Катедри за рачунарство и информатику
Математичког факултета
Универзитета у Београду

Извештај о прегледу мастер рада Јелене Тодоровић

Одлуком Катедре за рачунарство и информатику и Наставно-научног већа Математичког факултета (на Седници ННВ одржаној 24.06.2016) именовани смо за чланове Комисије за преглед и одбрану мастер рада

Реализација сервиса за издавање дигиталних сертификата и протокола за проверу валидности издатих сертификата

кандидата Јелене Тодоровић, студента мастер академских студија Математичког факултета Универзитета у Београду.

У раду се проучава слој сигурних сокета (Secure Socket Layer - SSL) који представља сигурносни протокол за комуникацију на интернету, инфраструктура јавних кључева (Public Key Infrastructure - PKI) која је неопходна за успешно функционисање SSL-а, као и ентитети ауторизовани за издавање дигиталних сертификата (Certification Authority - CA).

Имајући у виду степен коришћења интернет комуникације, проблем безбедности интернет комуникације постаје изузетно значајан. Данас већина веб сервера и веб прегледача подржава SSL као де факто, стандард безбедне комуникације између клијента и сервера. За успешно коришћење SSL-а, потребно је успоставити PKI. Инфраструктура јавних кључева има велики значај при чувању поверљивих информација, као и за обезбеђивање свих потребних алата при заштити електронског пословања. Да би инфраструктура била функционална, неопходно је да буду оперативни ентитети ауторизовани за издавање дигиталних сертификата.

Поред прегледа система PKI, сертификационог тела и његовог начина функционисања, у раду су приказане и криптографске методе за шифровање, очување интегритета података и проверу идентитета.

Приликом израде овог мастер рада, осмишљен је и развијен софтвер, који реализује обављање операција сертификационог тела. За реализацију сертификационог тела коришћен је алат командне линије OpenSSL, који омогућава извршавање криптографских функција. Развијени софтвер подржава процесе издавања, повлачења и провере валидности дигиталних сертификата, као и управљање дигиталним сертификатима у смислу повлачења сертификата и могућности провере њихове валидности.

Извршена је анализа активности приликом рада са сертификатима на основу које је касније сам процес имплементиран. По извршеној анализи, моделована је база података, чија структура подржава захтеве саме апликације. Приликом развоја и имплементације се водило рачуна о томе да се касније могу додавати нове функционалности нпр. издавање корисничких сертификата као и увођење привилегија корисницима овог веб сервиса. Сам софтвер је имплементиран коришћењем Јава технологија (JavaEE и оквир за развој Spring) уз примену обрасца дизајна „модел-поглед-контролер“ (MVC).

Рад чини седам поглавља (Увод, Криптографија, Инфраструктура са јавним кључевима, Реализација сертификационог тела, Примена дигиталних сертификата, Закључак и Литература), иза којих следи списак скраћеница и списак слика. У првом поглављу се описује проблем који се проучава и дају уводне напомене. Друго поглавље садржи опис криптографске основе – симетричне и асиметричне шифарске системе, хеш функције и дигиталне потписе, као и сам протокол SSL. Треће поглавље садржи опис инфраструктуре јавних кључева, њених елемената и архитектуре. У поглављу које потом следи, описани су важни аспекти реализације сертификационог тела: архитектура ситема, технологије које се користе, структура базе података, употреба алата OpenSSL

(припрема окружења, креирање корених кључева и сертификата, креирање кључева и сертификата средњег слоја, генерисање серверских сертификата и повлачење сертификата), као и реализација протокола OCSP за проверу валидности сертификата. Пето поглавље се односи на примену електронских сертификата у домену електронске трговине, електронског пословања и интеренета ствари. Шесто садржи закључна разматрања. Седмо поглавље садржи списак коришћене литературе (списак са 10 референци). Рад садржи укупно 47 страна.

Рад садржи квалитетан приказ релевантних појмова, техника и радова из домена проучавања, који су пажљиво илустровани погодним примерима.

Закључак

Увидом у финални текст рада дошли смо до закључка да је рад квалитетно написан, да је кандидат јасно приказао изложену проблематику од основних појмова, до њихове креативне и технолошке примене. Рад „Реализација сервиса за издавање дигиталних сертификата и протокола за проверу валидности издатих сертификата“ у потпуности задовољава захтеве који се постављају у изради мастер рада и предлажемо да се одобри његова јавна одбрана.

др Владимир Филиповић, ванр. проф

др Душан Тошић, ред. проф.

др Миодраг Живковић, ред. проф.