

## НАСТАВНО-НАУЧНОМ ВЕЋУ

**Предмет:** Оцена научне заснованости теме докторске дисертације кандидата Марка Мићовића, мастер инжењера електротехнике и рачунарства, под насловом „**Заштита приватности на мрежном слоју применом шифровања са очувањем формата**”.

Одлуком бр. 75-30 од 16.01.2024. године, именовани смо за чланове Комисије за оцену научне заснованости теме докторске дисертације кандидата Марка Мићовића за израду докторске дисертације и научне заснованости теме „**Заштита приватности на мрежном слоју применом шифровања са очувањем формата**” (енгл. *Network Layer Privacy Protection Using Format Preserving Encryption*).

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

## ИЗВЕШТАЈ

### 1. Подаци о кандидату

#### 1.1. Биографски подаци

Марко Мићовић рођен је 3. јула 1993. године у Београду. Основну школу „Стеван Синђелић” завршио је као носилац Вукове дипломе. Трећу београдску гимназију, на природно-математичком смеру, завршио је са одличним успехом.

Основне академске студије на Електротехничком факултету у Београду, на одсеку Електротехника и рачунарство, уписао је 2012. године. Основне академске студије на модулу Рачунарска техника и информатика завршио је 2016. године са просечном оценом 9,04. Дипломски рад на тему „*Систем за идентификацију сигурених уједињених бесконтактних картица*” под менторством ванредног професора др Милоша Цветановића одбранио је са оценом 10. Током основних студија био је на стручној пракси у фирми „Микроелектроника”.

Мастер академске студије на Електротехничком факултету у Београду уписао је 2016. године. Мастер академске студије на модулу Рачунарска техника и информатика завршио је 2018. године са просечном оценом 10. Мастер рад на тему „*Окружење за прикупљање информација о извршавању програма*” под менторством доцента др Саше Стојановића одбранио је са оценом 10.

Докторске академске студије на Електротехничком факултету у Београду уписао је 2018. године на модулу Рачунарска техника и информатика. Положио је све испите са просечном оценом 10,00. У истраживачком раду оријентисао се ка областима уграђених уређаја и рачунарских мрежа. Похађао је летњу школу ACACES (*Advanced Computer Architecture and Compilation for High-performance Embedded Systems*) 2019. године. Током мастер и докторских академских студија има објављена 2 научна рада у часопису са SCI листе, 3

научна рада на страним конференцијама и 9 научних радова на домаћим конференцијама као аутор или коаутор.

Почев од децембра 2016. године запослен је Електротехничком факултету у Београду. У периоду од 2016. до 2018. године био је изабран у звање сарадник у настави. У периоду од 2018. до 2022. године био је изабран у звање асистент и тренутно је ангажован на предметима: Рачунарске мреже 1, Рачунарске мреже 2, Микропроцесорски системи, Оперативни системи 1, Системски софтвер и Програмирање мобилних уређаја. Био је на стручном усавршавању у фирми „Elsys Eastern Europe”.

За време периода у току којег је запослен на Електротехничком факултету учествује на више научних и комерцијалних пројеката. Учесник је или је био учесник на неколико научних пројеката: 1) „Развој дигиталних технологија и умрежених сервиса у системима са уграђеним електронским компонентама” који финансира Министарство просвете, науке и технолошког развоја; 2) „Иновација групе предмета из области рачунарских мрежа, интернета и заштите података“ и 3) „УНАР - Унапређење наставе из Архитектуре рачунара” које је финансирало Министарство просвете, науке и технолошког развоја; 4) „*Advancing novel textual similarity-based solutions in software development (AVANTES)*” који је финансирао Фонд за науку Републике Србије; и 5) „*Belgrade Data Innovation Hub (BELDIH)*” - *HORIZON 2020*. Учествовао је као предавач у програму преквалификација у области информационих технологија који је организовао Развојни програм Уједињених нација током 2019, 2021, 2022. године. Сарађивао је у склопу комерцијалних пројеката са неколико фирми као и колегама са других катедри Електротехничког факултета. Најистакнутији такав пројекат јесте „*Развој и реализација софтвера за прорачун звучне изолације*” у сарадњи са фирмом „URSA”.

