VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE
UNIVERZITETA SINGIDUNUM

Beograd
Danijelova 32

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 4-251-1/2015 od 28.09.2015.godine, određeni smo za članove Komisije za pregled, ocenu i usmenu odbranu doktorske disertacije VladimiraStanojevića, master pod nazivom: "*Evaluacija novog pristupa u zaštiti VoIP komunikacija*".

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

REFERAT

1. UVOD

1.1 Hronologija odobravanja i izrade disertacije

VladimirStanojević je upisao doktorske studije na Singidunum univerzitetu školske 2012/2013. godine. Položio jesvih 12 ispita, sa srednjom ocenom 10. Zahtev za odobravanje teme za izradu doktorske disertacije podneo je 2015. godine. Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 4-251-1/2015 od 28.09.2015.godine, formirana je Komisijau sastavu:

1. dr Mladen Veinović, redovni profesor, Univerzitet Singidunum, Beograd
2. dr Milan Milosavljević, redovni profesor, Univerzitet Singidunum, Beograd
3. dr Petar Spalević, redovni profesor, Fakultet Tehničkih Nauka, Univerzitet u Prištini

zaocenu teme i podobnosti kandidata za izradu doktorske disertacije pod nazivom:"*Evaluacija novog pristupa u zaštiti VoIP komunikacija*".Na osnovu pozitivnog izveštaja Komisije Senat Univerziteta Singidunum je 2015. godine odobrio rad na izradi doktorske disertacije.Za mentora je imenovan prof. dr Mladen Veinović. Završnu verzija doktorske disertacije u elektronskom i štampanom obliku Vladimir Stanojević je predao Univerzitetu 15. 08. 2016. godine.

1.2. Naučna oblast disertacije

Tema disertacije kandidata je u oblasti Zaštita sistema i podataka, za koju je Fakultet za informatiku i računarstvo Univerziteta Singidunum matičan.

1.3. Biografski podaci o kandidatu

Vladimir Stanojević je rođen 1976. godine u Šapcu, gde je po završenoj osnovnoj

školi, pohađao i završio gimnaziju, prirodno-matematički smer (kao redovan učenik) i školu učenika u privredi-smer radio TV mehaničar (kao vanredan učenik), naporedo.

1995. godine je upisao Fakultet Organizacionih Nauka, smer Informacioni sistemi.

Od početka studija uključen u nekoliko stručnih projekata, od kojih je najznačajniji projekat kopirajt zaštite programskih sadržaja korišćenjem posebne tehnike obeležavanja flopi diskete, kao idejni tvorac i realizator tog projekta.

Od 1996. godine, preko studentske zadruge za vreme studiranja radi na FON-u kao demonstrator laboratorijskih vežbi na predmetu „Principi Programiranja".

U više navrata pisao i izlagao radove za vreme studija na SinFon-u.

1997. godine koautor praktikuma laboratorijskih vežbi za isti predmet.

1997. Dobitnik zlatne plakete za rad „Analiza računarskih virusa sa aspekta zaštite izvršnih programa" na SinFon-u.

2000. godine kao apslovent, u određenim životnim okolnostima se okreće projektima u privredi, te početkom 2001. godine osniva svoje privatno preduzeće radi bavljenja projektima u privredi kako u zemlji, tako i u inostranstvu.

Neki od referentnih projekata su:

- Informacioni sistem za upravljanje voznim parkom za CASTROL s.p.a.
- Hardvesko-softverski sistem za autonomnu elektronsku akviziciju podataka sa uređaja na liniji tehničkih pregleda za motorna vozila svih kategorija, i umrežavanje celog sistema na teritoriji Republike Srpske, za Ministarstvo Saobraćaja, Centar za motorna vozia, Banja Luka.
- Poslovno informacioni sistem „EnterCom" koji koristi više desetina privrednih subjekata u Republici Srbiji
- Sistem za evidenciju radnog vremena sa bezkontaktnim RFID karticama (hardversko i softversko rešenje) „CheckPoint" koje je u upotrebi u više desetina kompanija na teritoriji Republike Srbije

Od 2006. godine proširuje delatnost firme i na sisteme tehničkog obezbeđenja objekata, stiče distributersku i instalatersku licencu Kanadske kompanije PARADOX.

