КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 26.11.2024. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Александра Стефанова, дипл. инж. Електротехнике и рачунарства, под насловом „Апликација за аутентификацију порука коришћењем алгоритма AES-CMAC“. Након прегледа материјала комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Александар Стефанов је рођен 09.03.2000. године у Панчеву. Завршио је основну школу „Јован Јовановић Змај” у Панчеву као вуковац. Уписао је гимназију „Урош Предић“ у Панчеву и коју је завршио са одличним успехом. Електротехнички факултет уписао је 2018. године. Дипломирао је као студент на одсеку за Телекомуникације и информационе технологије 2018. године са просечном оценом 7,92. Дипломски рад одбранио је у септембру 2023. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за Информационо комуникационе технологије уписао је у октобру 2023. године. Положио је све испите са просечном оценом 10.

2. Извештај о студијском истраживачком раду

Кандидат Александар Стефанов је у оквиру припреме за рад на својој мастер тези проучио AES и MAC алгоритме, модове рада AES алгоритма, као и спецификацију алгоритма AES-CMAC који је требао да се реализује у оквиру тезе. Пошто је циљ тезе била софтверска имплементација апликације за размену порука која користи AES-CMAC алгоритам, Александар је истражио који алати и програмски језици су адекватни за израду апликације, а на основу претходно дефинисаног концепта рада апликације. За реализацију апликације изабран је рад у Django радном оквиру, па је Александар детаљније проучио и продубио своје познавање овог радног оквира. Након обављеног студијског истраживачког рада, Александар је приступио изради своје мастер тезе.

3. Опис мастер рада

Мастер рад обухвата 60 страна, са укупно 78 слика, 1 табелом и 15 референци. Рад садржи увод, 4 поглавља, закључак (укупно 6 поглавља), списак коришћене литературе, списак слика и списак табела.

Предмет рада представља имплементацију апликације за размену и аутентификацију порука, при чему се за аутентификацију користи AES-CMAC алгоритам. У оквиру реализације је коришћен Django радни оквир и Python програмски језик. У оквиру тезе је детаљно описан програмски код апликације, као и употреба апликације и њене могућности.

У уводном поглављу је истакнут значај размене података и сигурности комуникације, са посебним нагласком на компоненту аутентификације која је предмет тезе. Потом је изложена структура остатка тезе по поглављима.

Друго поглавље садржи теоретске основе коришћеног AES-CMAC алгоритма. У оквиру овог поглавља, дат је детаљан опис самог AES алгоритма и његових основних функција. Потом је дат опис CMAC алгоритма, и поређење са сличним CBC-MAC алгоритмом.

Треће поглавље даје веома детаљан опис програмског кода апликације. Изложена је комплетна архитектура апликације. Наведени су фајлови у стаблу пројекта са њиховим

улогама и коментарима њиховог садржаја. Потом су детаљно описани кодови *backend* и *frontend* делова апликације.

Четврто поглавље садржи опис рада апликације, као и упутство како се користи апликација. Дати су примери успешне и неуспешне аутентификације порука, а показана је и размена порука између рачунара и мобилног телефона употребом реализоване апликације.

У петом поглављу је приказан рад апликације у виртуелном окружењу, између две виртуелне машине. Ово поглавље даје основу за једноставно и сигурно окружење за тестирање и испитивање сигурносних аспеката реализоване апликације, али и других сличних апликација, као и за даљи развој.

Шесто поглавље представља закључак који резимира резултате мастер тезе наводећи смернице за евентаулна будућа унапређења апликације. Потом су дати списак референци, списак слика и списак табела.

4. Анализа рада са кључним резултатима

Мастер рад Александра Стефанова, дипл. инж. Електротехнике и рачунарства, се бави имплементацијом апликације за размену и аутентификацију порука помоћу AES-CMAC алгоритма. Кључни доприноси рада кандидата на тези су следећи:

1) реализована софтверска апликација за размену и аутентификацију порука;
2) детаљно објашњен програмски код апликације;
3) креирано виртуелно окружење за једноставно тестирање и будући развој апликације.

5. Закључак и предлог

Кандидат Александар Стефанов, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно реализовао апликацију за размену и аутентификацију порука помоћу AES-CMAC алгоритма. Демонстриран је рад апликације и за успешну и неуспешну аутентификацију порука, а дате су и смернице за будућа унапређења апликације. Александар је показао да је способан да осмисли дизајн и архитектуру апликације и потом на основу осмишљеног концепта да успешно реализује софтверско решење. Током рада на тези, Александар је показао да веома успешно и ефикасно решава изазове и проблеме са којима се сусретао током развоја апликације. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата за размену и аутентификацију порука помоћу AES-CMAC алгоритма, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 26.12.2024. године

Чланови комисије:

др Зоран Чича, ред. професор

др Дејан Драјић, ред. професор