КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 14.07.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Наталија Гвозденовић под насловом „Креирање малвера коришћењем великих језичких модела". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Наталија Гвозденовић је рођена 16.07.2002. године у Београду. Завршила је основну школу „Владислав Рибникар" у Београду као вуковац и ђак генерације. Уписала је Трећу београдску гимназију, коју је такође завршила као вуковац и ђак генерације. Током школовања такмичила се из математике, хемије и српског језика, освајајући награде на окружним такмичењима и остваривши више учешћа на републичким такмичењима. У првом и другом разреду средње школе освојила је по другу награду на републичком такмичењу из математике. Електротехнички факултет у Београду уписала је 2021. године, на Модулу за софтверско инжењерство. Дипломирала је у октобру 2025. године са просечном оценом 9,63, а дипломски рад одбранила је са оценом 10. Током студија остварила је ангажовање од преко 90 сати као демонстратор на факултету. Такође, током студија је била ангажована као ментор и предавач на школама програмирања за децу са посебним интересовањем за програмирање, у организацији Фондације Петља. Мастер студије на Електротехничком факултету у Београду, на Модулу за рачунарску технику и информатику, уписала је у новембру 2025. године.

2. Извештај о студијском истраживачком раду

Кандидаткиња Наталија Гвозденовић је као припрему за израду мастер рада проучила релевантну литературу из области безбедности великих језичких модела, агентских система, криптографије и детекције малвера. У оквиру студијског истраживачког рада анализирани су приступи у којима језички модел генерише програмски код или води фазе напада.

Полазна тачка истраживачког рада био је рад Ransomware 3.0, чија је архитектура детаљно анализирана. Упоредо је прегледан и јавно доступан извршни узорак PromptLock, преузет са сервиса за размену узорака малвера, искључиво путем статичке анализе без покретања. Циљ прегледа био је следећи: разумевање фазног тока рансомвера, увид у начин на који се упити на природном језику уграђују у извршни бинарни фајл, и сагледавање улоге Луа интерпретера као носиоца малициозне логике и SPECK алгоритма као криптографског задатка. У припреми је размотрено мерење тог истог тока под различитим варијантама упита у односу на оригинални рад, као и отворена питања у погледу граничних услова по величини модела и профилу жртве које споменути рад не разрешава.

Анализирана је употреба оркестрационог оквира LangGraph за конструкцију графа стања у вишефазном агенту, са детерминистичким контролним тачкама и управљањем током. Разматрани су различити начини приступа великим језичким моделима – преко јавног програмског интерфејса и путем локалног извршавања – са освртом на последице по поновљивост и мерљивост резултата.

Проучени су лаки криптографски алгоритми чији код велики језички модел може да синтетише – поред SPECK-128, такође ChaCha20 и Ascon, победник NIST такмичења за лаку криптографију – са становишта сложености синтетисане скрипте и способности различитих модела да их имплементирају. Одвојено је испитана појава полиморфизма у генерисаном Луа коду: да ли модел у узастопним пролазима понавља исти програмски образац или мења текст и структуру скрипте.

Посебну пажњу кандидаткиња је посветила питању детекције извршног облика оркестратора. Анализирана је читљивост уграђених упита у бинарном фајлу на диску, одзив антивирусних алата на споменути узорак PromptLock. На крају је размотрена потреба за изолованом лабораторијом у којој се исти ток може поновити, а исправност шифровања верификовати на пробном скупу датотека, без ризика по интегритет контролног окружења.

3. Опис мастер рада

Мастер рад обухвата 105 страна без насловне стране, са укупно 39 слика, 46 табела и 26 референци. Рад садржи шест поглавља и закључак, списак коришћене литературе, списак скраћеница, списак слика, списак табела, три прилога и захвалницу.

