УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 07.07.2020. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Бранислава Рајића под насловом „Детекција скенирања слабости веб апликација анализом понашања корисника“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Бранислав Рајић је рођен 03.10.1996. године у Београду. Завршио је основну школу „Светозар Милетић" у Београду као ђак генерације. Уписао је Девету гимназију „Михаило Петровић Алас“ у Београду, коју је завршио као одличан ђак. Електротехнички факултет уписао је 2015. године. Дипломирао је у року као студент на Одсеку за рачунарску технику и информатику 2019. године са просечном оценом 8,76. Дипломски рад одбранио је 2019. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу Софтверско инжењерство уписао је у октобру 2019. године. Положио је све испите са просечном оценом 9,80. Запослен је у струци на позицији софтвер инжењера преко годину дана.

2. Опис мастер рада

Мастер рад обухвата 47 страна, са укупно 15 слика, 20 табела и 23 референце. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Уведен је појам алата за динамичко тестирање веб апликација (*DAST – Dynamic application security testing*) и појам детекције упада у системе на основу препознавања аномалија у понашању.

У другом поглављу је дат кратак преглед особина *HTTP* протокола, идентификоване су улазне тачке малициозних интеракција приликом хакерских напада и рањивости које су присутне у модерним веб апликацијама.

У трећем поглављу је најпре приказана архитектура Лабораторије за безбедност Електротехничког факултет у којој су алати за динамичко тестирање покретани, а њихово понашање снимано, као и веб апликација која је била мета симулираних напада. Подробно је анализиран начин функционисања алата и навигација кроз апликацију. Истакнуте су рањивости које *DAST* алати проверавају у фази скенирања, а то је урађено за следеће алате: Nikto, OWASP ZAP, Arachni и Vega. Извештаји које су алати поднели су анализирани ради идентификације лажних узбуна, те су на основу детектованих стварних мањкавости оцењене релевантности испитиваних софтвера.

У четвртом поглављу детаљно је објашњен приступ анализе мрежног саобраћаја на основу статистика мрежних токова на транспортном слоју. Након кратког осврта на најчешће протоколе у употреби, истраживан је приступ Канадског института за сајбер безбедност у генерисању ових особина кроз њихов алат *CICFlowMeter* као и скуп података *CICIDS-2017* намењен истраживању упада у системе.

У петом поглављу су уведени основни појмови машинског учења. Одлучено је да се у експерименталном делу рада користе алгоритми К најближих суседа, метода потпорних

вектора, као и алгоритам случајне шуме. Како би се скуп података допунио бенигним саобраћајем, преузети су подаци из скупа *CICIDS-2017.* Затим је извршено сужавање скупа значајних одлика за детекцију неуобичајеног понашања, те је за сваки од поменутих алгоритама машинског учења обучен модел који са високом прецизношћу детектује интеракције са *DAST* алатима као малициозне. Испитиване су могућности ране детекције, када се класификатори примењују након одређеног броја пакета у току, а пре завршетка тока. На основу ових резултата, предложен је и имплементиран прототип система за детектцију упада у веб апликације, надоградњом постојећих особина *CICFlowMeter* софтвера.

Шесто поглавље је закључак у оквиру кога су сумирани подаци о анализираним *DAST* алатима, уочени проблеми који се јављају у јавно доступним скупу података за детекцију упада *CICIDS-2017,* као и резултати експеримената који су спроведени у овом раду. Описан је значај ових резултата, као и могућа њихова примена за прототип система за детекцију упада.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Бранислава Рајића се бави идентификацијом статистичких особина мрежног саобраћаја које се могу користити за обучавање алгоритама машинског учења ради детекције неуобичајеног понашања приликом интеракције са веб апликацијама. У оквиру рада су симулиране малициозне интеракције које су комбиноване са бенигним интеракцијама из јавно доступног скупа података *CICIDS-2017*. Из скупа одлика мрежних токова на транспортном слоју које генерише софтвер *CICFlowMeter* издвојене су оне које су значајне за класификацију.

Основни доприноси рада су: 1) компаративна анализа алата за динамичко тестирање веб апликација; 2) проналажење кључних одлика за адекватну класификацију мрежног саобраћаја, као и изградња модела који са високом прецизношћу могу да разликују малициозне и бенигне интеракције; 3) имплементација прототипа система за детекцију упада на основу резултата добијених у експерименталном делу рада.

4. Закључак и предлог

Кандидат Бранислав Рајић је у свом мастер раду развио методологију за детекцију припремних фаза напада на веб апликације кроз коришћење алгоритама машинског учења произвевши моделе који могу са високом прецизношћу да детектују малициозиозна скенирања веб апликација.

Кандидат је исказао самосталност и систематичност у свом поступку.

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Бранислава Рајића под насловом „Детекција скенирања слабости веб апликација анализом понашања корисника“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 29.1.2021. године

Чланови комисије:

Др Павле Вулетић, ванредни професор

Др Жарко Станисављевић, ванредни професор