VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE
UNIVERZITETA SINGIDUNUM

Beograd
Danijelova 32

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 1- 2199/2013 od 30.09.2013.godine, određeni smo za članove Komisije za pregled, ocenu i usmenu odbranu doktorske disertacije Nenada Ristića, master pod nazivom: "*Jedno rešenje za zaštitu izvornog koda skript jezika na bazi kriptografskih mehanizama*".

Posle pregleda dostavljene Disertacije i drugih pratećih materijala, Komisija je sačinila sledeći

R E F E R A T

1. UVOD

1.1 Hronologija odobravanja i izrade disertacije

Nenad Ristić je upisao doktorske studije na Singidunum univerzitetu školske 2010/2011. godine. Položio je svih 12 ispita, sa srednjom ocenom 10. Zahtev za odobravanje teme za izradu doktorske disertacije podneo je 2013. godine. Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 1-1617/2013 od 20.06.2013.godine, formirana je Komisija u sastavu:

1. dr Mladen Veinović, redovni profesor, Univerzitet Singidunum, Beograd
2. dr Aleksandar Jevremović, vanredni profesor, Univerzitet Singidunum, Beograd
3. dr Goran Šimić, redovni profesor, Vojna akademija

za ocenu teme i podobnosti kandidata za izradu doktorske disertacije pod nazivom: "*Jedno rešenje za zaštitu izvornog koda skript jezika na bazi kriptografskih mehanizama*". Na osnovu pozitivnog izveštaja Komisije Senat Univerziteta Singidunum je 2013. godine odobrio rad na izradi doktorske disertacije. Za mentora je imenovan prof. dr Mladen Veinović. Završnu verzija doktorske disertacije u elektronskom i štampanom obliku Nenad Ristić je predao Univerzitetu 25.02.2016. godine.

1.2. Naučna oblast disertacije

Tema disertacije kandidata je u oblasti savremenih informacionih tehnologija, za koju je Fakultet za informatiku i računarstvo Univerziteta Singidunum matičan.

1.3. Biografski podaci o kandidatu

Nenad Ristić rođen je 29.03.1982. godine u Bijeljini, Republika Srpska. U Bijeljini je završio osnovnu školu "Vuk Karadžić" i Srednju Elektrotehničku školu „Mihajlo Pupin".

Školske 2006/2007. godine upisao je Fakultet poslovne informatike, Univerziteta Sinergija u Bijeljini, na kome je 2009. godine diplomirao sa prosečnom ocenom 9.33.

Master studije upisao je na Fakultetu za informatiku i računarstvo (smer "Savremene informacione tehnologije") Univerziteta Singidunum. Master rad odbranio je kod mentora prof dr Mladena Veinovića 2010. godine i stekao akademski naziv mastera informatičara. Tokom master i doktorskih studija radio je i radi kao asistent na predmetima „Osnovi računarske tehnike", „Računarske mreže", „Baze podataka", „Operativni sistemi", „Osnovi zaštite informacija", „Infomatika" i „Kriptologija".

Na Univerzitetu Sinergija 2009. godine izabran je u zvanje asistenta za užu naučnu oblast "Informatika i računarstvo", a 2012 godine izabran u zvanje višeg asistenta za užu naučnu oblast "Informatika i računarstvo".

Kao autor ili koautor objavio je 20 radova na domaćim i međunarodnim konferencijama i časopisima.

2. OPIS DISERTACIJE

2.1. Sadržaj disertacije

Doktorska disertacija pod naslovom: "*Jedno rešenje za zaštitu izvornog koda skript jezika na bazi kriptografskih mehanizama*" ima ukupno 101+9 strana. Disertacija ima šest poglavlja i spisak literature. Poglavlja su:

1. Uvod, 5 strana
2. Teorijske i kriptološke osnove i okvir, 41 strana
3. Pregled postojećih rešenja, 23 strane
4. Model predloženog rešenja, 13 strana
5. Ekspreimentalna analiza, 12 strana
6. Zaključak, 7 strana.