Od 2008. godine sklapa ugovor za regionalno održavanje mreže POS terminala i bankomata većine banaka koje posluju na teritoriji Republike Srbije i Bosne i Hercegovine.

Od 2010. godine, posle ozbiljnih zdravstvenih problema, odlučuje da se profesionalno bar delom vrati u univerzitetske vode, te naknadno završava diplomske studije, pa 2012. Godine upisuje Master studije na univerzitetu SINGIDUNUM, i završava ih pre roka, te upisuje i doktorske studije na programu „Napredni sistemi zaštite".

Od 2014. godine stekao je zvanje sudskog veštaka u oblasti informacione tehonologije.

Učestvovao je na više stručnih skupova i konferencija, a za vreme doktorskih studija autor je više radova objavljenih na međunarodnim konferencijama i časopisima:

2. OPIS DISERTACIJE

2.1. Sadržaj disertacije

Doktorska disertacijapod naslovom: "*Evaluacija novog pristupa u zaštiti VoIP komunikacija*" ima ukupno 97 strana. Disertacija ima pet poglavlja i spisak literature. Poglavlja su:

1. Uvod, 6 strana
2. Komunikacioni sloj, 25 strana
3. Šifrovanje sadržaja, 31 strana
4. Postavke sistema šifrovane komunikacije, 21 strana
5. Zaključak, 2 strane.

U disertaciji ima ukupno 56 slika, 10 tabela. Literatura sadrži 54 biblografske jedinice.

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 nedostaci kod postojećih pristupa, kao i prednosti pristupa korišćenog u tezi. Navedeni su originalni naučni doprinosi teze kao i korišćene naučne metode i postupci.

U drugom poglavlju se obrađuje komunikacioni sloj sistema, dat je prikaz postojećih telekomunikacionih kapaciteta i aktuelnih standarda. Zatim je ustanovljen maksimalni standard za kvalitet prenosa glasa koristeći postojeće raspoložive kapacitete telekomunikacione infrastrukture.

U skladu sa time je postavljeno testno okruženje za proveru i evaluaciju pretpostavljenog modela, i po izvršenju testiranja u kako idealnim, tako i tačno kvantifikovanim neidealnim uslovima, dati su rezultati tih ispitivanja.

Na osnovu dobijenih rezultata, pretpostavljeno je da se može koristiti još skromniji model koji bi bio duplo efikasniji/otporniji na neidealne uslove u komunikacionoj infrastrukturi.

U nastavku poglavlja je testno okruženje prekonfigurisano u skladu sa ovom pretpostavkom i izvršeni su istovetni testovi i merenja te ocena dobijenih rezultata.Svi rezultati su originalni rezultati naučnog rada.

Uzorci prenosa glasa su snimljeni i dostavljeni u elektronskom obliku kao dodatak radu.

U trećem poglavlju, dat je osvrt na osnove šifarskih sistema, uz kritički osvrt na iste, te odabir najpogodnijeg šifarskog sistema za kriptozaštitu glasa. Ukazano je na suštinske razlike u kriptozaštiti glasa za razlku od teksta, kao i razlike u pristupu kriptoanalize istih.

Odabran je princip šifarskog sistema koji je najpogodniji i to "jednokratna beležnica" I pritom je naglašeno koliko je suštinski bitno da šifarski ključevi budu zaista jednokratni.

U nastavku trećeg poglavlja, predlažu se i ispituju (statistički) dostupni sadržaji na internetu, sa posebnim akcentom na slikama, audio zapisima i video zapisima. Detaljno je ispitano više

vrsta takvih sadržaja, i dati su rezultati kako u samom radu, tako i u elektronskom obliku kao prilog rada. Ovi rezultati takođe su originalni naučni doprinos.

U četvrtom poglavlju se inicijalne i izvedene ideje i prethodni rezultati iz prethodnih poglavlja "objedinjuju" u cilju formiranja šifarskog sistema za zaštitu govorne komunikacija.

U prvom delu četvrtog poglavlja se prvo identifikuju nedostajući elementi za kompletiranje predmetnog sistema kriptozaštite, i definišu njihova potrebna svojstva kako sa upotrebne tačke gledišta tako i sa tačke gledišta eliminacije/minimiziranja do praktično nultog nivoa identifikovanih bezbednosnih pretnji a u odnosu na konkretni element sistema kriptozaštite.

