Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu

Komisija za studije drugog stepena Elektrotehničkog fakulteta u Beogradu na svojoj sednici održanoj 04.07.2011. godine imenovala nas je u Komisiju za pregled i ocenu master rada dipl. inž. Andrija Ilića pod naslovom „Implementacija i analiza metoda za zaštitu komunikacije u okviru RADIUS protokola na FreeRADIUS platformi". Nakon pregleda dobijenih materijala Komisija podnosi sledeći

IZVEŠTAJ

Biografski podaci

Ilić Andrija je rođen 1983. godine u Užicu, živeo u Arilju do početka studija kada prelazi u Beograd. Završio je osnovnu školu „Stevan Čolović" u Arilju. Pohađao je Gimnaziju opšteg smera u Arilju i završio je sa odličnim uspehom. Na osnovne studije na Elektrotehničkom fakultetu u Beogradu upisao se 2002. godine. Osnovne studije na smeru Računarska tehnika i informatika završio je 2010. godine, sa prosečnom ocenom 7,89 i ocenom 10 na diplomskom radu sa temom „Vizuelni simulator TMS sistema" iz oblasti Ekspertskih sistema, na kome je mentor bio Prof. Dr. Nikolić Boško i stekao zvanje diplomirani inženjer elektrotehnike i računarstva. Od 2006. radio u nekoliko firmi u Beogradu, pretežno kao *web developer*, a osnivač je i jedne od neprofitnih bežičnih mreža u Beogradu. Od 2011. radi kao Java EE programer za uglednu stranu kompaniju.

Podaci o master radu

Master rad dipl. inž. Andrije Ilića sadrži 67 strana teksta, zajedno sa slikama i prilozima. Rad sadrži 6 glava, spisak literature i 3 priloga. Spisak literature sadrži dvadeset referenci na knjige, naučne i stručne radove i veb sajtove.

Glava 1, Uvod, predstavlja uvod u kome su opisani predmet i cilj rada. Ukratko je opisan problem, motiv za njegovo rešavanje i predloženo rešenje (zaštita komunikacije RADIUS protokola). Pored toga, predočen je i opis metodike izrade master rada kao i opis same strukture rada. Pomenut je eduroam servis kao primer servisa koji upotrebljava RADIUS servere za potrebe svog funkcionisanja.

Glava 2, Opis tehnologije, prikazuje manje ili više detaljan pregled tehnologija koje su upotrebljene za izradu rešenja prezentovanog u ovom radu, u zavisnosti od relevantnosti opisane tehnologije za ovaj rad. Za svaku tehnologiju je napomenuto zašto se baš ona koristi ili zašto bi trebalo da se koristi i dat je pregled karakteristika i osobina same tehnologije. Takođe su prezentovani problemi eduroam servisa, a objašnjen je i razlog za uvođenje novih protokola (RadSec) i modela poverenja u okviru RADIUS infrastrukture. Opisani su RADIUS, RadSec i DTLS protokoli, a dat je i kratak pregled SSL/TLS protokola. Potom su prezentovana softverska rešenja koja implementiraju ove protokole (FreeRADIUS, RadSecProxy i OpenSSL). Na kraju poglavlja je obrazloženo na koji način je odabrano rešenje.

Glava 3, Opis rešenja, je najobimnija glava u radu. Na samom početku je definisano test okruženje i njegove karakteristike. Potom je prezentovan model rešenja polaznog problema u okviru definisanog test okruženja. Nakon toga sledi poglavlje o načinu pripremanja i konfigurisanja test okruženja. Detaljno je opisan postupak instalacije i pokretanja softvera koji se koristi u okviru test okruženja. Potom sledi poglavlje u kojem je detaljno opisano konfigurisanje CentOS operativnog sistema kao i FreeRADIUS i RadSecProxy servera. Opisano je kako se generišu SSL/TLS sertifikati korišćenjem FreeRADIUS paketa za generisanje sertifikata. Na kraju, prikazano je kako se koristi eapol_test alat za testiranje čitavog sistema u okviru test okruženja.

Glava 4, Demonstracija rešenja, prikazuje kako se, nakon što je test okruženje postavljeno i konfigurisano kako je to objašnjeno u prethodnom poglavlju, startuje test okruženje aktiviranjem eapol testova i vrši se analiza sistema. U ovom poglavlju se detaljno prati rad svakog servera na putu RADIUS poruke od NAS uređaja, preko FreeRADIUS servera sve do RadSecProxy servera u *remote* domenu, a potom preko RadSecProxy servera do FreeRADIUS servera u *home* domenu. Dat je pregled svih serverskih izveštaja o radu, a data su i obrazloženja tih izveštaja, na putu autentifikacione poruke od *remote* NAS servera do *home* FreeRADIUS autentifikacionog servera. Domeni su posmatrani u zasebnim celinama.

Glava 5, Analiza rešenja, se bavi analiziranjem rezultata prethodnog poglavlja kao i analizom čitavog koncepta rešenja. Takođe je dat kratak kritički osvrt na prednosti i mane upotrebljenih tehnologija u okviru prezentovanog rešenja.

Glava 6, Zaključak, je poglavlje u kome se daje pregled celokupnog rada od postavke, testiranja do analize testova na definisanom test okruženju. Povlači se kratka paralela između rešenja u ovom radu i mogućeg rešenja u okviru eduroam servisa. Takođe, poredi se usvojeno besplatno rešenje otvorenog koda (FreeRADIUS server i RadSecProxy server) sa komercijalnim rešenjima poput Radiator servera. Na kraju su prezentovane osnovne i najvažnije informacije o tome šta je urađeno, sta su doprinosi master rada i kakvi su planovi za budući razvoj i unapređenja rešenja

Zaključak

U ovom master radu kandidat razmatra problem zaštite komunikacije RADIUS protokola u okviru FreeRADIUS platforme upotrebom RadSecProxy servera i DTLS protokola. Kandidat analizira rad DTLS protokola kao i njegovu implementaciju u okviru RadSecProxy servera sa ciljem eventualne implementacije u okviru eduroam servisa. Cilj je da se ispita bezbednost i skalabilnost kriptovanog tunela koji ostvaruju *proxy* serveri koji se logički nalaze između FreeRADIUS servera. U poređenju sa komercijalnim rešenjem (Radiator), opšta ocena je da je predloženo rešenje (besplatni FreeRADIUS i RadSecProxy serveri) zadovoljilo preliminarna očekivanja i da ima još prostora i mogućnosti za njegova dalja unapređenja, što je svakako plan za budući razvoj.

Na osnovu gore navedenog, Komisija predlaže Nastavno-naučnom veću Elektrotehničkog fakulteta u Beogradu da prihvati rad „Implementacija i analiza metoda za zaštitu komunikacije u okviru RADIUS protokola na FreeRADIUS platformi" dipl. inž. Andrije Ilića kao master rad i odobri javnu usmenu odbranu.

Beograd, 23.09.2013.

Članovi Komisije:

Prof. dr. Zoran Jovanović,

Doc. dr Pavle Vuletić