УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

06.12.2013. 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 Бориса Дамјановића.

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

С поштовањем,

СЕКРЕТАР ФАКУЛТЕТА

Гордана Алексић Славински, дипл. правник

Јове Илића 154, 11000 Београд, Србија, Тел.: (011) 3950-800, Факс: (011) 2461-221
ПИБ: 100383934, Матични број: 07004044, Текући рачун: 840-1344666-69
Е пошта: dekanat@fon.bg.ac.rs; Посетите: www.fon.bg.ac.rs

Образац 1.

Факултет организационих наука

УНИВЕРЗИТЕТ У БЕОГРАДУ

04-03-11/ 236
(Број захтева)

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

06.12.2013.
(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)
Адаптибилна примена AES алгоритма код савремених оперативних система

НАУЧНА ОБЛАСТ: ОРГАНИЗАЦИОНЕ НАУКЕ

ПОДАЦИ О КАНДИДАТУ:

1. Име, име једног од родитеља и презиме кандидата:
   Борис (Стеван) Дамјановић
2. Назив и седиште Факултета на коме је стекао високо образовање: Висока школа за економију и информатику, Приједор
3. Година дипломирања: 2008. године
4. Назив приступног рада кандидата: Адаптибилна примена AES алгоритма код савремених оперативних система
5. Назив факултета на коме је приступни рад одбрањен: ФОН
6. Година одбране приступног рада: 2013. 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: 04.12.2013. 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.

Република Србија
Универзитет у Београду
Факултет организационих наука

Број индекса: 2010/5005
04-03-11/248
Датум: 17.12.2013.

На основу члана 161. Закона о општем управном поступку и службене евиденције, издаје се

УВЕРЕЊЕ О ПОЛОЖЕНИМ ИСПИТИМА

Борис Дамјановић, име једног родитеља Стеван, рођен 02.06.1965.године, у месту Бања Лука, Босна и Херцеговина, 2010/11. школске године уписан на докторске академске студије на 1. годину, 2013/14. школске године први пут уписан у 3. годину, самофинансирање, студијски програм Информациони системи и менаџмент, Информациони системи, током студија положио је испите из следећих предмета:

Р.бр.	Шифра	Назив предмета	Оцена	ЕСПБ	Фонд часова**	Датум
1.	Д00001	Управљање подацима	10 (десет)	10	I:(45+0+60)	30.06.2011.
2.	Д00064	Рачунарске мреже – одабрана поглавља	10 (десет)	10	III:(45+0+60)	18.07.2011.
3.	Д00004	Структуре података и алгоритми	10 (десет)	10	III:(45+0+60)	04.07.2012.
4.	Д00082	Системи заштите информационих система	10 (десет)	10	II:(45+0+60)	03.09.2012.
5.	Д00083	Технологија чувања података	10 (десет)	10	II:(45+0+60)	03.09.2012.
6.	Д00002	Развој информационих система	10 (десет)	10	I:(45+0+60)	22.10.2012.
7.	Д00012	Интеракција човека и рачунара - одабрана поглавља	10 (десет)	10	II:(45+0+60)	01.04.2013.
8.	Д00005	Софтверске архитектуре	10 (десет)	10	II:(45+0+60)	11.04.2013.
9.	Д00068	Методологија научно – истраживачког рада	10 (десет)	10	III:(45+0+60)	20.05.2013.

* - еквивалентиран/признат испит.
** - фонд часова је у формату (предавања+вежбе+остало).

Општи успех: 10,00 (десет и 00/100) , по годинама студија (10,00, 10,00, /).

Виши стручни сарадник за докторске студије

_____
др Марина Јовановић-Миленковић

Страна 1 од 1

ПОДАЦИ О МЕНТОРУ

за кандидата Бориса Дамјановића

Име и презиме ментора: Симић Дејан

Звање: редовни професор

Списак радова који квалификују ментора за вођење докторске дисертације

(Навести: име и презиме аутора, наслов рада, наслов часописа, број часописа, година издања, ISBN (DOI) број, IF):

1. Damjanović Boris, **Simić Dejan**, "Performance Evaluation of AES Algorithm under Linux Operating System", PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A, Mathematics, Physics, Technical Sciences, Information Science, Vol. 14, No. 2, pp. 173-183, April-June 2013., ISSN: 1454-9069, **IF 0.537** (2012), **SCIe**
2. 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 0.36** (2012), **SCIe**
3. 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 1.186**, (2010), **SCIe**
4. 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**
5. 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: 0.256** (2010), **SCIe**

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

А)

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 _____ М.П. _____

05-01 бр 3/158-5
9.12.2013.

Поводом предлога Већа студијског програма докторских академских студија, а на основу члана 56. Статута Факултета, на седници Наставно-научног већа одржаној 4.12.2013. године, једногласно је донета следећа

О Д Л У К А

Усваја се Извештај Комисије за оцену научне заснованости пријављене докторске дисертације кандидата на докторским студијама Бориса Дамјановића под насловом »АДАПТИБИЛНА ПРИМЕНА *AEC* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА«. 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
- Секретару органа управљања и стручних органа
- Архиви

Наставно-научном већу ФОН-а

Одлуком Научно- наставног већа ФОН-а од 13.11.2013. год. именовани смо у Комисију за оцену научне заснованости пријављене докторске дисертације кандидата **Бориса Дамјановића**, под насловом:

"АДАПТИБИЛНА ПРИМЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА"

и на основу тога подносимо следећи

И З В Е Ш Т А Ј

1. ПОДАЦИ О КАНДИДАТУ

Општи биографски подаци и образовање

Борис Дамјановић је рођен 02.06.1965. године у Бања Луци. Завршио је средњу Електротехничку школу у Приједору. Високу школу за економију и информатику Приједор завршио је 2008. године у Приједору са просечном оценом 9.61. Након тога уписао је дипломске академске студије – Мастер на Факултету организационих наука у Београду, студијски програм Информациони системи и технологије, студијско подручје Информациони системи. Мастер рад под насловом "Имплементација и проширење *AES* алгоритма" одбранио је 15. јуна 2010. године са оценом 10. Од септембра 2008. године запослен је на Високој школи за економију и информатику Приједор, као сарадник у настави, а од септембра 2010. године на истој школи запослен је као предавач.

