Fakultet elektrotehnike i računarstva

Modul: Telekomunikacije i informatika

Javna pokretna mreža (ak. god. 2014./2015.)

3. domaća zadaća

Zadatak:

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

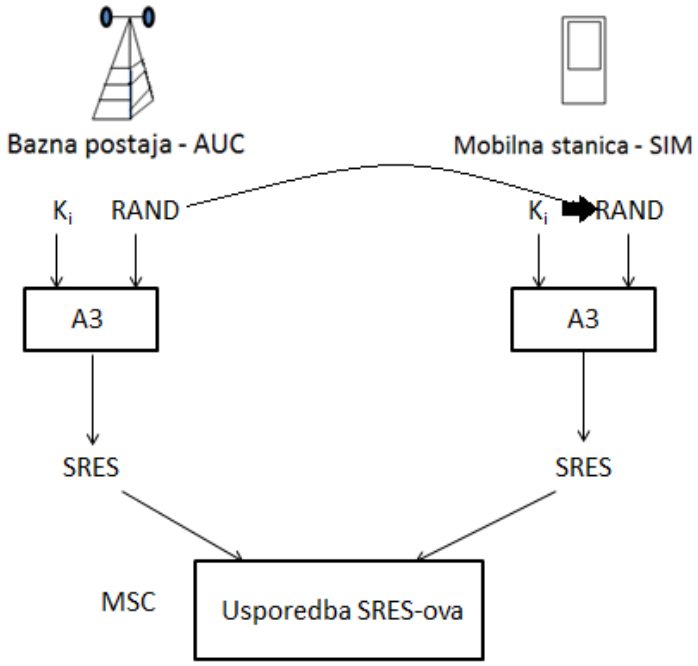
Rješenje:

Za razumijevanje postupaka u ostvarivanju sigurnosti u GSM mreži potrebno je poznavati sljedeće pojmove:

- MSISDN – pozivni broj pretplatnika kojeg dodjeljuje mrežni operator, a nalazi se u HLR-u i na SIM kartici
- IMSI – međunarodni identitet mobilnog pretplatnika kojeg također dodjeljuje mrežni operator te se nalazi u HLR-u i na SIM kartici
- IMEI – međunarodni identitet pokretne opreme, odnosno jedinstveni broj uređaja kojeg dodjeljuje proizvođač uređaja i on se nalazi u registru za identifikaciju opreme, EIR-u
- K_i – jedinstveni tajni 128-bitni ključ koji omogućuje provjeru autentičnosti pretplatnika i pohranjen je u centru za provjeru autentičnosti (AUC) i na SIM kartici. Koristi se u autentifikaciji koja se sastoji u provjeri posjeduje li MS K_i.

Iz razloga što su u SIM-u pohranjeni IMSI i K_i koji moraju biti tajni, SIM se štiti PIN tajnim kodom. Poznaje li netko naš IMSI, može se lažno predstaviti i neovlašteno pristupati mreži. Kao zaštita od takve prijetnje služi autentifikacija korisnika prilikom svakog zahtjeva za registracijom. Kad korisnik pristupa SIM-u upisuje tajni broj PIN, zatim preko SIM-a pristupa mreži i tad se odvija autentifikacija. Bazna stanica

generira slučajni 128-bitni broj RAND koji šalje pokretnoj postaji. U baznoj stanici u centru za autentifikaciju AUC i u SIM-u autentifikacijskim algoritmom i tajnim ključem K_i šifrira se RAND i kao rezultat dobija SRES (engl. *Signed Response*), 32-bitni potpisani odgovor. U MSC-u se uspoređuje SRES generiran u AUC-u i SRES generiran u SIM-u te ako su jednaki autentifikacija je uspješna. Postupak autentifikacije prikazan je na Slici 1.

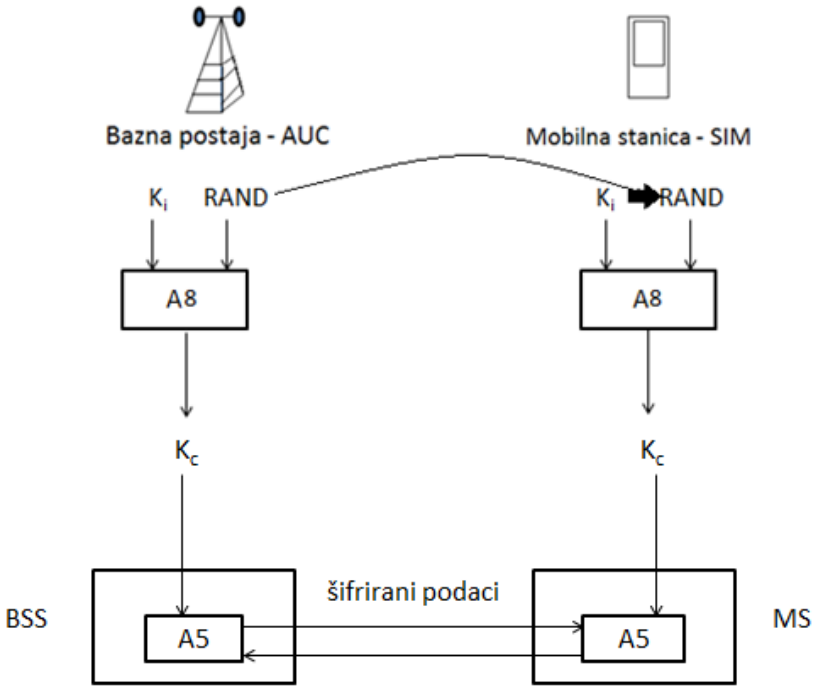


Slika 1 Postupak autentifikacije

Od sigurnosne prijetnje gubitka ili krađe pokretne opreme štitimo se pomoću IMEI broja. Prijavimo li gubitak ili krađu mrežnom operateru, to se zapisuje u EIR čime se izgubljenom ili ukradenom uređaju onemogućuje autentifikacija, i u HLR čime se izgubljenom ili ukradenom SIM-u zabranjuje pristup mreži.

Kako je IMSI jednoznačno povezan s MSISDN-om, postoji mogućnost da netko na zračnom sučelju dohvati naš IMSI te ustanovi našu lokaciju i prati kretanje. Kao zaštita od takve prijetnje, pretplatniku se dodjeljuje privremeni identitet TMSI (engl. *Temporary Mobile Subscriber Identity*) da mu se prikrije identitet preko zračnog sučelja. TMSI se iznova dodjeljuje pri svakom ažuriranju lokacije.

Još jedna od sigurnosnih prijetnji je prisluškivanje na zračnom sučelju zbog čega štitimo i komunikacijski kanal. U tu svrhu koriste se sigurnosni algoritmi A3 (autentifikacijski algoritam), A5 (algoritam za šifriranje) i A8 (algoritam za generiranje ključa). Algoritmom A8 dobivamo 64-bitni ključ za šifriranje K_c pomoću slučajnog broja RAND i ključa K_i. Pomoću K_c šifriramo i dešifriramo podatke koji se prenose između pokretne i bazne stanice. Algoritam A5 se koristi za šifriranje podataka između MS i mreže koji se prenose na zračnom sučelju.



Slika 2 Generiranje ključa i šifriranje

Literatura:

1. Predavanje iz Javne pokretne mreže, 3. Ćelijski koncept i arhitektura GSM mreže, http://www.fer.unizg.hr/_download/repository/JPM-2015-03n.pdf
2. Predavanje iz Javne pokretne mreže, 11. Sigurnost pokretne mreže, http://www.fer.unizg.hr/_download/repository/JPM-2015-11n_notes.pdf