УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

09.01.2013. године
Београд,

УНИВЕРЗИТЕТ У БЕОГРАДУ
Веће научних области техничких наука

Београд
Студентски трг бр 1

У прилогу дописа достављамо потребну документацију за давање сагласности на предлог теме докторске дисертације кандидата мр Драгана Кораћа.

Захтев се доставља у складу са чланом 54 Закона о Универзитету.

С поштовањем,

СЕКРЕТАР ФАКУЛТЕТА

Гордана Алексић Славински, дипл. правник

Образац 1.

Факултет организационих наука

УНИВЕРЗИТЕТ У БЕОГРАДУ

04-03-11/3
(Број захтева)

Веће научних области техничких наука
(Назив стручног већа коме се захтев упућује сходночл 6. и члану 7. ст. 1. овог Правилника)

09.01.2013.
(Датум)

ЗАХТЕВ
за давање сагласности на предлог теме докторске дисертације

Молимо да, сходо члану 57. ст. 3. Закона о универзитету («Службени гласник РС» бр. 21/02), дате сагласност на предлог теме докторске дисертације: (пун назив предложене теме докторске дисертације)
Модел заштите информација у системима за менаџмент идентитета и управљање приступом

НАУЧНА ОБЛАСТ: ОРГАНИЗАЦИОНЕ НАУКЕ

ПОДАЦИ О КАНДИДАТУ:

1. Име, име једног од родитеља и презиме кандидата:
   мр Драган (Милан) Корађ
2. Назив и седиште Факултета на коме је стекао високо образовање: Машински факултет Бања Лука
3. Година дипломирања: 1999. године
4. Назив магистарске тезе кандидата: Информациони системи обавјештајних агенција транзиционих земаља у контексту европских интеграција
5. Назив факаултета на коме је магистарска теза одбрањена: Факултет информационих технологија, Паневропски Универзитет Аперион , Бања Лука
6. Година одбране магистарске тезе: 2009. година
7. Назив факултета на коме је кандидат завршио докторске студије: /
   Одсек, смер или група: /
   Година завршетка докторских студија: _____

Обавештавамо вас да је: НАСТАВНО НАУЧНО ВЕЋЕ ФОН-А
(назив надлежног тела факултета)

на седници одржаној: 26.12.2012. године размотрило предложену тему и закључило да је тема подобна за израду докторске дисертације.

ДЕКАН ФАКУЛТЕТА

_____

Проф. др Милан Мартић

Прилог:

1. Предлог теме докторске дисертације са образложењем.
2. Акт надлежног тела факултета о подобности теме за израду докторске дисертације.

05-01 бр. 3/155-7

Поводом предлога Већа студијског програма докторских академских студија, а на основу члана 56. Статута Факултета, на седници Наставно-научног већа одржаној 26.12.2012. године, једногласно је донета следећа

О Д Л У К А

Усваја се Извештај Комисије за оцену научне заснованости пријављене докторске дисертације кандидата мр Драгана Корађа под насловом »МОДЕЛ ЗАШТИТЕ ИНФОРМАЦИЈА У СИСТЕМИМА ЗА МЕНАЏМЕНТ ИДЕНТИТЕТА И УПРАВЉАЊЕ ПРИСТУПОМ«. За ментора се предлаже др Дејан Симић, ред. проф. ФОН-а.

Извештај се доставља Већу научних области техничких наука Универзитета у Београду.

Председник Наставно научног већа

Проф. др Милан Мартић

Доставити:
- Стручном сараднику за ПДС
- Ментору
- Вишем референту органа управљања и стручних органа
- Архиви

ПОДАЦИ О МЕНТОРУ

за кандидата Драгана Кораћа

Име и презиме ментора: Дејан Симић

Звање: редовни професор

Списак радова који квалификују ментора за вођење докторске дисертације:

1. Stanković Srđan, **Simić Dejan**, Nenadović Goran, "Merchant Web Applications Defense in E-commerce Enviroment", INFORMATION JOURNAL, published by International Information Institute in Tokyo, Vol. 15, No. 8, ISSN 1343-4500, pg. 3301-3312., August 2012., **IF: 0.25** (2011), **SCIe**
2. Kostrešević Mladen, **Simić Dejan**, "Security measures for protection of e-Government IT infrastructure", TTEM – Technics, Technologies, Education, Management, Vol. 6, No. 3, ISSN 1840-1503, pg. 801-810., 2011., **IF: 0.351** (2011), **SCIe**
3. Lazović Miroslav, **Simić Dejan**, "Botnets: the evolution and possible solution", TTEM – Technics, Technologies, Education, Management, Vol. 6, No. 3, ISSN 1840-1503, pg. 829-835., 2011. , **IF: 0.351** (2011), **SCIe**
4. Trikoš Mladen, **Simić Dejan**, "Providing strong access control in campus computer network by using RADIUS server", TTEM – Technics, Technologies, Education, Management, Vol. 6, No. 2, ISSN 1840-1503, pg. 482-488., 2011., **IF: 0.351** (2011), **SCIe**
5. Milovanović Miloš, Bogićević Marija, Lazović Miroslav, **Simić Dejan**, Starčević Dušan, "Choosing Authentication Techniques in E-procurement System in Serbia", ARES 2010, IEEE Proceedings of Second International Conference on Availability, Reliability and Security, pp. 374-379, Krakow, Poland, 15-18. February 2010.
6. Savić Dušan, **Simić Dejan**, Vlajić Siniša: "Extended Software Architecture based on Security Patterns", Informatica, International Journal, Vol. 21, No. 2, pg. 229-246, June 2010, ISSN: 0868-4952, **IF 1.040**, (2009), **SCIe**
7. Šućurović Snežana, **Simić Dejan**, "An Approach to Access Control in Electronic Health Record", Journal of Medical Systems, Vol. 34, No. 4, pg. 659-666, 2010., Springer Netherlands, DOI: 10.1007/s10916-009-9279-4, ISSN: 0148-5598, **IF 0.654**, (2009), **SCIe**
8. Vidaković Dragan, **Simić Dejan**, "A Novel Approach to Building Secure Systems", ARES 2007, IEEE Proceedings of Second International Conference on Availability, Reliability and Security, pp. 1074-1084, Vienna, Austria, 10-13. April 2007.
9. Prodanović Radomir, **Simić Dejan**, "A Survey of Wireless Security", Journal of Computing and Information Technology, Vol. 15, Number 3, ISSN: 1330-1136, pg. 237-255., 2007.
10. Jovičić Bojan**, Simić Dejan,**"Common Web Application Attack Types and Security Using ASP.NET", Comput. Sci. Inf. Syst., Vol. 3, Number 2, pg. 83-96., December 2006., ISSN: 1820-0214**, IF 0.324, SCIe**
11. Prodanović Radomir, **Simić Dejan,**"Holistic Approach to WEP protocol in Securing Wireless Network Infrastructure", Comput. Sci. Inf. Syst., Vol. 3, Number 2, pg. 97-113., December 2006., ISSN: 1820-0214, **IF 0.324**, **SCIe**