Почевши од школске 2008/2009 године кандидат је као сарадник у настави на Високој школи за економију и информатику у Приједору учествовао у припреми, извођењу вежби и предавања на предметима: Заштита рачунарских система и Архитектура и функција рачунара. Почев од школске 2010/2011 године, кандидат је као предавач на Високој школи за економију и информатику учествовао у припреми, извођењу вежби и предавања на предметима: Базе података 1, Базе података 2, Заштита рачунарских система и Архитектура и функције рачунара.

Списак објављених радова

Кандидат Борис Дамјановић је објавио више научних радова у часописима националног и међународног значаја, као и у зборницима домаћих конференција.

Рад објављен у часопису међународног значаја (***SCIe* листа**):

- Damjanović B. & Simić D. (2013), Performance evaluation of AES algorithm under LINUX operating system, Proceedings of the Romanian Academy - series A: Mathematics, Physics, Technical Sciences, Information Science,Volume 14, number 2/2013, pp. 177-183, **IF (2012): 0.537**.

Рад објављен у часопису међународног значаја:

- Damjanović B. & Simić D. (2011), Comparative implementation analysis of AES algorithm, JITA – Journal of Information Technology and Applications, Vol. 1, No. 2, ISSN 2232-9625, pp. 119-126., December 2011.

Радови објављени у часописима националног значаја:

- Дамјановић Б. & Симић Д. (2013), Експерименти са могућим модификацијама *AES* алгоритма, ИнфоМ, Бр. 46, стр. 34-39, 2013. год., Београд

- Дамјановић Б. & Симић Д. (2013), Преглед примењених приступа за софтверску енкрипцију података у различитим оперативним системима, ИнфоМ Бр. 47, стр. 32-37, 2013. год., Београд

- Микић Ђ., Микић Н., Дамјановић Б. (2012), Оцењивање релевантности критерија управљачког протокола на бази приоритета и матричне анализе, Транзиција, Вол.14, Бр.30, 2012. год., Тузла

Радови објављени на домаћим конференцијама:

- Дамјановић Б., Симић Д. (2013), Преглед примењених приступа за софтверску енкрипцију података у различитим оперативним системима, *InfoTech* 2013, Аранђеловац

- Дамјановић Б., Марјановић З. (2013), Неки аспекти унутрашње структуре СУБП *Firebird* базе података, *InfoTech* 2013, Аранђеловац

- Дамјановић Б., Раниловић М. (2010), Стандарди, теоретске претпоставке и напредни алати као пут ка побољшању ефикасности израде информационих система, Ефикасност у привреди 2010, Зрењанин

- Раниловић М., Дамјановић Б. (2010), Менаџмент у осигурању, Ефикасност у привреди 2010, Зрењанин

2. ПРЕДМЕТ И ЦИЉ ИСТРАЖИВАЊА

Предмет истраживања

Карактеристика савремених рачунарских система је успоравање раста брзине једнопроцесорских система на досадашњи начин и окретање произвођача хардвера вишепроцесорским системима, процесорима са више језгара (тј. *multi-core* системима), као и хардверским акцелераторима.

Хетерогеност и реконфигурабилност хардверских и софтверских компонената које се користе за побољшање перформанси *AES* алгоритма намеће потребу постојања јединственог интерфејса у оквиру оперативног система за приступ криптографским могућностима хардвера и софтвера са стандардизованим и униформним начинима иницијализације и позивања појединих компоненти. У таквим сложеним системима се поред проблема мапирања, услед хетерогености хардверских склопова и софтверских решења јавља и потреба тражења што ефикаснијих начина коришћења расположивих хардверских и софтверских ресурса. Наведена реконфигурабилност хардверских ресурса и софтверских решења ствара још и потребу могућности прилагођења датог оперативног система и доношење одлуке коју од тренутно расположивих компонената користити за добијање најбољих перформанси.

Предмет истраживања је анализа искоришћености расположивих криптографских хардверских и софтверских ресурса од стране савремених оперативних система у имплементацији *AES* алгоритма. Могућност адаптибилне примене *AES* алгоритма у оквиру оперативног система у зависности од доступних ресурса представља централни проблем који се истражује у овом раду.

Кандидат ће у раду дати свеобухватан преглед стања у области примене криптографије у оперативним системима и приказ актуелних истраживања. У раду ће бити дефинисан методолошки приступ за адаптибилну примену *AES* алгоритма у оперативним системима у зависности од доступних ресурса, биће урађена конкретна имплементација и на крају биће дат критички осврт на предложено и имплементирано решење.

Циљеви истраживања

Примарни циљ овог истраживања је развој модела за адаптибилну примену *AES* алгоритма на нивоу оперативног система. Модел је потребно реализовати креирањем јединственог и једноставног интерфејса за приступ ресурсима и њиховим мапирањем, као и креирањем посебног алгоритма који одлуку о коришћењу расположивих ресурса доноси пре покретања функције шифровања/дешифровања, а на основу претходно меморисаних резултата извршења појединих хардверских и софтверских компонената и имплементација, као и појединих посебних услова које задају корисници.

Секундарни циљеви су побољшање перформанси рачунарског система при извршавању *AES* алгоритма, истрживање могућности модификације *AES* алгоритма повећањем броја бита кључа уз смањен утрошак процесорске снаге. Поред тога, секундарни циљеви обухватају истраживање постојећих и нових решења за паралелизацију извршења *AES* алгоритма.

