Varnost v mobilnih sistemih UMTS

Iztok HUMAR, Sašo TOMAŽIČ
Laboratorij za telekomunikacije
Fakulteta za elektrotehniko
Univerza v Ljubljani
Tržaška 25, 1000 Ljubljana, Slovenija
email: iztok.humar@fe.uni-lj.si
web: http://www.ltfe.org/iztok

Abstract
Important aspects of security in the UMTS are discussed in this paper. The threats and requirements derived from threat analysis are defined, the security architecture is explained and network access security mechanisms are outlined.

Uvod

Tretja generacija mobilnih sistemov bo prinesla širok nabor telekomunikacijskih storitev, vključno z govorom, videom, podatkovnimi povezavami in kompleksnimi multimedijskimi storitvami. Digitalna omrežja pa hkrati prinašajo uporabnikom možnost uporabe dodatnih storitev povezanih z varnostjo, ki temeljijo na uporabi USIM – pametne kartice, ki identificira naročnika v omrežju. Varnostni sistemi v UMTS sistemih morajo zagotavljati overjanje, šifriranje, integriteto in druge varnostne storitve, ki si jih bomo ogledali v nadaljevanju.

1. Grožnje varnosti 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 overjenega uporabnika, da je legitimen element sistema in na ta način od njega pridobi zaupno informacijo. Prav tako lahko vsiljivec pretenta legitimen sistem, da je overjen 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.
- **Prepuščanje (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 zmanjševanje dostopnosti ali nedostopnost storitev)

- **Poseganje (Intervention):** Vsiljivec prepreči uporabo storitev overjenemu uporabniku z motenjem prometa, signalizacije ali krmilnih informacij.
- **Blokada virov (Resource Exhaustion):** Vsiljivec prepreči overjenemu uporabniku dostop do storitve s preobremenitvijo storitve.
- **Zloraba storitev (Abuse of services):** Vsiljivec 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:

- **Pretvarjanje (masquerading):** Vsiljivec dostopa do storitev s pretvarjanjem, da je uporabnik ali omrežna entiteta ali domače omrežje HE
- **Zloraba privilegijev (Misuse of privileges):** Uporabnik ali strežno omrežje lahko zlorabi svoje privilegije za nepooblaščen dostop do storitev ali informacij.

Grožnje, navedene v zgoraj naštetih kategorijah se lahko razdelijo glede na naslednje točke napada:

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

2. Varnostne zahteve

Iz analize zgoraj navedenih groženj, ki pretijo varnosti v sistemih tretje generacije, so izpeljane varnostne zahteve.

2.1. Zahteve za varen dostop do storitev

Potreben pogoj, da lahko uporabnik dostopa do 3G storitev, je veljaven USIM. Zahteve predvidevajo sposobnost preprečevanja dostopa do 3G storitev vsiljivcem, ki se pretvarjajo, da so pooblaščeni uporabniki. Prav tako mora biti možno preveriti, ali je strežno omrežje overjeno za ponujanje 3G storitev za uporabnikovo domače okolje in sicer na začetku in med uporabo ponujenih storitev.

2.2. Zahteve za varno zagotavljanje storitev

Zahteve te skupine predvidevajo zmožnost, da ponudniki storitev overijo uporabnika na začetku in med uporabo storitev ter na ta način onemogočijo vsiljivcem nepooblaščen dostop do ponujenih storitev.

Obstajati mora zmožnost zaznavanja in odpravljanja sleparske uporabe storitev ter alarmiranja ponudnika storitev o zlorabah. Predvideno je beleženje poročil o dogodkih. V primeru zlorab se predvideva zmožnost preprečevanja dostopa posameznim USIM do posameznih ali vseh 3G storitev.

Strežna omrežja morajo biti sposobna preverjati izvor uporabniškega prometa, signalizacijo podatkov in krmilne podatke na radijskih vmesnikih ter onemogočiti, 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.

2.3. Zahteve za zagotavljanje sistemske integritete

Zahteve te skupine zagotavljajo zaščito pred nepooblaščenimi spremembami uporabniškega prometa, signalnih in krmilnih informacij, posebno na radijskih vmesnikih, zaščito pred nepooblaščenimi spremembami uporabniških podatkov, naloženih in shranjenih v terminalu ali USIM, zaščito pred nepooblaščenimi spremembami uporabniških podatkov, obdelanih in shranjenih pri ponudniku storitev.

Zagotavljajo podatke o viru in integriteti aplikacij in podatkov, naloženih na terminal in UICC ter zmožnost preverjanja le-teh. Prav tako je potrebno zagotoviti njihovo zaupnost.

Prav tako morajo biti zagotovljeni podatki o izvoru ter integriteta overovitvenih podatkov, posebej šifrirnega ključa (chiper key) na radijskem vmesniku.

Obstajati mora možnost komunikacije med operatorji prek varne infrastrukture.