Identifikovan je, obrađen i predložen način funkcionalne podele i "skrivanja" osetljivih delova sistema u cilju prevencije identifikacije čak i polaznih tačaka za napade na kriptozaštini system, da bi se uopšte mogla obavljati bilo kakva kriptoanaliza.

Predložen je nekonvencionalni metod korišćenja Tor mreže za deo distribuiranog sistema kriptozaštite, i detaljno opisan i obrazložen nivo postignute sigurnosti kako tog dela tako i celog sistema.

Zatim je detaljno opisan i obrazložen deo sistema koji se odnosi na odabir i dodelu jednokratnog šifarskog ključa i verifikacije istog između učesnika.

Konačno, prikazano je i detaljno dokumentovano rešenje za uspostavljanje direktne komunikacije između 2 učesnika preko interneta što sistem čini amofrnijim i prikrivenijim sa aspekta pokušaja lociranja predmetnog saobraćaja na internetu, pa samim tim i bezbednijim.

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

3. OCENA DISERTACIJE

3.1. Savremenost i originalnost

Istraživanja u oblasti razvoja novih sistemima za zaštitu govora su danas veoma aktuelna i usmerena su ka projektovanju i realizaciji rešenja, kao i izučavanje potencijalnih kontra mera i kontra-kontra mera takvih sistema. Kandidat je razvio i analiziraonovi distribuirani sistem kritpozaštite govora i ukazao na prednosti u odnosu na do sada korišćene pristupe.

U ovom kontekstu, kandidat je svoju originalnost potvrdio na korektan i uverljiv način-objavljivanjem radova u međunarodnim naučnim časopisima i međunarodnim naučnim konferencijama (5 radova, od čega jedan u časopisu sa impakt faktorom).

3.2. Osvrt na referentnu i korišćenu literaturu

U izradi disertacije korišćena je obimna literatura iz širokog dijapazona oblasti kriptografije, računarskih mreža, digitalizacije i obrade zvuka, 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 konkretan kontekst.

3.3. Opis i adekvatnost primenjenih naučnih metoda

Kandidat je u svomistraživačkom radukoristio više različitih postupaka. Najpre je uvidom u literaturu, zajedno sa mentorom došao do zaključka o potrebi za razvojem i evaluacijom novog efikasnogsistema kriptozaštite glasovne komunikacije. Detaljnom analizom raspoloživih pristupa uočeni su nedostaci, sagledane su potencijalne mogućnosti za unapređenjei formulisan je cilj istraživanja: razvoj i promocija novih postupaka u razvoju, implementaciji i evaluaciji sistema kritpozaštite govorne komunikacije.

U postupku razvoja i evaluacije novog pristupa kriptozaštite govora, kandidat je pokazao samostalnost i inventivnost pre svega u raslojavanju i funkcionalnoj podeli sistema, određivanju optimalne strukture sistema uz konstantnu brigu o suštinskim bezbednosnim aspektima sistemaCeo sistem je funkcionalno evaluiran i verifikovan i simulacijom impolementiranih funkcija, te poređenjem sa odgovarajućim referentnim vrednostima.

Prednosti i nedostaci predloženog pristupa su 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 razvoja i implementacije kriptozaštinih sistema govora. Naime, prezentovano rešenje sadrži više novih fundamentalnih pristupa iz kojih se mogu kreirati mnogobrojne varijacije sa više nego zadovoljavajućim nivoom bezbednosti

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:

- Utvrđivanje potrebnih/raspoloživih kapaciteta telekomunikacione infrastrukturte, pa modelovanje sistema prema istim. Uspostavljanje realnog testnog okruženja i testiranje te verifikacija modela, korigovanje modela i re-testiranje istog sa kvalitativnim i kvantitativnim merenjima i prikazom rezultata istih,
- Predlog novog rešenja za kriptozaštitu govora, i predlog modela jednokratnog ključa, te istraživanje i evaluacija vrednosti predloženih materijala za šifarske ključeve,

- Doprinos razvoju proceduralnog okruženja i sofverske osnove za implementaciju celog sistema korišćenjem aktuelnih softverskih alata i tehnologija za podršku razvoja i unapređenjasistema za kriptozaštitu govora.

