

МОЛБА

Школска 2024/25. година

ПОДАЦИ О ПОДНОСИОЦУ МОЛБЕ

Презиме:	Врачаревић	Име:	Александар
Е-пошта:	mi211082@alas.matf.bg.ac.rs		
Број индекса:	1082/2021	Статус:	Самофинансирање
Ниво студија:	Мастер академске студије		

Тип: пријава теме мастер рада

Број молбе: m1082/2021-6

Катедра: Катедра за рачунарство и информатику

Примена метода дубоког учења у нападу на криптографске алгоритме споредним каналима

САДРЖАЈ МОЛБЕ:

Значај теме и области:

Криптографски алгоритми у широкој употреби су математички безбедни, међутим, њихово извршавање на физичким уређајима чини их подложним нападима споредним каналима (енг. side channel attacks – SCA). Ови напади користе физичке карактеристике уређаја, као што су потрошња енергије, електромагнетно зрачење и време извршавања, како би открили информације о тајним кључевима који се користе у криптографским операцијама. Иако су први облици ових напада познати од краја двадесетог века, њихова ефикасност се значајно повећала применом метода машинског учења (енг. machine learning). Истраживања у области SCA најчешће користе вишеслојни перцептрон (енг. multi layer perceptron – MLP) и конволутивне неуронске мреже (енг. convolutional neural network – CNN). Развој механизма пажње (енг. attention), посебно у оквиру трансформер модела, показао је потенцијал за побољшање анализе споредних канала.

Специфични циљ рада:

Циљ рада јесте да покаже потенцијал техника метода дубоког учења у анализи споредних канала, посебно кроз архитектуре које интегришу механизме пажње (енг. squeeze-and-excitation, convolutional block attention mechanism примењене на CNN моделе) са класичним приступима као што су MLP и стандардни CNN, користећи јавно доступне скупове података. С обзиром на то да мерење физичких споредних канала подразумева коришћење скупе и неретко тешко доступне опреме, овај рад ће, осим постојећих скупова података, укључити и синтетичке податке генерисане помоћу Unicorn алата за емулацију. Овакав приступ обезбеђује лако доступну и контролисану платформу за експерименте. Додатни циљ рада је приказ практичне примене напада споредним каналима на Zephyr OS апликацију у сценарију деанонимизације корисника Bluetooth уређаја.

Комисија:

1. Ментор: Младен Николић
2. Председник: Јована Ковачевић
3. Члан: Александар Картељ

ПРИЛОЗИ МОЛБИ:

1. образац молбе за одобрење теме мастер рада

Београд, 28. мај 2025.

(потпис)

(Попуњава надлежна особа)

☒ ОДОБРАВА СЕ	29. мај 2025., Мирослав Марић (датум, име, презиме и потпис)
☐ НЕ ОДОБРАВА СЕ	

ОБРАЗЛОЖЕЊЕ: