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. Татјане Милојевић под насловом „Анализа безбедности у LoRaWAN мрежама". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Татјана Милојевић је рођена 10.02.1996. године у Лазаревцу. Завршила је основну школу „Милорад Лабудовић Лабуд" у Барошевцу, као ђак генерације. Уписала је Гимназију у Лазаревцу, коју је завршила као вуковац. Електротехнички факултет уписала је 2015. године. Дипломирала је 2021. године са просечном оценом 7,76. Дипломски рад под називом „Практична имплементација VLAN *Trunking* протокола" одбранила је у јануару 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за Информационо комуникационе технологије уписала је у октобру 2021. године. Положила је све испите са просечном оценом 8,40. Од 2020. године запослена је у компанији "Dotnetworks d.o.o", на позицији инжењер пројектант у оквиру службе за пројектовање приступних мрежа.

2. Извештај о студијском истраживачком раду

Кандидат Татјана Милојевић је као припрему за израду мастер рада урадила истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирана су постојећа решења и проблеми у оквиру безбедности у LoRaWAN (*Long Range Wide Area Network*) мрежама.

Анализом релевантне литературе утврђено је да је безбедност у LoRaWAN мрежама обезбеђена на нивоу мреже и апликације, употребом стандардизованих AES криптографских алгоритама, као и употребом кључева сесије за шифровање и аутентификацију података.

Анализом решења је утврђено да је развој нових верзија LoRaWAN протокола значајно допринео унапређењу безбедности, нарочито у погледу руковања кључевима и активирања уређаја. Ово истраживање је такође показало да постоје одређене слабости у оквиру безбедности које би потенцијално могле бити искоришћене од стране нападача у различитим врстама напада које могу угрозити интегритет, поверљивост и доступност мреже. Ипак, уз одређена побољшања безбедности у погледу управљања кључевима и сигурносних механизама, LoRaWAN протокол представља перспективно решење за обезбеђивање безбедне комуникације у IoT (*Internet of Things*) апликацијама.

3. Опис мастер рада

Мастер рад обухвата 57 страна, са укупно 29 слика, 1 табелом и 16 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља) и списак коришћене литературе.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је значај IoT концепта у савременом начину живота као и LPWAN (*Low Power Wide Area Network*), водећа IoT технологија која је у могућности да одговори високим захтевима у погледу робусности, скалабилности и енергетске ефикасности мреже које IoT поставља.

У другом поглављу рада је описана кратка, уводна историја LPWAN технологије, као и разлози зашто је ова технологија у погледу примене у оквиру IoT апликација стекла предност наспрам традиционалних бежичних комуникационих технологија. Поред најпознатије LoRaWAN технологије, ово поглавље даје кратак преглед осталих LPWAN технологија: LTE-M, NB-IoT и Sigfox технологије чиме је дат увод у LoRaWAN.

У трећем поглављу је дат опис LoRaWAN технологије. Најпре је дат опис физичког слоја, јединствене модулационе технике као и фреквенцијских опсега који се користе. У наставку поглавља дат је кратак хронолошки преглед развоја LoRaWAN протокола од стране LoRa алијансе и најзначајнијих побољшања које су нове верзије донеле. Затим је дат преглед архитектуре LoRaWAN мреже у зависности од тога која је верзија протокола имплементирана као и преглед уређаја који се користе у мрежи и формата порука који се преносе на *uplink*-у *downlink*-у. За крај овог поглавља дат је преглед широког спектра најпознатијих примена LoRaWAN-а у оквиру IoT апликација.

Четврто поглавље детаљно описује механизме за остваривање безбедности који се користе у оквиру LoRaWAN технологије. Посебан акценат стављен је на процесе персонализације и активације уређаја, пошто су ово процеси у оквиру којих се додељују потребни параметри безбедности. Дат је детаљан опис два метода активације уређаја, *Over-The-Air-Activation* (OTAA) и активација персонализацијом (ABP - *Authentication By Personalisation*), процеса помоћу којих се уређај придружује мрежи и стиче кључеве сесије, најзначајније параметре безбедности. Пошто се ови процеси разликују у зависности од тога која верзија LoRaWAN протокола је имплементирана, дат је опис и поређење за сваку од верзија. Како су у реалности уређаји који користе различите верзије протокола принуђени да коегзистирају и неопходно је да буду компатибилни, дат је опис два сценарија у којима различити уређаји који се користе у мрежи припадају различитим верзијама протокола и њиховог понашања у овим ситуацијама. На крају овог поглавља је дат преглед потенцијалних слабости безбедносних параметара које користе уређаји и до чега може довести уколико су поузданост и интегритет ових параметара компромитовани, као и преглед циљева безбедности које има LoRaWAN мрежа. Ове слабости представљају увод у конкретне нападе који се могу десити у реалности у оквиру LoRaWAN мрежа.

У оквиру петог поглавља су описани најпознатији напади на доступност, поверљивост и интегритет LoRaWAN мрежа. Описани су начин на који долази до ових напада и слабости протокола које доводе до следећих напада: MITM (*Mai in the Midle*) напад, напад поновне репродукције порука, напад лажирања потврде пријема, напад прислушкивања, ометања и напад промене бита. Осим описа на који начин долази до ових напада и на који начин их нападачи могу спровести, предложене су и одређене контра мере које се могу спровести у оквиру мреже како би се ови напади избегли или како би се ублажио њихов утицај на безбедност мреже.

Шесто поглавље је закључак у оквиру кога је дата рекапитулација претходних поглавља и описан значај спроведене анализе безбедности за тренутне примене LoRaWAN технологије у оквиру IoT апликација али и будућност IoT-а јер су безбедна и поуздана комуникација у оквиру IoT-а основа иновација и друштвеног напретка.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Татјане Милојевић се бави питањем безбедности у LoRaWAN мрежама, са посебним осврtом на унапређење механизама за заштиту података и аутентификацију уређаја у различитим применама у оквиру IoT-а. LoRaWAN технологија, због својих могућности да обезбеди комуникацију великом броју уређаја, на великим удаљеностима и уз ниску потрошњу енергије, налази широку примену у различитим IoT апликацијама где су сигурност и интегритет података од огромног значаја.

У оквиру овог рада, анализирани су постојећи безбедносни механизми LoRaWAN протокола и идентификоване су њихове предности али и слабости које могу бити

искоришћене у различитим врстама напада који могу угрозити интегритет, поверљивост и доступност мреже. Посебан акценат је стављен на унапређење сигурности кроз примену нових криптографских техника и оптимизацију процеса активације уређаја.

Основни доприноси рада су:

1) анализа безбедносних аспеката LoRaWAN мрежа;

2) предлагање мера за побољшање заштите података и аутентификације уређаја у IoT апликацијама;

3) сагледавање могућности имплементације предложених мера у реалним LoRaWAN мрежама у различитим IoT сценаријима.

5. Закључак и предлог

Кандидат Татјана Милојевић је у свом мастер раду успешно анализирала питање безбедности у LoRaWAN мрежама и предложила решења за побољшање заштите података и аутентификације уређаја у IoT окружењима. Предложене мере могу значајно да унапреде сигурност LoRaWAN мреже и омогуће поузданију примену у различитим IoT апликацијама.

Кандидаткиња је исказала самосталност и систематичност у своме приступу, као и иновативне елементе у решавању комплексних проблема безбедности.

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

Београд, 12.09.2024. године

Чланови комисије:

Др Младен Копривица, доцент

Др Горан Марковић, ванредни професор