Оквирна листа релевантних библиографских извора која ће се користити приликом израде докторске дисертације:

[1] Akdemir, K., Dixon, M., Feghali, W., Fay, P., Gopal, V., Guilford, J., Ozturk, E., Wolrich, G. and Zohar, R. (2010), Breakthrough AES Performance with Intel AES New Instructions, Intel White Paper, Intel Corporation

[2] Android Open Source Project, (2013) Notes on the implementation of encryption in Android 3.0, Android open source project Teach Info, http://source.android.com/tech/encryption/android_crypto_implementation.html

[3] Apache Fondation, (2013). Apache Commons Virtual File System (VFS), Available at: http://commons.apache.org/proper/commons-vfs/

[4] Apple Computer Inc. (2012), Apple Technical White Paper, Best Practices for Deploying FileVault 2, Deploying OS X Full Disk Encryption Technology, http://training.apple.com/pdf/WP_FileVault2.pdf

[5] Apple Corp. (2012). Best Practices for Deploying FileVault 2, Available at: http://training.apple.com/pdf/WP_FileVault2.pdf

[6] Arch Linux documentation, (2013). Disk Encryption, Available at: https://wiki.archlinux.org/index.php/Disk_Encryption

[7] Arnold, T.W., Dames, A., Hocker, M.D., Marik, M.D., Pellicciotti, N.A. and Werner, K. (2007), Cryptographic system enhancements for the IBM System z9, IBM Journal of Research and Development

[8] Basu, A. and Bhargav-Spantzel, A. (2012), AES-NI Performance Testing on Linux/Java Stack, Intel vPro Developer Community, Intel Corporation

[9] Bertoni, G., Breveglieri, L., Fragneto, P., Macchetti, M. and Marchesin, S. (2002), Efficient Software Implementation of AES on 32-Bit Platforms. CHES 2002: 159-171

[10] Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D. and Shamir, A. (2010), Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds, EUROCRYPT'10 Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques, Pages 299-319

[11] Blaze, M. (1993), A Cryptographic File System for Unix, ACM Conference on Computer and Communications Security

[12] Blevins, P.R. and Ramamoorthy, C.V. (1976), Aspects of a Dynamically Adaptive Operating System, IEEE Transactions on Computers, Volume:C-25, Issue:7

[13] Boyer B. (2008), Robust Java benchmarking, Part 1: Issues, Understand the pitfalls of benchmarking Java code, IBM developerWorks

[14] Boyer B. (2008), Robust Java benchmarking, Part 1: Statistics and solutions, Introducing a ready-to-run software benchmarking framework, IBM developerWorks

[15] Chakraborty D. and Rodriguez-Henriquez, F. (2009). Block Cipher Modes of Operation from a Hardware Implementation Perspective, Cryptographic Engineering, Springer

[16] Chakraborty, D., and Rodriguez-Henriquez, F. (2009), Block Cipher Modes of Operation from a Hardware Implementation Perspective, Cryptographic Engineering, Springer

[17] Christopher, C.J. (2010), Cryptographic Accelerators on the UltraSPARC T2 with the Solaris Cryptographic Framework, School of Computer Science, ANU, Available at: http://cs.anu.edu.au/student/projects/10S2/Reports/Cody%20Christopher.pdf

[18] Chung-wei Phan R. (2002), Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis, Cryptologia, 26(4):283–306

[19] Cid, C., Murphy, S. and Robshaw, M. (2006), Algebraic Aspects Of The Advanced Encryption Standard, Springer Science-Business Media, LLC.

[20] Copi, I.M., Cohen, C. and McMahon, M. (2010), Introduction to Logic, 14 edition, Prentice Hall

[21] Corner, M. and Noble, B. D. (2002), Zero-interaction authentication, The Eigth ACM Conference on Mobile Computing and Networking

[22] Daemen, J. and Rijmen, V. (2002), The Design Of Rijndael, Springer-Verlag, Inc.

[23] Damjanović, B. (2010), Implementacija i proširenje AES algoritma, Master rad, Fakultet organizacionih nauka, Beograd