U disertaciji ima ukupno 85 slika, 4 tabele i 15 numerisanih izraza. Literatura sadrži 80 biblografskih jedinica.

2.2. Kratak prikaz pojedinačnih poglavlja

U uvodu su prikazane ideje vodilje koje su motivisale istraživački rad na temi disertacije. Istaknuta je aktuelnost teme i dat presek do sada objavljenih rezultata u ovoj oblasti. Ukazano je na nedostatke kod postojećih pristupa zaštite, kao i prednosti pristupa analize i rešavanja problema

zaštite softverskih rešenja u Veb okruženju kroz prizmu standarnog kriptološkog modela. Navedeni su originalni naučni doprinosi teze i kratak pregled preostalih poglavlja.

Drugo poglavlje je organizovano u šest delova dela. U prvom delu date su osnove vezana za kriptografiju. U nastavku su analizirani klasični, simetrični i asimetrični šifarski sistemi. Prikazane su karakteristike i mogućnosti homomorne kriptografije. Takođe, dat je pregled stanja steganografije i kriptoanalize. Pored toga, dat je opis arhitekture, programskih jezika i revrznog inženjeringa. Posebna pažnja je posvećena je Veb okruženju.

Pregled postojećih rešenja obrađen je u trećem poglavlju. Opisani su dostupni načini za zaštitu, kako besplatna rešenje tako i komercijalna.

Originalni naučni rezultati kandidata prikazani su u četvrtom i petom poglavlju. U četvrtom poglavlju dat je predlog modela razvijen analizom slabosti postojećih rešenja. Pored toga u okviru ovog poglavlja prikazan je razvijen model sa analizom mogućnosti primene i moguće slabosti.

U petom poglavlju, izvršena je analiza vremena izvršavanja skripte zaštićene različitim dostupnim metodama. Skripta je zaštićena upotrebom tri metode maskiranja izvornog koda kao i metodom šifrovanja. Na kraju je urađeno testiranje predloženog rešenja kao i komparacija svih rešenja.

U zaključku teze su navedeni osnovni doprinosi disertacije i date su smernice za moguća dalja istraživanja u ovoj oblasti.

3. OCENA DISERTACIJE

3.1. Savremenost i originalnost

Istraživanja u oblasti analize i razvoja novih metoda zaštitu programskih rešenja, namenjenih za izvršavanje u serverskim Veb okruženjima su danas veoma aktuelna. Veb okruženje predstavlja, po pitanju zaštite, jedno od najizazovnijih izvršnih okruženja s obzirom na to da autor rešenja često nema nikakvu vezu, niti kontrolu nad njim. Poseban fokus rada čini analiza mogućnosti zaštite rešenja zasnovanih na interpreterskim jezicima. Kandidat je razvio novi pristup za sagledavanje problema i rešenja zaštite softverskih rešenja u Veb okruženjima kroz prizmu standardnog kriptološkog modela.

U ovom kontekstu, kandidat je svoju originalnost potvrdio na korektan i uverljiv način-objavljivanjem radova u međunarodnim naučnim časopisima i u zbornicima sa međunarodnih i domaćih naučnih konferencija.

3.2. Osvrt na referentnu i korišćenu literaturu

U izradi disertacije korišćena je obimna literatura iz oblasti zaštite, kriptoloških modela i dostupnih modela zaštite programskih rešenja polazeći od fundamentalnih referenci, pa sve do najnovijih radova u vrhunskim međunarodnim naučnim časopisima uključujući i sopstvene reference. Na osnovu tih referenci, originalni naučni rezultati do kojih je kandidat došao u disertaciji su stavljeni u korektan kontekst.

