentication reject* – zavrnitev VLR/SGSN enoti, v kateri je naveden razlog zavrnitve ter prekine s postopkom overjanja. VLR/SGSN pošlje *Authentication Failure Report* – sporočilo o napaki HLR enoti in eventuelno ponovno začne izvajati identifikacijski in postopek overjanja.

V primeru, da se vrednosti ujemata, pa USIM preveri, če je prejeta sekvenčna številka SQN v pravem območju. Če ni, potem odgovori s sporočilom *synchronisation failure* in prekine postopek overjanja.

Če je sekvenčna številka v pravem območju, potem USIM izračuna $RES=f2_K(RAND)$ in ga doda kot parameter v *user authentication response* – odzivu, ki ga pošlje nazaj VLR/SGSN enoti. USIM nazadnje izračuna šifrirni ključ $CK=f3_K(RAND)$ in integritetni ključ $K=f4_K(RAND)$. Zavoljo večje učinkovitosti so lahko parametri CK, IK in RES izračunani kadarkoli med postopkom overjanja (po prejemu naključnega števila RAND).

Če USIM podpira tudi funkcijo pretvarjanja c3 lahko izračuna GSM šifrirni ključ Kc iz UMTS šifrirnega in integritetnega ključa CK in IK. UMTS ključe se pošlje mobilni enoti MS skupaj z izpeljanimi GSM ključi za sodelovanje med GSM in UMTS sistemi.

USIM shrani ključa CK in IK do konca uspešne izvedbe AKA.

Po prejemu *user authentication response* VLR/SGSN primerja RES z pričakovanim XRES, ki je shranjen v overovitvenem vektorju. Njuno ujemanje pomeni uspešno opravljeno overjanje. Če se razlikujeta, VLR/SGSN pošlje *Authentication Failure Report* – sporočilo o

napaki HLR enoti in eventuelno ponovno začne izvajati identifikacijski postopek in postopek overjanja.

Ponovna uporaba in ponovno pošiljanje (RAND, AUTN) parametrov

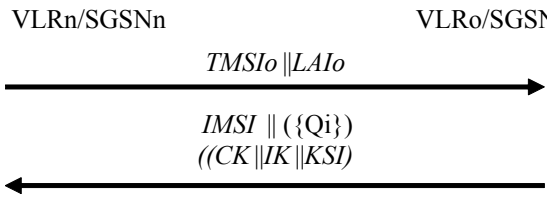
Preverjanje SQN števila je namenjeno preprečitvi ponovne uporabe kvinteta s strani VLR/SGSN v overovitvenem postopku. V splošnem namreč lahko VLR/SGSN uporabi overovitveni kvintet zgolj enkrat.

Obstaja izjema: Kadar VLR/SGSN pošlje overovitveno zahtevo in pri tem uporabi specifičen overovitveni kvintet, od mobilne enote (MS) pa ne prejme nobenega odziva (niti *authentication response* niti *authentication reject*), potem lahko že uporabljeni kvintet ponovno uporabi. Vendar pa od trenutka, ko prejme sporočilo z odzivom, ne sme več pošiljati istega overovitvenega vektorja in ga v te primeru izbriše. Na strani mobilne enote MS se zavoljo ponovne uporabe (brez postopkov resinhronizacije) shranjuje zadnja prejeta vrednost naključnega števila RAND, kot tudi pripadajoči podatki RES, CK in IK. V kolikor USIM vrača SRES in Kc (GSM dostop), se shranijo tej podatki. Ko mobilna enota sprejme overovitveno zahtevo, najprej preveri, če je število RAND ponovljeno in se temu primerno odzove. ME izbriše shranjene vrednosti RAND, RES oziroma SRES, takoj, ko je vzpostavljena povezava 3G varnostnega načina oziroma je povezava prekinjena.

4.3.4. Prenos IMSI in overovitvenih podatkov znotraj ene domene strežnega omrežja

Namen postopka je s strani uporabnika novo obiskanim VLR/SGSN zagotavljati podatke o začasni identiteti s strani prej obiskanih VLR/SGSN znotraj enega same domene strežnega omrežja.

Postopek je prikazan na Slika 4.8:



Slika 4.8: Prenos IMSI in overovitvenih podatkov znotraj ene domene

Postopek sproži novo obiskani VLRn/SGSNn po sprejemu zahteve za osvežitev podatkov o lokaciji od uporabnika, ki pošlje TMSIo in LAIo.

Sledijo naslednji koraki:

- VLRn/SGSNn pošlje *user identity request* - zahtevo za izkaz identitete uporabnika prej obiskanemu VLRo/SGSNo, sporočilu pa doda podatka TMSIo in LAIo.
- VLRo/SGSNo poišče uporabnikove podatke v bazi podatkov.

V kolikor najde uporabnika, potem vrne odgovor o identiteti uporabnika, ki vsebuje:

1. IMSI
2. eventuelne neuporabljene overovitvene vektorje

3. ali eventuelno trenutne varnostne podatke CK, IK in KSI v UMTS omrežjih oziroma Kc in CKSN podatke v GSM omrežjih

VLRo/SGSNo v nadaljevanju izbriše vse overovitvene vektorje in preostale podatke, ki jih je posredoval novo obiskanemu VLRn.

V kolikor uporabnika v bazi ne najde, potem v odgovoru (*user identity response*) pove, da uporabniške identitete ni mogoče najti.

Če VLRn/SGSNn sprejme odgovor o identiteti uporabnika (*user identity response*), ki vsebuje IMSI, shrani overovitvene vektorje in vse preostale sprejete varnostne podatke v bazo.

V kolikor VLRn/SGSNn sprejme odgovor o nezmožnosti najdbe iskane identitete, potem zažene postopek identifikacije s stalno identiteto.

4.3.5. Sinhronizacija overovitvenih vektorjev

Videli smo, da mehanizem medsebojnega overjanja temelji na dveh parametrih, ki sta oba shranjena v AuC in USIM: to sta statični glavni ključ ***K*** in dinamična sekvenčna številka SQN. Jasno je, da morata biti ta dva parametra sinhronizirana na obeh straneh. Ker je ***K*** ves čas enak, nam sinhronizacija le-tega ne predstavlja težav. Lahko pa se zgodi, da sinhronizacijo izgubi SQN. V tem primeru overjanje ne bi delovalo. Uporabijo se v ta namen razvite *re-sinhronizacijske* procedure. Z uporabo ključa K USIM informira AuC o trenutnem SQN. To stori z uporabo parametra AUTS, ki je sestavljen je iz dveh delov: SQN, zakritim z AK in kodo overovitve sporočila MAC-S, ki je izračunana z uporabo dodatne enosmerne funkcije f1* iz parametrov SQN, RAND, AMF in ***K***. Najmanj dva izmed navedenih parametrov sta prevzeta iz neuspešnega poskusa overovitve. f1* se mora načeloma razlikovati od f1, sicer bi lahko bili AUTN parametri privzeti za veljavne AUTS parametre in bi napadalec na ta način lahko vsaj motil overovitven mehanizem.

4.3.6. Obveščanje o overovitvenih napakah

Namen tega postopka je obveščanje o overovitvenih napakah. Strežno omrežje na ta način sporoča napake domačemu okolju. Postopek je razviden iz slike:

Postopek sproži strežno omrežje VLR/SGSN, ko pride do napake pri overovitveni proceduri. Poročilo o napaki pri overovitvi (*authentication failure report*) vsebuje podatke o identiteti uporabnika in kodo razloga o napaki.

4.4. Šifriranje v UTRAN

Za tem, ko sta uporabnik in omrežje overila drug drugega se lahko začne varna komnikacija. Kot je bilo že opisano doslej, se v ta namen uporablja šrifrirni ključ CK, ki ga poznata omrežje in terminal, po tem, ko sta uspešno izvedla postopek overjanja. Preden pa se šifriranje začne, se morata obe strani dogovoriti o algoritmu, ki bo uporabljen za šifriranje. V UMTS implementaciji 3GPP R99 je definiran en sam algoritem.

4.4.1. Pogajanje o šifriranju in integritetnem načinu

Ko MS želi vzpostaviti zvezo z omrežjem, mora omrežju sporočiti, kateri šifrirni postopek in kateri integritetni algoritem podpira. Tudi ta informacija mora biti zaščitena pred spremembami. Ker v tem trenutku RNC nima integritetnega ključa se integriteta sporočila o možnih šifrirnih postopkih zagotovi med postopkom vzpostavitve varnega prenosa z uporabo najbolj svežega IK.

Omrežje preveri zmožnosti zaščite identitete s potencialnimi algoritmi in eventuelno postavljene posebne zahteve:

- V primeru, da MS in omrežje nimata skupnih UMTS integritetnih algoritmov UIA, potem je zveza opuščena
- V primeru, da MS in omrežje imata vsaj en skupen UIA algoritem, potem omrežje izbere enega izmed združljivih verzij UIA algoritmov in ga uporabi za zvezo.

