KOMISIJI ZA STUDIJE II STEPENA
ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija za studije II stepena Elektrotehničkog fakulteta u Beogradu, na svojoj sednici održanoj 16.9.2014. godine, imenovalo nas je u Komisiju za pregled i ocenu master rada kandidata Dejane Lučić, dipl. inž. Elektrotehnike i računarstva, pod naslovom „**Sigurnost i privatnost u RFID tehnologijama**". Nakon pregleda materijala komisija podnosi sledeći

I Z V E Š T A J

1. Biografski podaci o kandidatu

Dejana Lučić je osnovnu školu i gimnaziju završila u Beogradu, nakon čega 2005. godine, upisuje Elektrotehnički fakultet, Univerziteta u Beogradu, odsek za Telekomunikacije i informacione tehnologije. Diplomirala je 2012. godine, na smeru za Radio komunikacije, sa radom na temu "Diskretna Furijeova transformacija konačne sekvence", sa prosečnom ocenom 7,73. Iste godine upisuje master studije na matičnom fakultetu i počinje da radi kao nastavnik u ETŠ "Nikola Tesla" u Beogradu, gde je i dalje zaposlena. Govori engleski jezik, a pasivno se služi i francuskim.

2. Opis master rada

Osnovni predmet istraživanja u radu je problem sigurnosti i privatnosti u RFID sistemima, a cilj sticanje uvida u tehnike kojima se sprečava zloupotreba korisničkih podataka. Osnovna ideja master rada je predstaviti najznačajnije sigurnosne mere koje se koriste za zaštitu privatnosti korisnika i sigurnosti RFID sistema, kao i načine na koje se ovaj sistem ugrožava. U radu su definisane ranjivosti RFID tehnologije, kao i pretnje, napadi i rizici koji su specifični za masovnu upotrebu RFID-a. U okviru ovog rada su vršene analize performansi alata i mehanizama koji se koriste za zaštitu sigurnosti i privatnosti, sa ciljem iznalaženja optimalnih rešenja za date napade na sistem.

Master rad kandidata sadrži 60 strana teksta, zajedno sa slikama, tabelama i dodacima. Rad se sastoji iz četiri osnovna dela koji sadrže veći broj poglavlja, uvoda, zaključka i spiska literature sa 20 referenci.

U prvom delu rada dat je osvrt na poreklo RFID sistema i njegov istorijski razvoj. Zatim su detaljno predstavljene komponente koje čine ovaj sistem, tj. njihova uloga, izgled, vrste (zavisno od tipa RFID sistema koji se koristi) i način rada. Dalje je objašnjen princip rada RFID-a, koji je zasnovan na radiofrekvencijskoj komunikaciji između taga i čitača i izmeni informacija.

U drugom delu rada uvodi se pojam sigurnosti i privatnosti, a potom se objašnjava koji su to ciljevi koje želimo postići uvođenjem mera koje će povećati sigurnost RFID sistema i zaštititi privatnost njegovih korisnika. Pod tim ciljevima podrazumevaju se važni sigurnosni zahtevi koji se koriste u gotovo svim sistemima, a to su tajnost (poverljivost), nekoliko tipova autentifikacije, autorizacija, neporecivost, dostupnost, integritet podataka i odgovornost. U ovom poglavlju takođe se navodi šta predstavlja ranjivost nekog sistema, šta predstavlja pretnju, kao i koje su to moguće pretnje za tag i čitač. Na kraju se definiše i izračunava rizik.

Treći deo rada bavi se sticanjem uvida u tehnike kojima se sprečava zloupotreba RFID tehnologije. Metode zaštite koje se najčešće koriste i koje su u ovom poglavlju analizirane su: klasična kriptografija, simetrična kriptografija, asimetrična kriptografija, heširanje, MAC i HMAC, digitalni i mobilni potpis. Navedeni su i neki dodatni mehanizmi koji takođe mogu obezbediti sigurnost RFID sistema, zatim zakonska ograničenja koja doprinose očuvanju privatnosti i bezbednosti, a i predložen je niz pravila kojih bi se trebalo držati sa ciljem da se smanji verovatnoća da će dati sistem biti zloupotrebljen.

U četvrtom delu rada vrši se komparativna analiza sigurnosnih mehanizama sa stanovišta stepena zaštite koji pružaju, brzine rada algoritma koji se koristi i sigurnosnih zahteva koji su zadovoljeni, zavisno od primenjene metode.

3. Analiza rada sa ključnim rezultatima

Master rad dipl. inž. Dejane Lučić bavi se uporednom analizom postojećih sigurnosnih alata i mehanizama za zaštitu RFID sistema, odnosno očuvanje njegovog integriteta. Izvršena je strukturalna analiza koja podrazumeva ostvarivanje uvida u najbitnije i specifične sigurnosne mere zaštite. Postojeće metode, koje se međusobno razlikuju po aspektu zaštite, efikasnosti, složenosti i troškovima ugradnje, komparativno su analizirane sa ciljem da se pronađu najoptimalnije mere koje je moguće implementirati.

Zaključeno je da se većina sigurnosnih mehanizama oslanja na kriptografiju, te da se na osnovu analize sigurnosnih metoda koje su korišćene u praksi, ne može reći da je jedna metoda superiornija u odnosu na druge. Stoga se zaključuje da potrebe sistema diktiraju metod zaštite. Pored toga, za postizanje najboljih rezultata i u najzahtevnijim sistemima gde su potrebne visoke performanse, dolazi se do zaključka da je neophodno koristiti kombinaciju nekoliko mehanizama, odnosno hibridnu šemu.

Osnovni doprinosi rada su sledeći:

- uvid u mogućnosti narušavanja bezbednosti RFID sistema i privatnosti njegovih korisnika,
- prikaz postojećih metoda i tehnika kojima se sprečava zloupotreba korisničkih podataka u RFID sistemima i
- klasifikovanje tehnika zaštite po stepenu efikasnosti, načinu rada i složenosti.

4. Zaključak i predlog

Na osnovu izloženog, imajući u vidu kompleksnost proučavanog problema, rezultate i zaključke do kojih je kandidat u svom samostalnom radu došao, Komisija smatra da rad kandidata Dejane Lučić „Sigurnost i privatnost u RFID tehnologijama“ ispunjava uslove da bude prihvaćen kao master rad i predlaže Nastavno – naučnom veću da kandidatu odobri javnu usmenu odbranu.

Beograd, 20.9.2014

Komisija:

Dr Dejan Drajić, docent

Dr Miroslav Dukić, red. Prof.