УНИВЕРЗИТЕТ СИНГИДУНУМ
Департман за последипломске студије
Данијелова 32, Београд

ВЕЋУ ДЕПАРТМАНА ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ

Одлуком Већа Департмана за последипломске студије број 4 - 62/2020 од 22.05.2020. године, одређени смо за чланове Комисије за оцену и одбрану докторске дисертације кандидата Милоша Јовановића под називом "**Једна класа криптографски заштићене аутентификације клијената заснована на опозивој биометрији**"

о чему подносимо следећи

ИЗВЕШТАЈ

1. Основни подаци о кандидату и докторској дисертацији

Милош Јовановић је рођен 23. августа 1991. године у Сремској Митровици. Средњу електротехничку школу је завршио у Шиду као ученик генерације. Дипломирао је на Факултету за информатику и рачунарство Универзитета Сингидунум са просеком 9,84 и завршио мастер програме у области информационих технологија и међународног бизниса и менаџмента на Универзитету Сингидунум (Република Србија) са просеком 10, Универзитету у Београду (Република Србија) и Мидлсекс универзитету (Уједињено Краљевство Велике Британије и Северне Ирске).

Докторске академске студије на студијском програму Напредни системи заштите, на Универзитету Сингидунум, уписао је школске 2015/2016. године.

Завршио је програм „Право, морална и политичка филозофија“ на Универзитету Харвард (САД), као и програм „Федералне резерве“ на Њујоршком институту за финансије. Усавршавао се у области лидерства и креативне економије у Сједињеним Америчким Државама, Уједињеном Краљевству, Швајцарској, Француској, Немачкој, Белгији, Холандији, Руској Федерацији, Народној Републици Кини. Носилац је признања Краљевског Дома Карађорђевића за изванредни успех.

Председник је OpenLink Групе. Члан је Савета за унапређење сектора информационо-комуникационих технологија Владе Републике Србије.

Његова тренутна истраживачка интересовања оријентисана су на сигурност података, информационо-комуникационе технологије, рачунарске мреже, криптографију и биометрију. Говори енглески, а служи се немачким и руским језиком. Живи и ради у Београду, Лондону и Њујорку.

Кандидат има следећи објављени рад категорије М22 чиме је испуњен предуслов за одбрану докторске дисертације:

Nemanja Maček, Saša Adamović, Milan Milosavljević, Miloš Jovanović, Milan Gnjatović, Branimir Trenkić (2019): "Mobile Banking Authentication Based on Cryptographically Secured Iris Biometrics". Acta Polytechnica Hungarica, Vol. 16, No. 1, pp. 45-62. ISSN 1785-8860. DOI: 10.12700/APH.16.1.2019.1.3. IF (2018) = 1,286. http://www.uni-obuda.hu/journal/Macek_Adamovic_Milosavljevic_Jovanovic_Gnjatovic_Trenkic_88.pdf (категоризација часописа у Кобсон бази је М22, а године која је изабрана за категоризацију је 2020).

Преостали објављени радови:

Списак резултата М20

[1] Maček, N., Adamović, S., Milosavljević, M., Jovanović, M., Gnjatović, M., & Trenkić, B. (2019). Mobile Banking Authentication Based on Cryptographically Secured Iris Biometrics. *Acta Polytechnica Hungarica, 16*(1), pp. 45-62. DOI: 10.12700/APH.16.1.2019.1.3. ISSN: 1785-8860.

Списак резултата М30

[1] Đokić, D., Jovanović, M., Aleksić, A., Valentirović, D., & Mitić, D. (2019). Artificially Intelligent Cloud Computing - The Ability to Prevent Errors. *The 10th International Conference on Business Information Security (BISEC 2018)*, pp. 20-24. ISBN 978-86-89755-17-6.

[2] Jovanović, M., Pinterič, U., Valentirović, D., Mitić, D., & Milašinović, M. (2019). Role of the Big Data in Digital Marketing - Context of the Security Framework. *The 10th International Conference on Business Information Security (BISEC 2018)*, pp. 46-50. ISBN 978-86-89755-17-6.

[3] Petrović, A., & Jovanović, M. (2018). Place of Blockchain in Economy. *International Scientific Conference EKOB 2018*, pp. 267-270. ISBN 978-86-900480-0-7.

[4] Mitić, D., Jovanović, M., Biga, N., Đaković, N., & Petrović, A. (2017). Big Data and Cyber Security: Contemporary Issues. *The 9th International Conference on Business Information Security (BISEC 2017)*, pp. 50-53. ISBN 978-86-89755-14-5.

[5] Jovanović, M., Milenković, D., Perković, M., Milenković, T., & Niković, V. (2016). The Use of Artificial Neural Networks in Clinical Medicine. *International Scientific*

Conference on ICT and e-Business Related Research - Sinteza 2016, pp. 111-117. DOI: 10.15308/Sinteza-2016-111-117. ISBN 978-86-7912-628-3.