## 1.2. Сечено научноистраживачко искуство

Марко Мићовић је у свом истраживачком раду показао изузетно интересовање за области рачунарских мрежа и системског софтвера, са посебним акцентом на развој софтвера за специјализоване архитектуре.

Уписао је докторске академске студије школске 2018/2019. године на Електротехничком факултету Универзитета у Београду, на Модулу за Рачунарску технику и информатику. Све испите предвиђене овим студијским програмом је положио са просечном оценом 10,00 и остварио 120 ЕСПБ. Списак положених испита приказан је у табели која следи:

| Назив предмета                                                   | Оцена | ЕСПБ | Датум полагања испита |
|------------------------------------------------------------------|-------|------|-----------------------|
| (13Д111ЛРМ) Локалне рачунарске мреже                             | 10    | 9    | 01.07.2019.           |
| (13Д111ИП) Интернет програмирање                                 | 10    | 9    | 10.07.2019.           |
| (13Д111ВЛС) Пројектовање рачунара у ВЛСИ техници                 | 10    | 9    | 07.02.2020.           |
| (13Д111СМ) Сензорске мреже                                       | 10    | 9    | 18.09.2020.           |
| (13Д111ОПА) Одабрана поглавља из архитектуре рачунарских система | 10    | 9    | 19.09.2020.           |
| (19Д111ВИЕ) Вештачка интелигенција и експертски системи          | 10    | 9    | 16.09.2021.           |
| (19Д051НМ) Неуралне мреже                                        | 10    | 9    | 22.09.2021.           |
| (19Д111НАМ) Напредни алгоритми машинског учења                   | 10    | 9    | 25.09.2021.           |
| (19Д091УНР) Увод у научни рад                                    | 10    | 6    | 01.07.2022.           |

|                                         |    |   |             |
|-----------------------------------------|----|---|-------------|
| (19Д111СДМ) Софтверски дефинисане мреже | 10 | 9 | 21.09.2022. |
|-----------------------------------------|----|---|-------------|

Кандидат је испунио све обавезе предвиђене наставним планом и програмом докторских студија: Студијски истраживачки рад I (15 ЕСПБ), Студијски истраживачки рад II (15 ЕСПБ) и Научно стручни рад (3 ЕСПБ).

Досадашњи резултати кандидата приказани су кроз више публикација на домаћим и међународним конференцијама као и два рада у часопису са SCI листе. У наставку следи списак публикација:

Радови у часописима са SCI листе:

1. M. Mićović, U. Radenković, P. Vuletić, **Network Layer Privacy Protection Using Format-Preserving Encryption**, Electronics, Vol. 12, No. 23, pp. 1 - 21, Nov, 2023. [ISSN: 2079-9292, M22, IF<sub>2022</sub>=2.9]
2. U. Radenković, M. Mićović, Z. Radivojević, **Evaluation and Benefit of Imprecise Value Prediction for Certain Types of Instructions**, Electronics, Vol. 12, No. 17, pp. 1 - 23, Aug, 2023. [ISSN: 2079-9292, M22, IF<sub>2022</sub>=2.9]

Радови на страним конференцијама:

1. A. Sriblanović, M. Dodović, M. Mićović, A. Rikalo, S. Stojanović, **Implementation of a unified modern interface for executing hardware simulation, synthesis, and verification processes of VLSI systems**, 2023 10th International Conference on Electrical, Electronic and Computing Engineering (IcETRAN), pp. 1 - 5, IEEE, East Sarajevo, Bosnia and Herzegovina, Jun, 2023. [M33]
2. M. Dodović, A. Sriblanović, M. Mićović, A. Rikalo, S. Stojanović, **Implementation of the Verification process with Universal Verification Methodology in the Computer Systems for the VLSI course**, 2023 10th International Conference on Electrical, Electronic and Computing Engineering (IcETRAN), pp. 1 - 5, IEEE, East Sarajevo, Bosnia and Herzegovina, Jun, 2023. [M33]
3. U. Radenković, M. Mićović, Z. Radivojević, **A mechanism for mitigation of branch prediction calculation latency**, ICIST 2020 - 10th International Conference on Information Society and Technology, pp. 146 - 149, Society for Information Systems and Computer Networks, Kopaonik, Serbia, Mar, 2020. [M33]

