УНИВЕРЗИТЕТ СИНГИДУНУМ
Департман за последипломске студије
Данијелова 32, Београд

ВЕЋУ ДЕПАРТМАНА ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ

Одлуком Већа Департмана за последипломске студије број 4 – 210-1/2019 од 02.11.2019. године, одређени смо за чланове Комисије за оцену и одбрану докторске дисертације кандидата Александра Мишковића, мастер, под називом "Унапређење протокола за размену кључева на бази личних идентификационих докумената пошиљаоца и примаоца", о чему подносимо следећи

И З В Е Ш Т А Ј

1. Основни подаци о кандидату и докторској дисертацији

Кандидат Александар Мишковић рођен је 03.12.1973. године у Крагујевцу. Звање дипломирани машински инжењер стекао је на Машинском факултету у Крагујевцу 2007. године. Докторске академске студије на студијском програму Напредни системи заштите, Универзитета Сингидунум, уписао је школске 2010/2011. године. Све испите предвиђене планом и програмом докторских студија је положио с просечном оценом 10 (десет) до 24.04.2013. године. Захтев за одобравање теме за израду докторске дисертације поднео је 2017. године.

Своју професионалну каријеру започео је новембра 2006. године у Високој техничкој школи струковних студија из Крагујевца као Стручни сарадник (асистент у настави за информатичку групу предмета и систем администратор).

Од фебруара 2009. године запослен је на неодређено радно време у Високој техничкој школи струковних студија из Крагујевца као Стручни сарадник (асистент у настави за информатичку групу предмета и систем инжењер информационих система и технологија).

Ангажовање Александра Мишковића у Високој техничкој школи струковних студија из Крагујевца за период школске 2007/2008. до 2019/2020. године односи се на предмете: Увод у програмирање, Објектно оријентисано програмирање, Програмски језици, Базе података, Пројектовање апликација база података, Примена рачунара, Рачунарске мреже и Рачунарска графика.

Његова тренутна истраживачка интересовања оријентисана су на безбедност података, информационе и комуникационе технологије, рачунарске мреже и криптографију.

Одлуком Већа Департмана за последипломске студије и међународну сарадњу Универзитета Сингидунум, број: 4 – 210-1/2019 од 02.11.2019. године, након измене трећег члана, формирана је Комисија у саставу:

1. Проф. др Младен Веиновић, редовни професор Универзитета Сингидунум, ментор,
2. Проф. др Милан Милосављевић, редовни професор Универзитета Сингидунум,
3. Проф. др Петар Спалевић, ред. проф. ФТН-а Универзитета у Приштини са привременим седиштем у Косовској Митровици

за оцену докторске дисертације под називом: "Унапређење протокола за размену кључева на бази личних идентификационих докумената пошиљаоца и примаоца". За ментора је именован проф. др Младен Веиновић. Завршну верзија докторске дисертације у електронском и штампаном облику Александар Мишковић је предао Универзитету 11.12.2019. године.

Списак резултата М22

1. Jovic, S., Babic, L., Miskovic, A., Cirkovic, B., & Camagic, I. (2019). Ranking of the most influential parameters for compressive strength of no-slump concrete prediction by neuro-fuzzy logic, Structural Concrete. https://doi.org/10.1002/suco.201900349, https://onlinelibrary.wiley.com/doi/abs/10.1002/suco.201900349

Списак резултата М33

1. Mišković A., Veinović M.; Komparativna analiza sertifikacionih tela u Srbiji; IEEE Conference: 19th Telecommunications Forum (TELFOR); DOI: 10.1109/TELFOR.2011.6143496; pp. 74-77, 2011.
2. Mišković A., Atanasijević S.; Analysis of the pull method for CRL list download by PKI simulation model; Sinteza 2014, https://doi.org/10.15308/sinteza-2014-620-624, pp. 620-624, 2014.
3. Aleksić N., Mišković A.; Establishment Of Quality Management In Higher Education; IV International Symposium ENGINEERING MANAGEMENT AND COMPETITIVENESS (EMC 2014); pp. 37 – 42; 2014.
4. Aleksić N., Mišković A.; The differences between the attitudes and knowledge of the Bologna Process and student of alternative programs in academia; International conference on information technology and development of education - ITRO 2014; pp. 373 – 379; 2014.

5. Aleksić N., Erić M., Mišković A.; Quality Assurance And Accredition In Higher Education; 6th DQM International Conference LIFE CYCLE ENGINEERING AND MANAGEMENT, ICDQM-2015; 2015.
6. Mišković A., Aleksić N.; Business Communication As Support Of Relations With The Public Through The Form Of Promotion Promotion In Higher Education; V International Symposium ENGINEERING MANAGEMENT AND COMPETITIVENESS (EMC 2015); pp. 189 – 194; 2015.
7. Uljarević D., Pantović V., Mišković A., Aleksić N.; An Overview of Steganographic Techniques and Methods Applied on Jpeg Images Using Different Transformational Techniques; Sinteza 2016, https://doi.org/10.15308/Sinteza-2016-165-172, pp.165-172, 2016.
8. Šarenac S., Šarenac I., Banković N., Aleksić N., Mišković A.; The Forecast And Analysis Of Students' Success On The Course „Computer Application"; VI International Symposium ENGINEERING MANAGEMENT AND COMPETITIVENESS (EMC 2016); pp. 182 – 187, 2016.
9. Nikolić D., Skerlić J., Šušteršić V., Radulović J., Mišković A.; Influence Of Hot Water Temperature In Dhw System On Building Exergy Optimization, 13th International Conference on Accomplishments in Mechanical and Industrial Engineering, DEMI 2017; pp. 177 – 184, 2017.
10. Skerlić J., Nikolić D., Šušteršić V., Radulović J., Mišković A., Stojanović B.; Analysis And Evaluation Of Solar Energy Systems, 13th International Conference on Accomplishments in Mechanical and Industrial Engineering, DEMI 2017; pp. 355 – 363, 2017.
11. Aleksić N., Mišković A., Antonijević A.; The impact on verbal and nonverbal communication, as one of the most important factors of quality teaching student – teacher; International conference on information technology and development of education - ITRO 2017; 2017.
12. Nikolic D., Skerlic J., Radulovic J., Mišković A, Environmetal Impact Of Solar Systems – Case Of Serbian Residential Building With Solar Collectors And Pv Panels, Quality FEST 2017, CD Conference proceedings и Зборник радова ISBN 978-99976-719-1-2, p. 45-52, Jahorina, BIH, oktobar 2017.
13. Skerlic J., Sudimac B., Nikolic D., Stojanović B., Radulovic J., Mišković A, Analysis And Assessment Of Building Envelope With Integrated Vegetation Modular Element For A Sustainable Future, Quality FEST 2017, CD Conference proceedings и Зборник радова ISBN 978-99976-719-1-2, p. 209-216, Jahorina, BIH, oktobar 2017.
14. J. Skerlić, D. Nikolić, J. Radulović, S. Jovanović, A. Mišković, Toward Future: Positive Net-Energy Buildings, 13th International Quality Conference, Kragujevac, Serbia, ISSN 2620-2832, 2019.

Списак резултата М52

1. J. Skerlić, D. Nikolić, B. Stojanović, D. Cvetković, A. Mišković, Optimization Performances Of A Solar Domestic Hot Water System Using Taguchi Method, (XXXIV међународно саветовање ЕНЕРГЕТИКА 2018, Златибор), Energija, ekonomija, ekologija, No. 1-2, Mart 2018, ISSN 03540-8651, p. 421-428.

Списак резултата М54

1. J. Skerlic, D. Nikolic, D. Cvetkovic, A. Miškovic, Optimal Position Of Solar Collectors: A Review, Applied Engineering Letters, Vol. 3, No. 4, pp. 129-134, 2018.

Списак резултата М63

1. Veinović M., Mišković A.; Metode za proveru statusa i validnosti digitalnih sertifikata; Sinergija 2012, 10. naučni skup, Bijeljina, pp. 53-58; 2012.
2. Aleksić N., Mišković A., Banković N.; Poznavanje i razlika između veština i sposobnosti u visokom obrazovanju; 1th National Conference With International Participation, Faculty of Technical Sciences in Čačak; pp. 235 – 240; 2016.
3. Mišković A., Veinović M.; Primena OPNET simulacionog softvera za izradu PKI simulacionog modela; YU INFO 2014, pp. 96 – 99; 2014.