2.4. Zahteve za zaščito osebnih informacij

- **Varnost uporabniških podatkov, ki se prenašajo prek omrežja**

V sklop zahtev za zagotavljanje uporabniških podatkov, ki se prenašajo preko omrežja sodijo: zmožnost zagotavljanja zaupnosti uporabniškim podatkom, signalnim in krmilnim podatkom posebno na radijskem vmesniku, zaupnosti podatkov o identiteti in lokaciji uporabnikov.

Uporabnik mora biti sposoben preveriti, ali so njegovi podatki in z njim povezane informacije med prenosom zaščitene. Tovrstno preverjanje mora zahtevati minimalen napor.

- **Varnost uporabniških podatkov, ki so shranjeni v sistemu**

Ponudnik mora biti sposoben zagotoviti zaupnost uporabniškim podatkom, ki jih shranjuje ali procesira.

Prav tako mora biti zagotovljena zaupnost uporabniškim podatkom, shranjenih na uporabniškem terminalu ali USIM.

2.5. Zahteve za terminal in USIM

- **Varnost vezana na terminal**

Terminal mora s svojimi lastnostmi odvračati od kraje.

Zagotovljeno mora biti onemogočanja dostopa do 3G storitev na posameznih terminalih, seveda pa mora biti onemogočeno tudi spreminjanje identitete terminalov z namenom, da bi zaobšli prepoved dostopa do storitev.

- **Varnost vezana na USIM**

Tako kot pri terminalu, je tudi pri USIM mogoče omejevati dostop. S tem je z USIM kartico omogočen dostop do 3G storitev samo tistim uporabnikom, ki so eksplicitno overjeni s strani naročnika.

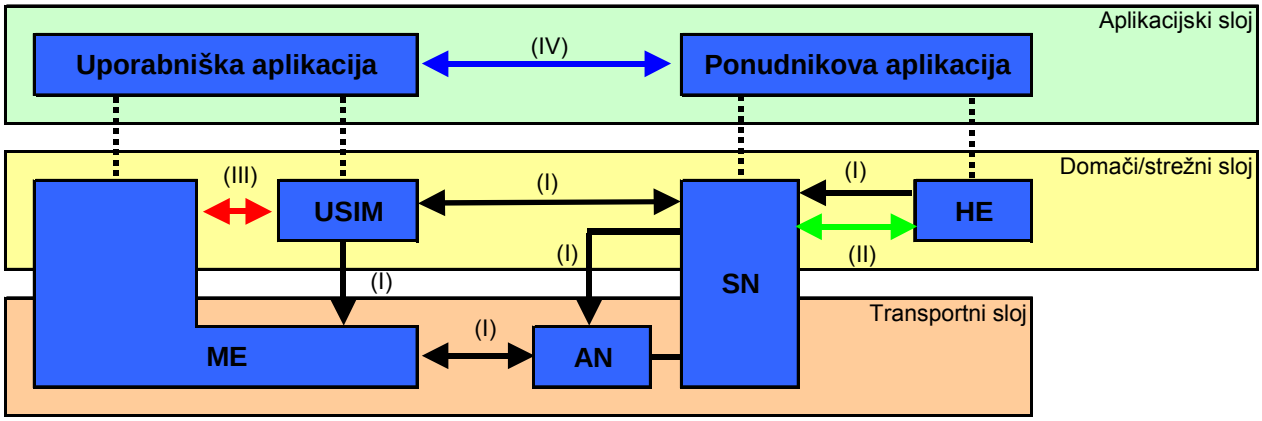
Tudi dostop do podatkov, shranjenih na USIM, je mogoče omejiti. Nekateri podatki, na primer, so dostopni samo overjenemu domačemu okolju, drugi pa so namenjeni le uporabi znotraj samega USIM (šifrirni ključi in algoritmi)

2.6. Zunanje zahteve - pravno/regulacijske zahteve

Agencije, ki delujejo pod pravnim nadzorom, morajo imeti možnost nadzorovati in prestreči vsak klic ali željo po vzpostavitvi klica ter preostale storitve in uporabniške namere, v skladu z nacionalno zakonodajo in regulacijami.

3. Pregled varnostne arhitekture

Na sliki 1 imamo pregled nad celotno 3G varnostno arhitekturo.



Slika 1: Pregled varnostne arhitekture

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

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

Skupina varnostnih lastnosti, ki omogoča uporabnikom, da preverijo uporabo varnostnih lastnosti in če zagotavljanje oziroma uporaba storitev temelji na mehanizmih varnega prenosa.

Za nekatere izmed skupin standardizacija še ni izdelana.

Skupine vsebujejo mehanizme, ki izvajajo njihov namen. V nadaljevanju si oglejmo povzetek pregleda mehanizmov za zaščito dostopa do omrežja.

4. Mehanizmi za zaščito dostopa do omrežja

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.