Радови на домаћим конференцијама:

1. У. Раденковић, В. Јоцовић, М. Мићовић, А. Милаковић, Д. Драшковић, **Скуп података софтверских клонова типа четири за обраду матрица**, Зборник радова 28. ИКТ конференције "ЈУ ИНФО 2022", pp. 36 - 40, Информационо друштво Србије, Копаноник, Србија, Март, 2022. [M63]
2. М. Мићовић, У. Раденковић, **Изазови у реализацији наставе на предмету основних студија Програмирање мобилних уређаја**, Примена слободног софтвера и отвореног хардвера ПССОХ 2021, pp. 1 - 7, Универзитет у Београду, Електротехнички факултет, Београд, Србија, Октобар, 2021. [M63]
3. Т. Шекуларац, М. Мићовић, Ф. Хаџић, Д. Драшковић, Б. Николић, **Софтверско препознавање покрета код пацијената са оштећеним моторним обрасцима**, Зборник радова конференције "ЈУ ИНФО 2020", pp. 269 - 273, Друштво за информационе системе и рачунарске мреже, Копаноник, Србија, Март, 2020. [M63]
4. У. Раденковић, М. Мићовић, Ф. Хаџић, З. Радивојевић, **Алат за тестирање система за предвиђање скокова**, Зборник радова 25. научне конференције "ЈУ ИНФО 2019", pp. 77 - 82, Информационо друштво Србије, Копаноник, Србија, Март, 2019. [M63]
5. М. Мићовић, У. Раденковић, В. Јоцовић, Т. Шекуларац, Ф. Хаџић, Ж. Шуштран, Д. Драшковић, **Имплементациони детаљи алгоритма шифровања CRYPTO1**, 24.

- конференција "ЈУ ИНФО 2018", pp. 26-30, Информационо друштво Србије, Копаоник, Србија, Март, 2018. [M63]
6. Ф. Хацић, З. Радивојевић, М. Мићовић, У. Раденковић, **Конфигурабилне аритметичко логичке јединице реализоване коришћењем проточне обраде**, 24. конференција "ЈУ ИНФО 2018", pp. 111-116, Информационо друштво Србије, Копаоник, Србија, Март, 2018. [M63]
  7. Д. Драшковић, Н. Којић, М. Мићовић, У. Раденковић, **Имплементација система за прикупљање података, генерисање кластера и препорука помоћу машинског учења**, 24. конференција "ЈУ ИНФО 2018", pp. 167-172, Информационо друштво Србије, Копаоник, Србија, Март, 2018. [M63]
  8. М. Вукасовић, М. Мићовић, У. Раденковић, В. Јоцовић, Д. Драшковић, **Примена виртуелне стварности у оквиру медицинских третмана**, 23. конференција "ЈУ ИНФО 2017", pp. 105-110, Информационо друштво Србије, Копаоник, Србија, Март, 2017. [M63]
  9. Д. Драшковић, М. Мићовић, У. Раденковић, М. Вукасовић, С. Делчев, В. Јоцовић, Ж. Шуштран, Б. Николић, **Реализација веб система за управљање и надгледање софтверских пројеката**, 23. конференција "ЈУ ИНФО 2017", pp. 99-104, Информационо друштво Србије, Копаоник, Србија, Март, 2017. [M63]

### 1.3. Оцена подобности кандидата за рад на предложеној теми

Дана 24.01.2024. године, кандидат Марко Мићовић је на Електротехничком факултету Универзитета у Београду усмено полагао испит о подобности предложене теме докторске дисертације и кандидата (докторски испит), пред комисијом у саставу:

- проф. др Захарије Радивојевић, доктор електротехничких наука, ванредни професор, Електротехнички факултет, Универзитет у Београду
- проф. др Дејан Симић, доктор електротехничких наука, редовни професор, Факултет организационих наука, Универзитет у Београду
- проф. др Зоран Чича, доктор електротехничких наука, редовни професор, Електротехнички факултет, Универзитет у Београду

На јавној усменој одбрани предложене теме Комисија је кандидата оценила оценом **задовољно**.

