УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Патре 5 • 78000 Бања Лука • Република Српска • Босна и Херцеговина
Централа: +387 51 221 820 • Деканат: +387 51 221 824 • Факс: +387 51 211 408
E-mail: office@etfbl.net • www.etfbl.net

Број: 20/3.1264 - 1277/16
Датум: 16.12.2016. године

На основу члана 59. Закона о високом образовању („Службени гласник Републике Српске“ број: 73/10, 104/11, 84/12 и 108/13), члана 24. Правила студирања на трећем циклусу студија Електротехничког факултета и члана 14. Статута Електротехничког факултета Универзитета у Бањој Луци, Наставно-научно вијеће на 39. сједници одржаној 16.12.2016. године, д о н о с и:

О Д Л У К У
о усвајању Извјештаја о оцјени подобности кандидата и теме за израду докторске дисертације

Члан 1.

Усваја се Извјештај о оцјени подобности кандидата и теме за израду докторске дисертације мр Огњена Јолцића под радним називом **„Адаптивни систем за детекцију DDoS напада у рачунарским мрежама“.**

Члан 2.

Саставни дио овог Извјештаја чини Записник о квалификационом дкторском испиту.

Члан 3.

Ова Одлука доставља се Сенату Универзитета у Бањој Луци ради добијања сагласности којом се одобрава израда докторске дисертације.

Достављено:
1. Сенату Универзитета
2. Кандидату,
3. Досије кандидата,
4. Референту за студије другог и трећег циклуса,
5. Архива ННВ-а,
6. А/а.

ДЕКАН
Проф. др Бранко Докић

УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Образац - 2

УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
БАЊА ЛУКА
Број: 1640
Дана: 08. 12. 2016.

ИЗВЈЕШТАЈ

о оцјени подобности теме и кандидата за израду докторске дисертације

I ПОДАЦИ О КОМИСИЈИ

Орган који је именовао комисију: Сенат Универзитета у Бањој Луци

Датум именовања комисије: 18.07.2016. године

Број одлуке: 02/04-3.2038-123/16

Састав комисије:

1. Јовановић Зоран | редовни професор | Природне науке, Рачунарске науке
   Презиме и име | Звање | Научно поље и ужа научна област
   Електротехнички факултет Београд | предсједник
   Установа у којој је запослен-а | Функција у комисији

2. Ђурић Зоран | ванредни професор | Природне науке, Рачунарске науке
   Презиме и име | Звање | Научно поље и ужа научна област
   Електротехнички факултет Универзитета у Бањој Луци | ментор
   Установа у којој је запослен-а | Функција у комисији

3. Марић Славко | редовни професор | Природне науке, Рачунарске науке
   Презиме и име | Звање | Научно поље и ужа научна област
   Електротехнички факултет Универзитета у Бањој Луци | члан
   Установа у којој је запослен-а | Функција у комисији

4. Вулетић Павле | доцент | Природне науке, Рачунарске науке
   Презиме и име | Звање | Научно поље и ужа научна област
   Електротехнички факултет Београд | члан
   Установа у којој је запослен-а | Функција у комисији

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме: Огњен, , Јолцић
2. Датум рођења: 14.08.1986. Мјесто и држава рођења: Бања Лука, Босна и Херцеговина

II.1 Основне студије

Година уписа: 2004. Година завршетка: 2008. Просјечна оцјена током студија: 8.87

Универзитет: Универзитет у Бањој Луци

Факултет/и: Електротехнички факултет

Студијски програм: Рачунарство и информатика

Звање: дипломирани инжињер електротехнике

II.2 Мастер или магистарске студије

Година уписа: 2009. Година завршетка: 2010. Просјечна оцјена током студија: 10.0

Универзитет: Универзитет у Бањој Луци

Факултет/и: Електротехнички факултет

Студијски програм: рачунарство Рачунарство и информатика

Звање: магистар рачунарства и информатике

Научна област: Рачунарске науке

Наслов завршног рада: Нови систем за тестирање сигурности web апликација

II.3 Докторске студије

Година уписа: 2012

Факултет/и: Електротехнички факултет

Студијски програм: Информационо-комуникационе технологије

Број ЕЦТС до сада остварених: 60 Просјечна оцјена током студија: 9.67

II.4 Приказ научних и стручних радова кандидата

Р. бр.	Аутори, наслов, издавач, број страница	Категорија[1]
1.	O. Joldzic, Z. Djuric, P. Vuletic, "A transparent and scalable anomaly-based DoS detection method", Computer Networks, Vol. 104: 27-42, 2016;	водећи часопис међународног значаја

Кратак опис садржине:
Intrusions and intrusive behaviour can be aimed at different parts of the system, ranging from lower-level network attacks intended to disrupt the flow of data in general, to higher-level attacks targeted against specific applications or services. Due to the constant growth of network traffic and the need to inspect the traffic thoroughly, intrusion detection and prevention are becoming increasingly complex and require significant computational resources. This paper presents a distributed, scalable solution for the detection of lower-level Denial-of-Service (DoS) attacks which are executed by transmitting overwhelming amounts of data with the intention of disrupting regular network service. Scalability is achieved by active traffic balancing among multiple traffic processors, exploiting the flexibility and network programmability that Software Defined Networking paradigm brings and packet processing based on device polling. Traffic processors can be elastically added into the pool depending on the traffic volume. The whole system is completely transparent to the external observers. The paper shows that the implemented balancing algorithm further improves the reliability of the intrusion detection.

Рад припада проблематици докторске дисертације: **ДА** НЕ ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
2.	O. Joldžić, Z. Đurić, D. Vuković "Building a Transparent Intrusion Detection and Prevention System on SDN", Norsk Informasjonssikkerhetskonferanse NISK 2014, Fredrikstad, Norveška, 2014;	зборник радова са научног скупа међународног значаја

Кратак опис садржине:
Network convergence, user mobility and various types of applications all contribute to the inhomogeneity of modern networks. The emergence of new technologies, unfortunately, increases the number of possible security threats to all parts of infrastructure. Therefore, network security protocols and mechanisms have to be able to respond to any security threat without affecting the performance of the network or degrading the quality of service. This paper presents an early stage concept of a transparent intrusion prevention system (TIPS) implemented using a combination of various technologies, most notably Software-Defined Networking (SDN) and poll-mode packet processing, which enables deep packet inspection in high-speed network environments.

Рад припада проблематици докторске дисертације: **ДА** НЕ ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
3.	O. Joldžić, Z. Đurić, D. Vuković "Experiences and Challenges in Implementing Adaptive Bitrate Multimedia Streaming for Live	зборник радова са научног скупа

[1] Категорија се односи на оне часописе и научне скупове који су категорисани у складу са Правилником о публиковању научних публикација („Службени гласник РС", бр. 77/10) и Правилником о мјерилима за остваривање и финансирање Програма одржавања научних скупова („Службени гласник РС", бр. 102/14).

	Multimedia Content", Proceedings of the 22nd Telecommunications Forum TELFOR 2014, pp. 909-912, Beograd, Srbija, 2014;	међународног значаја

Кратак опис садржине:
The process of network convergence and the increased availability of high speed networks has opened a number of possibilities in the field of multimedia content distribution. Above all, the popularity of mobile platforms and the accompanying user mobility requires the distribution platforms to be able to respond to changing network conditions and to maintain a satisfactory quality of service regardless of client device capabilities. This paper discusses the experiences and challenges in implementing an adaptive bitrate (ABR) multimedia streaming platform for live media content. Common streaming techniques and protocols used for live streaming are described, along with the basic principles of adaptive stream selection based on available bandwidth. As a proof of concept, adaptive bitrate streaming has been successfully implemented in a Digital Multimedia Distribution system called GSTV.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
4.	O. Joldžić, Z. Đurić "Video Streaming Protocol Extension for Session Control and Authorization", Proceedings of the International Conference on Systems, Signals and Image Processing - IWSSIP 2014, pp. 135-138, Dubrovnik, Hrvatska, 2014;	зборник радова са научног скупа међународног значаја

Кратак опис садржине:
With the constant increase in network availability and performance, multimedia delivery systems have gained widespread popularity in almost any type of network environment. The deployment of such systems was historically reserved for special, custom-designed infrastructures which were able to support a high throughput for a limited number of users. With the expansion of multimedia content delivery systems, particularly OTT (over-the-top) and IPTV (Internet Protocol Television), several very important issues had to be resolved in order to achieve a satisfactory level of service quality. One of the key challenges in deploying a global multimedia delivery system is the security of the content and the end-users involved in the process. This paper presents a novel approach to extending current video streaming protocol capabilities to support a high level of security and session control, without degrading the performance of the network. As a proof of concept, the approach presented in this paper has been successfully implemented in a Digital Multimedia Content Distribution System called GSTV.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
5.	O. Joldžić, Z. Đurić „A Scalable Load Balancing Solution for a Digital Multimedia Content Distribution Platform", Proceedings of the 1st International Conference on Electrical, Electronic and Computer Engineering IcETRAN 2014, Vrnjačka Banja, Srbija, 2014;	зборник радова са научног скупа међународног значаја

Кратак опис садржине:
The process of network convergence and the constant advancement in the area of network performance have resulted in an increase in availability of different types of digital multimedia content to network subscribers. A modern, converged network presents a unified infrastructure for content distribution, regardless of its type or other characteristics. In this context, any implementation

of digital video delivery networks has to resolve several important issues in order to provide its users a satisfactory level of service quality. One of the most important problems in this category is the implementation of a responsive and scalable platform that would be able to withstand high server loads caused by a large number of simultaneous requests. This paper presents an overview of a load balancing solution which is able to dynamically distribute the load across any number of nodes configured within the distribution cluster. As a proof of concept, the solution presented in this paper has been successfully implemented in a Digital Multimedia Content Distribution System called GSTV.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
6.	O. Joldžić, "Applying MapReduce Algorithm To Performance Testing in Lexical Analysis on HDFS", Proceedings of the 21st Telecommunications Forum TELFOR 2013, pp. 841-844, Belgrade, Srbija, 2013;	зборник радова са научног скупа међународног значаја

Кратак опис садржине:
This paper presents an overview of distributed data processing technology, and explores the possibilities and advantages of using this technology in lexical analysis of Cyrillic text. A detailed overview of one of the most widely used frameworks for processing large datasets – Apache Hadoop – is presented, along with a recommendation for planning and deployment of such systems. The paper also analyzes results obtained by running lexical analysis programs on a small Hadoop cluster and the effect of various configuration parameters on total execution times of the test programs.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
7.	O. Joldžić, D. Vuković, „The Impact of Cluster Characteristics on HiveQL Query Optimization", Proceedings of the 21st Telecommunications Forum TELFOR 2013, pp. 837-840, Belgrade, Srbija, 2013;	зборник радова са научног скупа међународног значаја

Кратак опис садржине:
Huge amount of data is stored by different kinds of applications for further analysis. Relational databases were used for decades as data storages, but in some cases they are not suitable for Big Data processing. To solve the problem, non-relational databases were developed. As a help for transferring data from relational databases to non-relational databases, adequate tools were developed. In this paper, a tool named Sqoop is presented.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
8.	O. Joldžić, Z. Đurić, „Security Issues of RESTful Web Services and the Possibilities of Automatic Security Vulnerability Detection", Infofest 2013, pp. 145-152, Budva, Crna Gora, 2013;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
The aim of this paper is to provide an extensive analysis of the RESTful web service technology,