Заокружити одговарајућу опцију(А,Б,В или Г):

А) У случају менторства дисертације на докторским студијама у групацији техничко-технолошких, природно-математичких и медицинских наука ментор треба да има најмање три рада са SCI, SSCI, AHCI или SCIe листе.
Б) У случају менторства дисертације на докторским студијама у групацији друштвено-хуманистичких наука ментор треба да има најмање три рада са релевантне листе научних часописа (Релевантна листа научних часописа обухвата SCI, SSCI, AHCI и SCIe листе, листу часописа које је Министарство за науку класификовало као М24 и додатну листу часописа коју ће, на предлог универзитета, донети Национални савет за високо образовање. Посебно се вреднују и монографије које Министарство науке класификује као М11, М12, М13, М14, М41 и М51.)
В) У случају израде докторске дисертације према ранијим прописима за кандидате који су стекли академски назив магистра наука ментор треба да има пет радова (референци) које га, по оцени Већа научних области, квалификују за ментора односне дисертације.
Г) У случају да у ужој научној области нема квалификованих наставника, приложити одлуку Већа докторских студија о именовању редовоног професора за ментора.

ДЕКАН ФАКУЛТЕТА

Датум 21.12.2012. М.П. _____

UNIVERZITET U BEOGRADU
FAKULTET ORGANIZACIONIH NAUKA

Nastavno-naučnom veću FON-a

Odlukom Nastavno-naučnog veća FON-a od 05.12.2012. imenovani smo u Komisiju za ocenu naučne zasnovanosti prijavljene doktorske disertacije kandidata Dragana Korać, pod naslovom:

"Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom"

i na osnovu toga podnosimo sledeći

IZVEŠTAJ

1. Podaci o kandidatu

1.1. Biografija kandidata

Dragan (Milan) Korać je rođen 24.09.1974. godine u Prijedoru. Osnovnu školu i srednju mašinsku je završio u Sanskom Mostu. Na Mašinskom fakultetu u Banjaluci, smer – proizvodno mašinstvo, diplomirao je 1999. godine na temu *Menadžment informacioni sistem.* Magistrirao je 2009. godine na Fakultetu informacionih tehnologija, Panevropskom univerzitetu Apeiron u Banjaluci gde je odbranio magistarski rad na temu "*Informacioni sistemi obavještajnih agencija tranzicionih zemalja u kontekstu evropskih integracija"*. Osnovne i postdiplomske studije je završio u roku, kao jedan od najboljih studenata u generaciji. Takođe, Dragan Korać je dugogodišnji vrhunski sportista, karatista i osvajač mnogih evropskih odličja.

1.2. Podaci o magistraturi

- *Tema*: "Informacioni sistemi obavještajnih agencija tranzicionih zemalja u kontekstu evropskih integracija"
- *Oblast*: Informacioni sistemi
- *Mentor*: Prof. dr Branko Latinović
- *Fakultet*: Fakultet informacionih tehnologija
- *Univerzitet*: Panevropski univerzitet Apeiron
- *Odbrana:* Magistarski rad je odbranjen 13.11.2009. godine u Banjaluci

1.3. Spisak objavljenih radova kandidata

1. Korać Dragan, "*Intelligence cycle in intelligence agency*" Kriminalističke teme, Sarajevo, 2010, UDC434.9 ISSN: 1512-5505, Radovi objavljeni u časopisu Kriminalističke teme se referiraju u Journal of Criminal Justice Issues (SCI).

2. Korać Dragan, "*Primjena kvantne kriptografije u transmisiji informacija u obavještajnim agencijama*" Zbornik radova (Informaciono-komunikacijske tehnologije: Razvoj nadzora) Banjaluka, 2010. Broj ISSN: 978-99955-49-47-3.

Prilog:

3. Korać Dragan "*Intelligence products in intelligence agencies*" Rad je prihvaćen za recenziju u međunarodnom vodećem, časopisu *European Journal of Crime, Criminal Law and Criminal Justice*, Brill.

1.4. Ocena podobnosti kandidata za rad na predloženoj temi

Na osnovu odbranjenog magistarskog rada pod nazivom "Informacioni sistemi obavještajnih agencija tranzicionih zemalja u kontekstu evropskih integracija", kao i na osnovu do sada objavljenih radova potvrđujemo da kandidat Dragan Korać poseduje potrebna znanja i sposobnosti za rad na predloženoj temi.

2. Predmet i cilj istraživanja

2.1. Prikaz predmeta istraživanja

Predmet istraživanja u okviru ove doktorske disertacije je model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom (IAM), kao i unapređenje postojećih metoda zaštite. Predmet je usmeren na autentifikacione mehanizme koji su ključni u procesu menadžmenta identiteta kao najvažnijoj disciplini za upravljanje i zaštiti pristupa informacijama i resursima u organizacijama. Značaj i važnost autentifikacije, kao fundamentalnog procesa u opštoj informacionoj zaštiti, ogleda se u pristupu različitim informaciono-tehnološkim (IT) sistemima koji treba da budu pravilno verifikovani. Pored procesa autentifikacije u menadžmentu identiteta neophodno je, uzeti u obzir i ostale osnovne komponente koje učestvuju u procesima zaštite. Menadžment identiteta pripada multidisciplinirаnoj oblasti koja se može locirati na razmeđu nauke o informacionim sistemima, nauke o organizaciji, menadžmentu, sociologije, ekonomije, tehničko-tehnoloških nauka, i sl.