## **2. Предмет и циљ истраживања**

Утицај комуникационих услуга и апликација на свакодневне активности као и ослањање на интернет се стално повећавају. Овај тренд је праћен бројним доказима да се употреба интернета и апликација опсежно прати и анализира. Мноштво података о личности се прикупља у безбедносне или комерцијалне сврхе. Стога су заштита приватности и анонимизација коришћења интернета важне теме истраживања већ неколико деценија. Подаци о личности се могу прикупити из различитих извора, директно из оперативних система или апликација, али и кроз анализу образаца мрежног саобраћаја и протокола које нека особа користи.

Приватност интернет претраживача је предмет бројних истраживања, која се углавном баве нападима на сам претраживач и праћењем од стране интернет страница. Временски напади (енгл. *timing attack*) преко бочних канала могу открити информације попут историје претраживања [1]. Овакви напади заснивају се на мерењу времена потребног за преузимање ресурса. Раније посећене интернет странице налазиће се у кешу, услед чега ће бити смањено време потребно за њихово преузимање. Детекција отиска интернет претраживача (енгл.

*browser fingerprinting*) омогућава идентификацију корисника на интернету [2]. Ова техника састоји се од прикупљања широког спектра података о уређају преко апликативног програмског интерфејса самог претраживача. Услед велике разноликости модерних уређаја на којима се користе претраживачи могуће је једнозначно идентификовати кориснике.

Већина комерцијалних интернет претраживача у позадини шаље велику количину података на своје сервере [3]. Међутим, слање података корисника на ове сервере не представља нарушавање приватности у општем случају. Дељење података о моделу и верзији уређаја, на пример, носи мали ризик по приватност. Проблем се јавља када је ове податке могуће директно повезати са одређеним корисником. Приватност је такође нарушена и услед слања историје претраживања јер је подложна једноставној деанонимизацији посебно у случају познавања *IP* (енгл. *Internet Protocol*) адреса [4]. Чак и без експлицитног слања историје претраживања, приватност се може угрозити уколико свака инстанца претраживача има свој јединствени идентификатор. Овакав идентификатор, када се шаље заједно са другим подацима, омогућава повезивање различитих преноса и праћење историје претраживања једног корисника.

Управо из наведених разлога постоји дугогодишње интересовање за онемогућавање праћења преко *IP* адресе претраживача. Најпознатија технологија у овој области јесте *Tor* (енгл. *The onion router*) [5]. Омогућава анонимно претраживање интернет страница кроз вишеслојну мрежу, која се састоји од три *Tor* сервера (названа и *onion* рутери) и троструког шифровања садржаја пакета. Коришћењем *Tor* система, веб сервер или посматрач на било којој посматраној тачки на интернету не могу да кажу које су обе крајње тачке комуникације, чувајући анонимност корисника на мрежном слоју. Међутим, таква заштита долази са извесним пеналима у погледу перформанси. Сваки пакет се дели на *Tor* ћелије са додатним заглављима, смањујући корисни део пакета. Обрада сваке појединачне ћелије укључује три шифровања и дешифровања између крајњих тачака. Додатно, путања којом пакети путују између крајњих тачака намерно није оптимална. Сви ови трошкови заједно често доводе до неугодног искуства приликом претраживања интернета. Такође, упркос великој употреби шифровања, добро је познато да је *Tor* систем подложен нападима одметнутих *Tor* рутера као и временским нападима. Праћењем саобраћаја на више тачака у мрежи и довођењем образаца саобраћаја у корелацију, могуће је открити крајње тачке комуникације. Ове слабости *Tor* система инспирисале су развој нових предлога за обезбеђивање анонимности на мрежном слоју.