[24] Damjanović, B. and Simić, D. (2011), Comparative Implementation Analysis of AES Algorithm, Journal of Information Technology and Applications, Banja Luka
[25] Damjanović, B. and Simić, D. (2013), Performance evaluation of AES algorithm under Linux operating system, Proceedings Of The Romanian Academy, Series A, Mathematics, Physics, Technical Sciences, Information Science, Volume 14, Number 2, pp. 177–183
[26] Damjanović, B. i Simić, D. (2013), Eksperimenti sa mogućim modifikacijama AES algoritma, InfoM 46/2013
[27] Damjanović, B. i Simić, D. (2013), Pregled primjenjenih pristupa za softversku enkripciju podataka u različitim operativnim sistemima, InfoM 47/2013
[28] Dandalisand, A. and Prasanna, V.K. (2000), An Adaptive Cryptographic Engine for IPSec Architectures, IEEE Symposium on Field-Programmable Custom Computing Machines
[29] Defreez, D. (2012), Android Privacy Through Encryption, Master Thesis of Science in Mathematics and Computer Science, Southern Oregon University
[30] Delaune, S., Kremer S. and Steel, G. (2008), Formal Analysis of PKCS#11, Research Report LSV-4
[31] Demirci, H. and Selçuk. A.A. (2008), A Meet-in-the-Middle Attack on 8-Round AES, Fast Software Encryption, Springer-Verlag Berlin, Heidelberg
[32] Di Biagio, A., Barenghi, A., Agosta and G. and Pelosi, G. (2009), Design of a Parallel AES for Graphics Hardware using the CUDA framework, IEEE International Symposium onParallel & Distributed Processing
[33] Diesburg S.M. and Wang, A.A. (2010), A Survey of Confidential Data Storage and Deletion Methods, ACM Computing Surveys (CSUR), Volume 43 Issue 1, Article No. 2
[34] Dobbertin, H., Rijmen, V. and Sowa, A. (2005), Advanced Encryption Standard AES, 4TH International Conference, Bonn, Germany, 2004, Springer-Verlag
[35] Edge, J. (2011), Desktop Summit: Crypto consolidation, Available at: https://lwn.net/Articles/454491/
[36] Ermelindo, M. (1997), Transparent Cryptographic File System, Linux Journal, Volume 1997 Issue 40es, Article No. 3
[37] Ferguson, N. (2006), AES-CBC + Elephant difuser A Disk Encryption Algorithm for Windows Vista, Microsoft White Paper
[38] FIPS197, Specification for the Advanced Encryption Standard (AES). (2001), Federal Information Processing Standards Publication 197, Available at: http://csrc.nist.gov/publications/
[39] Francia III, G.A. and Francia, R.R. (2007), An Empirical Study on the Performance of Java/.Net Cryptographic APIs, Information Security Journal: A Global Perspective, 16: 6, 344 — 354
[40] Georges, A., Buytaert, D. and Eeckhout, L. (2007), Statistically Rigorous Java Performance Evaluation, OOPSLA '07 Proceedings of the 22nd annual ACM SIGPLAN conference on Object-oriented programming systems and applications, Vol. 42, pg 57-76
[41] Georges, A., Buytaert, D. and Eeckhout, L. (2007), Statistically Rigorous Java Performance Evaluation, OOPSLA '07 Proceedings of the 22nd annual ACM SIGPLAN conference on Object-oriented programming systems and applications, Vol. 42, pg 57-76
[42] Georges, A., Eeckhout, L. and Buytaert, D. (2008), Java Performance Evaluation through Rigorous Replay Compilation, OOPSLA '07 Proceedings of the 22nd annual ACM SIGPLAN conference on Object-oriented programming systems and applications, Vol. 43, pp. 367-384
[43] Georges, A., Eeckhout, L. and Buytaert, D. (2008), Java Performance Evaluation through Rigorous Replay Compilation, OOPSLA '07 Proceedings of the 22nd annual ACM SIGPLAN conference on Object-oriented programming systems and applications, Vol. 43, pp. 367-384
[44] Gladman, B., (2007), A Specification for Rijndael, the AES Algorithm, Available at: http://gladman.plushost.co.uk/oldsite/cryptography_technology/rijndael/
[45] Gordon, S. (2013), Simplified AES Example, Security and Cryptography, Sirindhorn International Institute of Technology (SIIT) in Thammasat University, Bangkok, Thailand, Available at: http://hw.siit.net/files/001283.pdf

[46] Gordon, S. (2013). Simplified AES Example, Security and Cryptography, Sirindhorn International Institute of Technology (SIIT) in Thammasat University, Bangkok, Thailand, dostupno na: http://hw.siit.net/files/001283.pdf
[47] Gough, V. (2008), EncFS: Encrypted file system, http://arg0.net/wiki/encfs
[48] Gueron S. (2009), Intel's New AES Instructions for Enhanced Performance and Security, Fast Software Encryption, Lecture Notes in Computer Science Volume 5665, pp 51-66, Springer Berlin Heidelberg
[49] Gueron, S. (2012), Intel Corporation, White Paper, Intel Advanced Encryption Standard (AES) New Instructions Set
[50] Gupta, A., Ababneh, E., Han, R. and Keller. E. (2013), Towards Elastic Operating Systems, HotOS XIV, 14th Workshop on Hot Topics in Operating Systems
[51] Halcrow, M. (2007), eCryptfs: a Stacked Cryptographic Filesystem, Linux Journal, Volume 2007 Issue 156
[52] Harrington, P. (2012), Machine Learning in Action, Manning Publications Co.
[53] Harrison, O. and Waldron, J. (2010), GPU accelerated cryptography as an OS service, Transactions on computational science XI, Springer-Verlag Berlin, Heidelberg
[54] Hoban, A., Laurent, P., Betts, I. and Tahhan, M. (2013), Unleashing Linux*- Based Secure Storage Performance with Intel AES New Instructions, Intel Corporation, White Paper, Februar
[55] Hohmann, C. (2008) CryptoFS. http://reboot.animeirc.de/cryptofs/
[56] Honmann, C. (2008), CryptoFS. http://reboot.animeirc.de/cryptofs/
[57] Hook D. (2005), Beginning Cryptography with Java, Wrox Press
[58] Hurley, P.J. (2006), A Concise Introduction to Logic, Tenth edition, Thomson Wadsworth
[59] Huth, M. and Ryan, M. (2004), Logic in computer science, Modelling and Reasoning about Systems, Cambridge University Press
[60] IBM Corporation, (2009), IBM Blueprints, Securing Sensitive Files With TPM Keys
[61] Im, C., Jeong, M., Lee, J. and Lee, S. (2013), A Dynamically Reconfigurable Operating System for Manycore Systems, SAC '13 Proceedings of the 28th Annual ACM Symposium on Applied Computing
[62] Intel Corporation, (2013). Intel Advanced Encryption Standard (AES-NI) Ecosystem March 2013 update, Available at: http://www.intel.com/content/dam/www/public/us/en/documents/specification-updates/aes-ni-ecosystem-update.pdf
[63] Iwai, K., Kurokawa, T. and Nisikawa, N. (2010), AES Encryption Implementation on CUDA GPU and Its Analysis, First International Conference on Networking and Computing (ICNC)
[64] Keromytis, A.D., Wright, J.L., DE Raadt, T. and Burnside, M. (2006), Cryptography As An Operating System Service: A Case Study, ACM Transactions on Computer Systems (TOCS), Volume 24 Issue 1
[65] Lagger, A., Upegui, A., Sanchez, E. and Gonzalez, I. (2006), Self-Reconfigurable Pervasive Platform for Cryptographic Application, FPL 2006, International Conference on Field Programmable Logic and Applications
[66] Lagger, A., Upegui, A., Sanchez, E. and Gonzalez, I. (2006). Self-Reconfigurable Pervasive Platform for Cryptographic Application, FPL 2006, International Conference on Field Programmable Logic and Applications
[67] Lee, H.K., Malkin, T. and Nahum, E. (2007), Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices, IMC '07 Proceedings of the 7th ACM SIGCOMM conference on Internet measurement
[68] Li, G., Zheng, H. and Li, G. (2010), Building A Secure Web Server Based on OpenSSL and Apache, International Conference on E-Business and E-Government ICEE2010
[69] Lim, J., Gan, B. and Ting-Ting, C. (2002), A survey on NSS adoption intention, Proceedings of the 35th Annual Hawaii International Conference on System Sciences HICSS-35
[70] Liu, B. and Baas, B.M. (2013), Parallel AES Encryption Engines for Many-Core Processor Arrays, IEEE Transactions on Computers, Vol. 62, No. 3