Prav tako omrežje preveri zmožnosti šifriranja s potencialnimi algoritmi in eventuelno postavljene posebne zahteve:

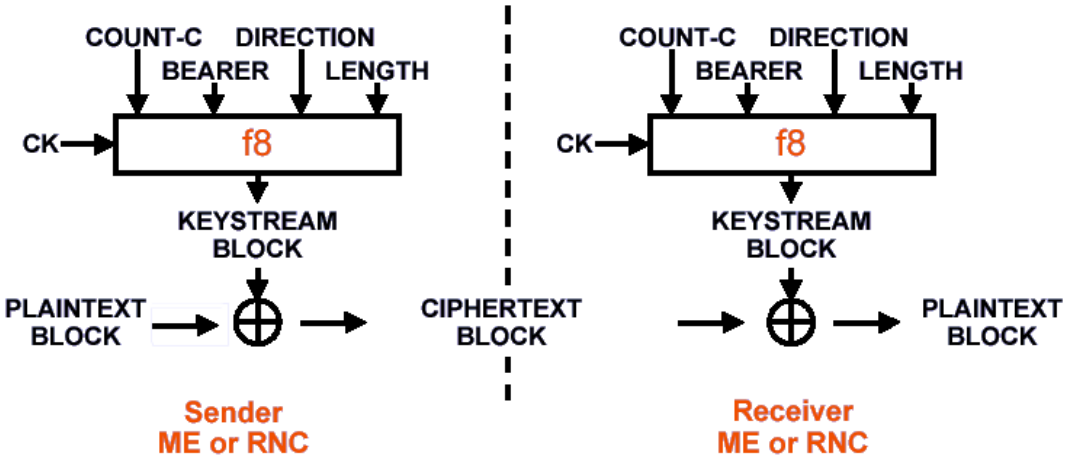
- V primeru, da MS in omrežje nimata skupnih UMTS integritetnih algoritmov UIA, potem je zveza opuščena
- V primeru, da MS in omrežje nimata skupnih UMTS integritetnih algoritmov UIA, uporabnik oziroma njegovo HE pa dovoli vzpostaviti tudi nešifrirano zvezo, potem se vzpostavi nešifrirana zveza
- V primeru, da MS in omrežje imata vsaj en skupen UIA algoritem, potem omrežje izbere enega izmed združljivih verzij UIA algoritmov in ga uporabi za zvezo.

4.4.2. Delovanje (de)šifrirnih mehanizmov v UMTS

Šifriranje in dešifriranje na strani omrežja izvaja v RNC, zato je potrebno ključ CK prenesti iz CN do omrežja radijskega dostopa (UTRAN). To se stori z specifičnimi RANAP sporočili imenovanimi ukazi za varnostni način (*security mode command*). Po tem, ko RNC sprejme CK, preklopi komunikacijo v šifrirni način z RRC ukazom za varnostni način (*security mode command*).

Šifrirni mehanizmi v UMTS temelji na *šifriranju pretoka podatkov (stream chipper concept)*, kot je to razvidno iz Slika 4.9. Nešifrirani podatki se bit-za-bitom dodajajo maključni maski, ki je generirana glede na šifrirni ključ CK in nekaj ostalih parametrov. Ta način šifriranja ima to prednost, da je maska generirana preden poznamo nešifrirane podatke. Zato je končna stopnja šifriranja zelo hitra operacija.

Dodatna prednost tega mehanizma je v tem, da je za dešifriranje uporabljen natančno enak mehanizem. Dodajanje maske dvakrat ima namreč natančno enak rezultat, kot bi nešifriranim podatkom prišteli ničle.



Slika 4.9: Šifriranje pretoka podatkov v UMTS

Ker šifrirna maska ni odvisna od nešifriranih podatkov, mora biti na vhodu šifrirnega algoritma neka parameter, ki spreminja masko. Sicer bi bili dvoji različni nešifrirani podatki P1 in P2 zaščiteni z enako masko, kar pa napadalcu olajša dešifriranje [4].

Šifriranje se izvaja na nivoju krmiljenja dostopa do medija (medium access control layer – MAC) ali na nivoju krmiljenja radijske povezave (radio link control layer – RLC) . V obeh primerih imamo števec, ki se spreminja v vsaki podatkovni enoti. Na nivoji MAC se ta števec imenuje CFN (Connection Frame Number), na nivoju RLC pa RLC sekvenčna številka (RLC sequence number RLC-SN). Ker pa se števec CFN oziroma RLC-SB prehitro obrne, je dodan še daljši števec, imenovan hyperframe number (HFN). Ta se poveča za eno, ko se krajši števec obrne. Skupaj tvorita števec imenovan COUNT-C, ki skrbi za zagotavljanje vedno drugačno maske znotraj šifrirnega algoritma. V principu bi se tudi daljši števec HFN lahko obrnil. Vendar pa se števec vedno, kadar je s postopkom AKA generiran nov ključ, števec postavi na nič. Overovitveni postopki so načeloma dovolj pogosti, da preprečujejo, da bise HFN obrnil.

Identiteta radijskega nosilca BEARER je prav tako eden izmed vhodnih parametrov šifrirnega algoritma, ker so števci za različne radijske nosilce med seboj neodvisni. Če tega parametra ne bi bilo, bi to zopet lahko pripeljalo v situacijo, ko bi z istimi vhodnimi parametri lahko generirali isto masko večkrat.

Jedro šifrirnega mehanizma je torej šifrirni algoritem, ki generira masko. Označen je z f8 [4]. Navadno bazira na blokovnem kodiranju (block chiper) imenovanem KASUMI [5]. Blokovno šifriranje se izvaja nad bloki 64 bitne dolžine. Transformacijo vodi 128 bitni ključ. V kolikor ta ni znan, iz izhodnih blokov ne moremo določiti vhodnih. V principu preostaneta še dva načina napada:

- Preizkusimo vse možne ključe, dokler ne najdemo pravega
- Zberemo enormno veliko tabelo 2^{64} vhodno – izhodnih parov

Oboje je v praksi nemogoče.

V primeru, da se ob začetku šifirane komunikacije ne izvede overjanje, se uporabi na zadnje uporabljan ključ CK. CK je namreč shranjen na USIM. Prav tako se shranjuje tudi pomembnejši del števca HFN.

Terminali morajo imeti implementiran šifrirni indikator, ki uporabniku med komunikacijo prikazuje, ali je uporabljeno šifriranje ali ne (vidnost in nastavljivost varnosti). Zavedati se moramo, da je šifriranje v UMTS zelo priporočljivo, vendar je še vedno zgolj opcijska možnost in ga je mogoče ukiniti.

4.4.3. Obdobje veljavnosti CK in IK

Overovitveni postopek in postopek dogovarjanja ni nujen za vzpostavitev klica. Zato obstaja možnost večkratne uporabe, kot tudi zlorabe ključev. Potrebujemo torej mehanizem, ki zagotavlja, da se istih ključev ne da uporabljati v nedogled, s čimer se izognemo napadom z dogovorjenimi ključi. USIM mora torej vsebovati mehanizem, ki omeji maksimalno količino podatkov, ki jo lahko zaščitimo z enim ključem.

Vedno, kadar se vzpostavi RRC (Radio Resource Control) zveza, se vrednosti $START_{CS}$ in $START_{PS}$ shranita na USIM. Ko se vzpostavi naslednja RRC povezava, se vrednosti preberejo iz USIM. ME mora zahtevati novo izmenjavo ključev, če sta vrednosti $START_{CS}$ in $START_{PS}$ dosegli maksimalno vrednost, določeno s strani operaterja, ključa CK in IK pa se izbrišeta iz USIM.

Mehanizem torej zagotavlja, da šifrirni/integritetni ključ ni uporabljen večkrat, kot je to dovoljeno s strani operaterja.

4.4.4. Identifikacija CK in IK

Identifikator nabora ključev (Key set identifier – KSI) je število, ki pripada šifrirnemu ključu, pridobljenemu v postopku zadnjega overjanja. Identifikator KSI izda omrežje in ga pošlje v sporočilu zahteve za overjanje mobilni postaji, ki ga shrani skupaj z izračunanima ključema CK in IK. KSI v UMTS sovpada z CKSN v GSM sistemu. USIM shrani en KSI/CKSN za PS domenski nabor ključev in enega za CS domeski nabor ključev.

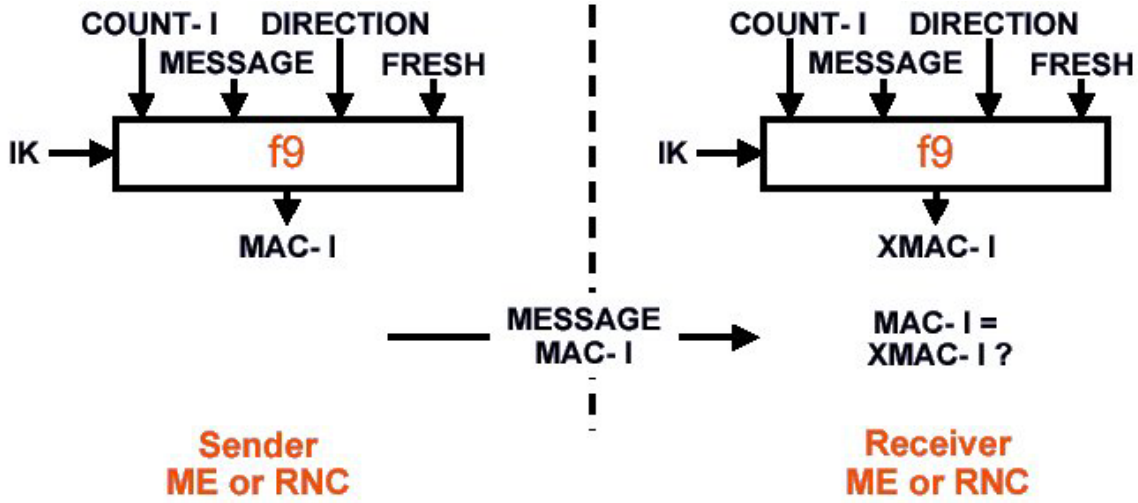
Namen KSI je identifikacija shranjenih ključev CK in IK omrežju, brez da bi ponovno zahtevali overovitveni postopek. Na ta način je omogočena ponovna uporaba šifrirnih ključev prek posameznih zahtev za povezavo.

KSI in CKSN imata enak format. Identifikator ključa je sestavljen iz treh bitov, torej imamo na razpolago 7 vrednosti za identifikacijo nabora ključev. Vrednost 111 se uporablja, da mobilna postaja identificira, da nima uporabnih ključev. Po brisanju je KSI vedno postavljen na 111. Vrednost 111 s strani omrežja je rezervirana.

4.5. Zaščita integritete RRC signalizacije

Namen zaščite integritete je overjanje vsakega indivindualnega kontrolnega sporočila. To je pomembno zato, ker nam procedura overjanja zagotavlja prisotnost pravih strank samo v postopku overjanja. Videli smo, da pristop vmesne entitete (man-in-the-middle), kot je denimo lažna bazna postaja, omogoča, da napadalec postopek overjanja izvede zgolj kot posredovanje sporočil med obema pravima izvornikoma, ko pa se zveza vzpostavi, pa tudi sam oddaja sporočila, saj bi ta bila v tem primeru brez overjanja individualnih sporočil brez

zaščite. Overjanje individualnih signalizacijskih sporočil pa omogoča nadzor nad njimi, kar pomeni, da so ponarejena sporočila odkrita in zavržena.



Slika 4.10: Izračun MAC-I in XMAC-I iz signalizacijskega sporočila

Integriteta sporočil je izvedena na RRC nivoju. Uporablja se za komunikacijo med terminalom in RNC, podobno kot šifriranje. Kot smo spoznali, se integritetni ključ IK, tako kot CK, generira med AKA proceduro.

Mehanizem zagotavljanja integritete temelji na konceptu kode za overjanje sporočil (message authentication code – MAC). To je enosmerna funkcija, ki je krmiljena s ključem IK. Funkcijo označujemo s f9 [4], njen izhod pa z MAC-I, ki je 32 bitni niz z naključnimi lastnostmi. MAC-I se doda vsakemu RRC sporočilu. Na enak način pa se MAC-I generira in preveri na sprejemni strani. Vhodni parametri v funkcijo f9 so: IK, RRC sporočilo, števec COUNT-I, bit, ki določa smer (downlin/uplink), naključno število FRESH. Števec COUNT-I je sestavljen na podoben način kot števec COUNT-C: zgornji del ga sestavlja HFN, spodnji del pa RRC sekvenčna številka. COUNT-I ščiti pred ponavljanjem že generiranjih kontrolnih sporočil – zagotavlja, da so vrednosti vhodnih parametrov različne vsakič, ko se zaščitna funkcija f9 izvede. Izvedba funkcije f9 je predstavljena na Slika 4.10.

Parameter FRESH določi RNC in ga pošlje UE. Potrebuje se za zaščito omrežja proti sumljivo izbranim začetnim vrednostim števca COUNT-I. Glavni del COUNT-I (HFN) je shranjen v USIM. Napadalec bi se lahko pretvarjal kot USIM in poslal omrežju premajhno vrednost. Če se procedura AKA ni izvedla, bi se zato uporabil starejši ključ IK, to pa bi omogočilo napadalcu ponarejanje RRC signalni sporočil z že posnetimi overovitvenimi parametri. Kot smo že povedali, vedno povečujoč se COUNT-I ščiti pred napadi, ki temelje na snemanju znotraj ene povezave, medtem ko FRESH ostaja med eno povezavo ves čas enak.

Pri algoritmu za zagotavljanje integritete se ne uporablja parameter, ki bi identificiral nosilca (BEARER), čeprav igra pomembno vlogo pri šifriranju podatkov. Ker je tudi na nivoju kontrolne ravni več hkratnih radijskih nosilcev, bi torej obstajala možnost za zamenjavo kontrolnih sporočil s tistimi, posnetimi na isti RRC povezavi, vendar na drugem radijskem nosilcu. Vendar pa je podatek o nosilcu vedno dodan sporočilu, še preden se

izračuna MAC. Tako ima nosilec vpliv na izračun MAC-I vrednosti in na ta način je sistem zaščiten tudi proti napadom z uporabo RRC sporočil, posnetih na drugem radijskem nosilcu.

Ob koncu velja povedati, da obstaja skupina RRC krmilnih sporočil, katerih integriteta ne more biti zaščitena z omenjenim mehanizmom. Sporočila, ki so poslana pred IK sploh ne morejo biti zaščitena. Tipičen primer takšnega sporočila je RRC zahtevek za vzpostavitev zveze (RRC connection Request).

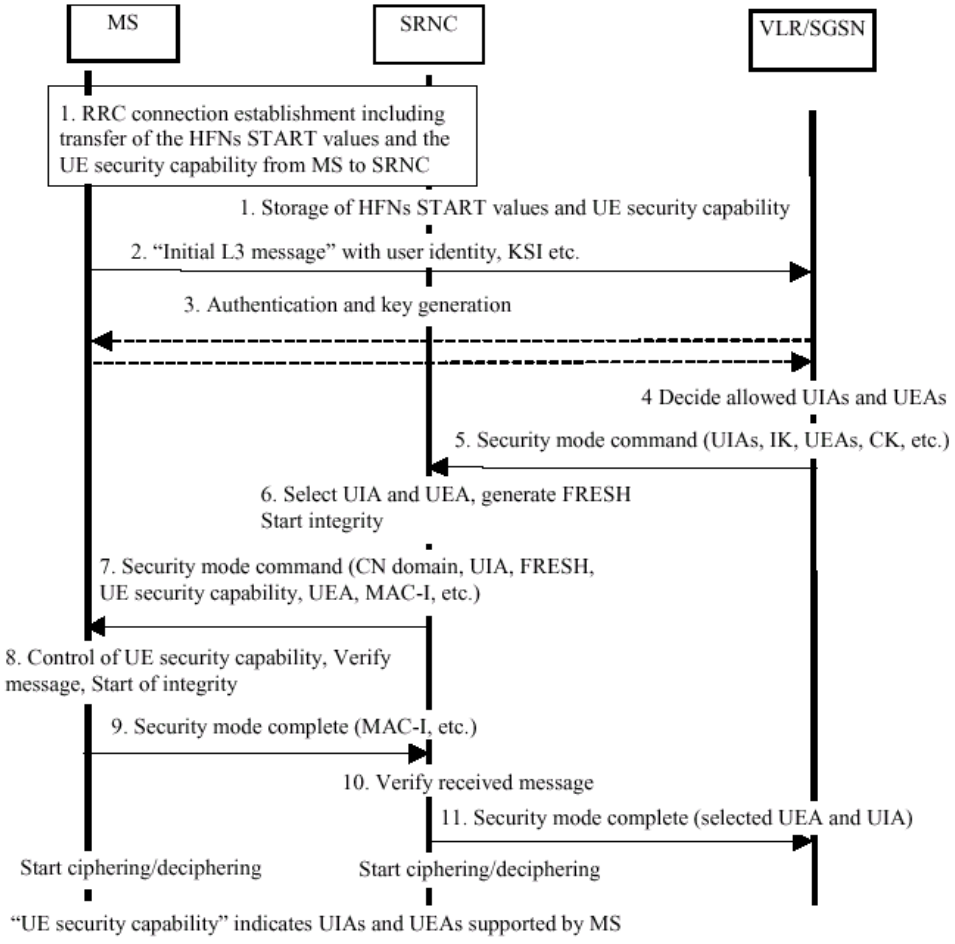
Algoritem, ki je namenjen zaščiti integritete temelji na isti osnovni funkciji kot algoritem za šifriranje. Za overjanje sporočil se lahko uporablja tudi poseben način delovanja KASUMI algoritma [5].

Mehanizem za zagotavljanje integritete pa v UTRAN ni uporabljen na nivoju uporabniške ravnine, temveč samo za signalizacijo, zavoljo izgube pri zmogljivosti. Obstajajo pa mehanizmi, s katerimi se lahko doseže podobne učinke, kot denimo periodično lokalo overjanje (periodic local authentication).

4.6. Postopek vzpostavitve varnega prenosa

Napravimo rezime in sestavimo zgoraj opisane elemente v celotno sliko: Splošen postopek za vzpostavitev zaščite šifriranja in integritete.