Предмет овог истраживања биће управо заштита од профилисања на мрежном слоју и цурења личних података ка трећим странама. Ако се претпостави да корисник интернета комуницира користећи статичку јавну *IP* адресу или може бити недвосмислено повезан са неком јавном *IP* адресом у одређеном периоду, у том случају, нападачи могу пратити понашање и навике корисника праћењем скупа посећених *IP* адреса [6]. Још детаљније информације се могу добити праћењем *DNS* захтева овог корисника, на основу којих се могу препознати његове навике и склоности [7,8]. Иако *IPv6* има механизме заштите приватности као што су ротација префикса и проширења приватности *IPv6*, недавна студија је показала да је приватност значајног дела крајњих корисника и даље угрожена [9]. Стога, уредба о општој заштити података Европске уније (енгл. *General Data Protection Regulation*), као и регулатива других земаља (нпр. Кина, Бразил, Канада, Јапан) *IP* адресе сматрају подацима који могу да идентификују личност (енгл. *personally identifiable information*) [10,11], што додатно иде у прилог констатацији да се посебна пажња мора посветити њиховој заштити.

Прошло је више од 20 година од првог издања *Tor*, а неки обрасци коришћења интернета су се од тада значајно променили. Данас је скоро сав интернет саобраћај шифрован [12], што доводи до питања да ли су додатни слојеви шифровања садржаја пакета потребни и оправдани, пре свега зато што не пружају додатну сигурност од одметнутих *Tor* рутера и временских напада. У склопу овог истраживања биће анализирани савремени алгоритми и протоколи и предложена решења за заштиту приватности на мрежном слоју што укључује

пре свега анализу коришћења алгоритама шифровања са очувањем формата (енгл. *Format preserving encryption*) за заштиту приватности података на мрежном слоју. Ови алгоритми омогућавају шифровање податка произвољне дужине на начин који омогућава замену поља заглавља пакета његовом шифрованом верзијом исте величине. Недавно су први такви протоколи, *FEA-1* и *FEA-2* [13] у Јужној Кореји и *FF1* и *FF3-1* [14] у Сједињеним Америчким Државама, прошли евалуацију и усвајање од стране релевантних тела за стандардизацију.

Циљ овог истраживања јесте доказивање оправданости коришћења алгоритама шифровања са очувањем формата у сврху заштите приватности кроз замагљивање (енгл. *obfuscation*) одређених делова заглавља пакета. Један од доприноса истраживања биће и предлог новог механизма заштите приватности заснованог управо на примени алгорита шифровања са очувањем формата. Такав систем требало би да врши замагљивање садржаја заглавља пакета тако да није могуће утврдити од ког хоста из заштићене мреже је пакет потекао. Циљ истраживања јесте да се на основу евалуације перформанси новог механизма за заштиту приватности утврди да ли је примена алгорита шифровања са сачуваним форматом изводљива за сваки пакет под реалним оптерећењем саобраћаја без значајног нарушавања перформанси.

Значај овог истраживања огледа се у томе да отвара нове видике на пољу заштите приватности, пре свега у домену замагљивања произвољно дефинисаног скупа поља у заглављу пакета. Замагљивање појединих поља у заглављу пакета није широко распрострањено највише због тога што су у обзир узимани блоковски алгоритми шифровања и алгоритми тока који у општем случају доводе до нарушавања стандардног формата заглавља пакета. Алгоритми шифровања са очувањем формата могу подстаћи распрострањенију примену замагљивања поља у заглављима пакета. Такође, значај ове теме огледа се генерално и у тренутним истраживањима о чему сведоче прикупљене референце о заштити приватности.

### 3. Полазне хипотезе

Предложено истраживање полази од следећих хипотеза:

- Постојећи механизми заштите приватности на мрежном слоју имају проблеме у погледу перформанси услед интензивне примене алгоритама шифровања или чувања стања током рада.
- Успостављање корелације између пакета посматраног корисника могуће је отежати замагљивањем (енгл. *obfuscation*) делова заглавља пакета.
- Употреба блоковских алгоритама шифровања у циљу замагљивања делова заглавља пакета није прикладна јер није могуће постићи довољно фину грануларност замагљивања што доводи до нарушавања стандардног формата тих заглавља или до потребе за сложеним праћењем стања активних сесија.
- Алгоритми шифровања са очувањем формата могу да се ефикасно користе за заштиту приватности на мрежном слоју и спречавање профилисања корисника.
- Реализација заштите приватности на мрежном слоју коришћењем алгоритама шифровања са очувањем формата је ефикаснија од постојећих механизма заштите о којима је извештавано у научним радовима и стандардизационим документима.
- Програмабилни мрежни уређаји омогућавају реализацију заштите приватности на мрежном слоју уз минимално нарушавање перформанси.