with a special consideration regarding the security issues that are encountered when deploying this type of web applications. For each of the possible security risks, this paper explores the necessary actions required to mitigate the risk and minimize the possibility of data corruption and further damage to the system. Finally, the issue of automated security testing is analyzed in order to provide a solution for successful threat detection.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
9.	Ж. Ивановић, М. Кнежић, О. Јолџић, „Програмско рјешење за надзор и управљање јавном расвјетом“, Симпозијум Енергетска ефикасност - ЕНЕФ 2013, пп. Б1/31-Б1/33, Бања Лука, Босна и Херцеговина 2013;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У овом раду описано је програмско рјешење за надзор и управљање јавном расвјетом. Програмско рјешење чине двије апликације, SyLiConWeb и SyLiConDesktop, посебно развијене за рад са уређајем SyLiConStation. Програмско рјешење верификовано је у оквиру пилот пројекта на подручју града Бања Лука.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
10.	О. Јолџић, З. Дејановић, Р. Дејановић, Д. Бајић, "Утицај перформанси система на планирање виртуелизационих окружења", INFOTEH 2012, пп. 838-842, Јахорина, Босна и Херцеговина, 2012	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У раду су описане основне карактеристике виртуелних рачунарских система. Дата је детаљна анализа предности виртуелизованих система над осталим типовима рачунарских архитектура, као и најзначајнији проблеми који се јављају приликом планирања имплементације оваквог рачунарског система. На крају рада је дато тестирање перформанси најчешће кориштених рјешења за виртуелизацију.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
11.	D. Vuković, O. Joldžić, „Static and Dynamic Analysis - Usage in Web Application Vulnerability Detection“, YU INFO 2011, Kopaonik, Srbija, 2011;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
This paper presents an overview of basic principles of static and dynamic analysis of web applications in vulnerability detection. A typical usage has been given for each of the techniques described in the paper, along with the special conditions that would deem the particular technique inapplicable. Finally, in order to illustrate the process of threat detection, a detailed example was given that utilizes both of the methods described in the paper.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
12.	З. Ђурић, О. Јолџић, "Преглед спецификација и техника заштите сервисно-оријентисаних апликација", ИнфоМ, 37/2011, 2011, пп. 16-24;	часопис националног значаја

Кратак опис садржине:
Сигурносни аспекти сервисно-оријентисаних апликација представљају веома значајан сегмент пројектовања и развоја информационих система, те им се из тог разлога мора поклонити посебна пажња у току цјелокупног животног циклуса апликације. У овом раду дат је детаљан преглед потенцијалних сигурносних пријетњи и напада којима су изложени *web* сервиси, а који могу довести до неовлаштеног приступа заштићеним дијеловима система или прекида функционисања сервиса. Поред тога, у овом раду дат је и преглед најчешћих напада усмјерених према комплетној инфраструктури сервисних и других типова *web* апликација. У раду су детаљно изложене и функционалности дефинисане најзначајнијим спецификацијама које за циљ имају повећање нивоа сигурности *web* сервиса - WS-Security i WS-SecurityPolicy.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
13.	З. Ђурић, О. Јолџић, "Компаративни преглед спецификација JavaServer Faces апликативног окружења", Симпозијум Индел 2010, пп. 372-376, Бањалука, Босниа анд Херцеговина;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У овом раду су описане основне карактеристике JavaServer Faces апликативног окружења за развој web апликација. Дат је компаративни преглед основних функционалности различитих верзија спецификације, као и предности и недостаци сваке од описаних верзија.

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЈЕЛИМИЧНО

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
14.	О. Јолџић, З. Ђурић, "Метрика за вредновање и класификацију сигурносних пропуста web апликација", Инфофест 2010, пп. 163-171, Будва, Црна Гора, 2010;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У овом раду је дат преглед основних група сигурносних пропуста у web апликацијама. Приказане су основне групе рањивости, као и ризици које њихова експлоатација од стране нападача може имати по комплетан информациони систем. Приказана су и постојећа рјешења из домена класификације и вредновања сигурносних пропуста у web апликацијама. У наставку рада је предложена метрика која ће омогућити јединствену класификацију рањивости откривених тестирањем према дефинисаном сигурносном индексу тестиране апликације који је добијен као резултат проведених тестова. Уз опис карактеристика метрике, предложена је и XML спецификација која омогућава додатни опис и анализу сигурносног индекса апликације добијеног примјеном метрике на резултате завршеног тестирања. Метрика је развијена са циљем повећања интероперабилности различитих рјешења за тестирање сигурности web апликација и увођења јединственог параметра који би омогућио директно поређење резултата тестирања добијених употребом различитих техника и алата доступних на тржишту.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
15.	О. Јолџић, З. Ђурић, "Приједлог рјешења за детекцију и класификацију сигурносних пропуста web апликација", InfoM, 34/2010, 2010, пп. 42-52;	часопис националног значаја

