NASTAVNO-NAUČNOM VEĆU ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za drugi stepen studija Elektrotehničkog fakulteta u Beogradu imenovala nas je za članove Komisije za pregled i ocenu master rada kandidata **Nadežde Dinić** pod naslovom **„Analiza bezbednosnih procedura u LTE mrežama"**. Nakon pregleda rada podnosimo Nastavno-naučnom veću sledeći

IZVEŠTAJ

1. Biografski podaci

Nadežda Dinić je rođena 06.08.1992. godine u Beogradu. Završila je Treću beogradsku gimnaziju. 2011. godine upisala je Elektrotehnički fakultet u Beogradu. Diplomirala je na Odseku za telekomunikacije i informacione tehnologije 2015. godine sa prosečnom ocenom 8,74. Diplomski rad odbranila je u julu 2015. godine sa ocenom 10. Diplomske akademske – master studije na Elektrotehničkom fakultetu u Beogradu, smer Sistemsko inženjerstvo i radio komunikacije, upisala je u oktobru 2015. godine.

2. Predmet master rada

Veliki napredak u bežičnim tehnologijama i rastuća potražnja za mobilnošću tokom telefoniranja i pristupa Internetu rezultovali su potrebom za izgradnjom boljih mobilnih mreža. Tokom razvoja, nastale su četiri generacije mobilnih mreža. LTE *(engl. Long Term Evolution)* mreža, kao četvrta generacija, pruža značajna poboljšanja funkcionalnosti mobilnih uređaja u prenosu podataka i multimedijskih sadržaja. Nadogradnja dostupnih usluga povećala je broj vrsta usluga na mobilnoj mreži. Samim time, povećao se i rizik od zlonamernih napadača. Napadi mogu usporiti ili u gorem slučaju paralizovati veliki deo mreže i prouzrokovati smanjenje dostupnosti usluga, što kao rezultat ima gubitak prihoda i smanjenje broja korisnika. Napadi mogu uticati na bilo koji deo mreže, zbog toga sistem zaštite mora pokrivati celu mrežu.

Kako su 4G *(engl. 4rd Generation)* mreže nadograđene na 2G i 3G mreže, još uvek se koriste sistemi GSM (*engl. Global System for Mobile Communications*), GPRS (*engl. General Packet Radio Service)* i UMTS (*engl. Universal Mobile Telecommunications System*). Postojeća zaštita je bila dovoljno dobra za prethodne generacije mobilnih mreža, ali je sa nadogradnjom sistema potrebno nadograditi i obnoviti zaštitu mobilnih sistema. Nadogradnjom prethodnih generacija javnih mobilnih mreža LTE mrežom ispravljeni si sigurnosni propusti koji su postojali u UMTS mrežama i prilagođene su bezbednosne procedure razvoju tehnologije kako bi se sprečili napadači od ugrožavanja sigurnosti mreže, i poverljivosti informacija.

Iz tog razloga u LTE mreži posebnu pažnju treba posvetiti sigurnosti i zaštiti kanala za komunikaciju. Predmet ovog rada je upravo analiza bezbednosnih procedura u LTE mreži, kao četvrtoj generaciji mobilnih komunikacionih sistema.

Cilj ovog rada je detaljna analiza ključnih procedura bezbednosti u LTE mreži, a u cilju postizanja bezbednosti u celoj LTE mreži. Upoređivanjem LTE, kao mreže bazirane samo na IP tehnologiji, sa prethodnim 2G/3G mrežama, prikazana je detaljna analiza zahteva proširenja mehanizma autentifikacije i broja ključeva u cilju sprečavanja napada koji se javljaju u modernim IT mrežama. U ovom radu je prikazan mehanizam autentifikacije i autorizacije kroz identifikaciju korisnika, tj. EPS-AKA procedura *(engl. Evolved Packet System – Authentication and Key Agreement)*. Takođe, analiziran je koncept hijerarhije ključeva kao i funkcija po kojima se ključevi izvode, KDF *(engl. Key Derivation Function)*. U radu je korišćen metod analize sigurnosti signalizacionih i korisničkih podataka, LTE bezbednosnih algoritama za očuvanje tajnosti i integriteta, kao i dodatnih funkcionalnosti evoluirane bazne stanice eNodeB *(engl. Evolved Node B)* i bezbednosti relejnog noda u odnosu na funkcionalnosti baznih stanica u 2G ili 3G mrežama. U okviru rada pažnja je posvećena i sigurnosti VoLTE-a *(engl. Voice over LTE)*.