Rastuća kompleksnost i povećanje konspirativnosti sveta je ozbiljan problem koji se ne može rešiti isključivo menadžmentom identiteta ali kao osnovni proces u informacionoj zaštiti on čini suštinsko jezgro u obezbeđivanju zaštite i poboljšanju efikasnosti. Tehnološki napredak u informacionoj zaštiti je uslovio i razvoj određenih pojedinaca ili grupa koji uvek pokušavaju da prodru u IAM (Identity and Access Management) sisteme i eksploatišu njegove slabosti. U korak sa tehnološkim razvojem, otvaraju se nove mogućnosti podrške menedžmentu identiteta pre svih personalnih autentifikacionih uređaja – PAD (personal authentication device). Arhitektura PAD-a korisnika stavlja u centar tehnološkog razvoja. Najveća je snaga PAD-a što omogućava različite autentifikacione i pristupne modele u menadžmentu identiteta kroz korisničku platformu putem komunikacionih kanala kao što su bluetooth ili bežičnih LAN ili čak dopušta komunikaciju direktno sa serverom kroz drugi kanal.

2.2. Ciljevi istraživanja

Glavni cilj istraživanja je model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom, kao i dizajnirati metod autentifikacije u korisničko-orijentisanom modelu arhitekture IAM sistema sa kojim se postiže visok nivo zaštite identiteta. Na taj način redukuju se praznine koje omogućavaju razvijanje posebnog oblika kriminala koji se manifestuje u vidu zloupotreba, krađa i neovlašćenog obelodanjivanja identiteta.

Opšti cilj istraživanja je usmeren na razvijanje modela autentifikacije koji bi adekvatno odgovorio izazovima koje digitalna revolucija donosi. Da bi se u potpunosti ostvario istraživački cilj, potrebno je da se omogući uvid u nedostatke u savremenim sistemima na osnovu kojih bi se uradilo poboljšanje u tom području menadžmenta identiteta. Poboljšanja treba da uključuju primenu novih tehnoloških dostignuća koja široko otvaraju vrata razvoju složenijih modela zaštite (dvostruka i višestruka autentifikacija) zasnovanih na multitehnološkom pristupu. Dvostruka autentifikacija treba da uključuje biometriju koja u skorijem vremenu nije bila dovoljno primenjena. Stoga, cilj istraživačkog rada treba da da i kritičku ulogu u procesu autentifikacije koja postaje imperativ za razumevanje zaštite u sistemima za menadžment identiteta i upravljanje pristupom. To znači da cilj problema determiniše kombinovanje različitih tehnologija koje razvijaju novi autentifikacioni sistem široko primenjiv u različitim aplikacijama čime se postavljaju novi izazovi za napadače. U tom kontekstu posmatranja, menadžment identiteta treba da omogući poboljšanje produktivnosti sigurnosti uz smanjenje troškova, te da uspostavi najbolju ravnotežu između upotrebljivosti, zaštite i privatnosti. Time bi se osigurao maksimalni nivo zaštite upravljanja identitetima sa većom interoperabilnošću i komplementarnošću bez mogućnosti preklapanja čime se omogućava i veća zaštita poverljivih informacija. Na taj način generalno bi se postavili temelji u sveobuhvatnijem razumevanju problemskog područja i sinergijskog pristupa.

2.3. Osvrt na relevantne bibliografske izvore i ostvarene rezultate koji su u vezi sa predmetom istraživanja

Problem istraživanja, u širem smislu reči, odnosi se na menadžment identiteta koji je subjekt ove doktorske disertacije. U užem smislu reči, problem istraživanja odnosi se na autentifikacione procese koji su ključni u menadžmentu identiteta. Današnji ubrzani razvoj digitalnih tehnologija je doveo do stvaranja neslućenih mogućnosti u elektronskom komuniciranju. Sa svim prednostima koje digitalna revolucija donosi ona istovremeno uslovljava razvoj novih oblika kriminala, pre svih krađe identiteta i fišing tehnika. U takvom kompleksnom digitalnom komuniciranju korisnici su obavezni da se digitalno identifikuju kako bi se znalo "ko, kada i gde" pristupa svojim logičkim i fizičkim resursima. Problem istraživanja se dodatno usložnjava činjenicom da poslovanje zahteva dostupnost internih aplikacija eksternim partnerima i kupcima, npr. B2B i veb kupcima, pri čemu internet korisnici poseduju i višestruke digitalne identitete. Praznine koje se javljaju u tom funkcionisanju omogućavaju razvoj krađe identiteta koja je postala jedan od najbrže rastućih kriminala u "e-dobu". Drugim rečima, problem istraživanja svodi se na rukovođenje digitalnim identitetima i zaštitom odgovarajućih kredencijala koji su uzrokovani razvojem pretnji krađa identiteta i fišing tehnika kao i rastućim brojem digitalnih identiteta. Takođe, prilikom izrade autentifikacionog mehanizma zaštite često se zanemaruje činjenica da korisnici imaju različite sposobnosti, potrebe, godine i umeća. Tradicionalni mehanizmi zaštite menadžmenta identiteta fokusirani su isključivo na zaštitni interes definisan u polju zaštitnog inženjeringa. Stoga, podrazumeva se da je visok nivo zaštite često preporučen i primenjen bez ozbiljnih korisničkih razmatranja i uzimanja u obzir korisničkih potreba i pristupačnosti. Na taj način istinski se postavlja pitanje korisničke upotrebljivosti i pristupačnosti u takvom autentifikacionom rješenju.