Predloženi postupci i modeli otvaraju put ka efikasnijim i pre svega bezbednijim sistemima kriptozaštite govora, jer su precizno definisane funkcionalne celine sistema, i ceo sistem je amorfno struktuirančime se umanjuju ako ne i eliminišu mogućnosti za kriptoanalitičke napade na sistem. Funkcionalno i vremenski razdvojeni procesi određivanja jednokratnog šifarskog ključa, i konkretne zaštićene govorne komunikacije su neka od najbitnijih unapređenja u navedenom sistemu. "Skrivanje" centralnog čvora za dodelu ključeva u Tor mreži takođe dodatno podiže bezbednost celog sistema. Predloženi ssitem se u potpunosti bazira na softverskim tehnikama, nije potrebna upotreba nikakvog posebnog hardvera.Takođe sistem je ceo tako koncipiran da nije moguća "sistemska provala sistema" kompromitovanjem pojedinačnog korisnika/uređaja, što čini sistem izuzetno pogodnim za dugotrajnu upotrebu.

4.2. Kritička analiza rezultata istraživanja

U prvoj fazi kandidat je razmatrajući raspoloživu literaturu u oblasti teme disertacijeizvršio kritičku analizu dostupnih informacija i korektno definisao cilj istraživanja. U istraživačkom radu koristio je mogućnost kritičkog preispitivanja i pogodne načine verifikacije dobijenih rezultata. Svi elementi predloženg sistema evaluirani su i verifikovani direktnim merenjima i poređenjem rezultata 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

Bojan P. Prlincevic, Stefan R. Panic,Petar C. Spalevic, Milan A. Misic, Abdalmalik Amniesi,Vladimir Stanojevic:"On the Transmission of Double Watermarked Image over Rician FSO Channel",ELEKTRONIKA IR ELEKTROTECHNIKA,ISSN 1392-1215,VOL.22,NO.3,2016, DOI http://dx.doi.org/10.5755/j01.eie.22.3.15320

Kategorija M63

1. 1. V. Stanojević, M. Veinović: *Internet Robotic Software –Potential and Application, Sinteza 2014,* p.863-867, DOI: 10.15308/SInteZa-2014-863-867, 2014

2. V. Stanojević, M. Veinović: *Administriranje i zaštita LAN mreže obrazovne institucije multifunkcionalnim Linux Box-om,* Časopis NIR (Issue 6) p.31-41,ISSN 2233-1603, UDK 004.7, 2014.

3. V. Stanojević,*Tehnike reverznog inženjeringa Andorid Aplikacija i kontramere,* I Međunardno savetovanje Upravljanje znanjem i informatika,p.35-42, 2015.

4. V. Stanojević: *JAFFA Framework*, 2.međunarodnosavetovanje"Upravljanje znanjem i informatika", 2016.

5.MIŠLJENJE KOMISIJE I PREDLOG

Na osnovu izloženog, komisija konstatuje da doktorska disertacija Vladimira Stanojevića,master informacionih tehnologija, pod naslovom *"Evaluacija novog pristupa u zaštiti VoIP komunikacija"* ispunjava sve formalne i suštinske uslove predviđene Zakonom o visokom obrazovanju, kao i propisima univerziteta Singidunum u Beogradu. Doktorska disertacija VladimiraStanojevića sadrži naučne doprinose koji se sastoje u razvoju i evaluaciji sistema kriptozaštite govora.

Tokom celokupne izrade doktorske disertacije, kao i na ukupnom radu na dokorskim studijama, kandidat je pokazao nesumnjivu sposobnost za samostalni nauučnoistraživački rad. Stoga članovi Komisije sa zadovoljstvom predlažu Veću departmana za poslediplomske studije i medjunarodnu saradnju da se doktorska disertacija pod naslovom "*Evaluacija novog pristupa u zaštiti VoIP komunikacija*" kandidata Vladimira Stanojevića, mastera u oblasti informacionih tehnologija prihvati, izloži na uvid javnosti i uputi na konačno usvajanje Senatu univerziteta Singidunuma u Beogradu.

Beograd, _____ 2016. godine

Članovi komisije:

dr Mladen Veinović, redovni profesor,
Univerzitet Singidunum, Beograd

_____

dr Milan Milosavljević, redovni profesor,
Univerzitet Singidunum, Beograd

_____

dr Petar Spalević, redovni profesor,
Fakultet Tehničkih Nauka, Univerzitet u Prištini

_____