KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 30.09.2014. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Aleksandra Dželetovića, dipl. inž. Elektrotehnike i računarstva, pod naslovom „Implementacija sigurnog IP tunela baziranog na AES enkripciji". Nakon pregleda materijala komisija podnosi sledeći

IZVE Š TAJ

1. Biografski podaci o kandidatu

Aleksandar Dželetović je rođen 20. decembra 1990. godine u Prištini. Završio je Srednju elektrotehničku školu "Nikola Tesla" u Beogradu. Elektrotehnički fakultet Univerziteta u Beogradu upisao je 2009. godine. Diplomirao je 2013. godine na odseku Telekomunikacije i informacione tehnologije, smer Sistemsko inženjerstvo. Master studije na Elektrotehničkom fakultetu u Beogradu, smer Sistemsko inženjerstvo i radio komunikacije, upisao je 2013. godine.

2. Opis master rada

Master rad obuhvata 30 strana, sa ukupno 11 slika, 6 tabela i 10 referenci. Unutar rada se nalaze i programski kodovi pojedinih delova realizovane implementacije. Rad sadrži uvod, 3 poglavlja, zaključak (ukupno pet poglavlja) i literaturu. Predmet rada je hardverska implementacija predajnog i prijemnog dela sigurnog IP tunela pri čemu je korišćena AES enkripcija za postizanje sigurnosti komunikacije preko tunela. Realizovana implementacija omogućava da se na jednostavan način formiraju i konfigurišu sigurni tuneli u IP mrežama. Implementacija je realizovana programskim kodom u VHDL jeziku. Dizajn je kompajliran u ISE razvojnom okruženju za razvoj dizajna za FPGA čipove proizvođača Xilinx. Rezultat kompajliranja je pokazao da realizovana implementacija ne troši mnogo hardverskih resursa. Pošto se koristi pajplajn implementacija AES šifrovanja/dešifrovanja podržani su i visoki protoci korisničkih paketa. Za simuliranje ponašanja i verifikaciju dizajna upotrebljen je ISim simulator. Verifikacija dizajna je izvršena propuštanjem korisničkih paketa kroz tunel i proverom da na suprotnoj strani tunela izlaze originalni korisnički paketi koji su i poslati kroz tunel. Kompletan programski kod implementacije, kao i kod korišćen pri verifikaciji, priložen je na CD-u zbog obima koda.

U uvodnom poglavlju opisan je značaj sigurnosti Internet komunikacije, kao i primena tunela za postizanje sigurne komunikacije. Izložen je cilj teze, kao i struktura ostatka teze po poglavljima.

U drugom poglavlju su date osnove virtuelnih privatnih mreža i upotreba tunela u okviru njih. Takođe je dat pregled postojećih tehnologija za formiranje tunela.

U trećem poglavlju je dat opis realizovane implementacije. Detaljno je opisan rad realizovane implementacije, kao i ulazni i izlazni signali realizovanog dizajna. Opisani su prijemni i predajni deo. U okviru opisa predajnog dela je detaljno opisan blok za AES enkripciju korisničkih paketa, kao i blok koji vrši enkapsulaciju korisničkih paketa. U okviru opisa prijemnog dela je detaljno opisan blok za AES dekripciju korisničkih paketa, kao i blok za izvlačenje korisničkih paketa iz primljenog IP paketa.

U četvrtom poglavlju je opisan postupak verifikacije realizovanog dizajna. Takođe, dat je tabelarni pregled performansi koji pokazuje da realizovani dizajn ima skromne hardverske zahteve.

Na kraju teze je izložen zaključak koji sumira rezultate rada, izlaže potencijalne primene implementacije i navodi mogućnosti daljeg unapređenja realizovanog rešenja. Na kraju rada data je literatura, sa 10 referenci, koja je korišćena prilikom izrade master rada.

3. Analiza rada sa ključnim rezultatima

Master rad Aleksandra Dželetovića, dipl. inž. Elektrotehnike i računarstva, bavi se hardverskom implementacijom predajnog i prijemnog dela sigurnog IP tunela, pri čemu je korišćena AES enkripcija za postizanje sigurnosti. Osnovni doprinosi rada su: 1) hardverska implementacija predajnog i prijemnog dela sigurnog IP tunela; 2) efikasne implementacije AES šifrovanja i dešifrovanja koje omogućavaju visok protok korisničkih paketa; 3) realizovana implementacija nema veliku potrošnju hardverskih resursa.

4. Zaključak i predlog

Kandidat Aleksandar Dželetović, dipl. inž. elektrotehnike, je u svom master radu uspešno realizovao hardversku implementaciju predajnog i prijemnog dela sigurnog IP tunela. Aleksandar je pokazao veliku posvećenost u radu, i kreirao je kvalitetnu implementaciju koja se lako može iskoristiti u praksi. Realizovana implementacija može da se iskoristi u okviru Internet rutera za kreiranje sigurnih tunela u IP mrežama. Na osnovu izloženog, Komisija predlaže predlaže Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad kandidata Aleksandra Dželetovića, dipl. inž. elektrotehnike, prihvati kao master rad i kandidatu odobri javnu usmenu odbranu.

Beograd, 17.11.2014. godine

Komisija:

Dr Zoran Čiča, docent

Dr Dejan Drajić, docent