Кратак опис садржине:
У овом раду су анализирани сигурносни аспекти web апликација у информационим системима. Изложени су типови архитектура web апликација и значајне особине везане за сигурност информационих система. Приказане су особине најзаступљенијих напада на web апликације, као и начини заштите за сваки од описаних напада. Описани су начини тестирања web апликација, технике за откривање сигурносних пропуста, начини класификације тестова према особинама и начину извођења и дат је преглед постојећих рјешења за тестирање сигурности web апликација. У другом дијелу рада детаљно је описан WASTT - ново рјешење за откривање и класификацију сигурносних пропуста у web апликацијама, развијено од стране аутора овог рада. Приказана је модуларна структура система, начин употребе и могућности развијеног система.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
16.	О. Јолџић, З. Ђурић, "Типови напада на web сервисе", INFOTEH 2010, пп. 482-486, Јахорина, Босна и Херцеговина, 2010;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У овом раду су анализирани сигурносни проблеми код имплементације web сервиса у информационим системима. Приказани су најпознатији системи за категоризацију сигурносних пријетњи за web сервисе. Описани су најзаступљенији типови конкретних напада, начин њиховог извођења, сигурносни ризици и посљедице успјешног извођења сваког од напада. За сваки приказани напад је описан начин за отклањање пропуста и минимизацију могућности губитка података или оштећења система.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
17.	З. Ђурић, О. Јолџић, "WSSECTEST – алат за детекцију сигурносних пропуста код web сервиса", YU INFO 2010, Копаоник, Србија, 2010;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
Без обзира на велики број предности које web сервиси доносе, постоје и одређени недостаци ове технологије. Највећи број ових недостатака односи се на сигурност web сервиса. У овом раду говори се о сигурности web сервиса, нападима на web сервисе, посебно SQL injection нападу на web сервисе. У раду је представљен WSSECTEST – алат за детекцију сигурносних пропуста код web сервиса.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
18.	З. Ђурић, О. Јолџић, "Сигурност web апликација", Инфофест 2009, пп. 204-212, Будва, Црна Гора, 2009;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У посљедњих неколико година web апликације све више добијају на значају. Из тог разлога постале су веома атрактивни циљеви за нападаче, а сигурност web апликације је постала веома важан сегмент у њиховом дизајну и имплементацији. Резултати нарушавања сигурности web апликација могу донијети велику финансијску корист за потенцијалног нападача, али и велику финансијску штету за власника или корисника апликације. Веома често мете оваквих напада су web апликације код којих нарушавање сигурности може резултирати откривањем бројева кредитних картица, информација о корисничким налозима, али и откривањем других повјерљивих информација.
Конвенционална сигурносна рјешења, попут кориштења фиревалл уређаја, HTTPS (*Hypertext Transfer Protocol Secure*) протокола за приступ web апликацији или различитих криптографских техника, нису довољна. Додатни проблем сигурности web апликација представљају и софтверска рјешења која су развијана унутар самих компанија које пружају одређену услугу путем web апликација, а обично од стране развојних тимова недовољно едукованих на пољу сигурности web апликација.
У овом раду се анализира проблем сигурности web апликација. У секцији 2 описана је архитектура web апликација и указано је на специфичност проблема сигурности web апликација. У секцији 3 описане су различите врсте напада на web апликације. Детаљно су описани SQL (*Structured Query Language*) *injection* и XSS (*Cross-site scripting*) напади, као најзаступљеније врсте напада на web апликације. У секцији 4 описани су начини анализе и побољшања сигурности web апликација. На крају рада дат је закључак.

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Р. бр.	Аутори, наслов, издавач, број страница	Категорија
19.	О. Јолцић, З. Ђурић, "Могућност тестирања сигурносних пропуста у web апликацијама са приједлогом рјешења система за тестирање", Инфофест 2009, пп. 213-220, Будва, Црна Гора, 2009;	зборник радова са научног скупа националног значаја

Кратак опис садржине:
У данашње вријеме, граница између динамичних web апликација и стандардних (десктоп) апликација је све мања. Ако се узме у обзир данашњи глобални развој информационих технологија, није нереално претпоставити да ће у врло кратком временском року web апликације у потпуности преузети улогу примарних алата у свакодневном раду. Међутим, са повећањем могућности ових апликација све су веће потребе за увођењем додатних сигурносних механизама које би омогућиле несметан рад. Зависно од области примјене и специфичних технологија које се употребљавају потребно је оријентисати се на различите аспекте сигурности. Управо из тог разлога је потребно развити модуларно окружење које би омогућило, како ауторима тако и корисницима, тестирање сигурносних механизама и указивање на евентуалне сигурносне пропусте.
У овом раду анализирају се могућности тестирања сигурносних пропуста у web апликацијама. У секцији 2 описани су основни типови напада на web апликације и начин њиховог извођења. У секцији 3 дати су типови тестова за web апликације. У секцији 4 описана су познатија рјешења за тестирање сигурносних пропуста у web апликацијама. У секцији 5 дат је приједлог рјешења система за тестирање. На крају рада дат је закључак

Рад припада проблематици докторске дисертације: ДА НЕ **ДЈЕЛИМИЧНО**

Да ли кандидат испуњава услове? **ДА** НЕ

III ПОДАЦИ О МЕНТОРУ

Др Зоран Ђурић рођен је у Градишци, 08.04.1977. године. Дипломирао је на Војнотехничкој академији у Београду 2001. године, магистрирао је 2004. године на Електротехничком факултету Универзитета у Београду, а докторирао 2008. године на Електротехничком факултету Универзитета у Бањој Луци. Од 2001. године до 2009. године радио је у Поштама Српске, док је од 2005. године на Електротехничком факултету Универзитета у Бањој Луци радио као спољни сарадник, у звању вишег асистента. Од 2009. године запослен је на Електротехничком факултету Универзитета у Бањој Луци. У звање доцента изабран је 2009. године, а у звање ванредног професора 2014. године. Током рада на Електротехничком факултету имао је задужења на већем броју предмета у оквиру свих циклуса студија.
У периоду од фебруара 2013. године до октобра 2015. године обављао је дужност продекана за научноистраживачки рад на Електротехничком факултету Универзитета у Бањој Луци.
Учествовао је у већем броју међунарднох пројеката (TEMPUS, HERD и пројекти подржани од стране WUS Austria), као и у бројним националним пројектима.
Објавио је преко 60 научних и стручних радова у међународним и националним часописима и конференцијама.
Члан је IEEE.

Радови из области којој припада приједлог докторске дисертације:

Р. бр.	Аутори, наслов, издавач, број страница
1.	O. Joldzic, Z. Djuric, P. Vuletic, "A transparent and scalable anomaly-based DoS detection method", Computer Networks, Vol. 104: 27-42, 2016;
2.	Z. Đurić, D. Gašević, "FEIPS - a Secure Fair-Exchange Payment System for Internet Transactions", The Computer Journal, Vol. 58(10): 2537-2556, 2015;
3.	Z. Djuric, "WAPTT - Web Application Penetration Testing Tool", Advances in Electrical and Computer Engineering, Vol. 14, No. 1, pp. 93 - 102, 2014;
4.	O. Joldzic, Z. Djuric, D.Vukovic, "Building a Transparent Intrusion Detection System on SDN Networks", NISK 2014, 2014;
5.	Z. Đurić, D. Gašević, "A Source Code Similarity System for Plagiarism Detection", The Computer Journal, Vol. 56(1): 70-86, 2013;
6.	Z. Đurić, O. Marić, D. Gašević, "Internet Payment System: A New Payment System for Internet Transactions", Journal of Universal Computer Science, Vol. 13(4): 479 - 503, Springer-Verlag, 2007;

