КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 20.08.2024 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Михаило Јовановић под насловом ,,Анализа посредних напада на модул за обезбеђивање поверења у платформу". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Михаило Јовановић је рођен 23.01.2001. године у Крагујевцу. Првих шест разреда основне школе завршио је у ОШ „Драгиша Луковић – Шпанац“, док је седми и осми разред, као и средњу школу, завршио у одељењу обдарених ученика у математичкој гимназији у Првој крагујевачкој гимназији као вуковац. Електротехнички факултет уписао је 2019. године. Дипломирао је на Одсеку за софтверско инжењерство са просечном оценом 8,11. Дипломски рад одбранио је у септембру 2023. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство, уписао је у октобру 2023. године. Положио је све испите са просечном оценом 9,40. Професионално искуство стиче у компанијама SYRMIA, Telesign, OneTrust и Bio Protocol. Суоснивач је стартап компанија Athena AI и Applied Scientific Intelligence, у којој је тренутно руководилац истраживања и бави се развојем модела машинског учења и рачунарских симулација у области рачунарске кардиологије и моделовања електрофизиологије срца. Коаутор је седам истраживачких радова, од којих је један представљен на радионици AI4Science у оквиру конференције ICML 2026 и награђен признањем „Best AI Scientist Award“.

2. Извештај о студијском истраживачком раду

Кандидат Михаило Јовановић је у оквиру припреме за израду мастер рада проучио релевантну литературу из области криптографије, безбедности рачунарских платформи и бочних напада на модуле типа Trusted Platform Module (TPM). Анализирани су развој и архитектура стандарда TPM 1.2 и 2.0, дискретне, интегрисане, фирмверске и виртуелне имплементације, PCR регистри, хијерархије, објекти, политике и формати команди и одговора. Посебно су проучени TIS/FIFO интерфејс и комуникација преко SPI магистрале, као и могућност пасивног издвајања BitLocker VMK кључа током аутоматског откључавања. У оквиру временске анализе проучени су алгоритам ECDSA, утицај кратког nonce-а на трајање потписивања, напад TPMFail, проблем скривеног броја и редукција решетке алгоритмима LLL и BKZ. Размотрени су модели нападача, други физички бочни канали и контрамере, укључујући извршавање у константном времену и шифровање параметара сесије. На основу спецификација припремљен је детерминистички симулатор TPM 2.0 модула, TIS/FIFO интерфејса и SPI магистрале, са пасивним анализатором сигнала и моделом временског канала погодним за поновљиве експерименте.

3. Опис мастер рада

Мастер рад обухвата 62 стране без насловне стране, са укупно 22 слике, 12 табела, 27 исечака кода и 37 референци. Рад садржи увод, пет поглавља и закључак (укупно седам поглавља), списак коришћене литературе, списак скраћеница, спискове слика, табела и исечака кода, као и два прилога са ознакама, упутствима за покретање и параметрима за понављање експеримената.

Прво поглавље образлаже предмет, мотивацију и циљ рада, указује да исправан криптографски алгоритам не гарантује безбедност физичке имплементације и издваја два анализирана канала: трајање ECDSA потписивања и комуникацију дискретног TPM модула преко магистрале.

Друго поглавље приказује развој стандарда TPM, врсте имплементација и случајеве употребе, а затим описује PCR регистре, безбедно подизање система, хијерархије, објекте, политике, TIS/FIFO интерфејс и формат команди стандарда TPM 2.0.

Треће поглавље поставља модел нападача и теоријску основу оба напада. Временски напад повезује ECDSA потпис, кратак nonce, проблем скривеног броја, редукцију решетке и TPMFail, док анализа магистрале обухвата пасивно прислушкивање и пренос BitLocker VMK кључа.

Четврто поглавље описује архитектуру симулатора, његове модуле, TIS/FIFO регистре, SPI пренос, TPM команде и PCR стање, као и аутомат интерфејса, маршалинг пакета, временски модел, поновљивост

симулације и ограничења у односу на стварни хардвер.
Пето поглавље приказује експерименте: временску анализу ECDSA потписа и опоравак приватног P-256 кључа редукцијом решетке, као и реконструкцију приступа регистрима, TPM команди и одговора из SPI сигнала и издвајање VMK кључа из одговора TPM2_Unseal.
Шесто поглавље тумачи практични значај резултата и разматра контрамере: извршавање независно од тајне, шифровање параметара сесије и додатну ауторизацију.
Седмо поглавље сумира доприносе и ограничења симулације и предлаже даљи рад на стварним SPI и временским мерењима TPM уређаја.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Михаила Јовановића бави се анализом временских и магистралних бочних канала код TPM модула. У раду је успешно развијено спецификацијско, детерминистичко in-silico окружење које обухвата TPM 2.0, TIS/FIFO интерфејс и SPI магистралу. Пасивни анализатор реконструише протокол искључиво из сигнала на пиновима, док је интерно стање симулатора употребљено тек за накнадну проверу. У истом окружењу успешно су изведени временски напад TPMFail на ECDSA потписивање и пасивно прислушкивање комуникације при аутоматском откључавању BitLocker-a.
Основни доприноси и резултати рада су: 1) развој поновљивог симулатора пута захтева од фирмвера, преко чипсета и TIS/FIFO регистара, до TPM-a и назад; 2) моделовање временског цурења при ECDSA потписивању и испитивање утицаја Гаусовог мерног шума различите јачине; 3) математичко моделовање вероватноће успешног избора потписа и потврда опоравка кључа из великог скупа мерења чак и при мерном шуму вишеструко јачем од корисног временског сигнала; 4) реконструкција приватног P-256 кључа понављаним избором подскупова и BKZ/LLL редукцијом, уз јавну проверу кандидата из потписа; 5) реконструкција 150 приступа регистрима, 20 комплетних команди и 20 одговора из 46.865 узорака SPI сигнала и издвајање свих 32 бајта VMK-a из успешног одговора TPM2_Unseal; 6) анализа контрамера које обухватају извршавање у константном времену, шифровање параметара TPM сесије, додатну ауторизацију и физичку заштиту магистрале.

5. Закључак и предлог

Кандидат Михаило Јовановић је у свом мастер раду успешно развио и употребио контролисано окружење за анализу два безбедносно значајна бочна канала TPM модула. Експериментално је приказао опоравак приватног P-256 кључа из временских мерења и издвајање целог BitLocker VMK кључа из пасивно снимљене SPI комуникације. Кандидат је исказао самосталност и систематичност у раду, као и способност да сложене криптографске и протоколске механизме имплементира, експериментално провери и критички протумачи.

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Михаила Јовановића под насловом „Анализа посредних напада на модул за обезбеђивање поверења у платформу“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 03.09.2026. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 03.09.2026.

др Жарко Станисављевић Ванредни професор
сагласан, 03.09.2026.

Михајло Огризовић Асистент
сагласан, 03.09.2026.