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 **Marije Milosavljević** pod naslovom **„Uporedna analiza bezbednosnih procedura u 3GPP mrežama“**. Nakon pregleda rada podnosimo Nastavno-naučnom veću sledeći

IZVEŠTAJ

1. Biografski podaci

Marija Milosavljević je rođena 24.02.1992. godine u Jagodini. Završila je Gimnaziju u Lazarevcu. 2011. godine upisala je Elektrotehnički fakultet u Beogradu. Diplomirala je na Odseku za telekomunikacije i informacione tehnologije 2015. godine sa prosečnom ocenom 7,85. Diplomski rad odbranila je u septembru 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

Razvoj telekomunikacionih mreža, u stopu prati i razvoj sigurnosnih mehanizama. Ovaj mehanizam se pokazao kao preko potreban, i zbog toga se njegov razvoj odvija paralelno sa razvojem mreža. U današnje vreme, kada s kako poslovni, tako i privatni, deo života odvija preko mobilnih uređaja, sama izgradnja mreža nosi sa sobom odgovornost, da obezbedi korisnicima sigurnu komunikaciju i da održi integritet podataka. Kada dođe do razvoja mreža nove generacije, javlja se tendencija da se zadrže sigurnosni mehanizmi koji su korišćeni u mrežama prethodne generacije, koliko god je to moguće. Promena arhitekture mreže uslovljava i promenu samih procedura koje se koriste kao sigurnosni mehanizmi.

Kada se kao posledica loših sigurnosnih mehanizama javlja veliki gubitak novca, i na strani operatora i na strani korisnika, jasno je da ti mehanizmi moraju biti što bolji i što dugoročniji. Pod terminom dugoročniji smatra se da budu otporni na napade duži niz godina. Sam napredak u kriptoanalizi ne sme da dovede do toga da ceo sistem bude ugrožen. Iz tih razloga se uvodi više algoritama koji se koriste kao srž funkcija koje vrše šifrovanje i zaštitu integriteta.

Uvođenje novih, kolokvijalno rečeno, 4G mreža koje imaju težnju ka *flat* arhitekturi, vuče sa sobom nove probleme. Jedan od tih problema jeste, do koje tačke mreže treba da se obezbedi sigurnost komunikacije. Kod 3G mreža, odgovor na ovo pitanje se dobio krajnje jednostavno, jer postoji element RNC koji se nalazi na sigurnoj lokaciji, i zaštita se implemetirala do ove tačke. Kod 4G mreža, ovaj element ne postoji. Jedna od mogućnosti je da se sigurnost ostvari do eNodeB čvora koji nije postavljen na sigurnu lokaciju. Pa su iz tih razloga definisani novi sigurnosni mehanizmi koji se tiču eNodeB čvora. Ovo je jako bitno zbog AS signalizacije. Sa druge strane što se tiče NAS signalizacije, njena zaštita je uvučena dublje u mrežu, i proteže se sve do MME čvora.

Za razliku od 3G mreža, 4G mreže koriste više ključeva, i tu se javlja hijerarhija. Definisane su metode derivacije, kao i sama uloga i u kom se mrežnom elementu koristi određeni ključ.

Izabrani su novi algoritmi u odnosu na 3G mreže, pri čemu su ispoštovani kriterijumi odabira. Algoritmi ne smeju funkcionisati na sličan način, kako bi se izbegla ranjivost sistema, ukoliko dođe do otkrića vezanih za sam algoritam.

U ovom radu biće analizirane arhitekture 3G i 4G mreža, kao i same posledice koje one ostavljaju na sigurnosne mehanizme. Biće obrađenje metode koje se koriste za autentifikaciju korisnika, kao i razlike koje se javljaju između iste metode u okviru mreža različite generacije. Pojam „obostrana“ autentifikacija, koja se koristi kod mreža ovih generacija, biće objašnjena i napraviće se razlika u samim tim autentifikacijama. Pored toga biće naglašeno gde se zaista autentifikuje mreža od strane korisnika. Veliki akcenat će biti stavljen na zaštitu signalizacionih ravni, kao i na razliku koja se javlja a uslovljena je samom arhitekturom mreže. Pored signalizacionih, bitni su i korisnički podaci, pa će i njima biti posvećena pažnja, kako sa stanovišta zaštite integriteta, tako i sa stanovišta potrebe za njihovim šifrovanjem. Objašnjeni će biti i algoritmi koji se koriste, kako bi se uvidela njihova složenost.

3. Osnovni podaci o master radu

Master rad kandidata **Marije Milosavljević „Uporedna analiza bezbednosnih procedura u 3GPP mrežama“**, obuhvata 90 strana štampanog teksta sa 33 slike i 2 tabele. Rad je organizovan tako da sadrži pregled rada, uvod, pet poglavlja, zaključak, spisak literature, spisak skraćenica, spisak slika i spisak tabela.

4. Sadržaj i analiza rada

U prvom poglavlju biće reči o sigurnosti uopšteno. Objašnjena je podela sigurnosti u zavisnosti od tačke gledišta, kao faze analize prilikom dizajniranja sigurnosnog sistema.

U drugom poglavlju se opisuju mreže treće generacije i njihova arhitektura, kao i bitni mrežni elementi. Objašnjene su funkcije i protokoli 3GPP sistema. Pošto je reč o sigurnosti, analizirane su sigurnosne karakteristike UMTS mreže Release 1999, 4 i 5. Najveća ranjivost telekomunikacione mreže je u njenom pristupnom delu, pa se zato objašnjava enkripcija pristupne mreže. Posebna pažnja je posvećena zaštiti tajnosti i integriteta poruka koja se ostvaruje pomoću algoritama za kriptovanje. Objašnjen je princip rada KASUMI algoritma koji se koristi za kriptovanje podataka.

U trećem poglavlju je opisana arhitektura 4G mreža, upoređena sa arhitekturom 3G mreža, a objeašnjene su i posledice koje su nastale zbog te različitosti. Kako mreže nove generacije treba da unaprede „slabosti“ mreža ranijih generacija, bilo je neophodno analizirati novitete koji se tiču AKA protokola autentifikacije. Nova arhitektura uslovila je razlike u signalizacionim ravnima. U ovom poglavlju objašnjeni su principi rada algoritam za enkripciju SNOW3G.

U okviru ovog rada realizovani su KASUMI i SNOW3G algoritmi u Java programskom jeziku.

U zaključku je napravljen kratak rezime teme i dati zaključci do kojih se došlo prilikom izrade rada.

5. Zaključak i predlog

Master rad Marije Milosavljević prikazuje uporednu analizu bezbednosnih procedura u 3GPP mrežama. Glavni doprinosi master rada su sledeći:

- Detaljna analiza bezbednosnih procedura u 3G i 4G mrežama, sa akcentom na njihovim različitostima.
- Analiza 3GPP (*engl. 3rd Generation Partnership Project*) bezbednosnosnih tehničkih specifikacija sa stanovišta uvođenja novih, poboljšanih procedura sigurnosti.
- Realizacija KASUMI i SNOW3G algoritam za kriptozaštitu u Java programskom jeziku.

Na osnovu izloženog, članovi Komisije predlažu Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da rad Marije Milosavljević, pod naslovom **„Uporedna analiza bezbednosnih procedura u 3GPP mrežama”** prihvati kao master tezu i da kandidatu odobri javnu usmenu odbranu.

Beograd, 01.09.2017.

Članovi komisije:

Prof. dr Nataša Nešković

Prof. dr Aleksandar Nešković