KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 26.05.2015. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Ivane Arsenijević, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Implementacija i testiranje sigurne klijent server komunikacije između servera i Android aplikacije". Nakon pregleda materijala komisija podnosi sledeći

IZVE Š TAJ

1. Biografski podaci o kandidatu

Ivana Arsenijević je rođena 05.05.1989. godine u Beogradu. Gimnaziju je završila u Beogradu sa odličnim uspehom. Elektrotehnički fakultet u Beogradu je upisala 2008. godine, na Odseku za Telekomunikacije i informacione tehnologije. Diplomirala je u oktobru 2013. godine sa prosečnom ocenom na ispitima 7.83, na diplomskom 10. Master studije na Elektrotehničkom fakultetu u Beogradu je upisala novembra 2013. na modulu za Sistemsko inženjerstvo i radio komunikacije. Položila je sve ispite sa prosečnom ocenom 9.2.

2. Opis master rada

Master rad obuhvata 44 strane, sa ukupno 22 slike i 6 referenci. Unutar rada se nalaze i programski kodovi najvažnijih delova Android aplikacije koja omogućava sigurnu komunikaciju sa serverom. Rad sadrži uvod, 4 poglavlja, zaključak (ukupno šest poglavlja) i literaturu. Predmet rada je implementacija Android aplikacije koja omogućava sigurnu komunikaciju sa serverom u cilju dobijanja podataka od strane servera – u realizovanoj aplikaciji u pitanju je stanje računa korisnika. Realizovana implementacija se sastoji iz dve celine – klijent dela aplikacije i server dela aplikacije. Oba dela aplikacije su napisana u Java jeziku. Klijent deo aplikacije se povezuje na server pri čemu se klijent autentifikuje svojim login podacima. Server potom generiše javni i privatni RSA ključ, pri čemu klijentu šalje javni ključ. Klijent generiše AES ključ koji će se koristiti u razmeni podataka sa serverom, i potom koristeći javni ključ dobijen od servera šalje šifrovan AES ključ serveru. Server u bazi podataka pronalazi podatke koje treba da pošalje klijentu (stanje na računu) i potom te podatke šifruje AES ključem dobijenim od klijenta. Šifrovani podaci se šalju klijentu, koji ih dešifruje i prikazuje dobijene podatke na ekranu Android pametnog telefona. Očigledno, RSA se koristi za razmenu AES ključa, a potom se AES kao brža varijanta šifrovanja koristi za sigurnu razmenu podataka između servera i klijenta. Realizovana implementacija se lako može prilagoditi i prenosu drugačijih podataka pošto bi princip razmene ključeva i podataka i dalje ostao isti.

U uvodnom poglavlju opisan je značaj sigurne komunikacije. Opisan je predmet i cilj teze, i na kraju je ukratko predstavljena struktura ostatka teze po poglavljima.

U drugom poglavlju su predstavljene osnove sigurne komunikacije sa posebnim osvrtom na najpoznatije algoritme šifrovanja sa simetričnim i asimetričnim ključevima, kao i na najpoznatije algoritme autentifikacije. Takođe, na kraju poglavlja je data kratka specifikacija realizovane Android aplikacije.

U trećem poglavlju je dat detaljan opis server dela aplikacije, pri čemu su u tekstu teze prikazani i releventni delovi koda.

U četvrtom poglavlju je dat detaljan opis klijent dela aplikacije, pri čemu su u tekstu teze prikazani i releventni delovi koda.

U petom poglavlju je prikazana verifikacija ispravnosti rada aplikacije, a demonstriran je i rad aplikacije u realnom okruženju.

Na kraju teze je izložen zaključak koji sumira rezultate rada, a takođe sadrži i predloge za moguću primenu i unapređenja realizovane aplikacije. Na kraju rada data je literatura, sa 6 referenci, koja je korišćena prilikom izrade master rada.

3. Analiza rada sa ključnim rezultatima

Master rad Ivane Arsenijević, dipl. inž. Elektrotehnike i računarstva, bavi se implementacijom Android aplikacije koja omogućava sigurnu komunikaciju između klijenta i servera. Osnovni doprinosi rada su: 1) realizovana implementacija sigurne komunikacije između Android klijent aplikacije i servera; 2) mogućnost lakog prilagođavanja realizovane aplikacije i složenijim tipovima komunikacije u odnosu na transakcioni vid komunikacije između servera i klijenta pošto se deo aplikacije koji se odnosi na sigurnost ne bi morao menjati.

4. Zaključak i predlog

Kandidat Ivana Arsenijević, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovala implementaciju Android aplikacije za sigurnu klijent server komunikaciju. Ivana je pokazala dobro poznavanje Java jezika i veoma brzo je uspešno realizovala aplikaciju koja ima veliki potencijal u praktičnoj primeni. Realizovana implementacija može da nađe višestruku primenu u praksi, poput sigurnog pristupanja raznovrsnim korisničkim podacima, realizacije sigurnih transakcija, itd . Na osnovu izloženog, Komisija predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad kandidata Ivane Arsenijević, dipl. inž. elektrotehnike, prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

Beograd, 06.07.2015. godine

Komisija:

Dr Zoran Čiča, docent

Dr Dejan Drajić, docent