КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 10.09.2024. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Славиша Блешић под насловом „**Детекција и превенција MITM напада у паметном кућном систему користећи енкриптован MQTT протокол** ”. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Славиша Блешић је рођен 06.02.1996. године у Београду. Завршио је основну школу „Краљ Петар Први” у Београду као одличан ђак. Уписао је Електротехничку школу „Никола Тесла” у Београду и коју је завршио са одличним успехом. Током школовања освојио је више првих награда на разним такмичењима из информатике. Електротехнички факултет уписао је 2015. године. Дипломирао је на одсеку за Електронику 2021. године. Дипломски рад одбранио је у септембру 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за електронику и дигиталне системе уписао је у октобру 2022. године.

2. Извештај о студијском истраживачком раду

Кандидат Славиша Блешић као припрему за израду мастер рада урадио је истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирана су постојећа решења и проблеми у области MITM напада, енкрипције у MQTT протоколима и сигурносних изазова у IoT системима. Истраживањем области утврђено је да се постиже најбоља заштита уколико се користе ChaCha20 енкрипција и Diffie-Hellman алгоритам за размену кључева. Сагледане су предности и мане различитих енкрипционих метода и изнети су закључци на основу добијених резултата.

3. Опис мастер рада

Мастер рад обухвата 49 страна, са укупно 11 слика и 5 референци. Рад садржи увод, 7 поглавља и закључак (укупно 7 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. У овом поглављу су изнесене и анализиране кључне информације о безбедности у IoT системима, са посебним фокусом на MQTT протокол.

У другом поглављу је описана теоријска основа MITM (Man-in-the-Middle) напада, укључујући различите методе напада као што су ARP spoofing и DNS spoofing. Дато је детаљно објашњење механизама који нападачима омогућавају да пресрећу и модификују комуникацију у паметним кућним системима.

Треће поглавље обрађује MQTT протокол, описујући његову архитектуру, функционалности и слабости које га чине рањивим на MITM нападе. Додатно, анализирани су сценарији који укључују пресретање података између уређаја у паметним кућама.

Четврто поглавље представља детаљну анализу симулације MITM напада у стварном IoT окружењу. Приказан је пример како се изводи ARP spoofing напад на систему који користи MQTT протокол за комуникацију између сензора и контролера.

Пето поглавље говори о мерама заштите од MITM напада. Објашњене су технике енкрипције и аутентификације као што су ChaCha20 и Diffie-Hellman размена кључева. Такође, приказана је имплементација ових механизама у Python програмском језику.

Шесто поглавље је закључак, где су сумирани добијени резултати и понуђене препоруке за унапређење сигурности паметних кућних система који користе MQTT протокол.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Славише Блешића се бави проблематиком детекције и превенције MITM напада у паметним кућним системима користећи енкриптован MQTT протокол. Поред детаљног објашњења Man-in-the-Middle (MITM) напада, анализирани су проблеми који се јављају у комуникацији IoT уређаја у паметним кућама, где је MQTT протокол подложан пресретању и манипулацији података. Дат је преглед могућности сигурносних алата и техника за заштиту MQTT комуникације, као што су ChaCha20 енкрипција и Diffie-Hellman размена кључева. Реализација је илустрована симулацијом MITM напада на локално постављеној IoT мрежи.

Основни доприноси рада су: 1) Објашњење проблематике MITM напада у MQTT протоколу у контексту IoT уређаја; 2) Приказ и методологија заштите MQTT комуникације употребом енкрипције и аутентификације; 3) Илустрација симулације MITM напада и мере заштите кроз примену ChaCha20 алгоритма и Diffie-Hellman размене кључева.

5. Закључак и предлог

Кандидат Славиша Блешић је у свом мастер размотрио проблематику MITM напада у MQTT протоколу у контексту IoT уређаја и приказао методологију заштите MQTT комуникације употребом енкрипције и аутентификације. У раду је успешно решио проблем примене ChaCha20 алгоритма и Diffie-Hellman размене кључева којим се реализује заштита MQTT комуникације.

Кандидат је исказао самосталност и систематичност, као и практичне имплементационе елементе у решавању проблематике овог рада.

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

Београд, 13. 09. 2022. године

Чланови комисије:

Др Милан Поњавић, редовни професор

Др Владимир Рајовић, ванредни професор