3.3. Opis i adekvatnost primenjenih naučnih metoda

Kandidat je u svom istraživačkom radu koristio više različitih postupaka. Najpre je uvidom u literaturu, zajedno sa mentorom došao do zaključka o potrebi za analizom postojećih modela zaštite kroz standardni kriptološki model i razvojem novog otvorenog modela, sa podrazumevano javno dostupnim izvornim kodom. Detaljnom analizom raspoloživih pristupa uočeni su nedostaci,

sagledane su potencijalne mogućnosti uvođenja novog modela i formulisan je cilj istraživanja: objektivna analiza efikasnosti postojećih rešenja, kao i davanje osnove i predlaga novog rešenja koje bi odgovorilo na nedostatke postojećih rešenja.

U postupku analize i razvoja modela, kandidat je pokazao samostalnost i inventivnost u izboru standardnog kriptološkog modela za analizu, određivanju slabosti postojećih rešenja i razvnoju otvorenog modela zaštite. Razvijeni model je verifikovani poređenjem sa odgovarajućim referentnim vrednostima.

Prednosti i nedostaci predloženog pristupa na bazi analize standardnim kriptološkim modelom kritički sagledani i na kraju disertacije su date smernice za moguća dalja istraživanja.

3.4. Primenljivost ostvarenih rezultata

Rezultati do kojih je kandidat došao u svojoj disertaciji mogu imati neposrednu primenu u oblasti analize i zaštite softverskih rešenja u Veb okruženjima. Naime, analizom ovakvim pristupom utvrđuje se efikasnost i mogućnosti primene komponenata sa otvorenim izvornim kodom u kreiranju pouzdanog izvršnog Veb okruženja, odnosno okruženja u kojem će biti moguće izvršavanje zaštićenog softverskog rešenja.

3.5. Ocena dostignutih sposobnosti kandidata za samostalni naučni rad

Kandidat je u svom dosadašnjem radu pokazao kvalitete presudne za uspešan istraživački rad: sposobnost uočavanja problema i postavljanje korektnog cilja istraživanja, shvatanje i proširivanje teorijskih koncepata, originalnost, sposobnost da teorijske metode pretoči u algoritme, strukture podataka i računarske programe, kao i da kritički analizira dobijene rezultate.

4. OSTVARENI NAUČNI DOPRINOS

4.1. Prikaz ostvarenih naučnih doprinosa

Originalni naučni doprinosi disertacije se mogu formulisati na sledeći način:

- Razvoj novog pristupa za sagledavanje problema i modela zaštite softverskih rešenja u Veb okruženjima kroz prizmu standardnog kriptološkog modela.
- Analiza efikasnost pristupa i mogućnosti primene komponenata sa otvorenim izvornim kodom u kreiranju pouzdanog izvršnog Veb okruženja, odnosno okruženja u kojem će biti moguće izvršavanje zaštićenog softverskog rešenja.
- Primenom modela proširuje se osnovni kontekst analize, odnosno analizu se proširuje na različitim nivoima prevođenja i izvršavanja izvornog koda, uključujući reverzni inženjering kao sredstvo podrazumevano dostupno napadaču u pokušaju narušavanja zaštite.
- Doprinos razvoju modela za zaštitu softverskih (programskih) rešenja od neovlašćenog korišćenja i izmene gledano kroz prizmu klasičnih kriptoloških modela.

Analizom postojećih ograničenja pristupa, odnosno ostvarivanja praktične upotrebljivosti i mogućnosti uvođenja u Veb okruženje, identifikovani su doprinosi u rešenju problema zaštite rešenja zasnovanih na interpreterskim jezicima. Dodatno, na osnovu suštinskih i arhitekturnih zahteva računarstva od poverenja jasnije je postavljena podloga za razvoj definisanog pouzdanog izvršnog Veb okruženja. Ove analize i definisanje mogućnosti predstavljaju poseban doprinos u pogledu definisanja daljih pravaca istraživanja, sa ciljem ostvarivanja prihvatljivog nivoa zaštite, čak i kod primene najrigoroznijih kriptoanalitičkih napada.