#### 4. Научне методе истраживања

На самом почетку биће детаљно истражени постојећи механизми за заштиту приватности представљени у отвореној литератури као што су *HORNET* [15], *TARANET* [16], *PHI* [17], *LAP* [18], *DOVETAIL* [19] и *Tor*. Посебна истраживачка пажња биће усмерена ка механизмима за заштиту приватности *SPINE* и *PINOT* чији се принцип рада заснива на замагљивању оригиналних *IP* адреса. Ограничења постојећих механизма биће издвојена зарад њихове елиминације кроз предлог новог механизма за заштиту приватности. Такође, упоредна анализа постојећих алгоритама шифровања са очувањем формата биће извршена ради формирања најприкладнијих кандидата за укључивање у нови механизам за заштиту приватности.

Прототип новог механизма за заштиту приватности биће развијан у алату *mininet* за брзу израду прототипа софтверски дефинисаних мрежа. У оквиру алата *mininet* биће формирана виртуелна мрежна топологија са могућношћу интеграције *bmv2* (*Behavioral Model v2*) алата као софтверске имплементације *P4* свича. Референтни *P4* свич *bmv2* представља софтверско извршно окружење за *P4* програме. На овај начин могућа је верификација прототипа новог механизма за заштиту приватности, као и процена перформанси и потребних ресурса без приступа стварним физичким уређајима. Статистичком анализом случајности излаза криптографских алгоритама који се користе у оквиру алгоритама шифровања са очувањем формата биће предвиђени начини за повећање перформанси уз очување нивоа заштите.

Након имплементације новог механизма за заштиту приватности за физичка извршна окружења, евалуација перформанси биће реализована коришћењем савремених алата за активно праћење мрежа. Алат *iPerf2* користи се за мерење протока за *TCP* саобраћај [20]. *PF\_RING Zero-Copy* алат броји колико пакета се обради у секунди [21]. Алат *Sockperf* мери просечно кашњење пакета између два учесника у комуникацији [22]. На основу извршених мерења биће представљена евалуација новог механизма за заштиту приватности. Упоредна анализа новог механизма и постојећег „несвесног” *DNS* преко *HTTPS* (енгл. *Oblivious DNS over HTTPS*) као механизма за заштиту од *DNS* профилисања биће такође извршена.

#### 5. Очекивани научни допринос

Очекује се да доприноси овог рада буду остварени у следећим правцима:

- Преглед и свеобухватна анализа постојећих механизма за заштиту од профилисања коришћењем података добијених анализом мрежног саобраћаја који ће обухватити начине њиховог функционисања као и сажетак познатих недостатака сваког од датих механизма.
- Доказ оправданости коришћења алгоритама шифровања са очувањем формата у сврху замагљивања делова заглавља пакета.
- Дефиниција принципа рада новог система за заштиту приватности на мрежном слоју са следећим особинама: транспарентан за корисника, без чувања стања приликом рада, независност од конкретног протокола, једноставна конфигурација, усклађеност са правним прописима.
- Имплементација предложеног система за заштиту приватности за наменски хардвер на програмабилним мрежним картицама као и засебан програмски модул.
- Резиме ограничења процеса имплементације у случају конфигурисања равни података мрежних картица коришћењем програмског језика *P4* за програмирање процесора пакета независних од протокола.
- Анализа механизма за детекцију оптималног тренутка за промену коришћеног криптографског материјала у циљу несметаног рада и очувања постојећих токова података.

Евалуација примене предложеног система за заштиту приватности у поставци са истим циљем као и „несвесни” *DNS* преко *HTTPS* који је усвојен од стране IETF (*Internet Engineering Task Force*), али са очекивано бољим перформансама.

