КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 3.9.2024. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Драгана Мањић под насловом „Имплементација клијента за аутоматско управљање дигиталним сертификатима веб сервера". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Драгана Мањић је рођена 10.8.1999. године у Чачку. Завршила је основну школу "Иво Андрић" у Прањанима као вуковац. У Гимназији у Чачку је такође била вуковац. Електротехнички факултет је уписала 2018. године. Дипломирала је на одсеку за Рачунарску технику и информатику 2022. године са просечном оценом 7,6. Дипломски рад је одбранила у септембру 2022. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство, је уписала у октобру 2022. године. Положила је све испите са просечном оценом 8,00.

2. Извештај о студијском истраживачком раду

Кандидат Драгана Мањић је урадила истраживање релевантне литературе која се односи на проблем успостављања дигиталних сертификата на веб серверима, те нови протокол аутоматског управљања дигиталним сертификатима (енг. *Automatic Certificate Management Environment,* ACME) дефинисан у RFC 8555. Урађено је детаљно истраживање овог протокола, његов значај и допринос, а затим и анализа начина на који протокол функционише, процеса које подржава, од којих се компоненти састоји, како су оне међусобно повезане, као и који су расположиви алати за формирање тестних и продукционих окружења.

3. Опис мастер рада

Мастер рад обухвата 44 стране, са укупно 28 слика и 40 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља) и списак коришћене литературе, списак скраћеница и списак слика.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је проблем аутоматизованог додељивања дигиталних сертификата за веб сервере, а тиме и значај ACME протокола, као протокола за аутоматизацију овог процеса.

У другом поглављу је дат генерални увод о дигиталним сертификатима, те је дат њихов начин рада и употреба. Такође су наведене врсте сертификата које постоје.

У трећем поглављу су детаљно анализирани процеси ACME протокола. Објашњене су функционалности протокола као што су начин преноса порука, начин управљања сертификатима, процес њиховог издавања и провера ауторизације. Приказане су и могуће претње за ACME протокол и могуће сигурносне мане.

Четврто поглавље детаљно описује реализовану имплементацију ACME клијента и његову архитектуру. Објашњено је потребно окружење и компоненте неопходне за рад клијента, као што је постојање ACME сервера на локалу. Како се у раду користе и други сервери, приказани су дијаграми који објашњавају ток комуникације учесника у ACME протоколу. Затим је изложена детаљна анализа имплементације сваког од помоћних сервера,

док кључни део представља опис имплементације клијента. Сам клијент има скуп функција за његову иницијализацију, за рад са криптографским кључевима, са сертификатима и за реализацију ACME протокола. Све поменуте групе функција су детаљно описане.

У оквиру петог поглавља је представљена демонстрација рада клијента. Све описане функционалности ACME клијента из четвртог поглавља су овде сумиране кроз пример функционисања и тока извршавања клијента на основу одређене улазне команде. Такође су приказане и поруке које клијент и сервер размењују током процеса издавања сертификата.

Шесто поглавље је закључак у оквиру кога су резимирани резултати рада. Описан је значај ACME протокола и уопштено информационе безбедности.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Драгане Мићић се бави унапређењем једног од фундаменталних механизама којима се данас реализује сигурност интернет услуга – доделом серверских сертификата веб сервера. Кључни део рада представља имплементацију ACME клијента за аутоматизацију овог процеса и детаљну анализу функционисања реализоване имплементације. Основни доприноси рада су: детаљна анализа постојећег ACME протокола и његов значај и утицај на коришћење протокола HTTPS на интернету; један пример имплементације ACME клијента који приказује како је могуће практично применити описани протокол и искористити протокол у циљу унапређења сигурности на интернету.

5. Закључак и предлог

Кандидат Драгана Мићић је у свом мастер раду успешно представила имплементацију ACME клијента и анализу процеса и технологија везаних за издавање и управљање дигиталним сертификатима веб сервера. Предложено решење може значајно да унапреди методе заштите интернет сервера и корисника, омогућавајући аутоматизовано управљање сертификатима и правовремени одговор на безбедносне инциденте.

Кандидат Драгана Мићић је исказала 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. Драгана Мићић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 12.09.2024. године

Чланови комисије:

_____

др Павле Вулетић, в. проф.

_____

Др Жарко Станисављевић, в. проф.