

# КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 11.09.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Илија Кулић под насловом „Рана атестација сигурне виртуелне машине са подршком за пуну енкрипцију диска“. Након прегледа материјала Комисија подноси следећи

## ИЗВЕШТАЈ

### 1. Биографски подаци кандидата

Илија Кулић је рођен 02.08.2000. у Лозници. Завршио је основну школу „Свети Сава“, а потом уписао гимназију „Вук Караџић“, коју је завршио као вуковац. Електротехнички факултет уписао је 2019. године. Дипломирао је 2023. године на одсеку за Рачунарску технику и информатику са просечном оценом 9.18. Мастер студије на Електротехничком факултету наставља 2023. године на одсеку за Софтверско инжењерство, а такође уписује и мастер студије на Техничком универзитету у Бечу 2024. године, такође на одсеку за Софтверско инжењерство.

### 2. Извештај о студијском истраживачком раду

Кандидат Илија Кулић је као припрему за израду мастер рада урадио истраживање TEE (енг. Trusted Execution Environment) технологија, алата и комерцијалних производа у области сигурног процесирања (енг. Confidential Computing) којој припада тема мастер рада. Конкретно, анализирани су AMD SEV-SNP и TPM технологије, као и open source SNPGuard алат за покретање сигурних виртуелних машина са FDE подршком, који имплементира атестациони протокол који се заснива на AMD SEV-SNP технологији. Анализом овог алата, дефинисана и имплементирана је модификација алата и атестационог протокола, у виду додатне подршке за TPM атестацију, што је главна тема овог рада.

### 3. Опис мастер рада

Мастер рад обухвата 47 страна, са укупно 19 слика, 16 табела и 34 референце. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља) и списак коришћене литературе. Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је проблем сигурности података приликом процесирања у облаку и модел сигурног процесирања. Наведено је потенцијално решење за имплементацију сигурних виртуелних машина употребом TEE технологија и енкрипције диска и дефинисан је циљ рада као истраживање механизма за атестацију сигурних виртуелних машина са подршком за AMD SEV-SNP и TPM TEE технологије.

У другом поглављу је дат генералан опис TEE технологија од којих су детаљно описане AMD SEV-SNP и TPM технологије. Такође описан је и модел напада хипервизора које ове технологије спречавају.

У трећем поглављу су описани различити концепти и open source алати који су употребљени за имплементацију решења у овом раду, као што су: LUKS, initramfs, QEMU и други. Такође описани су и комерцијални производи за сигурно процесирање у понуди великих провајдера услуга у облаку, попут: Microsoft Azure и Amazon AWS.

Четврто поглавље детаљно описује SNPGuard пројекат који је употребљен као темељ за модификацију атестационог протокола, као и саму модификацију алата и изворног кода протокола како би подржао додатну TPM атестацију. Приложени су дијаграми и табеле који приказују и описују кораке приликом извршавања атестационог протокола.

У оквиру петог поглавља дата је дискусија имплементираних модификација атестационог протокола. У оквиру дискусије анализирани су перформансе, ограничења, сигурност имплементираних протокола, као и потенцијална будућа побољшања.

Шесто поглавље је закључак у оквиру кога је резимирано имплементирано решење, његове користи и ограничења и његово место у области сигурног процесирања у облаку.

### 4. Анализа са кључним резултатима

Мастер рад дипл. инж. Илије Кулића се бави проблематиком удаљене атестације сигурне виртуелне машине са подршком за пуну енкрипцију диска. Удаљена атестација има кључну улогу у успостављању поверења у сигурност и интегритет процесираних података на сигурној виртуелној машини, што је од великог значаја код процесирања осетљивих података попут медицинских и финансијских података. Имплементирано решење је тестирано на серверу са хардвером који поседује AMD SEV-SNP функционалности и софтверски емулираном vTPM уређају. Имплементирано решење је такође могуће тестирати на платформи која пружа сигурну имплементацију vTPM уређаја као што је COCONUT SVSM.

Основни доприноси рада су: 1) приказ и методологија имплементације протокола за удаљену атестацију; 2) примена имплементираног протокола на продукционим решењима за сигурно процесирање у облаку; 3) могућност даљег развоја протокола и интеграције са COCONUT SVSM пројектом.

## 5. Закључак и предлог

Кандидат Илија Кулић је у свом мастер раду успешно имплементирао решење за удаљену атестацију сигурне виртуелне машине у виду атестационог протокола, као и алат за покретање сигурних виртуелних машина са подршком за AMD SEV-SNP и vTPM механизме који су развијени као модификација постојећег SNPGuard алата.

Имплементирана модификација пружа додатни ниво сигурности при атестацији сигурне виртуелне машине и заснива се искључиво на open source технологијама.

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. Илије Кулића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 15.10.2025. године

Чланови комисије:

---

др Павле Вулетић Редовни професор  
сагласан, 15.10.2025.

---

Данко Миладиновић Асистент  
сагласан, 15.10.2025.