

Univerzitet u Beogradu  
Elektrotehnički fakultet

## KOMISIJI ZA STUDIJE II STEPENA

Na sednici Komisije za studije II stepena Elektrotehničkog fakulteta u Beogradu, koja je održana 31.01.2017. godine, imenovani smo u Komisiju za pregled i ocenu master rada kandidata dipl. inž. Teone Tatović, pod naslovom Implementacija injekcije kriptografskih ključeva, kriptografske zaštite memorije i softvera I.MX namenskog sistema. Komisija je pregledala priloženi rad i podnosi sledeći

### IZVEŠTAJ

#### 1. Biografski podaci o kandidatu

Teona Tatović rođena je 29.01.1992. u Kragujevcu, gde je završila prirodno-matematički smer Prve kragujevačke gimnazije. Na studije na Elektrotehničkom fakultetu u Beogradu se upisala 2010 god. Osnovne studije na odseku Elektronika završila je 2014. godine sa prosečnom ocenom 9.47 i ocenom 10 na diplomskom radu. Master studije na Elektrotehničkom fakultetu, na smeru Elektronika, upisala je iste godine i položila sve ispite sa prosečnom ocenom 9.80.

#### 2. Opis i organizacija rada

Master rad kandidata sadrži 107 strana teksta, zajedno sa slikama, apendiksima, listom slika, listom skraćenica, listom tabela i spisom literature. Rad je podeljen na 7 poglavlja, od kojih dva čine uvod i zaključak i 7 apendiksa sa programskim kodom.

Prvo poglavlje predstavlja uvod u kome su opisani predmet i cilj rada. Dat je pregled rada po poglavljima.

U drugom poglavlju je opisano trenutno stanje istraživačkog polja koje se bavi kriptografskom zaštitom namenskih sistema. Opisani su glavni problemi kojima se ovo istraživačko polje bavi, data je terminologija ovog istraživačkog polja, i opisani su i upoređeni razni principi koji se primenjuju u industriji danas.

U trećem poglavlju je opisan namenski sistem sa akcentom na kriptografske periferije sistema, i opisane su softverske komponente namenskog sistema. Opisani su korišćeni softverski alati.

Četvrto poglavlje opisuje primer proizvodnje namenskih sistema koji obavlja kriptografske operacije u svojim aplikacijama. Ovo poglavlje detaljno opisuje problem kojim se ova teza bavi, i opisuje princip injekcije kriptografskih ključeva u toku proizvodnje namenskih sistema na kriptografski bezbedan način.

U petom poglavlju su opisani detalji implementacije zaštite softvera namenskog sistema od izmena u toku i nakon proizvodnje.

Šesto poglavlje opisuje implementaciju zaštite memorije koja omogućuje zaštitu osetljivih podataka na namenskom sistemu.

U sedmom poglavlju dat je zaključak sa osvrtom na moguća poboljšanja opisane implementacije.

#### 3. Analiza rada sa ključnim rezultatima

Predmet rada je implementacija kriptografske zaštite softvera i.MX namenskog sistema od izmena i zaštita memorije namenskog sistema od pristupa neautorizovanih korisnika.

Implementacija ova dva principa omogućuje injekciju kriptografskih ključeva u toku proizvodnje namenskog sistema. Ova implementacija predstavlja rešenje za učestalu potrebu proizvođača namenskih sistema da zaštite funkcionalnost namenskih sistema nakon proizvodnje i zaštite svoj poslovni model. Za implementaciju su korišćene sveprisutne *open source* softverske komponente što omogućuje korišćenje prikazanih rešenja i ideja na raznim hardverskim platformama.

Koncept rešenja je teorijski opisan, dati su implementacioni detalji rešenja i dat je programski kod ključnih komponenti rešenja.

U radu je formulisana problem kojim se rad bavi, opisan je hardver i softver namenskog sistema, detaljno su opisani su algoritmi koji su deo implementacije uz priložen programski kod i opisano je testiranje rešenja.

#### 4. Zaključak i predlog

Kandidat Teona Tatović je u svom master radu na sistematičan i metodičan način ispitala mogućnosti korišćenja kriptografske zaštite u namenskim računarskim sistemima. Rezultati ovog istraživanja mogu značajno doprineti usmeravanju i definisanju novih pravaca istraživanja u ovoj oblasti. Sva istraživanja, razvoj i eksperimentisanja kandidat Teona Tatović je sprovedla samostalno.

Na osnovu gore navedenog, imajući u vidu sadržaj i kvalitet priloženog rada, rezultate i zaključke do kojih je kandidat u svom samostalnom radu došao, članovi Komisije predlažu Komisiji za studije II stepena Elektrotehničkog fakulteta u Beogradu da rad kandidata dipl. inž. Teone Tatović pod nazivom Implementacija injekcije kriptografskih ključeva, kriptografske zaštite memorije i softvera I.MX namenskog sistema, prihvati kao master rad i kandidatu odobri usmenu odbranu.

Beograd 20.03.2017. godine

Članovi komisije:

  
Dr Nenad Jovičić, docent

  
Dr Jelena Popović-Božović, docent