[71] Lloyd J. (2013), Botan C++ crypto library, Available at: http://botan.randombit.net/index.html
[72] Lovrić, M., Komić, J., Stević, S., Zečević, T., Žižić, M. and Kočović J. (2008). Statistička analiza - metodi i primjena, Ekonomski fakultet, Univerzitet u Banja Luci, Banja Luka, BiH
[73] Malita, F. (2013). LUFS: Linux Userland FileSystem. http://lufs. sourceforge.net
[74] Manangi, S.J., Chaurasia, P. and Singh, M.P. (2010), Simplified AES for Low Memory Embedded Processors, Global Journal of Computer Science and Technology, Vol. 10 Issue 14
[75] Manavski, S.A. (2007), CUDA Compatible GPU as an Efficient Hardware Accelerator for AES Cryptography, IEEE International Conference on Signal Processing and Communications,
[76] Mavrogiannopoulos, N. and Josefsson, (2013). The GnuTLS manual, Free Software Foundation, Inc., Nikos Mavrogiannopoulos
[77] Metakides, G. and Nerode, A. (1996), Principles of logic and logic programming, Elsevier B.V.
[78] Microsoft Corp. (2005), Using Encrypting File System, Tech. rep. Available at: http://technet.microsoft.com/en-us/library/bb457116.aspx.
[79] Microsoft Corp. (2008), How EFS works. Tech. Rep. Available at: http://technet.microsoft.com/en-us/library/cc962103.aspx
[80] Microsoft Corp. (2012). FIPS 140 Evaluation, Available at: http://technet.microsoft.com/en-us/library/cc750357.aspx
[81] Microsoft Corp. (2013) Microsoft CryptoAPI and Cryptographic Service Providers, TechNet. http://technet.microsoft.com/en-us/library/ cc962093.aspx
[82] Moffat, D. (2012), How to Manage ZFS Data Encryption, Oracle technetwork
[83] Mozilla Developer Network, (2013). Network Security Services (NSS), Available at: https://developer.mozilla.org/en-US/docs/NSS
[84] Mozilla Developer Network, (2013). NSS 3.14.2 release notes, Available at: https://developer.mozilla.org/en-US/docs/NSS/NSS_3.14.2_release_notes
[85] Mukherjee, B., and Schwan, K. (1994), Adaptive Operating System Abstractions: A Case Study of Multiprocessor Locks, Technical Report GIT-CC-94/39, College of Computing, Georgia Tech, June 1994.Submitted to ACM TOCS
[86] NVIDIA Corporation. (2012), NVIDIA CUDA C Programming Guide, Version 4.2
[87] OpenSSL Software Foundation, (2013). User Guide for the OpenSSL FIPS Object Module v2.0
[88] Orgill, G.L. (2005), Java Performance Of The Rijndael Encryption Algorithm Across Compilers And Virtual Machines, Master Thesis, Brigham Young University
[89] Paranjape, K.H. (2005) Right To Your Own Devices, Linux Gazette, May
[90] Petullo, W.M. (2007), Disk encryption in Fedora: Past, present and future, RedHat Magazine, Available at: http://magazine.redhat.com/2007/01/18/
[91] Red Hat Inc, (2013), Fedora CryptoConsolidation, https://fedoraproject.org/wiki/FedoraCryptoConsolidation
[92] Rogaway, P. (2011), Evaluation of Some Blockcipher Modes of Operation, Cryptography Research and Evaluation Committees (CRYPTRECl)
[93] Rogaway, P. (2011). Evaluation of Some Blockcipher Modes of Operation, Cryptography Research and Evaluation Committees (CRYPTRECl)
[94] Rott J. (2011), Intel AESNI Sample Library, Available at: http://software.intel.com/en-us/articles/download-the-intel-aesni-sample-library
[95] Saarinen, M.J.O. (2005), Encrypted watermarks and linux laptop security, Proceeding WISA'04 Proceedings of the 5th international conference on Information Security Applications, Springer-Verlag Berlin, Heidelberg
[96] Samara, S., Orfanus, D. and Janacik, P. (2009), Towards biologically inspired decentralized self-adaptive OS services for distributed Reconfigurable System on Chip (RSoC), ACM SIGBED Review - Special Issue on the 2nd International Workshop on Adaptive and Reconfigurable Embedded Systems (APRES'09)
[97] Sandberg, R., Goldberg, D., Kleiman, S., Walsh, D. and Lyon, B. (1985), Design and Implementation of the Sun Network Filesystem, USENIX Conference Proceedings, USENIX Association, Berkeley, CA, Summer