Некатегоризовани међународни часописи:

1. D. Nikolic, J. Skerlic, V. Šušteršič, J. Radulović, A. Mišković, Influence Of Hot Water Temperature In Dhw System On Building Exergy Optimization, Annals of Faculty Engineering Hunedoara – International Journal of Engineering, Vol.16, No.1, pp. 111-115, ISSN 1584-2665, 2018.

Докторска дисертација кандидата Александра Мишковића је урађена на укупно 100 страна, од чега 12 страна чине прилог и списак литературе. Списак литературе обухвата 80 референци које чине научни радови, књиге, зборници радова, законски прописи, као и електронски извори. Уз основни текст дисертација садржи и 58 слика.

Докторска дисертација кандидата Александра Мишковића је била подвргнута провери софтвером за установљавање преклапања/плагијаризма (iThenticate Plagiarism Detection Software). *Укупан процентуални износ запажених преклапања износи 4% дисертације.*

2. Предмет и циљ истраживања

Предмет рада докторске дисертације је унапређење протокола за размену усаглашавање тајних симетричних криптографских кључева. Разматрају се актуелни проблеми везани за безбедну електронску дистрибуцију тајних кључева и аутентификацију корисника система

за тајну комуникацију. У раду се анализирају постојећа решења у области истраживања и предлаже се сопствено решења које се заснива на симетричним и асиметричним шифарским системима и на коришћењу јединствених криптолошких параметара који се налазе на личним идентификационим документима грађана Србије. Добро је познато да тајност симетричних криптографских система не почива на тајности алгоритама за шифровање већ на тајности криптографских кључева, који се користе за иницијализацију алгоритама за шифровање. У савременим системима за комуникацију који се данас углавном заснивају на Интернет комуникацијама и бежичном преносу, када брзине преноса података непрестано расту, а повећава се и број нових услуга са интуитивним интерфејсима, проблем електронске дистрибуције тајних симетричних кључева постаје све више тзв. "уско грло". Када би овај проблем био решен, тј. када би се математички могла потврдити апсолутна тајност у електронској дистрибуцији кључева, то би довело до револуционарних промена у професионалним и комерцијалним системима за заштиту тајности у преносу података. Основни допринос ове дисертације се односи на употребу личних идентификационих докумената са чипом, који садрже јединствене податке за сваког грађанина. Комбиновањем криптографских метода које обезбеђују тајност, аутентичност и интегритет, уз примену стеганографских метода за размену информација на скривен начин, корисницима предложеног решења се пружа могућност да на ефикасан и сигуран начин размењују тајне поруке, уверени да оне нису у међувремену промењене од стране неког трећег лица и да су тајни кључеви размењени на сигуран начин.

Циљ истраживања је унапређење протокола за размену тајних симетричних криптографских кључева. Извршена је анализа постојећих приступа у овој области с циљем да се побољша ниво заштите приликом тајне размене информација и добије основа за развој сопственог модела.

Практични циљ овог истраживања огледа се у развоју и примени једног новог свеобухватног модела за тајну комуникацију. Ново решење се заснива на коришћењу јединствених параметара који се налазе на идентификационим документима грађана и на примени стеганографских техника за сакривање и утискивање кратких секвенци у различите стандардне медије за комуникацију (слика, текст, говор, видео, мејл комуникација и сл.). Развијено решење нема теоријску подлогу за професионалне системе заштите, али је веома употребљиво за комерцијалну употребу. Лако се може реализовати и користити у свакодневном раду великог броја стандардних корисника сервиса на Интернету.

Спроведена анкета међу студентима прве године Високе техничке школе струковних студија у Крагујевцу, одмах након уписа, указује на то да развој предложеног модела за тајну комуникацију може да допринесе већој друштвеној прихватљивости и да подстиче кориснике да користе средства за заштиту приватности која су им лако доступна. С подизањем опште свести о једноставности употребе предложеног модела и указивањем на

широк спектар могућности који се нуде крајњим корисницима друштвени циљ овог истраживања би био у потпуности задовољен.

3. Хипотетички оквир истраживања

На основу циљева рада произилази следећи хипотетички оквир који се састоји од генералне хипотезе и посебних хипотеза.