4.2. Kritička analiza rezultata istraživanja

U prvoj fazi kandidat je razmatrajući raspoloživu literaturu u oblasti teme disertacije izvršio kritičku analizu dostupnih informacija i korektno definisao cilj istraživanja. U istraživačkom radu koristio je mogućnost kritičkog preispitivanja i pogodne načine verifikacije dobijenih rezultata. Razvijeni model verifikovan je poređenjem rezultata modelovanja sa odgovarajućim referentnim vrednostima (eksperimentalnim ili rezultatima računarskih simulacija). Uočene su i prikazane prednosti i nedostaci predloženog pristupa i ukazano na smernice mogućih daljih istraživanja.

4.3.Verifikacija naučnih doprinosa

Naučni doprinosi disertacije verifikovani su sledećim radovima kandidata:

Kategorija M23

1. Gojko Grubor, Milenko Heleta, **Nenad Ristić**, Ivan Barać, Integrated management model of the corporate digital forensic investigation, *Technical Gazette, Vol. 23/No. 6 2016, DOI: 10.17559/TV-20141121105105*

Kategorija M33

1. Aleksandar Jevremović, **Nenad Ristić**, Mladen Veinović. "Using cryptology models for protecting PHP source code." 11th international conference of numerical analysis and applied mathematics 2013: icnaam 2013. Vol. 1558. No. 1. AIP Publishing, 2013. DOI: 10.1063/1.4825491
2. **Nenad Ristić**, A Jevremović , M Veinović, „Identifikovanje homogenih fajlova upotrebom segmentnog hešovanja iniciranog sadržajem" 20th Telecommunications forum TELFOR 2012, Serbia, Belgrade, Novembar 20-22, 2012, 1665-1668
3. **Nenad Ristić**, A Jevremović , M Veinović, „Sistem segmentovane zaštite korisničkih podataka u Veb aplikacijama" Infoteh-Jahorina Vol. 12, Mart 2013, 915-918
4. Aleksandar Jevremović, Mladen Veinović, Marko Šarac, **Nenad Ristić**, Dušan Stamenković, FatCookies: HTTP cookies based attack on Web sites availability, 2nd International Conference on Electrical, Electronic and Computing Engineering, 5/2015, Srebrno jezero.
5. **Nenad Ristić**, A Jevremović , M Veinović, „Upotreba metode segmentnog hešovanja iniciranog sadržajem za identifikovanje homogenih fajlova" Infoteh-Jahorina, Mart 2013, 998-1001
6. Nataša Simeunović, **Nenad Ristić** „Digitalna forenzika u funkciji forenzičkog računovodstva" Infoteh-Jahorina, Mart 2013, 1006-1010 (M33)
7. Dušan Regodić, Damir Jerković, Aleksandar Jevremović, **Nenad Ristić**, Marija Matotek - Aerodinamički koeficijent sile otpora vazduha pri simetričnom opstrujavanju letelice, Synthesis 2015,http://dx.doi.org/10.15308/Synthesis-2015-274-278 (M33)

8. Nataša Simeunović, **Nenad Ristić**, „Digitalna forenzička istraga manipulacije računovodstvenim softverom", Infotech 2013 ICT Conference & Exhibition, jun 2013, Aranđelovac
9. Jevremović Aleksandar, **Ristić Nenad**, Mladen Veinović „Improving Protection of PHP Source Code Using Cryptology Models" International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services – TELSIKS Niš, Serbia, 409 – 412, http://dx.doi.org/10.1109/TELSKS.2013.6704410 978-1-4577-2016-1/11
10. **Nenad Ristić**, Aleksandar Jevremović - One solution for protecting PHP source code, Sinteza 2014, doI: 10.15308/SInteZa-2014-616-619
11. **Nenad Ristić**, Aleksandar Jevremović, Mladen Veinović, Goran Šimić - An open-source solution for protecting PHP source code, IcETRAN 2014