[98] Sanders, J. and Kandrot, E. (2011), CUDA by Example, An Introduction to General-Purpose GPU Programming, Addison-Wesley
[99] Szeredi, M. (2008), Filesystem in USEr space, Available at: http://sourceforge.net/projects/avf
[100] The Legion of the Bouncy Castle, A lightweight cryptography API for Java and C#, Available at: http://www.bouncycastle.org/
[101] TrueCrypt Foundation, (2009). TrueCrypt User's Guide. Available at: www.truecrypt.org
[102] van Etten, D. (2009), Why Many Java Performance Tests are Wrong, Available at: http://java.dzone.com/articles/why-many-java-performance-test
[103] Weiss, J. (2004), Java Cryptography Extensions: Practical Guide for Programmers, Elsevier Inc.
[104] Williams, J.A. and Bergmann, N.W. (2004), Embedded Linux as a platform for dynamically self-reconfiguring systems-on-chip The International Conference on Engineering of Reconfigurable Systems and Algorithms, Las Vegas, Nevada, USA
[105] Wilt, N. (2013), The CUDA Handbook (A Comprehensive Guide to GPU Programming), Addison-Wesley
[106] Wright, C.P. (2004), Operating System Support for Extensible Secure File Systems, Technical Report FSL-04-02
[107] Xu, L. (2010), Intel Corporation, White Paper, Securing the Enterprise with Intel AES-NI
[108] Youseff, L., Beckmann, N., Kasture, H., Gruenwald, C., Wentzlaff, D. And Agarwal A. (2012),The Case for Elastic Operating System Services in fos, DAC '12 Proceedings of the 49th Annual Design Automation Conference
[109] Zadok, E. (2001), FiST: A System for Stackable File - System Code Generation, PhD Thesis, COLUMBIA UNIVERSITY
[110] Zadok, E., Badulescu, I. and Shender, A. (1998), Cryptfs: A Stackable Vnode Level Encryption File System, Technical Report CUCS-021-98. Computer Science Department, Columbia University, Available at http://www.cs.columbia.edu/~library/.
[111] Zadok, E., Badulescu, I. and Shender, A. (1999), Extending File Systems Using Stackable Templates, Proceedings of the USENIX Annual Technical Conference, Monterey, California, USA
[112] Zadok, E., and Nieh, J. (2000), FiST: A language for stackable file systems. In Proceedings of the Annual USENIX Technical Conference. USENIX Association, Berkeley, CA, 55–70

3. ПОЛАЗНЕ ХИПОТЕЗЕ

Општа хипотеза истраживања је:

X1: Постоји утицај адаптације оперативних система расположивим хардверским и софтверским ресурсима на побољшање перформанси и квалитета заштите применом *AES* алгоритма.

На основу опште хипотезе, а према предмету истраживања, издвајају се посебне хипотезе:
X1.1: Ако се успешно пројектују и имплементирају властита решења и идеје за коришћење како стандардом дефинисаног *AES* алгоритма тако и решења која користе нове хардверске могућности (попут паралелизације и *AES-NI* скупа инструкција) тада је могуће креирати и у пракси проверити универзалан и једноставан интерфејс за мапирање и коришћење различитих хардверских и софтверских компонената.

X1.2: Ако се успешно пројектују, моделирају и имплементирају статистичка метода регресионе анализе и концепт машинског учења који заједно анализирају перформансе

појединих криптографских ресурса, тада је могуће изградити адаптибилан модел за шифровање и дешифровање *AES* алгоритмом и имплементацију решења у оквиру виртуелног фајл система.

Из посебних хипотеза се даљим прецизирањем долази до појединачних хипотеза:

X1.1.1: Ако се успешно имплементирају властита решења *AES* алгоритма, тада је могуће стандардизовати елементарни модел интерфејса за двосмерну комуникацију – како од оперативног система ка криптографском ресурсу, тако и од криптографског ресурса ка оперативном систему.

X1.1.2: Ако се успешно имплементирају властита решења *AES* алгоритма и стандардан елементарни интерфејс за приступ ресурсима, тада је могуће имплементирати омотаче (*wrapper*) око криптографских ресурса (библиотеке, драјвере) независних произвођача.

X1.1.3: Ако се успешно моделирају, пројектују и имплементирају властита решења стандардом дефинисаног *AES* алгоритма, тада је могуће имплементирати одговарајуће нове идеје везане за проширење простора кључева алгоритма.

X1.1.4: Ако се успешно моделирају, пројектују и имплементирају властита решења *AES* алгоритма и потребни криптографски режими рада, тада је могуће имплементирати одговарајуће нове идеје за паралелизацију извршења алгоритма.

X2.1.1: Ако је могуће имплементирати стандардан елементарни интерфејс за приступ ресурсима, тада је могуће стандардизовати мерења и добијање међурезултата који су потребни за њихову статистичку анализу.

X2.1.2: Ако је могуће применити регресиону анализу на резултате рада појединих хардверских и софтверских ресурса, тада је могуће такве међурезултате обрађивати методама машинског учења ради доношења одлуке о најбољем избору криптографског ресурса.

4. НАУЧНЕ МЕТОДЕ ИСТРАЖИВАЊА

У овом истраживању биће примењене следеће научне методе:

- Прикупљање информација о постојећим начинима примене криптографије у оперативним системима, њихова анализа и класификација,
- Давање критичког осврта на постојећа решења и предлог адаптибилног приступа примене криптографије у оперативним системима,
- Моделовање архитектуре решења за адаптибилну примену *AES* алгоритма у оперативним системима,
- Експериментална провера предложеног решења на основу постављања софтверске и хардверске инфраструктуре и развоја програмског система за адаптибилну примену *AES* алгоритма у оперативним системима,
- Експериментална потврда основне хипотезе истраживања и мерење успешности прилагођења.