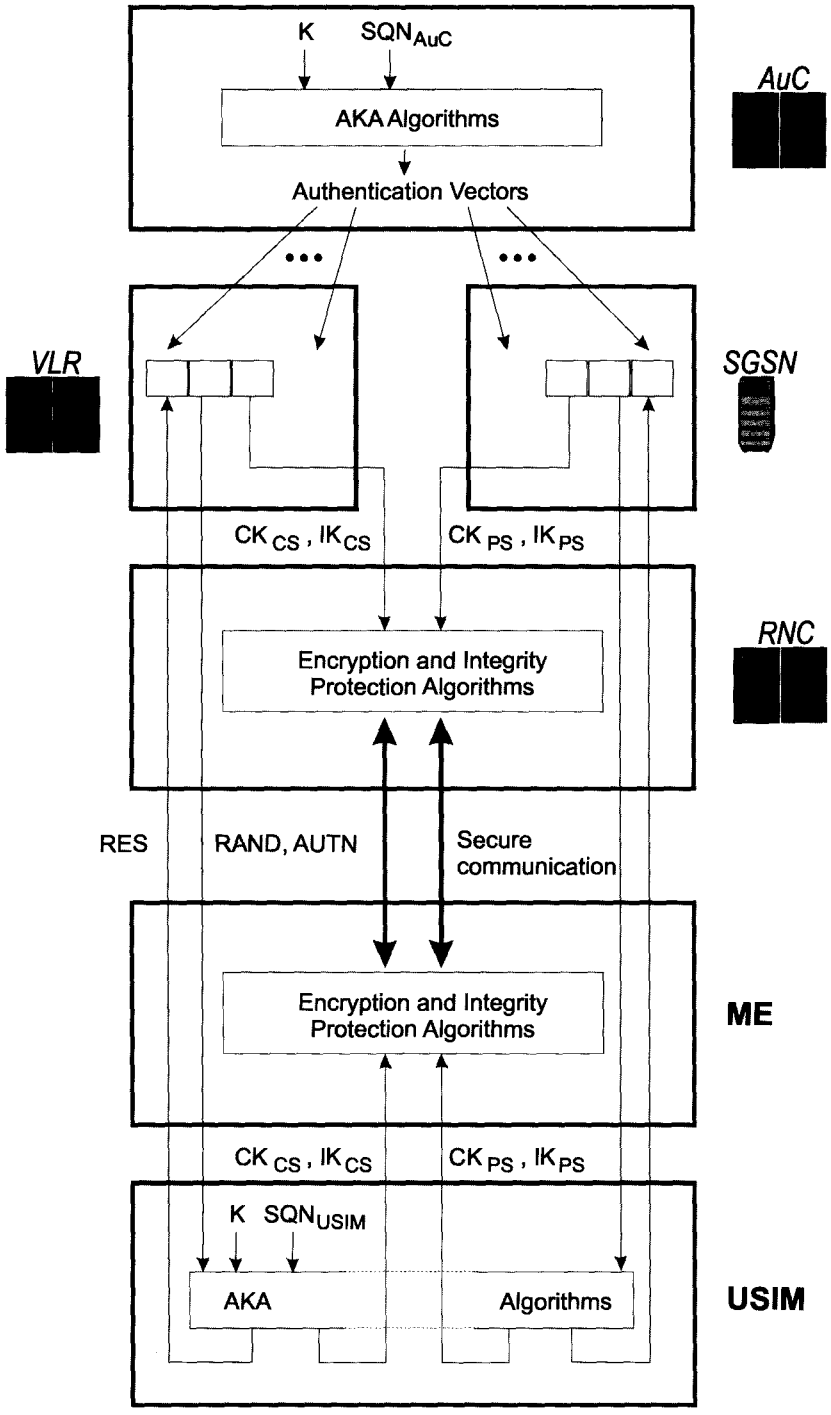
Potek sekvene sporočil, ki opisujejo prenos informacij potrebih za vzpostavljanje začetne povezave, potencialno overjanje in začetek zaščite integritete in šifriranja je razviden iz slike:



Opis vzpostavitve povezave:

1. RRC vzpostavljanje povezave vključuje prenos varnostnih podatkov od MS do RNS. Varnostni podatki so podatki o načinu šifriranja (UEA) in načinu zagotavljanja integritete (UIA), ki jih uporablja mobilna enota.
2. Mobilna enota pošlje inicializacijsko L3 sporočilo, ki vsebuje: Location Update Request, CM service requerst, Routing area update request, attach request, paging response, itd.) k VLR/SGSN enoti. To sporočilo vsebuje tudi uporabniško identiteto in KSI (Key Set Identifier).
3. Izvede se zahteva za preverjanje uporabniške identitete, overjanje uporabnika in generiranje ključev CK in IK. Sledi zapis novega KSI.
4. VLR/SGSN preveri, katerei način UEA in UIA je na razpolago za uporabo.
5. VLR/SGSN inicializira metode za zagotavljanje integritete in šifriranja tako da pošlje RANAP sporočilo SRNC. Sporočilo vsebuje seznam dovoljenih UIA in IK. Če je zahtevano še šifriranje povezave, vsebuje še UEA in CK.
6. SRNC se odloči, za enega izmed algoritmov s seznama dovoljenih algoritmov, ki jih podpira MS. Generira naključno število FRESH in inicializira integriteto v smeri prenosa proti ME.
7. SRNC generira Security mode command. To sporočilo vsebuje opis zmožnosti ME, FRESH in UIA, ki sta na voljo za uporabo in UEA, če je zahtevano še šifriranje podatkov.
8. Ob sprejemu sporočila *RRC Security mode command* MS preveri, ali je UE security capability enak tistemu, ki je bil poslan v inicializacijskem sporočilu. MS izračuna XMAC-I za prejeto sporočilo z uporabo UIA, shranjenega podatka za COUNT-I in prejetega FRESH parametra. MS preveri integriteto sporočila s primerjavo sprejetega MAC-I in XMAC-I.
9. Če je preverjanje uspešno, MS izdela sporočilo *RRC Security mode complete* in zanj izračuna MAC-I.
10. Na sprejemni strani SRNC izračuna XMAC-I za omenjeno sporočilo preveri integriteto s preverjanjem MAC-I in XMAC-I.
11. Prenos RANAP sporočila *Security Mode Complete*, ki vključuje tudi izbrane algoritme, od SRNC do VLR/SGSN zaključi omenjeno proceduro.

Čisto ob koncu si oglejmo shemo, ki prikazuje pregled storitev za zagotavljanje varnosti na nivoju dostopa in njihove medsebojne povezave. (Slika 4.11). Zaradi jasnosti slike so nekateri parametri, ki se prenašajo med elementi, izpuščeni.



Slika 4.11: Pregled storitev za zagotavljanje varnosti na nivoju dostopa (vir: [6])

5. Primeri uporabe mehanizmov javnih ključev za zagotavljanje varnosti v UMTS sistemih

Na internetu sem našel zanimiv primer uporabe mehanizmov javnih ključev za potrebe overovitve dostopa do omrežja in dogovora o ključih, ki jih je definiral Siemens AG v sodelovanju z ETSI SMG Security Group, ki je odgovorna za standardizacijo varnosti v UMTS sistemih. Obstajajo tri verzije protokola, imenovane protokol A, B in C. Opis je povzet po ASPeCT D02.

5.1. Varovanje dostopa do omrežja

5.1.1. Protokol A

Protokol se uporablja, kadar sta overjeni kopiji javnih ključev uporabnika in strežnega omrežja SN že dostopni na obeh straneh (pri uporabniku in SN) in se med samim protokolom ne izmenjata.

5.1.1.1. Cilji protokola

Protokol verzije A ima naslednje cilje:
- Medsebojna overovitev med uporabnikom in strežnim omrežjem
- Dogovoriti se o skupnem ključu K z medsebojno overovitvijo ključev
- Medsebojno potrditev ključev
- Medsebojno zagotovitev svežine ključev
- Onemogočiti prisluškovanje podatkom, ki jih pošilja uporabnik omrežju
- Zaupnost identitete IMSI uporabnika na radijskem vmesniku

5.1.1.2. Zahteve mehanizma

Verzija A protokola predpostavlja naslednja dejstva:
- Identiteta strežnega omrežja je znana uporabniku že na začetku protokola.
- Obstaja dogovorjen simetričen šifrirni algoritem *Enc*, kjer *Enc(K,X)* pomeni šifriranje podatkov *X* z uporabo ključa *K*.
- Obstajajo dogovorjene zgoščevalne funkcije *h1*, *h2*, *h3*.
- Obstaja dogovorjena končna skupina *G* z generatorjem *g*; to je multiplikativna skupina končnega polja ali podskupina eliptične krivulje, kjer je velik problem diskretnega logaritma.
- SN ima privaten ključ *n* in javni ključ g^n.
- Uporabnik ima asimetrični podpisni sistem z lastno transformacijo podpisa Sig_u. $Sig_u(M)$ pomeni podpis sporočila M.
- Overjena kopija uporabnikovega javnega ključa PK_U asimetričnega sistema za podpisovanje je dostopna SN.
- Overjena kopija javnega ključa g^n strežnega omrežja je dostopna uporabniku.

5.1.1.3. Opis protokola

Mehanizem sestavljajo tri sporočila, ki si jih izmenjata uporabnik in SN. HE in CA nista vključena v postopek. Sporočila si sledijo zaporedno, kot je razvidno tudi iz številčenja njihovih imen: M1, M2 in M3.

M1: User → SN: g^{RND_U}
M2: SN →. User: RND_N || $AUTH_N$ || *Enc(K,data1)*
M3: User →. SN: *Enc(K, Sig$_u$(h3(K||data1||data2)))* || *Enc(K, IMSI)* || *Enc(K, data2)*

X||Y označuje pripojitev podatkov X k Y.
Postopki protokolnih elementov sledijo v nadaljevanju.

Message M1:
Uporabnik izračuna g^{RND_U}, in ga pošlje SN.

Message M2:
Strežno omrežje izračuna
- $(g^{RND_U})^n$
- ključ seje $K = h1((g^{RND_U})^n \,||\, RND_N)$
- $AUTH_N = h2(K)$

SN pošlje RND_N, $AUTH_N$, in *Enc(K, data1)* uporabniku.

Message M3:
Uporabnik izračuna:
- $(g^n)^{RND_U}$
- ključ seje $K = h1((g^n)^{RND_U} \,||\, RND_N)$
- $AUTH_N = h2(K)$
- *Enc(K, Sig$_u$(h3(K||data1||data2)))*
- *Enc(K, IMSI)*
- *Enc(K, data2)*

$AUTH_N$ se primerja z vrednostjo, ki je bila prejeta od SN. Uporabnik pošlje *Enc(K, Sig$_u$(h3(K||data1||data2)))* || *Enc(K, IMSI)* in *Enc(K, data2)* strežnemu omrežju.
Strežno omrežje:
- Dešifrira vsak del sporočila z dešifrirnim algoritmom *Dec* in ključem seje *K*.
- Razpozna IMSI in ugotovi, s katerim javnim ključem (PK_U) je potrebno preveriti veljavnost podpisa.
- Pozna *K, data1, data2* in izračuna *h3(K||data1||data2)*
- Sprejme *h3(K||data1||data2)* iz *Sig$_u$(h3(K||data1||data2))* z algoritmom za preverjanje *Ver$_u$* in ključem PK_U preveri ti dve vrednosti.

