

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 07.10.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Славица Митровић под насловом „Сигурно израчунавање више учесника у сигурним виртуелним машинама са LUKS енкрипцијом“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Славица Митровић је рођена 07.09.2000. године у Аранђеловцу. Завршила је основну школу „Светолик Ранковић“ у Аранђеловцу као вуковац и ђак генерације. Уписала је гимназију „Милош Савковић“ у Аранђеловцу, математички смер, коју је такође завршила као вуковац. Током школовања такмичила се из области физике, математике и српског језика и освајала бројне награде. Електротехнички факултет, смер софтверско инжењерство, уписала је 2019. године. Дипломирала је 2023. године са просечном оценом 9,48. Дипломски рад одбранила је у септембру 2023. године са оценом 10, а од октобра исте године је запослена за стално у фирми Nutanix, након одрађене тромесечне праксе. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство, уписала је у октобру 2023. године.

2. Извештај о студијском истраживачком раду

Кандидат Славица Митровић је као припрему за израду мастер рада урадила истраживање о технологијама сигурних процесорских енклава и окружења за поверљиво извршавање (енг. Trusted Execution Environment) у области сигурне обраде података и израчунавања више учесника (енг. Secure Multi-Party Computation), којој припада тема мастер рада. Анализирани су следећи системи: Google Cloud Confidential Space, Azure Confidential Clean Rooms, Edgeless Systems, Ultraviolet и Cosmian VM. Указано је и на сигурносне или оперативне слабости које имају поједина од ових решења, што је трасирало пут за предлог оригиналне имплементације која је дата у раду. Посебно су анализирани постојећи алат SNPGuard за креирање виртуелних машина у оквиру AMD SEV-SNP технологије, као основа за даља проширења и изазови који постоје у области енкрипције диска, атестације и сигурног израчунавања од стране више учесника. Анализом решења је утврђено да проширење поменутог пројекта коришћењем механизма за енкрипцију диска представља перспективно решење које може да омогући сигурно израчунавање.

3. Опис мастер рада

Мастер рад обухвата 36 страна, са укупно 19 слика и 25 референци без насловне стране и садржаја. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, те спискове скраћеница и слика.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљена је технологија сигурног окружења извршавања, различите имплементације TEE технологије, технологија за енкрипцију података приликом мировања (чувања на диску) и сценарио обраде података више учесника (енг. Multiparty Computation). Такође је представљен и проблем складиштења кључева за сигурну обраду у којој учествује више корисника, као и решење тог проблема.

У другом поглављу је дат кратак преглед постојећих решења за обраду података од стране више корисника у сигурним окружењима. Дати су примери производа великих провајдера услуга у облаку и њихове предности и мане.

У трећем поглављу су детаљно представљене све технологије које су коришћене за израду пројекта као и концепти који су употребљени за имплементацију, атестацију сигурних виртуелних машина и тестирање решења. Такође је описано постојеће решење SNPGuard које је служило као основа и идеја за пројекат.

Четврто поглавље детаљно описује имплементацију решења од подешавања пројекта и подизања виртуелних машина до крајње обраде података и дат је приказ архитектуре система предложеног решења. Од посебног значаја је потпоглавље које говори о компоненти која се назива диск менаџер и која представља суштину пројекта. У том делу се говори о алатима за прављење енкрипционог диска и о механизмима заштите података који се користе.

У петом поглављу дата је анализа предложеног решења која укључује безбедносни модел и анализу сигурности. Описани су недостаци решења и предлози за унапређење.

Шесто поглавље је закључак у оквиру кога је резимирано имплементирано решење и описан његов значај и ограничења.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Славице Митровић се бави решавањем проблема сигурног израчунавања од стране више учесника коришћењем и комбиновањем метода шифровања диска и сигурних виртуелних машина. Кроз анализу и имплементацију предложеног модела приказано је како се комбиновањем механизма за шифровање диска (LUKS) и сигурних окружења извршавања коришћењем AMD SEV SNP технологије може обезбедити висок ниво поверљивости и интегритета података током обраде. Применом технологије сигурних процесорских енклава елиминише се могућност приступа подацима од стране неовлашћених корисника, укључујући и администратора платформе у облаку, док LUKS механизам обезбеђује да се подаци на трајном складишту чувају у шифрованом облику.

Основни резултати мастер рада укључују: 1) анализу постојећих алата и производа који пружају поверење у процес подизања сигурних виртуелних машина и исправан прототип система за инсталацију; 2) приказ поступка покретања свих неопходних софтверских компоненти за омогућавање сигурне обраде података више учесника кроз покретање сигурне виртуелне машине са потпуном енкрипцијом диска и енкриптованом оперативном меморијом; 3) приказ праваца наставка рада на развоју овог решења и даљих унапређења.

5. Закључак и предлог

Кандидат Славица Митровић је у свом мастер раду успешно истражила и предложила решење за сигурно израчунавање већег броја учесника у сигурним виртуелним машинама уз коришћење енкрипције диска. Предложено решење пружа јасан и практичан механизам да се задржи поверење између више учесника коришћењем ТЕЕ изолованог рачуна и представља основу производног решења за израчунавања више учесника.

Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Славице Митровић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 25.10.2025. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 25.10.2025.

Данко Миладиновић Асистент
сагласан, 25.10.2025.