Kategorija M63

1. Dejan Ćapara, Gojko Grubor, Dušan Regodić , **Nenad Ristić** - Plagiarism and copyright protection on the Internet - 14. Naučni skup sa međunarodnim učešćem Sinergija, decembar 2013. 240-247, 978-99955-26-32-0
2. 15. Prohaska Andrej, Gojko Grubor, **Nenad Ristić**, Angelina Njeguš - Electronic services availability in Bosnia and Herzegovina - 14. Naučni skup sa međunarodnim učešćem Sinergija, decembar 2013. 253-262, 978-99955-26-32-0
3. 16. Gojko Grubor, **Nenad Ristić**, Ivan Barać - Specifičnosti veštačenja u informacionim tehnologijama, 15. Naučni skup sa međunarodnim učešćem Sinergija, decembar 2014. ISBN: 978-99955-26-35-1 http://dx.doi.org/10.13140/2.1.4200.7842
4. 17. Nataša Simeunović, **Nenad Ristić** - Povezanost računovodstvene profesije i privrednog kriminaliteta, 15. Naučni skup sa međunarodnim učešćem Sinergija, decembar 2014. ISBN: 978-99955-26-35-1
5. 18. Gojko Grubor, Angelina Njeguš, **Nenad Ristić**, „Paradigma zaštite distribuiranog računarstva", 6. Naučni skup sa međunarodnim učešćem Sinergija, mart 2010. 176-184
6. G Grubor, A Njeguš, N Ristić, „Funkcionalno-bezbednosni aspekti veb 2.0 i veb 3.0" 6. Naučni skup sa međunarodnim učešćem Sinergija, mart 2010. 138-146
7. Gojko Grubor, Angelina Njeguš, **Nenad Ristić**, "Doprinos sistemu kvaliteta digitalnih forenzičkih servisa u cloud computing okruženju", 12. Naučni skup sa međunarodnim učešćem Sinergija, mart 2013. 56-65
8. **Nenad Ristić**, Aleksandar Jevremović , Mladen Veinović, "Poboljšavanje kvaliteta i nivoa zaštite korisničkih podataka u Veb okruženju", 12. Naučni skup sa međunarodnim učešćem Sinergija, mart 2013. 106-111

5. MIŠLJENJE KOMISIJE I PREDLOG

Na osnovu izloženog, komisija konstatuje da doktorska disertacija Nenada Ristića, master informacionih tehnologija, pod naslovom "*Jedno rešenje za zaštitu izvornog koda skript jezika na bazi kriptografskih mehanizama*" ispunjava sve formalne i suštinske uslove predviđene Zakonom o visokom obrazovanju, kao i propisima univerziteta Singidunum u Beogradu. Doktorska disertacija Nenada Ristića sadrži naučne doprinose koji se sastoje u razvoju novog pristupa za sagledavanje problema i modela zaštite softverskih rešenja u Veb okruženjima.

Tokom celokupne izrade doktorske disertacije, kao i na ukupnom radu kandidat je pokazao nesumnjivu sposobnost za samostalni nauučnoistraživački rad. Stoga članovi Komisije sa zadovoljstvom predlažu Veću departmana za poslediplomske studije da se doktorska disertacija pod naslovom " *Jedno rešenje za zaštitu izvornog koda skript jezika na bazi kriptografskih*

mehanizama" kandidata Nenada Ristića, mastera u oblasti informatike i računarstva prihvati, izloži na uvid javnosti i uputi na konačno usvajanje Senatu univerziteta Singidunuma u Beogradu.

Beograd, 01.03.2016. godine

Članovi komisije:

dr Mladen Veinović, redovni profesor,
Univerzitet Singidunum, Beograd

dr Aleksandar Jevremović, vanredni profesor,
Univerzitet Singidunum, Beograd

dr Goran Šimić, vanredni profesor,
Vojna akademija, Beograd