Хипотезе које чине основу овог рада:

- Развојем новог модела за тајну комуникацију који обједињује употребу личних идентификационих докумената са стеганографским методама побољшава се ниво заштите приликом тајне размене информација.
- Реализовани модел треба да обезбеди једноставност употребе, која треба да подстиче кориснике да користе средства за заштиту приватности која су им лако доступна. Представља систем са јасним параметрима за тајну комуникацију у који се може имати поверења.
- Примена личних идентификационих докумената у комбинацији са изабраном стеганографском техником потенцијалном нападачу у великој мери отежава процес разоткривања тајне комуникације, а самим тим умањује се и вероватноћа да ће доћи до криптоанализе шифрованих информација.

Посебне хипотезе:

- Корисници који желе да примењују предложени модел за тајну комуникацију морају да имају поверење тј. да користе услуге "треће стране од поверења", тј. сертификационог тела које издаје квалификоване дигиталне сертификате на личним идентификационим документима.
- *RSA* кључ од 2048 бита који се користи у личним идентификационим документима грађана Републике Србије се још увек сматра безбедним.

4. Методологија истраживања

Приликом израде докторске дисертације, примењене су различите научне методе које омогућују валидно остварење научног и друштвеног циља истраживања. У истраживању и прикупљању примарних и секундарних података, користиле су се методе из групе основних, опште научних, посебних и из групе статистичких метода за прикупљање података.

Избор истраживачких метода је употребљен да се истраживање и ток истраживачког процеса у свим фазама, тј. идентификацији и дефинисању проблема, планирању дизајна

истраживања, сакупљању, обради и анализи података, као и формулацији закључака, коректно спроведе у складу са основним принципима научно истраживачког рада. У прикупљању података примениће се: испитивање, анкета и метода анализе садржаја докумената.

Анализа ће бити остварена на два нивоа :

- на нивоу експерименталне анализе реалних субјеката и
- на нивоу секундарне анализе резултата ранијих истраживања и адекватне литературе.

5. Кратак приказ садржаја докторске дисертације

Докторска дисертација се састоји из 8 (осам) поглавља: Увод, Преглед у области истраживања, Теоријске основе истраживања, Преглед постојећих решења, Модел предложеног решења, Евалуација предложеног решења, Закључак и Литература.

У првом поглављу је описан предмет истраживања, назначени су мотиви за израду једног новог решења за тајну комуникацију, наведени су очекивани доприноси, приказана је методологија истраживања, дате су научне хипотезе и циљ истраживања.

Друго поглавље представља преглед у области истраживања. Методолошки су анализирани научни радови из врхунских међународних часописа, научни радови са релевантних међународних конференција и скупова, објављених књига и стандарда.

У трећем поглављу су описане теоријске основе које су релевантне за област истраживања. Дат је кратак преглед савремене криптографије, уз историјски осврт ка развоју криптографских система, као и теоретске основе стеганографије.

Четврто поглавље представља преглед постојећих решења која се већ користе и која су релевантна за област истраживања. Дат је приказ софтверских решења и описане су њихове предности и уочени недостаци. Број постојећих решења је сведен на она која су се користила за поређење са предложеним решењем за тајну комуникацију из ове дисертације.

Пето поглавље, јесте централно место ове дисертације и описује предложено решење за тајну комуникацију и приказује метод његове примене. Дат је опис проблема који је био и мотив за рад на овој докторској дисертацији. Детаљно се анализира примена асиметричних шифарских система за шифровање криптографских кључева за примену симетричних система. Као допринос, издваја се примена јединствених параметара са идентификационих личних докумената и развија се сопствени систем за шифровање на

бази криптографије са јавним кључевима примаоца. У следећем кораку се примењује стеганографска метода за утискивање шифрованог кључа у одговарајући тзв. стего носилац. На пријемној страни, развијен је алгоритам за инверзне операције тј. за издвајање шифрованог кључа и његову припрему за симетрични систем шифровања. Анализирају се ефекти стеганографије на стего носилац: без губитака, са губицима, меморијско увећање носиоца и сл. и изводе се одговарајући закључци.

Шестим поглављем су приказани резултати симулација модела који су довели до развоја новог система за тајну комуникацију, приказана су поређења предложеног решења са већ постојећим решењима описаним у поглављу четири. Приказани су резултати спроведене анкете са изведеним закључцима који су проистекли из исте. Дат је критички осврт на делове система за тајну комуникацију који могу да утичу на безбедну употребу истог и дате смернице за унапређење недостатака.