## 6. План истраживања и структура рада

Истраживање ће се састојати од следећих корака:

- На почетку истраживања ће се приступити детаљној анализи постојећих механизма за заштиту приватности. Биће осветљени начини на који се они могу применити, њихови доприноси, али и ограничења и сложености које уносе у апликативни и мрежни стек.
- Након тога, биће извршена компаративна анализа алгоритама шифровања са очувањем формата. У склопу тога посебна пажња биће посвећена криптоанализи и прегледу постојећих напада датих алгоритама шифровања.
- Наредни корак биће преглед архитектура програмабилних мрежних картица и мрежних акцелератора погодних за имплементацију предложеног система за заштиту приватности. Биће направљена упоредна анализа *FPGA* (енгл. *Field Programmable Gate Array*) и вишејезгарних система на чипу са високим степеном паралелизма.
- Потом ће се приступити имплементацији новог система за заштиту приватности на мрежном слоју. Систем ће бити имплементиран за већи број извршних окружења и користећи већи број програмских језика у циљу проналаска имплементације са најефикаснијом обрадом пакета.
- Наредни корак у истраживању биће спровођење евалуације имплементације новог система на физичким уређајима у условима реалног оптерећења мрежног саобраћаја.
- Разматрање употребе имплементiranог система на специфичан начин да се постигне бољи резултат него „несвесни” *DNS* преко *HTTPS*.

## Најрелевантније референце из отворене литературе у вези са тезом су:

1. Van Goethem, T., Wouter J., Nikiforakis, N. The Clock is still ticking: Timing attacks in the modern web. In Proceedings of the 22<sup>nd</sup> ACM SIGSAC Conference on Computer and Communications Security, October 2015; pp. 1382-1393.
2. Gómez-Boix, A., Laperdrix, P., Baudry, B. Hiding in the crowd: an analysis of the effectiveness of browser fingerprinting at large scale. In Proceedings of the 2018 world wide web conference, April 2018; pp. 309-318.
3. Leith, D. J.. Web Browser Privacy: What Do Browsers Say When They Phone Home?. IEEE Access, March 2021; Volume 9, pp. 41615-41627.
4. Weinberg, Z., Chen, E. Y., Jayaraman, P. R., Jackson, C. I still know what you visited last summer: Leaking browsing history via user interaction and side channel attacks. In 2011 IEEE Symposium on Security and Privacy, May 2011; pp. 147-161).
5. Tor Project | Anonymity Online. Available online: <https://www.torproject.org/> (accessed on 17 October 2023).
6. Hoang, N.P.; Niaki, A.A.; Gill, P.; Polychronakis, M. Domain Name Encryption Is Not Enough: Privacy Leakage via IP-Based Website Fingerprinting. In Proceedings of the Privacy Enhancing Technologies (PETs), Virtual Event, 12-16 July 2021; pp. 420-440.
7. Yan, Z.; Lee, J.H. The Road to DNS Privacy. Future Gener. Comput. Syst. 2020, 112, 604-611.
8. Khormali, A.; Park, J.; Alasmary, H.; Anwar, A.; Saad, M.; Mohaisen, D. Domain Name System Security and Privacy: A Contemporary Survey. Comput. Netw. 2021, 185, 107699.
9. Saidi, S.J.; Gasser, O.; Smaragdakis, G. One Bad Apple Can Spoil Your IPv6 Privacy. ACM SIGCOMM Comput. Commun. Rev. 2022, 52, 10-19.

