



# УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Булевар краља Александра 73, 11000 Београд, Србија

Тел. 011/324-8464, Факс: 011/324-8681

## КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 02.06.2015. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Богдана Савића под насловом „Анализа перформанси софтверских рутера са ИПсец протоколом“. Након прегледа материјала Комисија подноси следећи

### ИЗВЕШТАЈ

#### 1. Биографски подаци кандидата

Богдан Савић је рођен 15.03.1991. године у Београду. Математичку гимназију је завршио у Београду са одличним успехом. Електротехнички факултет у Београду уписао је 2010. године, на одсеку за Телекомуникације и информационе технологије. Дипломирао је у септембру 2014. године са просечном оценом 8,87. Дипломски рад оцењен је са 10. Мастер студије на Електротехничком факултету у Београду је уписао октобра 2014. на Модулу Системско инжењерство и радио комуникације. Положио је све испите са просечном оценом 8,00.

#### 2. Опис мастер рада

Мастер рад кандидата Богдана Савића под насловом „Анализа перформанси софтверских рутера са ИПсец протоколом“ обухвата 43 стране, са укупно 30 слика, 4 табеле и 11 референци. Рад је организован у 9 поглавља и садржи увод, 6 поглавља, закључак и списак коришћене литературе. На крају рада дата су 2 прилога.

Прво поглавље представља увод и описује предмет и циљ рада. Такође дат је и кратки преглед рада по деловима.

Друго поглавље даје основни преглед ИПсец протокола. Полази се од разлога за његов настанак. Затим се описују начини имплементације и начини заштите ИП пакета. Уводе се 3 протокола који заједно чине ИПсец. То су *Encapsulating security payload*, *Authentication header* и *Internet key exchange*.

Треће поглавље бави се криптографијом као неизоставним елементом у ИПсец технологији. Укратко су представљени релевантни алгоритми за енкрипцију и аутентификацију који су имплементирани, *Digital Encryption Standard*, *Advanced Encryption Standard*, *MD5* и *SHA*.

*Quagga* софтвер описан је у четвртном поглављу. Прво је дат њен историјат. Затим су наведени подржани протоколи. Дато је и кратко објашњење зашто се *Quagga* користи и које су њене предност у односу на специјализоване мрежне уређаје

У петом поглављу описан је рад *Strongswan* софтвера. Слично као и код *Quagga* софтвера дат је увид у историјат софтвера. Након тога поменути су битни конфигурациони фајлови. Уведен је појам *roadwarrior* корисника.

Шестим поглављем почиње практични део овог рада. Први тест односи се на тестирање *Strongswan* софтвера. Детаљно је описано како се инсталира и конфигурише *Strongswan* софтвер. Дефинисана је мрежа од 2 рачунара који међусобно размењују ИПсец пакете. На пријемном рачунару мерен је проток на линку. Бирани су различити алгоритми за енкрипцију и аутентификацију, и упоређене су њихове перформансе.

У седмом поглављу детаљно је описано како се инсталира и конфигурише *Quagga* софтвер. Изабрана је сложенија топологија, рачунари постају софтверски рутери а неки од

њих имају могућност слања ИПсец пакета. Прво је тестиран рад тзв. *roadwarrior* корисника. Он брзо мења своју локацију, и истовремено жели сачува активан ИПсец тунел до удаљене мреже. У другом делу показано је да софтверски рутер показује особине *VPN* гејтвеја. Рачунар са правилно конфигурисаним *Quagga* и *Strongswan* софтверима има способност да успешно одговори на промене у мрежи чувајући ИПсец тунел ненарушеним.

### 3. Анализа рада са кључним резултатима

Мастер рад кандидата Богдана Савића бави се улогом ИПсец протокола у интернет технологији. Како је безбедност постала јако битна ИПсец се намеће као неизоставна карика глобалне интернет мреже. На почетку рада кандидат, Богдан Савић, даје ИПсец протоколу теоријске основе објашњавајући разлог увођења, начине имплементације и најзначајније алгоритме који га сачињавају. У раду је демонстриран рад програма *Quagga* и *Strongswan* у оквиру имплементације мрежне безбедности.

Основни допринос рада чине практични тестови. Прво су испитивани алгоритми за енкрипцију и аутентификацију. Измерени су протоци при различитим алгоритмима и дато је њихово поређење према добијеним резултатима. Затим је на тестној мрежи испитиван рад *roadwarrior* корисника. Потврђено да корисници са *roadwarrior* особинама могу да партиципирају у ИПсец вези. На крају, кандидат је показао да *VPN* гејтвеји имају својства софтверских рутера и да су у стању да се самостално прилагоде променама у мрежи.


### 4. Закључак и предлог

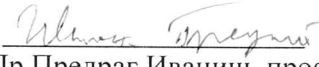
Мастер рад дипл. инж. Богдана Савића је приказао могућности и перформансе софтвера отвореног кода којим се може пружити мрежна заштита. Користећи хардвер опште намене, кандидат је тестирао неколико софтверских алата у лабораторијским условима, који могу бити полазна основа за коришћење ових софтвера у пракси или њихов даљи развој.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Богдана Савића под насловом „Анализа перформанси софтверских рутера са ИПсец протоколом“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 14. 09. 2016. године

Чланови комисије:

  
Др Александра Смиљанић, проф.

  
Др Предраг Иваниш, проф.