3. Domaća Zadaća

3.Inačica

3) Objasnite osnovne sigurnosne prijetnje u mreži UMTS (autentičnost pretplatnika, autentičnost opreme i tajnost komunikacije) te načine zaštite protiv njih.

UMTS mreža je jedna od tehnologija mreža treće generacije. Oblik UMTS-a koji se najčešće koristi je W-CDMA (Wideband Code Division Multiple Access). Uvođenje UMTS-a uvele su se nove usluge koje potražuju viši sigurnosni nivo od GSM-a, paralelno uz uvođenje postoji potreba ispraviti uočene greške i nedostatke kod GSM-a.

Glavne sigurnosne prijetnje u mobilnoj komunikaciji su od strane korisnika poput lažno predstavljanje (krađa tuđeg identiteta), prisluškivanje i sniffanje podataka nekog korisnika, krađa podataka od treće strane (spajanje na lažnu baznu stanicu), neovlašteno praćenje korisnika unutar mreže i slično. Zato se koriste različiti mehanizmi i mogućnosti zaštite koji se konstantno razvijaju da prate razvoj ostalih mobilnih usluga.

Nova mogućnost koju pruža UMTS je zaštita identiteta i lokacije pokretne stanice. U UMTS mreži provodi se autentifikacija mreže i korisnika. Mreža autentificira korisnika da spriječi lažno predstavljane (krađa identiteta) ili neovlašteno spajanje na mrežu. Novost je da i sam korisnik autentificira mrežu da spriječi spajanje na lažnu baznu stanicu (krađa podataka). Taj smjer autentifikacije je nov u odnosnu na GSM gdje je autentifikacija jednosmjerna.

Postupak autentifikacije koristi korisnički zahtjev (RAND), Odgovor mreže (XRES), ključ šifriranja i integriteta (CK, IK) i autentifikacijski token (AUTN).
Početak autentifikacije se započinje slanjem IMSI ili TIMSI -> VLR kao i kod GSM komunikacije. Nakon što VLR pošalje IMSI ili TIMSI AuC za autentificiranje korisnika njegove mreže, generira se vektor autentifikacije pomoću dobivenih podataka. Taj vektor se šalje nazad VRL koji je poslao zahtjev za autentificiranjem. Nakon što VLR zaprimi vektor, šalje nazad mobilnoj stanici RAND (korisnički zahtjev) i AUTN (token za autentifikaciju). Mobilna stanica šalje podatke kartici USIM koja generira na osnovnu primljenih podataka RES (odgovor). Ukoliko se primljeni XRES od AuC i RES od mobilne stanice poklapaju, korisnik je uspješno autentificiran i može započeti korištenje mreže. Dodatno, korisnik autentificira mrežu pomoću MAC i XMAC poruke koji se isto šalju u RES (odgovoru).

Dodatni sigurnosni mehanizam je da se jedan vektor autentifikacije može koristiti samo 1, svaki puta se generira novi. Na taj način se spriječava korištenje istog vektora za ponovno autentificiranje nekog korisnika. Pokraj toga, koriste se duži ključevi za šifriranje u odnosnu na GSM, podržan je novi F9 algoritam prilikom provjeravanja cjelovitosti i nova poboljšana metoda šifriranja, F8 algoritam.

Tajnost komunikacije postiže se korištenjem MAPsec u komunikaciji čvorova mobilne mreže. Obični podaci se kriptiraju i stavljaju se u „kontejner“ koji se nakon toga stavi u novu MAP poruku. Ta MAP poruka se kriptografski zaštiti izračunatom sumom koja se nalazi u MAP poruci. Da bi se pročitali ti isti podaci, potrebno je poznavati autentifikacije ključeve koji su poznati samo čvorovima. Na taj način podaci su zaštićeni od prisluškivanja, izmjeni ili krađe. MAPsec se bazira na principu IPsec.

LITERATURA:

Predavanja iz kolegija Javna pokretna mreža
http://www.fer.unizg.hr/_download/repository/JPM-2015-11n.pdf

Sigurnost mobilnih mreža, Carnet
http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-303.pdf

UMTS Security, Wikipedia
https://en.wikipedia.org/wiki/UMTS_security

Bezbednost mobilnih mreža najnovije generacije, Dušan Kilibarda
http://www.raf.edu.rs/docs/Diplomski_radovi/Bezbednost_mobilnih_mrea_najnovije_generacije.pdf