IV ОЦЈЕНА ПОДОБНОСТИ ТЕМЕ

IV.1 Формулација назива тезе (наслова)

Адаптивни систем за детекцију DDoS напада у рачунарским мрежама

Наслов тезе је подобан? **ДА** НЕ

IV.2 Предмет истраживања

Напад или интрузија на рачунарску мрежу/систем се дефинишу као било каква акција извршена са циљем прекида рада мреже/система или прибављања неовлаштеног приступа неком његовом заштићеном дијелу. Напади могу бити усмјерени према различитим дијеловима мреже/система, почевши од најнижих слојева OSI (енг. *Open Systems Interconnection*) модела, гдје настоје да

прекину сам ток података, па до напада усмјерених према конкретним апликацијама или сервисима на апликативном слоју OSI модела.
Повећање брзине комуникације у рачунарским мрежама и мрежна конвергенција, који су настали као посљедица развоја мрежних технологија, узроковали су драстично повећање броја корисника рачунарских мрежа, појаву читавог низа нових апликација и сервиса, те коришћење мрежа у свакодневним пословима. Мрежна конвергенција је довела до промјене самог процеса пројектовања рачунарских мрежа који је раније предвиђао постојање одвојене физичке инфраструктуре (медијума) за различите типове мрежног саобраћаја. Оваква врста сегментације на физичком слоју је омогућавала развој специјализованих апликација, уско прилагођених конкретној врсти саобраћаја и типу мреже, али је са собом повлачила и знатно веће трошкове имплементације инфраструктуре за различите типове саобраћаја. Са друге стране, конвергиране мреже омогућавају пренос различитих типова саобраћаја преко истог физичког медијума. У овом случају се од мрежних уређаја и апликација очекује да посједују механизме за класификовање саобраћаја различитог приоритета, како би се задржао одговарајући квалитет сервиса за различите типове саобраћаја.
Конвергенција има значајан утицај и на аспект сигурности рачунарских мрежа. Велика брзина комуникације и широка доступност мрежних технологија омогућава иницирање напада на различите елементе мрежне инфраструктуре без посједовања специјализоване опреме. Узимајући у обзир да се саобраћај преноси преко заједничког медијума, процес изоловања малициозног саобраћаја је знатно комплекснији, па обрада већег броја пакета који долазе из различитих токова потенцијално уноси знатно веће кашњење у комуникацији него што је то случај код неконвергираних мрежа.
Управо су све већа доступност рачунарских мрежа и повећање брзине комуникације имали велики утицај на развој одређених класа напада на рачунарске мреже и сервисе који се у овим мрежама налазе, а који се заснивају на оптерећивању мреже огромном количином нежељеног саобраћаја у циљу изазивања прекида нормалног функционисања мреже или отежавања приступа жељеним сервисима за легитимне кориснике. Ови напади су познати као DoS (енгл. Denial of Service) напади. Детекцију оваквих напада компликује чињеница да се прецизан шаблон њиховог извођења не може предвидјети унапријед, па није могуће припремити мрежу за њихову детекцију.
Предмет истраживање у овој тези јесте управо детекција DoS напада који настају као посљедица генерисања огромне количине саобраћаја према датој мрежи, без обзира на архитектуру посматране мреже и сервисе које она садржи.

Предмет истраживања је подобан? **ДА** НЕ

IV.3 Најновија истраживања познавања предмета дисертације на основу изабране литературе са списком литературе

Додатни проблем код детекције напада на конвергираним мрежама (које омогућавају пренос различитих типова саобраћаја преко истог физичког медијума [1]) је чињеница да су класе напада довољно међусобно различите да не постоји јединствен начин детекције који би био ефикасан против свих напада [2],[3],[4],[5]. Напади усмјерени према мрежној инфраструктури за циљ имају прекид функционисања једног дијела или комплетне мреже експлоатацијом неке конкретне слабости комуникационог протокола или слањем огромне количине података чија ће обрада заузети све ресурсе одредишног система, чиме се онемогућава комуникација легитимних корисника са датим системом. Овај други тип напада се у литератури најчешће идентификује као DoS напад и може бити иницран од стране једног пошиљаоца или од стране већег броја мрежних чворова (тзв. ботова) - у том случају се ради о дистрибуираном DoS (DDoS) нападу.
Процес детекције (D)DoS напада компликује чињеница да често није могуће разликовати саобраћај који чини сам напад од валидних корисничких пакета, па нема поузданог начина да се изглед напада предвиди прије појављивања и дефинише у форми обрасца (engl. *pattern*) који ће омогућити његову једноставну детекцију. С друге стране, код напада који за циљ имају експлоатацију конкретне слабости мрежних протокола, управо чињеница да се напад мора манифестовати на тачно одређен начин да би био успјешан, представља основу механизма за његову сигурну детекцију. Постоји читав низ рјешења која омогућавају администраторима да