5. ОЧЕКИВАНИ НАУЧНИ ДОПРИНОС

Најзначајнији очекивани резултат истраживачког процеса у предметној области је развој модела за адаптибилну примену *AES* алгоритма на нивоу оперативног система. Као резултат истраживања очекује се реализација виртуелног фајл система у коме је имплементиран аутономни агент који помоћу метода машинског учења и на основу емпиријских података доноси одлуку о томе који криптографски ресурс треба употребити за заштиту података помоћу *AES* алгоритма. Поред тога, очекивани резултати су проширења *AES* алгоритма и предлози решења за паралелизацију његовог извршења.

Очекивани научни допринос истраживања адаптибилне примене *AES* алгоритма у оквиру оперативних система огледа се у следећем:

- истраживању адаптибилности оперативних система за ефикасну употребу *AES* алгоритма;
- систематизацији и детаљној анализи досадашњих приступа енкрипцији унутар оперативних система;
- формалном опису модела и метода развоја фајл система за динамички адаптибилну примену *AES* алгоритма;
- истраживању могућности проширења *AES* алгоритма;
- истраживању експерименталних нових идеја за паралелизацију *AES* алгоритма коришћењем одговарајућих криптографских начина рада.

Стручни допринос истраживања се огледа у:

- имплементацији проширења *AES* алгоритма и експерименталној провери могућности имплементације нових идеја за паралелизацију *AES* алгоритма;
- систематизацији и детаљној анализи имплементације различитих модула који су у стању да користе расположиве хардверске и софтверске криптографске ресурсе који стоје на располагању савременим оперативним системима.

Друштвени допринос истраживања се огледа у следећем:

- резултати истраживања ће помоћи при идентификацији ресурса који од стране оперативног система могу да буду искоришћени за убрзање шифровања и дешифровања помоћу *AES* алгоритма;
- резултати истраживања ће допринети при анализи и дескрипцији процеса имплементације криптографске адаптибилности оперативних система *AES* алгоритму;
- резултати истраживања могу да буду искоришћени за даља унапређења *AES* алгоритма;
- резултати истраживања ће допринети при даљем развоју метода криптографске адаптибилности и ефикаснијем коришћењу криптографије у оквирима оперативних система.

Оперативни систем, односно виртуелни фајл систем који користи предложене концепте може да добије богатији и разноврснији избор криптографских ресурса из кога би описаним методама био у могућности да изабере најбољи ресурс са аспекта перформанси за примену криптографије у делу заштите података.

6. ПЛАН ИСТРАЖИВАЊА И СТРУКТУРА РАДА

План истраживања је дат у следећој табели:

Фаза	Задаци
1. Анализа постојећих резултата истраживања и решења у области криптографије у оквиру оперативних система	• Прикупљање информација (часописи, књиге, конференције, релевантне информације на Интернету)
2. Моделовање архитектуре решења за адаптибилну примену *AES* алгоритма у оквиру оперативних система	• Дефинисање кључних концепата • Истраживање техника за развој *AES* алгоритма • Истраживање техника за развој проширења *AES* алгоритма и његове паралелизације • Истраживање криптографских техника до данас примењених у оперативним системима • Истраживање техника машинског учења
3. Пројектовање модела криптографски адаптибилног виртуелног фајл система и криптографских модула	• Планирање (дефинисање захтева, анализа података, архитектуре и дизајна решења) • Пројектовање криптографских модула • Интеграција различитих делова модела
4. Постављање софтверске и хардверске инфраструктуре	• Инсталација и конфигурисање оперативних система, развојних алата, севера базе података на тестним платформама и др.
5. Развој система за адаптибилну примену AES алгоритма у оквиру оперативних система	• Развој криптографских модула • Развој аутономног агента • Развој механизама адаптације • Интеграција са виртуелним фајл системом
6. Емпиријско тестирање развијеног система	• Евалуација, тестирање и имплементација развијене методологије. Анализа резултата и корективне мере

Планирано трајање сваке од наведених фаза је 2 месеца.

Оквирни садржај докторске дисертације је:

1. Увод
   - 1.1 Дефинисање предмета истраживања
   - 1.2 Циљеви истраживања
   - 1.3 Полазне хипотезе
   - 1.4 Методе истраживања
   - 1.5 Очекивани доприноси докторске дисертације
   - 1.6 Структура и организација докторске дисертације
2. Енкрипција у оквиру оперативних система
   - 2.1 Начини енкрипције у оквиру оперативних система
     - 2.1.1 Начини енкрипције орјентисани ка медијуму за чување података (*storage encryption*)
       - 2.1.1.1 Системи датотека у корисничком простору (user space file systems) са аспекта примене криптографије
       - 2.1.1.2 Локални системи датотека који користе *NFS* механизме за шифровање и дешифровање
       - 2.1.1.3 Сложени (*stackable*) криптографски системи датотека
       - 2.1.1.4 *Disk based* системи за енкрипцију датотека
       - 2.1.1.5 *Block based* системи за енкрипцију датотека
     - 2.1.2 Мрежно оријентисани начини енкрипције
   - 2.2 Подршка криптографским акцелераторима у оквирима оперативних система
   - 2.3 Студије адаптибилности софтверских ресурса хардверским могућностима ради побољшања перформанси
   - 2.4 Компаративна анализа криптографских решења у оквиру оперативних система
3. Алгоритам *AES*
   - 3.1 Спецификација и формална репрезентација
     - 3.1.1 Стандардом дефинисани *AES* алгоритам
       - 3.1.1.1 Нотације и конвенције
       - 3.1.1.2 Математичке претпоставке
       - 3.1.1.3 Трансформације алгоритма *AES*
       - 3.1.1.3 Основне претпоставке за побољшање перформанси
         - 3.1.1.3.1 Сабирање и множење у *Galoa* пољима
         - 3.1.1.3.2 Генератори и основне идеје за оптимизацију *AES*-овог множења
         - 3.1.1.3.3 *T* табеле и *Gladmanove* идеје за оптимизацију
4. Технологије потребне за развој решења
   - 4.1 Технологије за имплементацију алгоритма *AES*
     - 4.1.1 Јава и потребне криптографске библиотеке и технологије
     - 4.1.2 *C/C++* и *AES NI* скуп инструкција
       - 4.1.2.1 Претходни радови
     - 4.1.3 *CUDA C* и паралелно програмирање као технологија за побољшање перформанси алгоритма *AES*
       - 4.1.3.1 Претходни радови
   - 4.2 Виртуелни фајл систем *Apache Commons*
   - 4.3 Машинско учење
     - 4.3.1 Регресиона анализа
   - 4.4 *Open source* СУБП *Firebird*
   - 4.5 *Java Database Connectivity* (*JDBC*)
   - 4.6 Технологија *Socket*-а и коришћене Јава и *C/C++* класе
   - 4.7 *XML* стандард