3. Osnovni podaci o master radu

Master rad kandidata Nadežde Dinić **„Analiza bezbednosnih procedura u LTE mrežama"**, obuhvata 68 strana štampanog teksta sa 55 slika i 2 tabela. Rad je organizovan tako da sadrži pregled rada, uvod, pet poglavlja, zaključak i spisak literature.

4. Sadržaj i analiza rada

U prvom poglavlju dat je uvod u problematiku, prezentovana je motivacija za odabir teme, kao i ciljevi koji treba da budu zadovoljeni radom. Pored toga je, takođe, dat i sažetak rada i kratak pregled organizacije rada.

U drugom poglavlju dat je pregled bezbednosne arhitekture GSM, GPRS i UMTS mreže. Ovim poglavljem su analizirani osnovni elementi bezbednosne arhitekture GSM/GPRS mreže, bezbednosni algoritmi kao i procedura autentifikacije pretplatnika prema mreži. Izloženi su i bezbednosni problemi i nedostaci GSM/GPRS mreža koji su ispravljeni bezbednosnom arhitekturom UMTS mreže uvođenjem novih algoritama, kao i mehanizma uzajamne autentifikacije između pretplatnika i mreže.

Treće poglavlje pruža pregled arhitekture LTE mreže preko funkcija elemenata mreže za pristup E-UTRAN (*engl. Evolved UMTS Terrestrial Access Network*) i unapređenog paketskog jezgra EPC (*engl. Evolved Packet Core*). Ovo poglavlje sadrži i pregled korisničke i kontrolne ravni kroz protokole koje one podržavaju.

Četvrto poglavlje sadrži opis bezbednosne arhitekture LTE mreže koja je implementirana preko više ravni: korisničke, kontrolne, sinhronizacijske i upravljačke. U LTE mreži se radi ostvarivanja bezbednosti koristi rešenje koje se zasniva na IPsec protokolu (*engl. Internet Protocol Security*) zajedno sa PKI (*engl. Public Key Infrastructure*).

U petom poglavlju je data detaljna analiza bezbednosnih procedura poređenjem sa 2G/3G bezbednosnim mehanizmima kroz sedam podpoglavlja. Analizirane su sledeće procedure: identifikacija, autentifikacija i autorizacija, koncept ključeva, bezbednosni algoritmi, bezbednost signalizacionih i korisničkih podataka, bezbednost bazne stanice, relejnog noda i VoLTE.

Šestim poglavljem su opisane pretnje sa kojima se korisnik može susresti kada koristi mobilni uređaj za komunikaciju, kao i neka od mogućih rešenja sigurnosnih problema.

U poslednjem sedmom poglavlju, izložen je zaključak. Sumiran je, takođe, sadržaj rada, istaknut je osnovni doprinos master teze i dati su predlozi za dalji rad, koji se odnose na unapređenje bezbednosti u LTE mreži.

5. Zaključak i predlog

Master rad Nadežde Dinić prikazuje analizu bezbednosnih procedura u LTE mrežama. Glavni doprinosi master rada su sledeći:

- Detaljna analiza bezbednosnih procedura u LTE mreži, kao i uporedna analiza sa sistemima prethodnih 2G/3G generacija.
- Analiza 3GPP (*engl. 3rd Generation Partnership Project*) bezbednosnosnih tehničkih specifikacija sa stanovišta uvođenja novih, poboljšanih procedura sigurnosti.

Na osnovu izloženog, članovi Komisije predlažu Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da rad Nadežde Dinić, pod naslovom **„Analiza bezbednosnih procedura u LTE mrežama“**, prihvati kao master tezu i da kandidatu odobri javnu usmenu odbranu.

Beograd, 02.09.2016.

Članovi komisije:

Prof. dr Nataša Nešković

Prof. dr Aleksandar Nešković