спецификују тачан начин манифестовања (тзв. потпис) напада кориштењем вриједности из заглавља мрежних пакета, како би напад могао бити детектован. Код детекције напада иницираних слањем огромне количине података, креирање спецификације потписа напада није могуће, јер нема елемената у заглављу пакета на основу којих би се напад могао препознати [6],[7],[8].
Једина могућност детекције (D)DoS напада представља праћење рада рачунарске мреже у нормалним условима, те покушај идентификовања неке аномалије у мрежном саобраћају који би сугерисао да је у току напад усмјерен против једног или више чворова на мрежи. Анализирањем статистичких параметара мрежног саобраћаја (првенствено ентропије појављивања одредишних адреса у пакетима мрежног слоја) [9],[10] и њиховим поређењем са референтним вриједностима које су измјерене у периодима нормалног функционисања мреже, дефинише се динамички праг вриједности параметара који показује да је напад у току. Оваква техника детекције зависи само од иницијалног периода "учења", па би систем био у стању да се адаптира на различите услове, чиме се елиминише потреба за познавањем обрасца манифестације напада, који у случају (D)DoS напада најчешће није ни доступан. Након почетног периода обучавања систем треба да буде у стању да игнорише флуктуације саобраћаја (без обзира на њихов обим) које не представљају активан напад, чиме би се избјегло класификовање нормалног режима рада мреже као напада.
Код имплементације било каквог сигурносног механизма или рјешења за детекцију напада на било којем слоју OSI модела, посебна пажња се мора обратити на нападе који су усмјерени против самог система за детекцију, односно на особине система које могу и саме представљати ризик по његов ефикасан рад. Конкретно, овакав систем мора бити дизајниран и реализован на начин да својим радом уноси минимално кашњење у комуникацији како његовом примјеном не би био нарушен квалитет мрежних сервиса, чак и за мреже изузетно великих брзина [11],[12],[13]. Ово је посебно значајно за системе за детекцију (D)DoS напада, јер се ради о огромним количинама података који морају бити обрађени да би се утврдило постојање напада, а након тога најчешће одбачени (ако су дио напада). Систем за детекцију напада мора функционисати тако да својим радом ни на који начин не омета и не отежава рад крајњих корисника [14],[15],[16].
Успјешан напад усмјерен директно на систем за превенцију напада у одређеним условима може бити једнако ефикасан за прекид рада мреже као и успјешно изведен (D)DoS напад усмјерен према неком другом мрежном чвору. Наиме, за успјешно спречавање напада, систем за превенцију мора бити постављен на све путање којима саобраћај улази у заштићени дио мреже, како би малициозни пакети могли бити блокирани након што се напад детектује. Успјешан напад усмјерен директно против система за детекцију би прекинуо примарну путању пакета и онемогућио комуникацију са дијелом мреже који се налази иза уређаја за детекцију напада. Из тог разлога, ефикасан систем за детекцију (D)DoS напада мора бити дизајниран и реализован тако да у потпуности контролише сву мрежну комуникацију, а да у исто вријеме буде невидљив (транспарентан) за остатак мреже (укључујући и уређаје који су му сусједни), како би нападачима било онемогућено да нападе усмјере директно према систему за детекцију.
Да би систем за детекцију могао ефикасно функционисати у мрежама великих брзина комуникације, мора бити омогућено његово скалирање уз повећање броја елемената који обрађују пакете. Повећање броја елемената за обраду пакета не смије утицати на функционалност детекције напада. Систем мора посједовати алгоритам за расподјелу оптерећења (распоређивање пакета) која неће значајно утицати на статистичке особине саобраћаја како би се и даље могла извршити класификација саобраћаја и детекција потенцијалних напада. Овакав механизам скалирања треба да омогући динамичко проширење система у случају када тренутни капацитет није одговарајући за дате мрежне услове [17].

Списак литературе:

[1] S.W. Cadzow, "Security mechanisms in converged networks", in: Proceedings of the First IEE International Conference on Commercialising Technology and Innovation, IET, 2005 .
[2] N. Hoque, M.H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, "Network attacks: taxonomy, tools and systems", J. Netw. Comput. Appl. 40 (2014) 307–324, doi: 10.1016/j.jnca.2013.08.001 .
[3] J. Mirkovic, G. Prier, P. Reiher, "Attacking DDoS at the source", in: Proceedings of 10th IEEE International Conference on Network Protocols, 2002, pp. 312–321, doi: 10.1109/ICNP.2002.1181418 .
[4] J. Steinberger, A. Sperotto, H. Baier, A. Pras, "Collaborative attack mitigation and response: a

survey", in: Proceedings of the 2015 IFIP/IEEE International Sym- posium on Integrated Network Management (IM), IEEE, 2015, pp. 910–913, doi: 10.1109/INM.2015.7140407 .
[5] S.T. Zargar, J.B. Joshi, D. Tipper, "A survey of defense mechanisms against dis- tributed denial of service (DDoS) flooding attacks", IEEE Commun. Surv. Tut. (2013) 2046–2069, doi: 10.1109/SURV.2013.031413.00127 .
[6] T. Fu, D. Zhang, L. Xia, M. Li, "Ipfix ie extensions for DDoS attack detection", internet draft, 2015, (https://tools.ietf.org/html/ draft- fu- dots- ipfix- extension- 00) .
[7] K. Wang, S.J. Stolfo, "Anomalous payload-based network intrusion detection", in: Recent Advances in Intrusion Detection, 7th International Symposium, RAID 2004, Sophia Antipolis, France, vol. 3224, 2004, pp. 203–222, doi: 10.1007/ 978- 3- 540- 30143- 1 _ 11 .
[8] J.J. Davis, A.J. Clark, "Data preprocessing for anomaly based network intrusion detection: a review", Comput. Secur. 30 (6-7) (2011) 353–375, doi: 10.1016/j. cose.2011.05.008 .
[9] A. Lakhina, M. Crovella, C. Diot, "Mining anomalies using traffic feature distributions", SIGCOMM Comput. Commun. Rev. 35 (4) (2005) 217–228, doi: 10.1145/ 1090191.1080118 .
[10] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments", Comput. Netw. 62 (2013) 122–136, doi: 10.1016/j.bjp.2013.10.014 .
[11] L. Deri , S.P.A. Netikos , V.D.B. Km , L.L. Figuretta, "Improving passive packet capture: beyond device polling", in: Proceedings of SANE 20 04, 20 04, pp. 85–93 . 10.1.1.58.3128
[12] Intel, "Intel data plane development kit: programmer's guide", 2013, (http: //www.intel.com/content/www/us/en/intelligent-systems/intel-technology/ intel- dpdk- programmers-guide.html) .
[13] Intel, "DPDK performance report", 2013, (http://www.intel.com/content/www/ us/en/intelligent-systems/intel- technology/intel- dpdk- programmers- guide. html) .
[14] S. Kandula , D. Katabi , M. Jacob , A. Berger , "Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds", in: Proceedings of the 2Nd Conference on Symposium on Networked Systems Design & Implementation - Volume 2, in: NSDI'05, USENIX Association, Berkeley, CA, USA, 2005, pp. 287–300 .
[15] K. Prasad , A. Reddy , K. Rao , "Discriminating ddos attack traffic from flash crowds on internet threat monitors (ITM) using entropy variations", Afr. J. Com- put. ICT 6 (2013) 53–62 .
[16] K. Li, W. Zhou, P. Li, J. Hai, J. Liu, "Distinguishing DDoS attacks from flash crowds using probability metrics", in: Proceedings of the Third International Conference on Network and System Security, 2009. (NSS '09.), IEEE, 2009, pp. 9–17, doi: 10. 1109/NSS.2009.35 .
[17] O. Joldzic, Z. Djuric, P. Vuletic "A Transparent and Scalable Anomaly-Based DoS Detection Method", Computer Networks (Elsevier), vol. 104, pp. 27-42, 2016;