5.1.2. Protokol B

Protokol se izvaja med uporabnikom in SN, če je veljaven certifikat javnega ključa z preverjanje podpisa uporabnika PK_U znan samo uporabniku, ne pa SN in certifikat z javnim ključem g^n SN dostopen samo strežnemu omrežju.

5.1.2.1. Cilji protokola

Ciljem, definiranim pri protokolu A, je pri protokolu B dodan še naslednji cilj:

- Izmenjava certificiranih javnih ključev med uporabnikom in SN

5.1.2.2. Opis protokola

Mehanizem je sestavljen iz treh sporočil med uporabnikom in SN. Domače okolje in CS zopet nista vključena v postopek.

M1: User → SN: $g^{RND_U} \,||\, id_{CA}$

M2: SN →. User: $RND_N \,||\, AUTH_N \,||\, Enc(K,data1) \,||\, \text{Cert}N$

M3: User →. SN: $Enc(K,\ Sig_u(h3(K||data1||data2))) \,||\, Enc(K,\ \text{Cert}U) \,||\, Enc(K,\ data2)$

Razlika med protokolom A in protokolom B je v tem, da uporabnik ne pozna javnega ključa SN in SN ne pozna javnega ključa uporabnika. Zato uporabnik v prvem sporočilu doda še identifikator CA id_{CA}, pri katerem lahko preverja veljavnost podpisov. SN v drugem sporočilu doda njen certifikat Cert$N$ podpisan s stran CA identificirane v M1. Uporabnik preveri certifikat in iz njega sprejme javni ključ g^n javnega omrežja, ki ga potrebuje za izračun $(g^n)^{RND_U}$. V tretjem sporočilu je namesto *IMSI* zašifriran uporabnikov certifikat Cert$U$. Iz njega SN sprejme javni ključ PK_U, ki ga uporabi za nadaljnje izračune.

5.1.3. Protokol C

Protokol se uporablja v primeru, ko overjena kopija javnega ključa uporabnika ni dostopna SN in overovljena kopija javnega ključa SN ni dostopna uporabniku.

5.1.3.1. Cilji protokola

Ciljem, definiranim pri protokolu A, so dodani še naslednji cilji:

- Prenos javnega ključa PK_U uporabnika, certificiranega s strani CA od certifikacijskega strežnika CS do SN.
- Prenos javnega ključa g^n SN certificiranega s strani CA med SN in uporabnikom.
- Zagotovitev s strani CA, da je javni ključ, ki ga certificira dejansko javni ključ SN.
- Zagotovitev uporabniku in SN, da certifikata SN in uporabnika nista bila preklicana.

5.1.3.2. Opis protokola

Mehanizem je sestavljen iz petih sporočil med uporabnikom, SN in CS. CS ima dostop do certifikatov – javnega ključa uporabnika, ki ga izda CA. HE, CS in CA so lahko združene v isti enoti.

Tudi v tem primeru bi si lahko podrobneje ogledali postopke elementov protokola, vendar bi to presegalo okvire seminarske naloge in si bralec lahko ogleda v literaturi [15].

5.2. Varnost med uporabniki in VASP-ji

V tem poglavju si bomo ogledali primer protokola, katerega uporaba je namenjena za komunikacijo med uporabnikom in ponudniki storitev z dodano vrednostjo (Value Added Service Provider – VASP), ki uporabnikom ponuja storitve. Pri razvoju se je izhajalo iz dejstva, da se obe strani želita medsebojno overiti in denimo – vzpostaviti plačilni mehanizem.

Obstajata dve verziji protokola, odvisno od tega, ali uporabnik in VASP posedujeta ključe, potrebne za preverjanje certifikatov sogovornika, ali pa jih more zagotoviti CS.

5.2.1. Protokol B

5.2.1.1. Cilji protokola

Protokol B je načrtovan za primer, ko uporabnik in VASP še nista izmenjala certifikatov z javnimi ključi. Za razliko od C inačice protokola pa imata uporabnik in VASP možnost preveriti drug drugega brez posredovanja CS. HE in CS sta lahko združena v isti enoti.

- Medsebojna overovitev med uporabnikom in VASP
- Dogovor o ključih med uporabnikom in VASP
- Medsebojna overovitev ključev
- Medsebojno potrditev ključev
- Medsebojno zagotovitev svežine ključev
- Onemogočiti prisluškovanje podatkom, ki jih pošilja VASP
- Zaupnost identitete uporabnika na radijskem vmesniku
- Vzpostavitev plačilnega mehanizma
- Izmenjava certifikatov z javnimi ključi med uporabnikom in VASP

5.2.1.2. Opis protokola

Obstaja več različic tega protokola. Sestavljen je iz treh sporočil. Za razliko od protokola B pri varnosti dostopa do omrežja tu ni potrebno šifrirati $(g^n)^{RND_V}$, se pa s ključem K šifrira celotno (podpisano) tretje sporočilo, kar onemogoča preverjanje podpisa in napade s pretvarjanjem z lažno identiteto.

Sporočila vsebujejo dodatne parametre (ch_data, α_T, IV), potrebne za vzpostavitev plačilnega mehanizma.

5.2.2. Protokol C

5.2.2.1. Cilji protokola

C-različica overjanja in vzpostavitve plačilnega protokola ima iste cilje kot protokol B, le da je zadnji nadomeščen z

- Izmenjava certifikatov z javnimi ključi za uporabnika (k VASP) in VASP (k uporabniku).

Dodan pa je še en cilj:

- Uporabniku in VASP je potrebno zagotoviti veljavnost certifikatov z javnimi ključi, VASP in uporabnika, ter preveriti, da nista bila preklicana.

5.2.2.2. Opis protokola

Tudi protokol C ima več možnih različic, Sestavljen je iz petih sporočil, ki si jih medsebojno izmenjajo uporabnik in VASP, VASP in CS, CS in VASP, VASP in uporabnik ter uporabnik in VASP.

5.3. Varnost med končnimi uporabniki

5.3.1. Splošno

Oglejmo si še medsebojno overjanje in izmenjavo sejnih ključev med dvema UMTS uporabnikoma. Slednji se lahko uporabijo za zaščito podatkov, ki jo med seboj izmenjujeta uporabnika.

5.3.1.1. Cilji protokola

Kot je že navedeno zgoraj, protokol zagotavlja medsebojno overjanje, izmenjavo sejnih ključev in potrditev ključev. Protokol ne zagotavlja zaupnosti identitet. To nam zagotavlja zaščita radijskih vmesnikov s šifriranjem na nižjih komunikacijskih nivojih.

5.3.1.2. Zahteve protokola

Protokol predpostavlja, da imata uporabnika zanesljivi kopiji javnih ključev z preverjanje podpisov drug drugega. Če to ne drži, uporabnika izmenjata certifikate pred ali med izvajanjem protokola. Prav tako morata preveriti tudi veljavnost obstoječih certifikatov. Če so certifikati izdani s strani različnih CA je potrebno izvesti še nekaj navzkrižnih certificiranj, navadno s strani CS.

5.3.1.3. Opis protokola

Protokol se izvede s tremi sporočili, ki jih uporabnik A in B izmenjata med seboj.

M1: User A→ User B: g^{RND_A}

M2: User B→ User A: $Sig_B(g^{RND_B} || g^{RND_A} || id_A) || h(K_{AB} || g^{RND_B} || g^{RND_A} || id_A))$

M3: User A→ User B: $Sig_A(g^{RND_A} || g^{RND_B} || id_B) || h(K_{AB} || g^{RND_A} || g^{RND_B} || id_B))$

6. Varnost na sistemskem in omrežnem nivoju

V tem poglavju bomo ogledali potencialne grožnje na nivoju omrežja in mehanizme, s katerimi se zavarujemo proti njim z željo po zagotavljanju zaupnosti in integritete pri komunikacij med različnimi omrežnimi elementi. Ti elementi lahko pripadajo enemu samemu omrežju ali pa različnim omrežjem. Še posebej slednji primer zahteva vpeljavo standardizirane rešitve, s katero lahko zagotovimo sodelovanje med različnimi operaterji.

Poslovna veriga 3G sistema vključuje različne akterje: *Naročnik*, *ponudnik omrežja*, *ponudnik storitev* in *ponudniki vsebin*. Primer, ko uporabnik storitev uporablja in jo plača, vsebuje vse akterje navedene poslovne verige. Ponudnik omrežja zagotavlja platformo preko katere se vzpostavljajo zveze, ponudnik storitev priskrbi USIM in storitev, ki jo uporabnik uporablja. Storitev potrebuje vsebino za katero skrbijo ponudniki vsebin. Ponudnik omrežja, ponudnik storitev in ponudnik vsebin se lahko fizično nahajajo v istem podjetju, ni pa nujno tako. Naročnik plača za storitev, vsi trije akterji pa si delijo dobiček.

6.1. Najpogostejše oblike napadov na omrežnem nivoju

Največ groženj komunikaciji med elementi omrežnega nivoja je podobnih grožnjam na dostopovnem nivoju. Med posameznimi aplikacijami obstajajo velike razlike, vendar bomo v nadaljevanju skušali ohraniti splošnost.