10. GDPR.Eu. What Is Considered Personal Data under the EU GDPR? Available online: <https://gdpr.eu/eu-gdpr-personal-data/> (accessed on 17 October 2023).
11. Finkel, M.; Lassey, B.; Iannone, L.; Chen, J. B. IP Address Privacy Considerations, Internet-Draft: draft-irtf-pearg-ip-address-privacy-considerations-01, 23 October 2022. Available online: <https://www.ietf.org/archive/id/draft-irtf-pearg-ip-address-privacy-considerations-01.txt> (accessed on 19 December 2023).
12. HTTPS Encryption on the Web-Google Transparency Report. Available online: <https://transparencyreport.google.com/https/overview?hl=en> (accessed on 17 October 2023).
13. Lee, J.K.; Koo, B.; Roh, D.; Kim, W.H.; Kwon, D. Format-Preserving Encryption Algorithms Using Families of Tweakable Blockciphers; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2014; Volume 8949, pp. 132-159.
14. Dworkin, M. Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption; NIST: Gaithersburg, MD, USA, 2016.
15. Chen, C.; Asoni, D.E.; Barrera, D.; Danezis, G.; Perrig, A. HORNET: High-Speed Onion Routing at the Network Layer. In Proceedings of the ACM Conference on Computer and Communications Security 2015, Denver, CO, USA, 12-16 October 2015; pp. 1441-1454.
16. Chen, C.; Asoni, D.E.; Perrig, A.; Barrera, D.; Danezis, G.; Troncoso, C. TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer. In Proceedings of the 3rd IEEE European Symposium on Security and Privacy, London, UK, 24-26 April 2018; pp. 137-152.
17. Chen, C.; Perrig, A. PHI: Path-Hidden Lightweight Anonymity Protocol at Network Layer. In Proceedings of the Privacy Enhancing Technologies, Minneapolis, MN, USA, 18-21 July 2017; pp. 100-117.
18. Hsiao, H.C.; Kim, T.H.J.; Perrig, A.; Yamada, A.; Nelson, S.C.; Gruteser, M.; Meng, W. LAP: Lightweight Anonymity and Privacy. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20-23 May 2012; pp. 506-520.
19. Sankey, J.; Wright, M. Dovetail: Stronger Anonymity in Next-Generation Internet Routing; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2014; Volume 8555, pp. 283-303.
20. A TCP, UDP, and SCTP Network Bandwidth Measurement Tool. Available online: <https://github.com/esnet/iperf> (accessed on 17 October 2023).
21. PF\_RING ZC (Zero Copy), Multi-10 Gbit RX/TX Packet Processing from Hosts and Virtual Machines. Available online: [https://www.ntop.org/products/packet-capture/pf\\_ring/](https://www.ntop.org/products/packet-capture/pf_ring/) (accessed on 17 October 2023).
22. Mellanox Network Benchmarking Utility. Available online: <https://github.com/Mellanox/sockperf> (accessed on 17 October 2023).

## 7. Закључак и предлог

На основу приложене документације и стеченог целокупног утиска о теми докторске дисертације и досадашњег научног рада кандидата Марка Мићовића, мастер инжењера електротехнике и рачунарства, Комисија је дошла до следећих закључака:

1. Кандидат испуњава све формалне и суштинске потребне услове прописане Законом о високом образовању, Статутом Универзитета у Београду и Статутом Електротехничког факултета Универзитета у Београду, за израду докторске дисертације.
2. Предложена тема **„Заштита приватности на мрежном слоју применом шифровања са очувањем формата”** јесте научно заснована, а резултати који ће проистећи израдом ове докторске дисертације представљаће значајан и оригиналан допринос

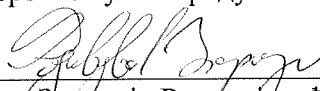
међународној научној заједници. Тема припада ужој научној области Рачунарска техника и информатика.

На основу свега претходно изложеног, Комисија са задовољством предлаже Наставно-научном већу Електротехничког факултета Универзитета у Београду да кандидату Марку Мићовићу одобри израду докторске тезе под насловом „**Заштита приватности на мрежном слоју применом шифровања са очувањем формата**” (енгл. *Network Layer Privacy Protection Using Format Preserving Encryption*), под менторством др Павла Вулетића, ванредног професора Електротехничког факултета Универзитета у Београду.

#### ЧЛАНОВИ КОМИСИЈЕ



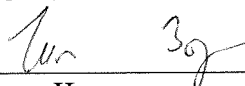
др Павле Вулетић, ванредни професор  
Универзитет у Београду – Електротехнички факултет



др Захарије Радивојевић, ванредни професор  
Универзитет у Београду – Електротехнички факултет



др Дејан Симић, редовни професор  
Универзитет у Београду – Факултет организационих наука



др Зоран Чича, редовни професор  
Универзитет у Београду – Електротехнички факултет