Избор литературе је одговарајући? **ДА** НЕ

IV.4 Циљеви истраживања

Основни циљ истраживања је верификација хипотезе да је могуће извршити успјешну детекцију DoS напада који настају као посљедица генерисања огромне количине саобраћаја према датој мрежи, без обзира на архитектуру посматране мреже и сервисе које она садржи. За такву детекцију је потребно предложити адаптивно и скалабилно рјешење које ће моћи детектовати аномалије у нормалном функционисању мреже, притом не утичући на перформансе такве мреже, односно њених сервиса. Скалабилност предложеног рјешења треба да се огледа у могућности једноставног проширења капацитета у погледу количине саобраћаја која може бити процесирана, а без негативног утицаја на могућности детекције напада - употребом намјенски дизајнираног алгоритма за распоређивање оптерећења на процесне елементе.

Циљеви истраживања су одговарајући? **ДА** НЕ

IV.5 Хипотезе истраживања: главна и помоћне хипотезе

Велики број постојећих рјешења за детекцију напада на мрежну инфраструктуру се заснива на познавању потписа (тј. начина манифестовања) напада прије него што се напад деси. Системи базирани на потпису (енгл. *signature-based*) су ефикасни у ситуацијама у којима се напади могу предвидјети са великом прецизношћу.

Хипотеза истраживања: За нападе који су засновани на огромној количини саобраћаја састављеног од валидног садржаја и који имају за циљ заузимање ресурса мреже (и, као посљедица, драстично смањење перформанси мреже или потпуно онемогућавање рада легитимним корисницима), могуће је дизајнирати систем за детекцију који ће бити базиран на статистичким аномалијама саобраћаја.

Оваквим приступом би се омогућило динамичко прилагођавање система за детекцију условима мреже, као и његова успјешна примјена чак и у ситуацијама у којима администратор не посједује предзнање о карактеристикама потенцијалних напада.

Помоћне хипотезе: Систем за детекцију напада на мрежну инфраструктуру требао би бити отпоран на нападе који су усмјерени директно против њега самог, а истовремено врло скалабилан како би се (без обзира на оптерећење, број процесних елемената и величину мреже) омогућио рад у условима високих брзина комуникације без нарушавања могућности детекције.

Хипотезе истраживања су јасно дефинисане? **ДА** НЕ

IV.6 Очекивани резултати хипотезе

Најважнији очекивани резултат јесте дизајн и имплементација систем за детекцију DDoS напада у рачунарским мрежама који ће бити базиран на статистичким аномалијама саобраћаја, а који треба да буде ефикасан, робустан и скалабилан. При томе, робусност система треба да се огледа и у отпорности на нападе који су усмјерени директно против самог система, а скалабилност и у могућности рада система у условима високих брзина комуникације при чему функција детекције не смије бити нарушена. Исто тако, дизајнирани систем треба да се динамички прилагођава условима мреже у којој функционише.

Очекивани резултати представљају значајан научни допринос? **ДА** НЕ

IV.7 План рада и временска динамика

Фазе израде докторске дисертације су:

1. Анализа постојећег стања у области детекције (D)DoS напада на мрежну инфраструктуру,
2. Дизајнирање алгоритма за детекцију напада,
3. Дизајнирање алгоритама за расподјелу оптерећења,
4. Пројектовање система за детекцију (D)DoS напада у складу са радном хипотезом,
5. Развој пројектованог рјешења,
6. Утврђивање перформанси рада дијела система за распоређивање оптерећења мрежне комуникације,
7. Утврђивање преформанси рада дијела система за детекцију (D)DoS напада,
8. Потврђивање радне хипотезе кроз статистичку анализу добијених резултата.
   Анализа резултата истраживања ће се вршити упоређивањем и графичким приказивањем добијених статистичких података.

План рада и временска динамика су одговарајући? **ДА** НЕ

IV.8 Метод и узорак истраживања

Потврда резултата истраживања извршиће се путем симулације рада система за детекцију кориштењем рјешења развијеног на бази предложеног концепта. У процесу симулације користиће се подаци о секвенцама стварних напада који су кориштени и од стране других актуелних рјешења.

Основне научне методе истраживања које ће се примјењивати у раду су:

- Прикупљање, анализа и систематизација доступне литературе,
- Пројектовање и имплементација алгоритма за детекцију напада на мрежну инфраструктуру,
- Пројектовање и имплементација алгоритма за расподјелу оптерећења,
- Статистичка анализа експерименталних резултата.