Načini, kako izvesti napad nad omrežnimi storitvami so omejeni le s človeško domišljijo. Navedimo le nekatere izmed njih:

- Socialne mahinacije (Social enineering)
- Prisluškovanje (sniffing)
- Pretvarjanje (spoofing)
- Prevzemanje sej (Session hijacking)
- Onemogočanje uporabe (Denial of service)

Socialne mahinacije (Social enineering) večinoma ne štejejo med ogrožanje varnosti, je pa ključnega pomena v mnogih napadih. Če se osredotočimo na uporabnika, potem mahinacijo predstavlja zloraba terminala – to je nepooblaščena pridobitev uporabnikovega PIN na takšen ali drugačen način. Tovrstnim mahinacijam se uporabnik lahko zoperstavi le tako, da vestno skrbi za svoj PIN. Podobni poskusi mahinacij se pojavljajo tudi na strani omrežnega operaterja. Neredkokdaj se zgodi, da vzdrževalci omrežij prejmejo sumljive klice, oseba na drugi strani pa jih sprašuje po uporabniškem imenu in geslu za omrežne naprave, ker da je odgovorna oseba na dopustu ali na drug način nedostopna. Običajno gre za socialno mahinacijo spričo katere lahko pomembne uporabniške informacije končajo v napačnih rokah. Večina “hackerjev” na ta način začne napad na omrežje; pridobi dostop do vitalnih ali nevitalnih delov omrežja. V IP omrežju so tovrstni vdori relativno pogosti, medtem ko se v svetu telekomunikacij ne pojavljajo tako pogosto, ker tovrstna oprema ni tako enostavno dosegljiva, ljudji ki jo vzdržujejo pa se zavedajo odgovornosti pri ravnanju z njo.

Prisluškovanje (eavesdropping, sniffing):. Prisluškovanje mediju je zelo težko - marsikdaj pa celo nemogoče zaznati in ga fizično preprečiti. Napadalec se z uporabo prisluškovanja želi

dokopati do uporabniških podatkov, še posebej pa so na udaru sistemski podatki, kot so uporabniška imena in gesla. Programi za izvajanje prisluškovanja (sniffer) so javno dostopni na Internetu, ker predstavljajo uporabno orodje za nadzor prometa v omrežju in ugotavljanje oziroma predvidevanje morebitnih težav v omrežju. V napačnih rokah pa lahko predstavljajo izjemno zmogljivo orodje, s katerim lahko napadalec neslišno prisluškuje podatkom na omrežnem nivoju.

S prisluškovanjem zbrane informacije se po obdelavi lahko uporabijo za naslednji metodologijo napada: *pretvarjanje (spoofing)*. Pri tej metodi se napadalec predstavlja kot nekdo drug in sprejema podatke, ki so namenjeni nekomu drugemu. Na ta način »nadomesti« pravega sprejemnika v povezavi. Napadalec lahko tudi sam skuša vzpostaviti povezavo s ponarejenim naslovom, vendar pa je to veliko težje, zato običajno prepusti, da vzpostavitev zveze opravi pravi uporabnik, šele nato pa napadalec oddaja podatke z njegovim naslovom v omrežje. Ker danes veliko ljudi opravlja transakcije preko omrežnega sloja (delo od doma, plačevanje računov, itd.) je ta način vdora lahko dokaj učinkovit za (nepooblaščen) dostop do informacij.

Če gre napadalec še korak dlje, potem *prevzame sejo (session hijacking)* – prevzame nadzor nad celotno povezavo. Kot smo že omenili, niti močni mehanizmi za overjanje ne onemogočajo kasnejšega prevzema seje. V ta namen so potrebni mehanizmi za zagotavljanje integritete.

Z onemogočanjem uporabe (Denial of Service DoS) napadalec ne zbira podatkov, pač pa onemogoča uporabo storitve ostalim uporabnikom, ki bi storitev želeli uporabiti. V splošnem pri tovrstnih napadih napadalec generira velike količine motilnega prometa, s katerim doseže, da se oddaljena storitev uporabnikom ne odziva. Ideja je torej porabiti vse razpoložlive zmogljivosti vira storitve. Ker se napadalec navadno ne odziva s potrditvami, strežnik ne sprošča virov; zapolni se celotna čakalna vrsta. Posamezni viri se sicer sproščajo po preteku izteka časovnika (timeout), vendar jih napadalec takoj spet zapolni z novimi zatevami.

Bolj kompleksni DoS napadi so izvedeni hkratno iz več sistemov. Navadno so uporabljeni v kombinaciji s katero izmed metod napada, opisanih zgoraj. (DoS napad iz ukradenih naslovov). DoS napadi so izjemno nevarni, ker so zelo učinkoviti in se manifestirajo v ekonomskih posledicah. Zaščita proti njim je težko izvedljiva, orodja za njihovo izvedbo pa so brezplačno na voljo na Internetu.

V tem poglavju smo bežno opisali večino možnih izvedb napada, na katere lahko računamo na omrežnem nivoju. Glede na nevarnost, ki jo grožnje povzročajo, še posebej ob dejstvu, da so orodja za njihovo izvedbo brezplačno dostopna na Internetu, pretnje le-teh nikakor ne gre zanemarjati. Varnostni mehanizmi so torej veriga (celotnega sistema = varnost komunikacije, varnost podatkov, varnost signalizacije), ki je močna toliko, kot je močan njen najšibkejši člen. Z drugimi besedami: varovati je potrebno vse nivoje: algoritme, protokole, povezave, poti od točke do točke, aplikacije, itd.

6.2. Pregled 3GPP varnosti na omrežnem nivoju

Kot je bilo že predstavljeno v uvodu, je bila ena izmed pomanjkljivosti varnostne arhitekture 2G sistemov ravno nezaščitena izmenjava overovitvenih podatkov med različnimi omrežji. Šifrirni ključi (chipper key), uporabljeni za zaščito podatkov na radijskem vmesniku, se prenašajo nezaščiteni med omrežji. Razlog za to leži v podobnosti z omrežji SS7: Samo relativno majhno število uporabnikov ima dostop do teh omrežij. V UMTS Release 99 omrežju je struktura jedrnega omrežja še vedno precej podobna strukturi GSM omrežja; rešitve za odpravo omenjenih pomanjkljivosti so se zato iskale pri izboljšanju varnosti prometa med CN.

V kasnejših izvedbah pa se je omrežna struktura spremenila in je IP prevzel vodilno vlogo na omrežnem nivoju. Čeprav to ne pomeni, da se signalizacija med različnimi jedrnimi omrežji prenaša preko javnega IP omrežja pa to kljub temu pomeni enostavnejši dostop do prometa, kajti napadalci z znanji omrežij IP so najbolj množični.

Osnovno orodje, uporabljeno za zaščito prometa med jedrnimi omrežji je IPSEC protokol, ki zagotavlja tako zaupnost kot integriteto komunikaciji na nivoju IP. Z uporabo IPSEC protokola se lahko komunicirajoče entitete tudi medsebojno overijo. Vseeno pa ostaja kritičen problem upravljanje s ključi (key management): generiranje, menjava in distribucija ključev, ki se uporabljajo v algoritmih za zagotavljanje zaupnosti in integritete. Glede na to, da IPSEC v zadnjem času pridobiva vse večji razmah tudi v javnih IP omrežjih za izvedbo storitev VPN (privatna omrežja preko javnih omrežij) in je bila ta tematika obdelana v več drugih seminarskih kot tudi diplomskih delih, se z njo na tem mestu ne bomo ukvarjali.

Za dodatno zaščito v IP omrežjih so varnostni mehanizmi SS7 v UMTS Release 5 razširjeni z mehanizmi, razvitimi za MAP protokol. Imenujejo se MAPSEC, protokolu pa omogočajo zaupnost in integriteto (način zaščite 0 ne zagotavlja zaščite, način zaščite 1 zagotavlja integriteto, način zaščite 2 pa zagotavlja tako integriteto kot zaupnost). Upravljanje s ključi pri MAPSEC protokolu je izvedeno na podoben način kot v IPSEC.

Za zagotavljanje zaupnosti podatke originalne MAP operacije zašifriramo. Dodana je varnostna glava, ki označuje način dešifriranja informacije. Za zagotavljanje integritete se uporablja MAC, ki se izračuna za nešifrirane podatke. Časovno odvisen parameter skrbi, da ne prihaja do zlorab s ponovitvami.

Varnost MAPSEC temelji na IKE protokolu. Za ključe skrbijo entitete z imenom KAC (Key Administration Centres), ki delijo ključe med ostalimi CN elementi znotraj omrežja. Zato je bila potrebna razširitev IKE protokola (nov IETF standard).

7. Varnost na nivoju aplikacij in storitev

Varnost v omrežju je izvedena v skladu z OSI modelom. Vsak nivo v sistemu OSI ima svoje varnostne namene. Za poenostavitev in lažji pregled, razdelimo protokole na dve glavni področji: varnost na nivoju povezav (link-by-link security), varnost na nivoju poti (end-to-end security).

Pri prvi zaščiti je osnovna ideja, da je komunikacijska pot (path) sestavljena iz povezav (link). Vse, kar se prenaša preko določene povezave je zaščiteno (šifrirano). Ker to velja za vse povezave vzdolž poti, je cela komunikacijska pot varna. Slabost tega načina je v tem, da je promet, ki je napačno usmerjen, lahko prebran in zlorabljen, česar končni uporabnik niti ne izve.

Če pa je varnost zagotovljena z višjimi OSI nivoji, potem govorimo o varnosti na nivoju poti (end-to-end security) V tem primeru so podatki zaščiteni (šifrirani) do ciljnega uporabnika. Podatki so v tem primeru dobro zaščiteni, vendar pa še vedno ostaja možnost zlorabe z analizo prometa *(traffic analysis)*: napadalec uspe ugotoviti, kdo pošilja podatke in kdo jih sprejema, ne uspe pa prebrati vsebine. Ker sta pogostost komunikacije in čas komunikacije včasih že sama po sebi zgovorna podatka, se marsikdaj za zaščito uporablja kombinacija obeh področij. Šifriranje na nivoju povezav onemogoča analizo informacij o usmerjanju, šifriranje na nivoju poti pa nam omogoča zaščito podatkov.

Kot smo že opazili, je v posebnih primerih (celična omrežja) za dostopa do omrežja na povezavnem nivoju (link layer) zahtevano overjanje. V 3G omrežjih za podatke, potrebne za šifriranje in zagotavljanje integritete poskrbi procedura overjanja.