У уводу је уведен сценарио LLM-оркестрираног ренсомвера. Постављена су три истраживачка питања евалуације која воде кроз цео рад. Друго поглавље обухвата преглед литературе и модел претње. Анализирана је промена парадигме у односу на традиционални статички малвер, представљена је таксономија LLM-базираних претњи и праћена еволуција ренсомвера до концепта Ransomware 3.0. Треће поглавље посвећено је анализи постојеће архитектуре Ransomware 3.0 и референтног узорка PromptLock: фазама рада, упитима на природном језику и јавно доступном извршном коду. Поглавље представља теоријски темељ за сопствену лабораторијску имплементацију. Четврто поглавље описује експериментално окружење са два слоја. Први слој је ток писан у програмском језику Python заснован на оквиру LangGraph, који имплементира фазе рада ренсомвера, бележи мерења кроз контролне тачке и врши повратну проверу шифровања на пробном фајлу. Други слој је Го оркестратор који се компајлира у низ извршних узорака у зависности од одабране конфигурације улазних упита.
Пето поглавље дефинише методологију мерења. Основна јединица експеримента је тројка (језички модел, профил жртве, скуп упита), чијом варијацијом се мере разлике у понашању система. Уведене су контролне тачке и додатне метрике које нису присутне у досадашњој литератури. Шесто поглавље приказује емпиријске резултате у односу на три постављена истраживачка питања, уз анализу методолошких ограничења. У закључку су сажети научни доприноси рада, безбедносне импликације употребе фазног мерења и предлози за даља истраживања.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Наталије Гвозденовић бави се евалуацијом способности великих језичких модела да у контролисаној лабораторији самостално прођу све фазе креирања ренсомвера – од пописа диска жртве до синтезе кода за шифровање и поруке уцене. Полазећи од концепта Ransomware 3.0 и јавног узорка PromptLock, кандидаткиња је изградила сопствени мерни оквир у коме се исти ток може поновити, упоредити међу моделима и независно верификовати. Ток је реализован у LangGraph окружењу, са контролним тачкама по фазама и повратном провером исправности шифровања на пробном фајлу. Исти програм уграђен је у Го оркестратор – функционалан лабораторијски узорак малвера који се компајлира у низ Windows и Linux извршних фајлова – ради мерења детектабилности на Microsoft Defender алату и сервису VirusTotal.
Основни доприноси рада су: 1) поновљива лабораторија у којој се криптографски задатак верификује на пробном фајлу, а контролни документи жртве остају нетакнути; 2) систематска евалуација модела по фазама; 3) кључни емпиријски налаз да ране фазе напада пролазе код већине испитаних модела, док је проблематична синтеза исправног Луа кода за шифровање; 4) анализа одабира мета која показује да модели одлуке доносе на основу назива датотеке, а слабо откривају осетљив садржај иза безазленог имена; 5) квантитативна анализа полиморфизма генерисаних Луа скрипти, која показује да се код за шифровање битно разликује међу пролазима; 6) анализа детектабилности Го узорака, која показује PromptFilecoder детектује искључиво узорке у чији је код дословно уграђен C-нацрт, при чему исту етикету на VirusTotal платформи даје само Microsoft-ов детектор, док извршни узорци генерисани без нацрта или са вариранim упитима на испитаној машини остају неозначени.

5. Закључак и предлог

Кандидаткиња Наталија Гвозденовић је у свом мастер раду успешно реализовала и евалуирала лабораторијски оквир за мерење LLM-оркестрираног ренсомвер тока и детектабилности његовог извршног облика. Показала је да ране фазе тока код већине модела пролазе, а да се неуспех дешава на синтези исправног кода за шифровање, у зависности од породице модела. Кандидаткиња је исказала самосталност и систематичност у раду, као и способност да релевантне резултате експериментално прикаже и протумачи. На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Наталије Гвозденовић под насловом „Креирање малвера коришћењем великих језичких модела" прихвати као мастер рад и кандидаткињи одобри јавну усмену одбрану.

Београд, 11.09.2026. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 11.09.2026.

Теодора Радаљац Асистент
сагласан, 11.09.2026.