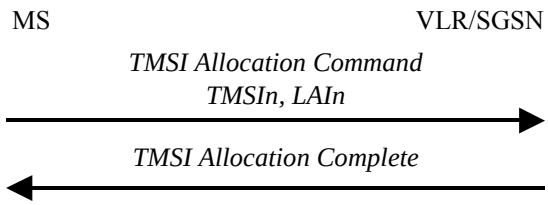
TMSI se uporablja pri zahtevi za priklop, zahtevah za storitve, osvežitvah lokacije, zahtevah za ponovno vzpostavitev povezave, zahtevah za izklop, itd.

Postopki so podobni mehanizmom uporabljenih v sistemih GSM.

Postopek določanja TMSI

Postopek se izvede takoj po vzpostavitvi šifriranja.

VLR izračuna 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.



Slika 2: Postopek določanja TMSI

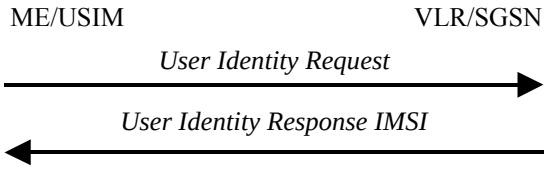
Po sprejemu TMSIn ga uporabnik shrani ter avtomatično odstrani stari TMSIo. Uporabnik pošlje potrdilo o sprejemu VLR.

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

4.2. Identifikacija s stalno identiteto

Mehanizem 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. To se, denimo, zgodi ob prvi prijavi v omrežje ali kadar omrežje ne more določiti IMSI iz TMSI, s katerim se želi uporabnik identificirati.

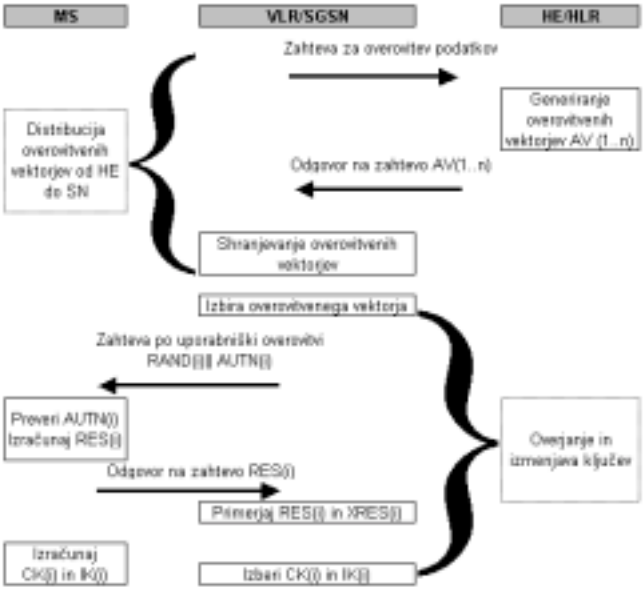


Slika 3: Identifikacija s stalno identiteto

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, zato je tovrstno predstavljanje omrežju smiselno uporabljati le v nujnih primerih.

4.3. Overjanje in dogovor o ključih

Naveden mehanizem zagotavlja medsebojno overjenje med uporabnikom in omrežjem. Oba morata namreč poznati skrivni ključ seje *K*, ki je dostopen samo USIM in v AuC v uporabnikovem HE.



Slika 4: Overjanje in izmenjava ključev

Ta mehanizem je bil izbran zaradi zagotavljanja združljivosti z obstoječo varnostno arhitekturo GSM sistema ter s tem pospeševanja prehoda iz GSM na UMTS sistem. Mehanizem temelji na protokolu zahteva/odziv (challenge/response), ki je identičen overjanju GSM uporabnika in sporazumevanju o ključih, združenim s protokolom, ki temelji na sekvenčnem štetju enkratnih prehodov za mrežno overjanje, izpeljanim iz ISO standarda.

VLR/SGSN pošlje zahtevo za overjanje. HE/AuC se odzove z urejenim poljem overovitvenih vektorjev, razvrščenim po sekvenčnih številkah, ki jih vrne VLR/SGSN. Vsak overitveni vektor vsebuje naslednje komponente:

- Naključno število RAND
- Pričakovan odziv na naključno število XRES
- Šifrirni ključ CK in integritetni ključ IK
- Overovitveni žeton AUTN

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

Ko VLR/SGSN začne overjanje in dogovarjanje o ključih, izbere naslednjega izmed vektorjev urejenega polja in pošlje parametra RAND in AUTN uporabniku. 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.

Literatura

[1] Refik Molva, Didier Samfat, Gene Tsudik: **Authentication of mobile users**, IEEE Network, March/April 1994, str 26-34

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

[3] 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, July 1998, str 1480-1497

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

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

[6] ETSI, Technical Specification: Universal Mobile Telecommunication System (UMTS), 3G Security, **Security Threats and Requirements – TS 21.133**, 1999-12, http://www.3gpp.org/

[7] ETSI, Technical Specification: Universal Mobile Telecommunication System (UMTS), 3G Security, **Security Architecture – TS 33.102**, 2001-03

[8] USECA: UMTS **Security Architecture**, december 1998