Метод и узорак су одговарајући? **ДА** НЕ

IV.9 Мјесто, лабораторија и опрема за експериментални рад

За потребе експерименталног рада биће имплементирано лабораторијско окружење у којем ће бити симулирани DDoS напади на рачунарску мрежу. Систем ће бити имплементиран кориштењем виртуелне инфраструктуре на стандардном потрошачком хардверу. Кориштењем виртуелне инфраструктуре ће бити показана једноставност проширења капацитета система. За имплементацију ће бити искориштен VMWare ESXi виртуализацијски софтвер, помоћу којег ће бити креиран одговарајући број процесних елемената базираних на оперативном систему Linux.
Виртуелизација мрежних елемената система ће бити реализована кориштењем Mininet и Open vSwitch рјешења за виртуелизацију рачунарских мрежа уз употребу SDN технологије за управљање радом програмабилних мрежних уређаја. У ову сврху ће бити искориштен Ryu контролер уз апликацију за управљање и комуникацију са процесним елементима развијену у програмском језику Python.
Процесни елементи ће бити развијени у програмском језику C кориштењем библиотеке под називом DPDK која омогућава обраду мрежних пакета без употребе прекидне технике, чиме се побољшавају перформансе система у мрежама великих брзина.
Систем ће у току рада генерисати статистичке податке о оптерећењу и ентропији. За анализу ових података и приказивање резултата у раду биће искориштене могућности програмског пакета MATLAB.

Услови за експериментали рад су одговарајући? **ДА** НЕ

IV.10 Методе обраде података

За верификацију рада развијених алгоритама ће бити кориштени различити сетови података састављени од мрежног саобраћаја прикупљеног из стварних рачунарских мрежа. Прикупљени пакети ће бити репродуковани у тестном окружењу како би се симулирао редован рад мреже и како би се систему омогућило да прикупи податке потребне за доношење одлуке о постојању напада у мрежи. Напади на мрежу ће бити симулирани кориштењем сетова података састављних од огромног броја намјенски креираних мрежних пакета кориштењем генератора DDoS напада.
Систем ће доносити одлуку о нападу на основу статистичких података о броју пакета и количини обрађеног саобраћаја које сваки процесни елемент прикупља у реалном времену у току сваког радног интервала. Као основна метрика за анализу прикупљених података ће бити кориштена ентропија вриједности појединих поља у заглављу пакета у току и изван напада на мрежу.
Додатно, поређење прикупљених статистичких података о оптерећењу појединих процесних елемената ће се моћи искористити за функционисање и валидацију резултата алгоритма за распоређивање оптерећења.

Предложене методе су одговарајући? **ДА** НЕ

V ЗАКЉУЧАК

Кандидат је подобан	**ДА**	НЕ
Тема је подобна	**ДА**	НЕ

На основу увида у рад кандидата, приложену документацију, биографију и библиографију, Комисија је закључила да кандидат мр Огњен Јолџић испуњава све прописане услове за одобрење теме за израду докторске дисертације, у складу са важећим Законом о Универзитету и на начин предвиђен Статутом Универзитета у Бањој Луци.

Комисија сматра да је предложена тема веома актуелна, као и да се на основу до сада остварених научних и истраживачких резултата кандидата могу очекивати значајни резултати. Исто тако, Комисија је јединствена у оцјени да су концепт и предложене методе истраживања адекватне постављеној радној хипотези, као и да ће кандидат дати свој оригинални научни допринос у области истраживања. У прилог овој тврдњи иде и чињеница да је кандидат објавио рад у часопису са SCI листе, са импакт фактором.

Узимајући у обзир све наведено, Комисија предлаже Наставно-научном вијећу Електротехничког факултета и Сенату Универзитета у Бањој Луци да прихвати тему за израду докторске дисертације „Адаптивни систем за детекцију DDoS напада у рачунарским мрежама" кандидата Јолџић Огњена, те да му омогући да приступи њеној изради.

Датум: 01.11.2016. године

проф. др Зоран Јовановић

Предсједник комисије

проф. др Зоран Ђурић

Члан 1

проф. др Славко Марић

Члан 2

доц. др Павле Вулетић

Члан 3

УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Патре 5 • 78000 Бања Лука • Република Српска • Босна и Херцеговина
Централа: +387 51 221 820 • Деканат: +387 51 221 824 • Факс: +387 51 211 408
E-mail: office@etfbl.net • www.etfbl.net

Датум: 26.09.2016. године

ЗАПИСНИК
о јавном представљању теме и програма истраживања докторске дисертације

Огњен Јолцић, број индекса: 3403/12, студент III циклуса студија на студијском програму **Информационо-комуникационе технологије**, модул Софтверске технологије, је пред Комисијом за оцјену подобности кандидата и теме за израду докторске дисертације у сљедећем саставу:

1. проф. др Зоран Јовановић, предсједник
2. проф. др Зоран Ђурић, ментор
4. проф. др Славко Марић, члан
5. доц. др Павле Вулетић, члан

приступио јавном представљању теме и програма истраживања докторске дисертације, са темом под називом „Адаптивни систем за детекцију DDOS напада у рачунарским мрежама".

Кандидат Огњен Јолцић је почео излагање у 10 часова. По завршеном излагању, кандидат је одговарао на питања чланова Комисије. Најважнија питања била су:

1. Главни параметри load balancing-а.
2. Како се ради baselining у мрежама и шта се сматра нормалном мрежом?
3. Могућности false positive детекције. Каква је улога администратора у непредвиђеним ситуацијама?
4. Подробније објаснити шему детекције напада.
5. Објаснити одређивање ентропије по процесорским елементима.
6. Веза ка менаџмент модулу; одбацивање напада у првој фази.
7. Како се понаша систем при веома јаком нападу на процесорске чворове?

Резимирајући кандидатово излагање, Комисија се сагласила да је добила одговоре на сва постављена питања, уз констатацију да изложени истраживачки рад представља важан допринос наставку истраживања и очекиваним резултатима.

Јавно представљање је завршено у 11:20 часова. Овај Записник чини саставни дио Извјештаја о подобности кандидата и теме за израду докторске дисертације.

Записник водио

Јовица Буловић

Предсједник Комисије
за оцјену подобности кандидата и
теме за израду докторске дисертације

Проф. др Зоран Јовановић