5. Модел и основне карактеристике имплементације адаптибилне примене *AES* алгоритма у савременим оперативним системима
   - 5.1 Захтеви истраживања
   - 5.2 Позиционирање примењених техника и технологија
     - 5.2.1 Позиција *Apache Commons* виртуелног фајл система у оперативном систему
     - 5.2.2 *JCA/JCE* криптографски API
     - 5.2.3 Криптографски модули
     - 5.2.4 Аутономни агент
   - 5.3 Заједничке карактеристике имплементираних криптографских модула
6. Једнонитне (*single threaded*) имплементације *AES* алгоритма
   - 6.1 Једнонитна *Delphi* / *Pascal* имплементација *AES* алгоритма
   - 6.2 Једнонитна Јава имплементација *AES* алгоритма
   - 6.3 Једнонитна *C/C++* имплементација *AES* алгоритма
   - 6.4 *C/C++* имплементација *AES* алгоритма заснована на *AES-NI* скупу инструкција
   - 6.5 Јава модули који се ослањају на *third party* криптографске библиотеке *Bouncy Castle* и *Oracle SUN*
   - 6.6 Емпиријска евалуација приказаних решења
7. Паралелна *CUDA C* имплементација *AES* алгоритма
   - 7.1 Архитектура решења
   - 7.2 Емпиријски резултати и имплементациона анализа
8. Једнонитни (*single threaded*) експерименти са могућим модификацијама *AES* алгоритма
   - 8.1 Преглед трансформација *AES* алгоритма
   - 8.2 Правила проширења
   - 8.3 Модификације стандардом дефинисаног алгоритма
     - 8.3.1 Имплементација модификација испод границе од 128 бита
     - 8.3.2 Имплементација модификација изнад границе од 256 бита
   - 8.4 Емпиријска евалуација приказаних решења
9. *CFB*, *OFB* и *CTR* криптографски начини рада у функцији примера паралелизације криптографског алгоритма
   - 9.1 Класификација криптографских начина рада (*Modes Of Operation*)
   - 9.2 Одабрани аспекти имплементације *CFB*, *OFB* и *CTR* начина рада
   - 9.3 Школски пример паралелизације алгоритма *AES* помоћу *CFB*, *OFB* и *CTR* криптографских начина рада
   - 9.4 Детаљи вишенитне (*multi threaded*) Јава имплементације
   - 9.5 Емпиријска евалуација приказане идеје
     - 9.5.1 Позиционирање у односу на властите стандардне Јава имплементације и проширења
     - 9.5.2 Позиционирање у односу на *C/C++*, *AES-NI* и *CUDA C* имплементације
     - 9.5.3 Позиционирање у односу на *third party* библиотеке
10. Архитектура решења за адаптибилну примену *AES* алгоритма на нивоу оперативног система
    - 10.1 Интеграција аутономног агента у виртуелни фајл систем
    - 10.2 Архитектура аутономног агента
    - 10.3 Статистички, улазно-излазни модул и модул селектор у функцији машинског учења
      - 10.3.1 Статистички модул и везљ са СУБП *Firebird*
      - 10.3.2 Модул селектор и доношење одлука
    - 10.4 Модел *XML* документа за униформну комуникацију између различитих делова система

10.5 Конфигурисање система и његов утицај на шему базе података
10.6 Комуникација са осталим модулима
10.7 Емпиријска евалуација примењеног решења
10.8 Евалуација путем студије случаја
10.9 Провера хипотеза методама природне дедукције
11. Закључак
12. Литература

7. ЗАКЉУЧАК И ПРЕДЛОГ

Комисија је утврдила да кандидат Борис Дамјановић, MSc. испуњава све услове, предвиђене Законом о високом образовању, за израду докторске дисертације, да је предложена тема актуелна, да је кандидат прикупио и свеобухватно се упознао са битним референцама из предметне области, као и да је, имајући у виду до сада објављене радове, показао склоност за научно-истраживачки рад, и предлаже Научно-наставном већу Факултета да се кандидату Борису Дамјановићу одобри израда докторске дисертације под насловом:

"АДАПТИБИЛНА ПРИМЕНА *AES* АЛГОРИТМА КОД САВРЕМЕНИХ ОПЕРАТИВНИХ СИСТЕМА"

За ментора предлажемо др Дејана Симића, редовног професора.

8. ПОТПИСНИЦИ ИЗВЕШТАЈА

Београд, 25.11.2013.год.

К О М И С И Ј А

_____
Др Дејан Симић, ред. проф. ФОН-а
Универзитет у Београду

_____
Др Душан Старчевић, ред. проф. ФОН-а
Универзитет у Београду

_____
Др Бошко Николић, ванр. проф. ЕТФ-а
Универзитет у Београду