**КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ**

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 04.06.2024. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Богдана Тепавчевића под насловом „Практична анализа безбедности IoT уређаја". Након прегледа материјала Комисија подноси следећи

**И З В Е Ш Т А Ј**

**1. Биографски подаци кандидата**

Богдан Тепавчевић је рођен 14.09.1998. године у Зрењанину. Завршио је основну школу „2. октобар" у Зрењанину као носилац дипломе „Вук Караџић" и ђак генерације. Уписао је Зрењанинску гимназију коју је завршио са одличним успехом. Током школовања освојио је више награда из математике и физике. Електротехнички факултет уписао је 2017. године. Дипломирао је 2022. године на одсеку за Телекомуникације и информационе технологије са просечном оценом 7,63. Дипломски рад под називом „Имплементација и анализа рада *First Hop Redundancy* протокола" је одбранио у септембру 2022. године са оценом 10. Дипломске академске-мастер студије на Електротехничком факултету, на модулу Информационо комуникационе технологије, уписао је у октобру 2022. године, Положио је све испите са просечном оценом 9,20. Тренутно запослен у компанији *Coming-Computer Engineering,* на радном месту *Cybersecurity engineer*.

**2. Извештај о студијском истраживачком раду**

Кандидат Богдан Тепавчевић је као припрему за израду мастер рада урадио истраживање релевантне литературе о безбедности IoT (*Internet of Things*) уређаја. Конкретно, од интереса је био преглед препорука најбоље праксе (*best practices*) института који делују на пољу информационе безбедности, у циљу што боље припреме за практичну анализу. Истраживањем области утврђена је систематичност у анализи безбедности, која је касније примењена на практичан рад. Практична рад се заснива на тестирању безбедности неких од уређаја доступних на тржишту, као и анализи утицаја коју компромитовање IoT уређаја има на остале елементе екосистема.

**3. Опис мастер рада**

Мастер рад обухвата 53 стране, са укупно 29 слика, 4 табеле и 32 референце. Рад садржи увод, 5 поглавља и закључак (укупно 7 поглавља) и списак коришћене литературе.

Увод представља предмет рада, као и опис поглавља.

У првом поглављу је дат кратак преглед појма и примене IoT уређаја. Наведени су примери области у којима се технологија користи.

У другом поглављу су детаљно представљени најпознатији напади на IoT системе, као што су *Mirai Botnet* и *Stuxnet*.

Треће поглавље детаљно описује више паралелних архитектура IoT уређаја, које су настајале по узору на TCP/IP, али прилагођених новим парадигмама које IoT технологија доноси. Такође, у оквиру овог поглавља обрађени су неки од протокола који имају могућност интеграције са TCP/IP слојевима.

У оквиру четвртог поглавља дат је приказ модела за IoT безбедност установљен на основу најбољих пракси *IoT Security Foundation Best Practices*, анализиран је OWASP модел који наводи 10 најпознатијих рањивости. Такође, кроз *MITTRE ATT&K Enterprise* модел

приказани су кораци које нападач спроводи како би напад спровео у дело, од истраживања о жртви, преко упада у систем, па до малициозних радњи на систему.

Пето поглавље је практична анализа рањивости уређаја и утицај њиховог компромитовања на окружење, разматран кроз архитектуру кућног (*home*) и пословног (*office*) екосистема. Након тога дате су препоруке за побољшање безбедности.

Шесто поглавље представља закључак у оквиру кога је описан значај безбедности као и тенденције које доводе до рањивих система и које мере предузети за ојачавање сигурности.

**4. Анализа рада са кључним резултатима**

Мастер рад дипл. инж. Богдана Тепавчевића се бави проблемом рањивости IoT уређаја. Данас је тржиште преплављено мноштвом IoT уређаја који су повезани на Интернет, а имају ограничене хардверске перформансе или неадекватно имплементиран TCP/IP (*Transmission Control Protocol/Internet Protocol*) протоколски стек. То је довело до неких од најпознатијих напада, који су узроковали немерљиву штету. У раду је спроведена практична анализа безбедности IoT уређаја који су повезани на Интернет и дате су препоруке којима је могуће смањити рањивости или бар њихову изложеност, како би целокупни систем био сигурнији. Анализа је спроведена на примерима две практичне архитектуре: кућно окружење (*home environment*) и пословно, канцеларијско окружење (*office environment*). У сврху тестирања уређаја коришћен је *Kali Linux*, *Linux* дистрибуција једнако распрострањена међу малициозним корисницима, као и лицима задуженим за сајбер безбедност. Анализирани су начини комуникације уређаја, отворени мрежни портови и оперативни систем.

Основни доприноси рада су:

1) Практичан приказ анализе безбедности неких од уређаја на тржишту,
2) Анализа неких од критичних рањивости уређаја, као и последице које могу да нанесу систему,
3) Препоруке којима би систем могао да се заштити.

**5. Закључак и предлог**

Кандидат Богдан Тепавчевић је у свом мастер раду успешно анализирао проблем рањивости IoT уређаја и спровео практичну анализу на примерима две практичне архитектуре: кућно окружење и пословно/канцеларијско окружење. Поред тога, дао је и препоруке за побољшање безбедности система које могу значајно да унапреде сигурност.

Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у практичној анализи и решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Богдана Тепавчевића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 13.09.2024. године

Чланови комисије:

_____
Др Младен Копривица, доцент

_____
Др Горан Марковић,
ванредни професор