7.1. Varnost na nivoju aplikacij

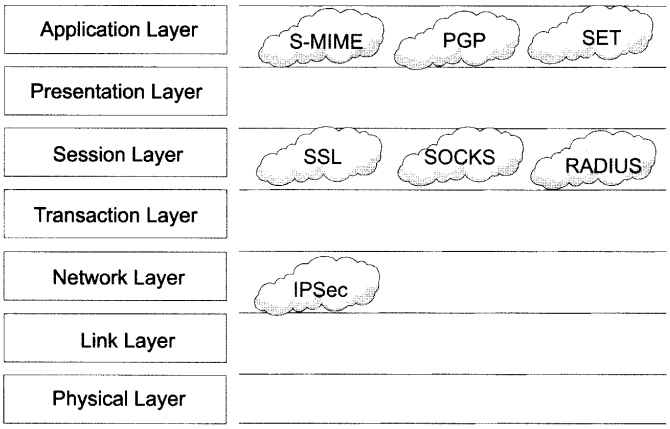
Najpogostejši mehanizmi za zagotavljanje zaščite na aplikacijskem nivoju so S-MIME, PGP, PEM, S-HTTP in SET.

S-MIME (Secure Multipurpose Internet Mail Extension) je protokol ki digitalno podpisuje in šifrira MIME sporočila. Razvit je bil pod okriljem RSA Date Security Inc. In temelji na Triple-DES šifrirnem algoritmu. Uporablja X.509 digitalne certifikate. S-MIME uporablja šifrino metodo javnih ključev RSA in Diffie-Hellman sistem za upravljanje ključev. SHA-1 (Secure Hash Algorithm #1) se uporablja za zagotavljanje integritete podatkov. Velik razmah je doživela druga verzija tega protokola: S-MIME v2; v letu 1999 pa je bila sprejeta že verzija 3.

PGP (Pretty Good Privacy) je brezplačna programska oprema, ki omogoča varno komunikacijo preko elektronske pošte. Zagotavlja zaupnost in overjanje elektronski pošti z uporabo šifriranja in elektronskega podpisa. PGP uporablja IDEA (International Data Encryption Algorithm) za enkripcijo in RSA za upravljanje s ključi in digitalno podpisovanje. Integriteta podatkov je zagotovljena z MD5 (Message Digest #5). Pri PGP algoritmu pa je uporabljen zelo zanimiv pristop za izmenjavo ključev. PGP uporablja porazdeljen sistem za hranjenje ključev; zato ne potrebuje CA (certificate authority), vsak uporabnik generira in distribuira svoj javni ključ. Uporabniki si medsebojno podpisujejo javne ključe, s tem pa

tvorijo med seboj povezano skupino PGP uporabnikov. Prednost te metode je odsotnost CA strežnikov, ki sicer predstavljajo nujno točko zaupanja. Vsak uporabnik pa mora imeti shranjeno kolekcijo podpisanih javnih ključev v datoteki. Vsak izmed teh ključev pa vsebuje polje, v katerem je zapisana stopnja, s katero zaupamo uporabniku. Uporabnik alhko to polje določi ročno. Slabost PGP pristopa pa je preklicevanje ključev. Če uporabnik privatni ključ izgubi ali pa mu je ta ukraden, potem mora o tem obvestiti ostale uporabnike, ki uporabljajo njegov javni ključ. Ker je za izmenjave tega podatka potreben določen čas, v tem vmesnem času že lahko pride do zlorabe.

Zgoraj predstavljena protokola sta namenjena uporabi pri elektronski pošti. Internet, še posebej ob souporabi mobilne komponente prihajajoče z uporabo sistemov 3G, pa je zelo zanimiv tudi za bančne transakcije. Te zahtevajo zelo zanesljivo povezavo, kajti od zaupanja vanje je odvisen njihov prodor. Visa in MasterCard sta v sodelovanju z ostalimi partnerji (IBM...) razvili protokol z imenom SET (Secure Electronic Transactions). SET uporablja sistem digitalnih certifikatov za preverjanje identitete vseh v SET transakcijo vključenih partnerjev. Originalen protokol je z vidika uporabnika videti relativno kompliciran za uporabo, zato so pred nedavnim izdelali novo verzijo, bolj enostavno za uporabo.



Slika 7.1: Primeri varnostnih protokolov po OSI nivojih

7.2. Varnost na nivoju seje

Na nivoju seje OSI protokolnega modela se uporablja SSL protokol. Prvi SSL protokol je razvil Netscape Communications Corporation za zagotavljanje privatnosti in zasebnosti in zanesljivosti med dvema komunicirajočima aplikacijama. SSL uporablja šifriranje z javnim ključem za izmenjavo t.i. ključev seje (session key) med odjemalcem in strežnikom. Ključ seje se uporablja za šifriranje http zahtevkov. Vsaka transakcija uporablja drug kljuc seje, tako da se nekdo, ki uspe odšifrirati eno transakcijo ne more dokopati do celotne seje. V preteklosti se je zaradi izvoznih omejitev uporabljal 40 bitni ključ (v USA 128 bitni ključ), danes pa so te omejitve odstranjene.

Iz SSL se je razvil TSL protokol (Transport Layer Protocol). Modificirana verzija tega protokola – optimizirana za brezžična omrežja – WTSL (Wireless Transport Layer Security) se uporablja tudi pri WAP sejah.

7.3. Varnost IMS

Glavni dodatek UMTS Release 5 je IP multimedijski podsistem (IP Multimedia Subsystem – IMS). Načrtovan je neodvisno od dostopovnega nivoja omrežja, zato varnost ne more temeljiti samo na mehanizmih, ki jih ponuja UMTS sistem. Nadzor nad IMS sistemom izvaja SIP protokol, ki nadzoruje uporabniško raven.

Medsebojno overjanje prestavlja temeljni kamen varnosti IMS. Zaupnost in integriteta signalizacije SIP sta zagotovljeni že na nivoju UMTS overjanja, ker se uporabljajo isti algoritmi pri UMTS kot tudi pri IMS. Ne glede na enakost uporabljenih mehanizmov pa je izvajanje overjanja lahko tudi neodvisno od UMTS ravni. Obstaja tudi možnost uporabe drugih ključev.

8. Zakonske omejitve

Ključen problem pri zagotavljanju varnosti predstavlja šifriranje informacij na tak način, da so dostopne samo pravemu prejemniku. V večjem delu seminarske naloge smo se ukvarjali z mehanizmi, ki nam omogočajo tovrstno funkcionalnost v prihajajočih omrežjih 3G (UMTS).

Vendar pa pri implementaciji tako široko uporabljane storitve tehnologija ne predstavlja edine omejitve. V mnogo državah lokalna zakonodaja in regulative omejujejo šifrirne algorime, ki se smejo uporabljati. Poleg tega lokalne organi postavljajo zahteve, ki jih morajo entitete UMTS "zgodbe" (ponudniki, uporabniki) upoštevati. Tako denimo, ponekod oblasti želijo imeti nadzor nad občutljivimi informacijami, nadzor nad uporabniki, kot naprimer možnost prisluškovanja klicem in nadzor nad podatkovnim prometom (tako vodovno

Zbirani podatki	**Opis**
Opazovan MSISDN	Ciljni MSISDN nadzorovanega naročnika
Opazovan IMSI	Ciljni IMSI nadzorovanega naročnika
Opazovan IMEI	Ciiljni IMEI nadzorovanega naronika. Preverja se ob vsakem klicu preko radijskega vmesnika
Tip dogodka	Opis dogodka, ki se izvede: Vzpostavitev, odgovor, handover, prekinitev zveze, SMS ...
Datum dogodka	Datum izvedbe dogodka v 3G MSC
Čas dogodka	Čas izvedbe dogodka v 3G MSC
Klicana številka	Klicana številka nadzorovanega naročnika
Povezana številka	Številke, ki so klicale nadzorovanega naročnika
Naslov ostalih entitet	Številka preostalih entitet za MOC, klicane entitete za MTC
Smer klica	Informacija o tem, ali je bil nadzorovn uporabnik klican ali je on klical: MOC/MTC
Informacija o lokaciji	Lokacija storitve, ki je zapisana v 3G MSC v času zabeležbe dogodka
Osnovna storitev	Podatek o osnovni storitvi
Dodatne storitve	Dodatne storitve, ki jih nadzorovani uporabnik uporablja.
Preusmeritev na št.	CF preusmeritev na številko
Razlog za prekinitev	Razlog za prekinitev ciljnega klica nadzorovanega uporabnika
SMS message	The SMS content with header which is sent with the SMS-service
Preusmeritev iz št.	Številka, s katere se je klic preusmeril na številko nadzorovanega uporabnika
SCI	Informacije, ki niso povezne s klicem, pa jih 3G MSC prejme od UE.

Tabela 8.1: Podatki, ki jih je mogoče zbirati v omrežju s preklapljanjem vodov z legalnim prisluškovanjem

komutiranim kot paketnim). Pri GSM sistemu je bila tovrstna funkcionalnost na vrhu spiska funkcionalnosti, ki jo je bil potrebno v omrežje dodati naknadno, medtem ko so zgoraj omenjene lokalne zahteve v 3G sistemih našrtovane že od samega začetka.

Zakonito prisluškovanje je sestavljeno iz treh delov:

- Prisluškovalna oprema/funkcionalnost
- Posredovalne naprave
- Prisluškovane informacije

Prisluškovalna oprema zbira podatke, zapisane v Lokalne oblasti določijo, katere podatke želijo zbirati in katere ne. Filtriranje opravijo posredovalne naprave, ki prikažejo le tiste podatke, ki jih definirajo lokalne oblasti. Filtrirane informacije se imenujejo dostopne prestrezene informacije. Poleg spiska naštetega v Tabela 8.1 obstajajo še drugi parametri, ki jih želijo lokalni organi nadzorovati. Tako, denimo, bo v bližnji prihodnosti potrebno locirati naročnika na 50 m natančno. Podobne informacije se že danes javljajo v primeru klicov v sili oziroma je na podlagi teh informacij v primeru klica na policijsko številko klic uporabnika preusmerjen v najbližjo lokalno policijsko postajo. Informacije o lokaciji se pridobivajo s posebnimi napravami, v sistemih 3G se imenujejo sistem za pozicioniranje. Opis teh pa je lahko predmet naslednje seminarske naloge. Morda pri drugem predmetu.

9. Pomanjkljivosti pri zaščiti podatkov v UMTS

Poglejmo si probleme v zvezi z zaščito podatkov v UMTS, ki jih lahko še vedno izpostavimo kot nerešene:

- Ključi za zagotavljanje integritete med UE in RNC, generirani v VLR/SGSN se prenašajo v nekriptirani obliki do RNC oziroma včasih tudi med RNC-ji.
- Uporabniškim podatkom ni mogoče zagotavljati integriteto
- V omejeno kratkem času med signalnimi procedurami so signalizacijki podatki nezaščiteni in izpostavljeni napadom

Zaščita integritete je izvedena le na omejih področjih sistema. Zaščiteni so le signalizacijski podatki, zaščita je omejena na komuniakcijo med SRNC in UE. Poleg tega obstaja nabor sporočil, ki so na radijskem vmesniku še vedno prisotna v popolnoma nezaščiteni obliki.

Protokoli, ki prenašajo ključe za zagotavljanje integritete so naslednji:

- MAP (med HLR/AuC in VLR/SGSN v jedrnem omrežju)
- RANAP (preko Iu vmesnika med VLR/SGSN in strežnim RNC)
- RNSAO (preko Iur- vmesnika med RNC v "handover" situaciji)

V UMTS Release 99 se ključi prenašajo nezaščiteni tako preko jedrnega kot tudi preko Iu/Iur vmesnikov. To predstavlja varnostno luknjo, katere se morajo operaterji zavedati. Linije, po katerih se podatki prenašajo morajo biti varovane fizično ali s šifriranjem na povezavi točka-točka.

V bolj zgodnjih specifikacijah varnosti je bilo določeno, da bo VLR/SGSN končna točka, kjer se terminira integriteta oziroma šifriranje. Ker ni več tako, morajo biti podatki zašččiteni na nivoju Iu vmesnika. Razvijalci so zaznali potrebo po realizaciji za zaščito celotnega omrežja, vendar pa RNC navadno podpira relativno veliko omrežje in če je nastanjen na isti lokaciji kot VLR/SGSN, potem je zaščito signalnih podatkov relativno enostavno izvesti. Problem zaščite Iu vmesnika pa nastopi pri omrežjih z več RNC-ji za vsak VLR/SGSN.

Dejstvo, da uporabniški podatki nimajo implementirane zaščite integritete, še ne pomeni, da se uporabniški podatki popolnoma prosto prenašajo preko omrežje.

Spremembe lahko ugotovijo mehanizmi za ugotavljanje napak, poleg tega pa so le-ti podatki tudi nekoliko manj na udaru, kajti napadalec ne ve natančno, kaj bo dobil, če bo dešifriral določen sklop podatkov.

Zadnja ugotovitev velja le za govorne informacije in morda splošne paketne informacije. Kadar pa gre za občutljive bančne transakcije, pa je potrebno vzpostaviti zaščito na nivoju poti (end-to-end).

Identifikacija s stalno identiteto in AKA se navadno izvede pred začetnkom vzpostavljanja varne zveze. Nezaščiteno prenašanje stalne identitete ogrozi zaupnost

uporabnikove identitete, lahko pa je identiteta tudi motena ali prevzeta. To je sicer bistveno bolj zapletena operacija kot zgolj prisluškovanje.

Med fazo dogovarjanja o ključih pa je možen napad z nedostopnostjo storitev, ki temelji na prenašanju nešifriranih varnih podatkov med UE in RNC. Napadalec, denimo, spremeni te podatke, ki jih UE pošilja RNC, zato jih ta ni sposoben shraniti in terminira povezovalni postopek, kar uporabnik občuti kot nedostopnost storitve.

10. Zaključek

Ta trenutek vstopamo v tretjo generacijo mobilne telefonije. Tudi Slovenci se bomo z njo srečali zelo kmalu. Postopki standardizacije so pognali korenine v prejšnje desetletje, prvič bi si tokrat upal trditi da prihaja do pravega zlivanja sveta IP, ki smo ga do sedaj imeli za računalniško omrežje in ga v določenih vidikih podcenjevali in telekomunikacijskega omrežja, ki je bil vedno razpoložljivo (s sedmimi deveticami), zanesljivo in varno.

Zlivanje v novo telekomunikacijsko omrežje prineslo tudi »hackerje«, ki poznajo in obvaldajo nove tehnologije. Kljub željam, da bi iz omrežij prejšnih generacij (2G) ter sveta IP pobrali čimveč pozitivnih lastnosti, z nabranimi izkušnjami pa odstranili morebitne pomanjkljivosti, je še predno je otrok privekal na svet s stališča varnosti že mogoče videti, da ni vse tako, kot je bilo obljubljeno.

V omrežjih druge generacije je bilo dalenač najbolj kritizirano zaotavljanje integritete podatkov. Predstavljena zaščita integritete v UMTS omrežju kaže bistven napredek v primerjavi z GSM. Integriteta je zgotovljena signalizacijskim podatkom med RNC in UE. V primeru, da šifriranje ni uporabljeno, bodisi zaradi lokalne regulative ali pa zaradi odločitve individualnega uporabnika, zgotavljanje integritete nudi zaščito proti prevzemom seje.

Uporabnički podatki niso zaščiteni pred manipulacijo. Za osnovno varnost je lahko poskrbljeno na višjih nivojih. Za nekatere uporabniške podatke to predstavlja zadostno zaščito.

Promet preko jedrnega omrežja (core traffic) ni zaščiten niti s šifriranjem, niti nima zagotovljene integritete. Signalizacijski podatki, kot tudi ključi, ki se kasneje uporabljajo za zaščito podatkov se prenašajo popolnoma nezaščiteni.

Vendar pa je potrebno povdariti, da se nekatere zadeve še vedno spreminjajo. Kljub temu, da je že prišlo do prvih implementacij, se standardizacija še vedno spreminja, vsekakor pa je potrebno povdariti, da je le-ta napisana zelo odprto; kot je razvidno tudi iz seminarske naloge, so nekateri deli napisani zelo splošno, in je algoritme za izvedbo mogoče določati naknadno, ali pa so lahko le-ti specifični za vsakega operaterja. To pa pomeni, da bo za razliko od omrežij 2G možno algoritme mogoče nadgrajevati tudi kasneje oziroma nekatere izmed morebitnih napak odpraviti tudi post-festum. To pa se meni osebno zdi zelo pomembna pridobitev.

11. Literatura

[1] ETSI, Technical Specification: Universal Mobile Telecommunication System (UMTS), 3G Security, **Security Threats and Requirements – TS 21.133**. December 1999, http://www.3gpp.org/

[2] ETSI, Technical Specification: Universal Mobile Telecommunication System (UMTS), 3G Security, **Security Architecture – TS 33.102**. Marec 2001, http://www.3gpp.org/

[3] ETSI, Technical Specification: **Specification of the MILENAGE Algorithm Set**: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5* **– TS 35.206**. April 2001, http://www.3gpp.org/

[4] ETSI, Technical Specification: **Specification of the 3GPP Confidentiality and Integrity Algorithms: f8 and f9 Specification – TS 35.201**. Julij 2001, http://www.3gpp.org/

[5] ETSI, Technical Specification: **Specification of the 3GPP Confidentiality and Integrity Algorithms: KASUMI Specification – TS 35.202**. Julij 2001, http://www.3gpp.org/

[6] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, V. Niemi: **UMTS Networks, Architecture, Mobility and Services**, John Wiley & Sons. 2001, str. 182-207

[7] R. Langnes: **Security in UMTS – Integrity**, Reprort, Telenor R&D. Februar 2001

[8] John Charles Francis, Holger Herbrig, Nigel Jefferies: **Secure Provision of UMTS Services over Diverse Access Networks**, IEEE Communications Magazine. Februrar 1998, str. 128-136

[9] Asha Mehrotra, Leonard S. Golding: **Mobility and Securitiy Management in the GSM System and Some Proposed Future Improvements**, Proceedings of IEEE, Vol. 86, No. 7. Julij 1998, str 1480-1497

[10] Refik Molva, Didier Samfat, Gene Tsudik: **Authentication of mobile users**, IEEE Network. Marc/april 1994, str. 26-34

[11] J. Francis, H. Herbrig, N. Jefferies: Secure Provision of UMTS Services over Diverse Access Networks, IEEE Communications Magazine. Februar 1998, str. 127-136

[12] G. Vanneste, J. Degraeve, g. Lyberopoulos, Y. Vithynos, C. Cooke: **Migration/Evolution Towards UMTS – Security Issues.** Junij 2000. http://www.esat.kuleueven.ac.be/cosic/aspect/papers/A061_E2.htm

[13] Kravcar Mateja: **Overovitev identitete naročnika omrežja GSM**, diplomska naloga, Fakulteta za elektrotehniko, Univerza v Ljubljani. Marec 1995

[14] Janos A. Csirik: **A guide to 3GPP security documents,** http://www.research.att.com/~janos/3gpp.html

[15] Peter Howard: **UMTS Security Architecture,** USECA. December 1998