Седмо поглавље је закључак где су јасно издвојени научни и стручни доприноси ове докторске дисертације и предложени су правци даљих истраживања

У осмом поглављу је дат списак литературе која је коришћена у овај докторској дисертацији.

6. Постигнути резултати и научни допринос докторске дисертације

Научни допринос овог рада односи се на примену јединствених параметара са личних идентификационих докумената за развој сопственог решења за заштиту тајних симетричних кључева. Поверење у параметре који се користе за сопствено решење почива на поверењу у рад квалификованих сертификационих тела. У овом раду коришћени су квалификовани сертификати које издаје МУП Републике Србије. Додатно, предложена је примена стеганографских техника за сакривање добијених шифрованих кључева у одговарајући стего носилац. У раду је показана ефикасност овог поступка код веб галерије слика које су дате у тзв. *jpeg* формату. Предложени поступа се ефикасно може применити и код других стандардних носилаца у данашњим комуникација (текст, слика, говор, видео), као и код стандардних комуникационих сервиса (мејл, *Viber, WhatsApp* и сл.). У дисертацији је извршена детаљна анализа доступних протокола за електронску дистрибуцију тајних симетричних криптографских кључева и указано је на потенцијалне слабости и предности предложеног решења.

У складу са до сада наведеним, основни доприноси докторске дисертације су:

- Развијен је нови протокол за размену тајних симетричних криптографских кључева на бази личних идентификационих докумената пошиљаоца и

примаоца. Предложено решење има низ криптолошких предности од којих се издвајају:

  - Не постоји потреба да се смешта и чува велики број тајних кључева код корисника пошто се они могу компромитовати,
  - За сваку нову комуникацијску сесију генерише се нови тајни кључ. Евентуална компромитација једног оваквог кључа не утиче на тајност осталих пренетих порука, пошто су оне шифроване другим кључем.
  - Остварује се потпуна *end-to-end* заштита за сваку комуникацију и за сваки пар учесника у тајној комуникацији.

- Развијено је сопствено решење које не захтева рад тзв. треће стране од поверења. Користе се само параметри који су издати од стране тела које издаје квалификоване дигиталне сертификате.
- Разматрана је примена стеганографских техника за сакривање шифрата у одговарајући тзв. стего носилац. На примеру *jpeg* слика показано је да сакривена информација не утиче на статистичке карактеристике, нити на меморијске карактеристике стего носиоца.
- Нови протокол је отпоран на велики број напада на мрежи.

Резултати рада се могу користити за широки спектар комерцијалних решења за комуникацију. Од корисника таквих решења се не захтева професионално познавање криптографије. Остварена комуникација се тешко може открити и обезбеђује висок степен тајности за апликације које користе тајне симетричне криптографске кључеве. За професионалне системе заштите, остварени резултат се може посматрати као корак више у заштити када се посматрају комбинована решења са надшифровањем и сакривањем шифрованог материјала.

7. Мишљење и предлог Комисије о докторској дисертацији

На основу свега изложеног Комисија је мишљења да докторска дисертација кандидата Александра Мишковића по својој теми, приступу, структури и садржају рада, квалитету и начину излагања, методологији истраживања, начину коришћења литературе, релевантности и квалитету спроведеног истраживања и донетим закључцима задовољава критеријуме захтеване за докторску дисертацију, те се може прихватити као подобна за јавну одбрану.

Сагледавајући укупну оцену докторске дисертације кандидата Александра Мишковића под називом "Унапређење протокола за размену кључева на бази личних идентификационих докумената пошиљаоца и примаоца" предлажемо Већу департмана за последипломске студије и Сенату Универзитета Сингидунум да прихвати напред наведену докторску дисертацију и одобри њену јавну одбрану.

Београд, 10/12/2019.

Чланови комисије:

проф. др Младен Веиновић, ментор

Редовни професор, Универзитет Сингидунум

проф. др Милан Милосављевић, члан

Редовни професор, Универзитет Сингидунум

проф. др Петар Спалевић, члан

Редовни професор, Универзитет у Приштини
са привременим седиштем у Косовској Митровици