УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 16.05.2017. године, именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Богдана Бошњака под насловом „Визуелна репрезентација МД5 хеш алгоритма и анализа напада на алгоритам“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Богдан Бошњак је рођен 15.06.1991. године у Београду. Гимназију је завршио у Београду са одличним успехом. Електротехнички факултет у Београду уписао је 2010. године, а дипломирао је у априлу 2015. године са просечном оценом на испитима 7,91, на дипломском 10. Мастер студије на Електротехничком факултету у Београду је уписао у септембру 2015. на Модулу за рачунарску технику и информатику. Положио је све испите са просечном оценом 9,20.

2. Опис мастер рада

Мастер рад обухвата 63 стране, са укупно 46 слика, 21 табелом и 16 референци. Рад садржи увод, 4 централна поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Објашњен је појам криптографских хеш функција, као и проблеми који доводе до потенцијалних напада на ове функције и дат је кратак преглед осталих поглавља рада.

У другом поглављу описан је начин рада МД5 алгоритма. Објашњени су сви кораци који постоје у алгоритму коришћењем блоковских дијаграма. Затим је дат пример једне улазне поруке и детаљно је описан сваки од корака кроз који та порука пролази да би се добио резултат рада алгоритма, тј. излазна хеш вредност. У оквиру одабраног примера дате су конкретне вредности израчунавања сваке операције у сваком кораку алгоритма.

У трећем поглављу објашњена је проблематика напада на МД5 алгоритам. Најпре је дат преглед историје познатих напада на алгоритам. Затим су наведене математичке теореме и операције потребне за анализу напада. На крају су приказани резултати једног познатог напада на алгоритам. У овом поглављу су још и представљене неке од техника модификација порука како би се испоштовали потребни услови које поруке морају задовољити да би произвеле исту вредност хеш функције.

У четвртом поглављу приказан је опис могућности реализованог система са детаљним описима сваке од функционалности које реализовани систем поседује. У склопу овог поглавља приказано је и неколико карактеристичних примера коришћења реализованог система.

У петом поглављу је дат детаљан опис имплементације реализованог решења. Имплементација је посматрана из три аспекта: алгоритма, графичког приказа и напада на алгоритам. Приликом објашњења коришћени су дијаграми секвенце најважнијих делова кода

и детаљно разматране неке од најважнијих пројектних одлука које су донесене како на почетку тако и за време израде самог решења.

У закључку (поглавље 6) дат је критички осврт на све што је урађено у оквиру рада и реализованог решења. Наведени су и предлози за будућа унапређења и проширења реализованог система.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Богдана Бошњака се бави проблематиком криптографских хеш функција и напада на исте. Криптографске хеш функције имају веома широку примену у различитим савременим сигурносним механизмима. Саме функције су најчешће веома комплексне и укључују велики број итерација и велики број различитих операција над подацима, па разумевање рада ових функција није једноставно. Из тог разлога је добро да постоји софтверски систем који омогућава приказ рада МД5 алгоритма са конкретним вредностима. Са друге стране МД5 је један од алгоритама који више није у употреби због успешних напада који се могу извести на овај алгоритам. Управо анализа познатих напада на овај алгоритам помаже да се схвати шта подразумева сигурност криптографских хеш функција.

Главни допринос рада представља софтверски систем за визуелну репрезентацију МД5 алгоритма. Систем има могућност уноса једне или две поруке упоредо, аутоматизовано обављање припремних радњи за извршавање алгоритма, извршавање самог алгоритма и приказ детаља извршавања свих корака алгоритма, као и могућност снимања резултата извршавања алгоритма у фајл што је погодно за каснију анализу.

У раду је извршена и анализа напада на МД5 алгоритам, а захваљујући могућности рада са две поруке у паралели у реализованом систему могу се видети упоредни резултати рада и разлике у резултатима, на пример за две поруке које дају исту хеш вредност.

4. Закључак и предлог

Кандидат Богдан Бошњак је у свом мастер раду успешно представио и анализирао рад МД5 хеш алгоритма и техника које се користе за напад на алгоритам. У оквиру рада кандидат је и успешно реализовао софтверски систем за визуелну репрезентацију МД5 алгоритма. Имплементирани софтверски систем се може применити као помоћно средство у едукацији, како за боље упознавање са начином рада алгоритма, тако и за разумевање недостатака алгоритма који су довели до избацивања алгоритма из практичне употребе.

На основу горе наведеног Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да прихвати рад „Визуелна репрезентација МД5 хеш алгоритма и анализа напада на алгоритам“ дипл. инж. Богдана Бошњака као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 18. 08. 2017. године

Чланови комисије:

Др Жарко Станисављевић, доцент

Др Павле Вулетић, доцент