Trenutno u svetu zaštita identiteta, a time i zaštita informacija, predstavlja najviši prioritet, goruću temu koja je uslovljena rapidnim razvojem i rastom internet usluga a time i mogućih zloupotreba, krađa i obelodanjivanja identiteta. Autentifikacija kao ključna u informacionoj zaštiti je u eksponencijalnom usponu te postoji brojna literatura koja se bavi navedenom oblašću [18,24,25,28,38,43,76,105]. U dostupnoj literaturi [4,24,4,64,76,82,107] nude se jaka autentifikaciona rešenja sa ciljem povećanja postojećih korisničkih autentifikacija, ali pri tom nije pronađen nijedan rad koji omogućava autentifikacione mehanizme zasnovane na tehnologiji dvostruke autentifikacije primenjene na korisničko-orijentisanoj platformi menadžmenta identiteta koja pri tom uključuje biometriju.

Takođe, u dostupnoj literaturi ne postoji nijedan rad koji ukazuje na detaljni pregled ili poređenje tehnologija autentifikacija u menadžmentu identiteta. U literaturi se mogu pronaći delimični pregledi tehnologija autentifikacija ili detaljni pregledi pojedinih tehnologija autentifikacije sa odgovarajućim predlozima poboljšanja autentifikacionih rešenja [2,4,27,30,65,78,79,82,85,98]. Svakako da je iz tih predloga vidljivo da je cilj budućih istraživanja usmeren na tehnologiju biometrije. Savremeni nivo

naučnih znanja u oblasti personalnog menadžmenta identiteta ne omogućava dobijanje potrebnih i dovoljno jakih mehanizama autentifikacije zasnovanih na biometriji. Stoga, postoji više radova koji se bave tom problematikom [4,19,31,35,76,79,95,96].

Prvobitna istraživanja u menadžmentu identiteta su se bazirala na modelima jednostruke autentifikacije, kakvi se mogu naći u literaturi, uglavnom baziranih na korisničkom imenu, lozinki ili otisku prsta [27,48,73,76,84,89]. U poslednje vreme sa ubrzanim tehnološkim napretkom daju se predlozi i razvoji novih, a istovremeno i složenijih modela višeslojnih autentifikacija [4,30,54,64,79,85,88,91,96,103]. Za onlajn bankarstvo, gde su motivacije za krađu identiteta i najveće, do sada se u literaturi mogu pronaći trenutna autentifikaciona rješenja zasnovana na personalnim autentfikacionim uređajima koja pri tom ne uključuju multibiometrijske tehnologije [30,54,64,85,91].

Kao polazna literatura za izradu ove disertacije koristiće se:

1. A.M. Al-Khouri, *eGovernment Strategies The case of the United Arab Emirates (UAE)*, European Journal of ePractice, 2012.

2. A.M. Al-Khouri, *PKI in Government Digital Identity Management Systems* The European Journal of ePractice, 2012.

3. A.M. Al-Khouri and Ahmad N. Al-Raisi, *Iris Recognition and the Challenge of Homeland and Border Control Security in UAE*, Elsevier Ltd. 2006.

4. A.M. Al-Khouri and J.Bal, *Digital Identities and the Promise of the Technology Trio:PKI, Smart Cards and Biometrics*, Journal of Computers Science, 2007.

5. A.M. Al-Khouri & Malek Bachlaghem, *Towards Federated Identity Management Across GCC: A Solution's Framework*, Global Journal of Strategies and Governance, Vol. 4, No. 1, 2011.

6. A.M. Al-Khouri, *PKI Technology: A Government Experience*, International Journal of Computer Science, Engineering and Information Technology Research, 2012.

7. A.M. Al-Khouri, *Corporate Government Strategy Development: A Case Study*, Business Management Dynamics, *2012*.

8. A.M. Al-Khouri, *Optimizing Identity and Access Management (IAM) Frameworks* International Journal of Engineering Research and Applications, Vol. 1, No. 3, 2011.

9. A.M. Al-Khouri, *PKI In Government Digital Identity Management Systems*, European Journal of ePractice n° 15, 2012.

10. A.M. Al-Khouri, *PKI in Government Identity Management Systems*, International Journal of Network Security & Its Applications, Vol.3, No.3, 2011.

11. A.M. Al-Khouri, *The Role of Digital Certificates in Contemporary Government Systems: The Case of UAE Identity Authority*, International Journal of Computer Science, Engineering and Information Technology Research, 2012.

12. Adam Barth, Collin Jackson, and John C. Mitchell. *Robust Defenses for Cross-Site Request Forgery*, ACM CCS, 2008.

13. Andrew Bortz, Adam Barth, and Alexei Czeskis. *Origin Cookies: Session Integrity for Web Applications*, W2SP, 2011.

14. Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, Llanos Abad. *Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps*, ACM FMSE, 2008.

15. Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, G. Pellegrino, A. Sorniotti. *From Multiple Credentials to Browser-based Single Sign-On: Are We More Secure?* IFIP Information Security Conference (SEC), 2011

16. Amazon Web Services, *AWS Identity and Access Management (IAM) Using IAM*, Kindle, 2012.

17. Andreas Pashalidis and Chris J. Mitchell, *Single Sign-On using Trusted Platforms*, Egham, Surrey, TW20 0EX, United Kingdom Anil K. Jain, Arun A. Ross and Karthik Nandakumar, *Introduction to Biometrics*, Springer, 2011.

18. Anoop M. Namboodiri and Anil K. Jain, *Multimedia Document Authentication using On-line Signatures as Watermarks*, Proceedings SPIE 5306, 2004

19. Arun A. Ross, Karthik Nandakumar and Anil K. Jain, *Handbook of Multibiometrics (International Series on Biometrics)*, Springer, 2011.

20. Audun Jøsang and Simon Pope, *User Centric Identity Management*, AusCERT Conference, Gold Coast, Australia, 2005.

21. Audun Jøsang, John Fabre, Brian Hay, James Dalziel, Simon Pope, *Trust Requirements in Identity Management*, Conference: ACSW Frontiers - ACSW , pp. 99-108, 2005.

22. Audun Jøsang, Muhammed Al Zomai, Suriadi Suriadi, *Usability and Privacy in Identity Management Architectures*, Proceedings of the fifth Australasian symposium on ACSW frontiers, Australia, 2006.

23. Axel Buecker, Simon Canning, Jay Devaney, Guillermo Rios and Satoshi Takahashi, *Single Sign-On Solutions for IBM FileNet P8: Using IBM Tivoli and WebSphere Security Technology*, GSA ADP, 2009.

24. Barish, M. *Design and Evalution of an Arcitectura for Ubiquitous User Authentication based on Identity Management Systems Paper preseented on International Joint Conference of IEEE*. Trustcom11/IEEE ICESS-11/FCST-11, 2011.

25. Bill Ballad, Tricia Ballad and Erin Banks, *Access Control, Authentication, and Public Key Infrastructure (Information Systems Security & Assurance)*, Jones & Bartlett Learning, 2010

26. Bobrowicz and V.N. Venkatakrishnan. *NoTamper: Automatically Detecting Parameter Tampering Vulnerabilities in Web Applications*, ACM CCS 2010.

27. Chin-Chuan Han, Hsu-Liang Cheng, Chih-Lung Lin, Kuo-Chin Fan *Personal authentication using palm-print features*,The Journal of The Pattern Recognition society, Elsevier Science, 2002.

28. Chris Inskeep, *Understanding Access Controls, Logon with Identification & Authentication (Information Security in Brief, 2012)*, Amazon Digital Services, 2012.

29. Chris Inskeep, *Understanding Access Controls, File Permissions (Information Security in Brief)*, Amazon Digital Services, 2012.

30. Christoffer Haglund, *Two-factor Authentication With a Mobile Phone*, Department of Information Technology, Lund University, Sweden, 2007.

31. Chuck Wilson, *Vein Pattern Recognition: A Privacy-Enhancing Biometric*, CRC Press, 2010.

32. Corbin H. Links, *IAM Success Tips: Identity and Access Management Success Strategies*, CreateSpace Independent Publishing Platform, 2008.

33. Daisuke Mashima, David Bauer, Mustaque Ahamad and Douglas M. Blough, *User-centric Identity Management Architecture Using Credential-holding Identity Agents*, IGI Global, 2012.

34. Dasun Weerasinghe, *Information Security and Digital Forensics: First International Conference, ISDF 2009, London, United Kingdom*, Springer, 2010.

35. Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A, and Minkyu Choi, *Biometric Authentication: A Review*, International Journal of u- and e- Service, Science and Technology vol. 2, No. 3, 2009.

36. Devdatta Akhawe, Adam Barth, Peifung Lam, John Mitchell, DawnSong. *Towards a Formal Foundation of Web Security*, IEEE Computer Security Foundations Symposium, 2010.

37. Dirk van Rooy & Jacques Bus, *Trust and privacy in the future internet—a research perspective*, Springer, 2010.

38. Dobromir Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*, Taylor and Fransis group, 2007.

39. E.Maler, D.Reed, *Options and Issues in Federated Identity Management*, IEEE Security & Privacy, vol.6 no.2, 2008.

40. E. Hayashi, N. Christin, R.Dhamija and A.Perrig, *Use Your Illusion; Security Authentication Usable Anywhere*, Symposium on Usable Privacy and Security (SOUPS), Pittsburg, USA, 2008.

41. Elisa Bertino Kenji Takahashi *Identity Management: Concepts, Technologies, and Systems (Information Security & Privacy)*, Artech house, 2011.

42. Emilio Mordini and Dimitros Tzovaras, *Second Generation Biometrics: The Ethical, Legal and Social Context (The International Library of Ethics, Law and Technology)*, Springer, 2012.

43. Exam REVIEW, *CAP Certified Authorization Professional Exam ExamFOCUS Study Notes & Review Questions 2012: Building your ISC2 exam readiness*, CreateSpace Independent Publishing Platform, 2012.

44. Fabian Monrose, Michael K. Reiter, SusanneWetzel, *Password hardening based on keystroke dynamics*, Springer, 2001.

45. Garcia, S.S., Gomez, O.A. & Perez E.B.*) Is Europe ready to provide a pan-European Identity Management System?* IEEE Securiti and Privacy, 2012.

46. Glasser U., Vajihollahi M., *Identity Management Architecture*, Simon Fraser Universitety, Canada, 2008.

47. Global Technology Audit The Institute of Guide (GTAG), *Identity and Access Management*, Internal Auditors, 2007.

48. Guthery, S.B., Cronin, M.J.: *Mobile Application Development with SMS and SIM Toolkit*. McGraw-Hill, New York, 2002.

49. Hansena M., Pfitzmannb A., Steinbrecherb S., *Identity managemant throughout one's whole life*, Information security tehnical report 13., 2008.

50. Hao Chen, David Wagner and Drew Dean. *Setuid demystified*, USENIX Security Symposium, San Francisco, CA, 2002.

51. Harold F. Tipton and Mickie Krause Nozaki, *Information Security Management Handbook, 2012 CD-ROM* , CRC Press, 2012.

52. Harold F. Tipton, Micki Krause, *Information Security Management Handbook Fifth ed. vol.3*, Taylor & Fransis group, 2006.

53. Harrop M., *Identity Management*, The Cottingham Group, ETSI Security Workshop, 2009.

54. J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, A. de Santos Sierra, *Authentication in mobile devices through hand gesture recognition*, Springer-Verlag 2012.

55. Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner and Ronald Leenes, *Privacy and Identity Management for Life*, 7th IFIP WG 9.2, International Summer School, Trento, Italy, Springer, 2012.

56. Jan Camenisch, Simone Fischer-Hübner and Kai Rannenberg, *Privacy and Identity Management*, Springer, 2011.

57. Jan Killmeyer Tudor, *Information Security Architecture*, Auerbach Publication, 2001.

58. Jason Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Syngress, 2011.

59. Jeff Scheidel, *Designing an IAM Framework with Oracle Identity and Access Management Suite*, McGraw-Hill Osborne Media, 2010.

60. Jesse Russell and Ronald Cohn, *OpenLDAP*, Book on Demand Ltd, 2012

61. Jin Z.P., Xu J., Xu M., Yheng N., *An Attribute-Oriented Model for Identity Management*, International Conference on E-Eduction, e-Business, e-Management and e-Learning, 2010.

62. K. Stefanova, D.Kabakchieva, Rnikolov, "*Design Principles of Identity Management Architecture Devolopment for Cross-Border eGoverment Service*", 10th European Conference on eGoverment, 2010.

63. Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, Nikhil Swamy. *Verified Implementations of the Information Card Federated Identity-Management protocol*, ACM ASIACCS, 2008.

64. Lach, J., *Using mobile devices for user authentication*. In Kwiecien, A., Gaj, P. Stera, P., eds.: Computer Networks, 17th Conference, CN 2010, Proceedings. Vol. 79 of Communications in Computer and Information Science. Springer, Berlin, 2010.

65. Lothar Fritsch, Kristin Skeide Fuglerud & Ivar Solheim, *Towards inclusive identity management*, IDIS(2010), Springer, 2010.

66. Marcin Dabrowski Piotr Pacyna, *Modular reference framework architecture for Identity Management*, IEEE Conference Publications, 2008.

67. Mark J. Burge and Kevin W. Bowyer, *Handbook of Iris Recognition (Advances in Computer Vision and Pattern Recognition)*, Springer, 2012.

68. Mark Stamp, *Information Security: Principles and Practice*, Jonh Wiley & Sons, 2011.

69. Marlin B. Pohlman, *Oracle Identity Management: Governance, Risk, and Compliance Architecture, Third Edition,* Tylor and Fransis group, 2012.

70. Matt Butcher, *Mastering OpenLDAP: Configuring, Securing and Integrating Directory Services*, Packt Publishing, 2007.

71. McCusker, J.P., Lebo, T,Chang,C., Silva,P.P. & McGuinness, D, *Parallel Identities for Managing Open Government Data*. Accepted for publication in IEEE Intelligent Systems, 2012.

72. Messaoud Benantar, *Access Control Systems: Security, Identity Management and Trust Models*, Springer, 2010.

73. Michael Burrows, Martín Abadi, and Roger Needham. *A logic of Authentication*. ACM Trans. Computer Systems, 1990.

74. Michael E. Whitman and Herbert J. Mattord, *Management of Information Security*, Course Technology, 2010.

75. Michael S. Zanger, *Current Federal Identity Management and the Dynamic Signature Biometrics Option,* Amazon Digital Services, 2012.

76. N. K. Ratha, J. H. Connell, R. M. Bolle, *Enhancing security and privacy in biometrics-based authentication systems,* IBM Systems Journal, Vol 40, No 3, 2001.

77. Nadia Nedjah, AjithAbraham and Luiza de MacedoMourelle, *Computational Intelligence in Information Assurence and Security,* Springer 2007.

78. Nandini, C., RaviKumar, C.N., *Multi-biometrics approach for facial recognition*. In: International Conference on Computational Intelligence and Multimedia Applications, vol. 2, 2007.

79. Nathan Clarke, *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*, Springer , 2011.

80. Norm Archer, Susan Sproule, Yufei Yuan and Ken Guo, *Identity Theft and Fraud: Evaluating and Managing Risk (Critical Issues in Risk Management)*, University of Ottawa, 2012.

81. P. Windley, *Digital Identity*, Sebastopol, USA: O'Reilly, 2005.

82. P.C. van Oorschot Tao Wan, *TwoStep: An Authentication Method Combining Text and Graphical Passwords*, Springer, 2009.

83. Peter Bernus, Kai Mertins, Gunter Shmidt, *Handbook on Architectures of Information Systems*, 2nd ed. Springer, 2006.

84. Pfitzman, A., *Multilateral Security: Enabling Technologies and Their Evalution*, R.Wilhelm(Ed.).Informatics-10 Years Back, 10Years Ahead, LNCS 2000, Springer, Heidelberg, 2001.

85. Qian Tao and Raymond Veldhuis *Biometric, Authentication System on Mobile Personal Devices*, IEEE Transactions On Instrumentation And Measurement, Vol. 59, No. 4, 2010.

86. R. Dhamija, L. Dusseault, "*The Seven Flaws Of Identity Management: Usability and Security Challenges,"* IEEE Security and Privacy,vol.6, 2008.

87. Raj Sharman, Sanjukta Das Smith and Manish Gupta *Digital Identity and Access Management: Technologies and Frameworks*, IGI Global, 2011.

88. Richard Chow, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Yuan Niu and Elaine Shi, *Authentication in the Clouds: A Framework and its Application to Mobile Users*, 17th ACM Conference on Computer and Communications Security, Chicago, 2010.

89. Richard E. Smith, *Authentication: From Passwords to Public Keys*, Addison-Wesley Professional, 2001.

90. Rui Wang, Shuo Chen, XiaoFeng Wang, and Shaz Qadeer. *How to Shop for Free Online – Security Analysis of Cashier-as-a-Service Based Web Stores.* IEEE Symposium on Security and Privacy, 2011.

91. S. Furnell, N. Clarke, and S. Karatzouni, *Beyond the 7 pin: Enhancing user authentication for mobile devices*, Computer Fraud & Security, 2008.

92. S. Shim, G.Bhalla, V.Pedyala, *Federated Identity Management* IEEEComputer, vol.38, 25, 2005.

93. Sally Hudson, *Identity and Access Management Forecasts and Trends*, *2005-2009*, IDC Research, 2007.

94. Sally Hudson, *Worldwide Identity and Access Management 2008-2012 Forecast and 2007 Vendors*, IDC, 2008.

95. Senk, C. & Dotzler, F. *Biometric Authentication as a service for Enterprice Identity Management Deployment*. Paper presented at Sixth International Conference on Availability, Reliability and Security, 2011.

96. Shimon K. Modi, *Biometrics in Identity Management: Concepts to Applications (Artech House Information Security and Privacy)*, Artech House, 2011.

97. Simić D., Milenković I. Bogićević M., *Identity Management – A Survey*, XIII International Symposium Symorg, Serbia, Zlatibor, 2012.

98. Simić Dejan, Šošević Uroš, Milenković Ivan, *Architectura of Comprehesive Identity and Access Management*, XXVII Naučno-Stručni Skup Infotech, Beograd, 2012.

99. The Government of the Hong Kong, *Temporary Security Credentials*, Kindle, 2012 Special Administrative Region, 2008.

100. Thomas L. Norman, *Electronic Access Control*, Butterworth-Heinemann, 2011.

101. Thomas R. Pltier, Justine Peltier, John Blackley, *Informatio Security Fundamentals*, CRC Press LLC, 2005.

102. Tipton. F.H.,Krause M., *Information Security Management Handbook Sixth Edition*, Taylor & Fransis group, 2007.

103. Torsten Noack & Herbert Kubicek, *The introduction of online authentication as part of the new electronic national identity card in Germany*, Springer, 2010.

104. V.Bertocci etal.. *Understanding Windows Cardspace: An Introduction to the Concepts and Challenges of Digital Identities*. Addison-Wesley Longman, 2008.

105. Vijayakrishnan Pasupathinathan, *Hardware-based Identification and Authentication Systems*, Ph.D Thesis, 2009.

106. Vivek Santuka, Premdeep Banga and Brandon J. Carroll, *AAA Identity Management Security*, Cisco systems, 2010.

107. Waleed A. Alrodhan and Chris J. Mitchell, *Enhancing User Authentication in Claim-Based Identity Management*, IEEE Conference Publications, *2010.*

108. Walter Fumy and Manfred Paeschke, *Handbook of eID Security*, Wiley-VCH, 2011.

109. Wayne J., *E-Journals Access and Management*,Routledge, Taylor&Fransis group, 2009.

110. Yuan Cao, *A survey of Identity Management Technology, Paper present at Information Theory and Information Security (ICITIS), 2010,* IEEE International Conference, 2010.

111. Yukio Itakura, Shigeo Tsujii, *Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures*, Springer-Verlag 2005.

ON-LINE

112. www.blog.janrain.com/2008/11/openid-user-eperience-data.html

113. www.blog.janrain.com/2009/01/relying-party-stats-as-of-jan-1st-2008.html (Jan Rain Blog)

114. www.blogs.msdn.com/b/jamesbrown/archive/2009/04/15/identity-providers.aspx (Identity Providers)

115. www.cogprints.org/6695/1/2-41-48.pdf (Web Single Sign-On Authentication using SAML)

116. www.developer.cisco.com/documents/4733862/4734214/Tech-note-Connect-SSO-whitepaper-c6.pdf (WebEx Connect - Single Sign On)

117. www.enisa.europe.eu (Elliot, J., Ford, M. & Birch, D.(2011). *Managing multiple electronic identities*.)

118. www.fischerinternational.com/competencies/global-identity-architecture.htm (*Global Identity Architecture*™)

119. www.google-code-update.blogspot.com/2008/10/google-moves-towaeds-single-sign on.html. (GoogleCode Blog)

120. www.identityblog.com (K.Cameron, Laws of IdentityBlog 2006)

121. www.id.ae/en/research-and-studies.aspx (Researches & Studies 2012)

122. www.infoq.com/minibooks/Identity-Management-Shoestring (G.Prasad, U. Rajbahandari, "*Identity Management ON Ashoestring*", 2011)

123. www.informatics.indiana.edu/xw7/papers/websso.pdf. (Rui Wang, Shuo Chen, XiaoFeng Wang. "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services".)

124. www.itolab.is.ocha.ac.jp/~itot/paper/ItotRICPE19.pdf (Single Sign On Architecture with Dynamic Tokens)

125. www.janrain.com/consumer-research-social-signin (Blue Research. "Consumer Perceptions of Online Registration andSocial Sign-In,")

126. www.ja-sig.org/product/cas/index.html (Central Authentication Service) (bezbjednost)

127. www.opengroup.org (S. Slone and The Open Group Identity Management Work Area, Identity Management White Paper, 2004)

128. www.kingsejong.co.kr/PDFs/AuthSvr.pdf (Single Sign-On Archictetura)

129. www.msdn.microsoft.com/en-us/magazine/cc163615.aspx (MSDN Magazine)

130. www.mthink.com/content/federated-and-centralized-it-architecture-models-for-portable ehrs (Federated and Centralized IT Architecture Models for Portable EHRs)

131. www.oasis-open.org/committees/security (OASIS Security Services (SAML) TC

132. www.opengroup.org/security/sso (The Open Group:Single Sign-On)

133. www.personalmag.rs/internet/najveca-krada-identiteta-u-istoriji/ (kradja identiteta)

134. www.redbooks.ibm.com/redpapers/pdfs/redp4423.pdf (A. Buecker, D. Bhatt, D.Craun,

135. www.sk.rs/2008/03/skpr01.html (SVET KOMPJUTERA - PRIMENA - High-tech)

3. Polazne hipoteze

3.1 Opšta hipoteza

Za realizaciju predmetnog problema istraživanja postavljena je sledeća osnovna (opšta) istraživačka hipoteza:

Razvojem novog jakog autentifikacionog mehanizma u korisničko-orjentisanom modelu menadžmenta identiteta zasnovanog na principu personalnog autentifikacionog uređaja, može se postići visok nivo zaštite identiteta.

3.2 Posebne hipoteze

Iz osnovne istraživačke hipoteze mogu se izvesti sledeće pojedinačne hipoteze:

- Proces razvoja mehanizma autentifikacije treba biti zasnovan na postojećim iskustvima i modelima.
- Personalni autentifikacioni uređaji podržavaju višestruke autentifikacione procese uključujući i biometrijske tehnologije.
- Analizom i prikazivanjem osnovnih mehanizama autentifikacije može se utvrditi potreba i efikasnost uvođenja jake autentifikacije.
- Procesom univerzalne jake autentifikacije može se omogućiti sigurnija zaštita identiteta.

4. Naučne metode istraživanja

Da bi se uspešno realizovali ciljevi istraživanja i potvrdile postavljene hipoteze, u doktorskoj disertaciji biće korišćene opšte naučne metode: analize i sinteze, apstrakcije i konkretizacije, generalizacije i specijalizacije i komparacije.

Analiza se koristi u postupku posmatranja tehnologija autentifikacije pri čemu se detaljno ulazi u strukturu problema, s ciljem uočavanja sličnosti i razlika.

Sinteza se koristi u spajanju odabranih tehnologija i metoda.

Apstrakcija i konkretizacija se koriste u postupku formiranja jake autentifikacije odnosno u procesu odabira pojedinačnih metoda i tehnologija autentifikacije.

Generalizacija i specijalizacija se koriste u postupku dizajniranja modela jake autentifikacije.

Komparacija obezbeđuje bazičnu procenu trenutnih autentifikacionih tehnika i metoda primenjenih u menadžmentu identiteta, radi formiranja sopstvenih predloga zaključaka.

Deskriptivna metoda koristi se u postupku opisavanja tehnologija i metoda autentifikacije i logičkih arhitektura menadžmenta identiteta.

5. Očekivani naučni doprinosi

Očekivani naučni doprinosi ovog rada su sledeći:

- Prikupljanje i sređivanje informacija u oblasti zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom.

- Analiza prikupljene literature, klasifikacija i kritički osvrt na postojeća rešenja.
- Sistematizacija znanja u oblasti zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom.
- Pregled i komparacija različitih tehnologija autentifikacija i arhitektura IAM sistema sa svim prednostima i nedostacima.
- Predlog arhitekture sistema za menadžment identiteta i upravljanje pristupom.
- Predlog modela zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom sa visokim stepenom zaštite.
- Potvrda praktične primene predloženog rešenja.

6. Plan istraživanja i struktura rada

6.1. Plan istraživanja

Plan istraživanja podrazumeva:

1. Prikupljanje literature i istraživanje na zadatu temu kroz pregled zbornika konferencija, časopisa, izvora na Internetu, i ostalih relevantnih izvora podataka.
2. Klasifikaciju podataka od interesa za istraživanje.
3. Analizu arhitektura sistema za menadžment identiteta i upravljanje pristupom.
4. Uporedni pregled arhitektura sistema za menadžment identiteta i upravljanje pristupom.
5. Kritički osvrt na postojeća rešenja.
6. Predlog arhitekture sistema za menadžment identiteta i upravljanje pristupom.
7. Predlog modela zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom.
8. Predlog i razvoj rešenja za autentifikaciju korisnika sistema.
9. Implementacija predloženog rešenja.
10. Analiza implementiranog rešenja.
11. Zaključak.

6.2. Struktura rada

Okvirna struktura kroz poglavlja doktorske disertacije je:

Glava I: Uvod

1.1. Osnovni pojmovi zaštite informacija
1.2. Potreba za zaštitom informacija
1.3. Principi informacione zaštite
1.4. Kontrola zaštite informacija

Glava II: Opis problema

2.1. Opis problema

Glava III: Menadžment identiteta

3.1. Identitet i digitalni identitet
3.2. Životni ciklus identiteta
3.3. Privatnost digitalnog identiteta
3.4. Krađa identita
3.5. Budućnost digitalnog identiteta

Glava IV: Menadžment identiteta i upravljanja pristupom (IAM)

4.1. Osnovi IAM
4.2. Osnovne komponente i funkcije IAM
4.3. Izazovi u IAM
4.4. Učesnici i zahtevi u IAM
4.5. Opšta infrastruktura IAM
4.6. Uloga i odgovornost IAM

Glava V: Metode autentifikacije

5.1. Uvod u autentifikaciju
5.2. Lozinka
5.3. Token
5.4. PKI
5.5. RFID
5.6. Pametna kartica
5.7. Biometrija

Glava VI: Dizajn novog modela zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom

6.1. Pregled postojećih modela zaštite informacija
6.2. Pregled postojećih autentifikacionih rješenja
6.3. Predlog novog modela zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom
6.4. Predlog arhitekture sistema za menadžment identiteta i upravljanje pristupom
6.5. Kombinovanje i integracija tehnologija autentifikacija u dizajniranju novog autentifikacionog rešenja.
6.6. Dizajn novog autentifikacionog mehanizma u korisničko-orijentisanom modelu IAM

Glava VII: Implementacija predloženog autentifikacionog mehanizma openLDAP protokolom

7.1. Pregled openLDAP-a
7.2. Primjer praktične primenjivosti
7.3. Verifikacija postavljene hipoteze
7.4. Buduća istraživanja

Glava VIII: Zaključak

Glava IX: Literatura

7. Zaključak i predlog

Na osnovu prethodno izloženog, komisija je konstatovala da predložena tema doktorske disertacije, pod nazivom **″Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom″,** po predmetu istraživanja, ciljevima i metodologiji ima naučnu zasnovanost i odgovara nivou doktorske disertacije. Predložena tema predstavlja značajnu oblast istraživanja sa teorijskog i praktičnog stanovišta.

Komisija je konstatovala da kandidat Dragan Korać ispunjava formalne uslove i poseduje sve potrebne kvalifikacije za odobravanje izrade doktorske disertacije na predloženoj temi.

Na osnovu iznetog, komisija za ocenu ispunjenosti uslova kandidata i naučne zasnovanosti teme doktorske disertacije predlaže Nastavno-naučnom veću Fakulteta organizacionih nauka da kandidatu Draganu Korać odobri izradu disertacije pod nazivom **″Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom″** i da se za mentora imenuje dr Dejan Simić, redovni profesor Fakulteta organizacionih nauka.

Beograd, 17.12.2012.god.

K O M I S I J A

Dr Dejan Simić, red. prof., mentor
Fakultet organizacionih nauka, Beograd

ČLANOVI KOMISIJE:

Dr Dušan Starčević, red. prof.
Fakultet organizacionih nauka, Beograd

Dr Boško Nikolić, vanr. prof.
Elektrotehnički fakultet, Beograd