[6] Jovanović, M., Rančić, N., Davidović, D., & Mitić, D. (2016). On Mitigation of Modern Cybercrime Threats. *International Scientific Conference on ICT and e-Business Related Research - Sinteza 2016*, pp. 137-142. DOI: 10.15308/Sinteza-2016-137-142. ISBN 978-86-7912-628-3.

[7] Biga, N., Jovanović, M., Perković, M., & Mitić, D. (2016). Modern Business Environment: Information Technology as a Shield Against Cyber Security Threats. *The 8th International Conference on Business Information Security (BISEC 2016)*, pp. 105-108. ISBN 978-86-89755-10-7.

Докторска дисертација кандидата Милоша Јовановића је урађена на укупно 126 страна, од чега 35 страна чине прилог и списак литературе. Списак литературе обухвата 145 референци које чине научни радови, књиге, зборници радова, законски прописи као и електронски извори. Уз основни текст дисертација садржи и 31 слику, 5 табела и 2 графикона.

Докторска дисертација кандидата Милоша Јовановића је била подвргнута провери софтвером за установљавање преклапања/плагијаризма (iThenticate Plagiarism Detection Software). *Укупан процентуални износ запажених преклапања износи 1% дисертације.*

2. Предмет и циљ истраживања

Полазећи од схватања да су биометријски подаци неопозиви у природи, и да компромитовање биометријских шаблона може довести до крађе идентитета корисника, што за последицу може имати различите облике злоупотребе, овај рад разматра следеће хипотезе:

H1. Тренутна решења за заштиту биометријских шаблона не обезбеђују довољно висок ниво сигурности шаблона и приватности корисника.

H2. Развојем сопственог биометријског система у коме биометријски шаблони остају шифровани или у најгорем случају опозиви током свих фаза њихове примене (складиштење, пренос и верификација) обезбеђује се практична употребљивост биометријске аутентификације у савременом отвореном мрежном окружењу.

Научни циљ овог рада је приказ једног новог начина криптографски заштићене аутентификације клијената помоћу биометријских података који, у поређењу са досадашњим истраживањима и достигнућама у овој области, унапређује сигурност и гарантује аутентичност приликом провере идентитета корисника. Посебна пажња је посвећена анализи постојећих решења за заштиту биометријских система за проверу идентитета са аспекта сигурности и заштите приватности. Намена ове анализе је да се прикаже ефикасност постојећих решења, и да се пружи основа за предлагање новог приступа који би ефикасно одговорио на недостатке постојећих решења.

Технички циљ овог рада је да се предложени начин криптографски заштићене аутентификације клијената имплементира кроз модуларни биометријски систем за проверу идентитета. Систем користи криптографију са јавним кључевима, генератор псеудослучајних бројева и опозиву биометрију. Неинвертибилна трансформација се извршава помоћу кључа који се налази на сигурном меморијском складишту уређаја. Биометријски шаблони су шифровани или, у најгорем случају, опозиви током свих фаза у раду система, изузев у фази издвајања обележја, што резултује системом који је отпоран на велики број напада. Предложени систем не користи процесорски захтевне операције, а генерисани биометријски шаблони су прихватљиве величине. Систем је процењен у домену провере идентитета корисника услуга мобилног банкарства базиране на биометрији дужице људског ока.

3. Хипотетички оквир истраживања

Тренутна решења за заштиту биометријских шаблона не обезбеђују довољно висок ниво сигурности шаблона и приватности корисника. Развојем сопственог биометријског система у ком биометријски шаблони остају шифровани или у најгорем случају опозиви током свих фаза њихове примене (складиштење, пренос и верификација) обезбеђује се употребљивост предложеног приступа у реалним доменима примене.

4. Методологија истраживања

Методологија истраживања у овом раду обухвата сложен и организован поступак заснован на логичким начелима и строгим математичким принципима типичним за анализу и синтезу криптографских механизама доказиве безбедности.

Сложеност предмета истраживања захтева примену:

- аналитичких основних метода – метод анализе, метод апстракције, метод специјализације и метод дедукције;
- синтетичких основних метода – синтезу, конкретизацију, генерализацију и индукцију;
- опште научних метода – хипотетичко-дедуктивну, аналитичко-дедуктивну, компаративну, математичку и статистичу методу моделовања.

Овај избор истраживачких метода је употребљен да се истраживање и ток истраживачког процеса у свим фазама, односно идентификацији и дефинисању проблема, планирању дизајна истраживања, критичкој анализи система, као и формулацији закључака коректно спроведе у складу са основним принципима научно истраживачког рада. Применом ових метода, како показују презентовани резултати истраживања, могуће је валидно остварење научног и друштвеног циља истраживања.

5. Кратак приказ садржаја докторске дисертације

Рад се састоји из 6 поглавља, структуираних садржајно на следећи начин.

У глави 1 дата су уводна разматрања, методолошки оквири истраживања и очекивани научни доприноси.

У глави 2 дат је преглед релевантних истраживања у области, при чеми су посебно обрађена питања биометријске верификације корисника, употребе опозиве биометрије и криптографске заштита биометријских шаблона.

Глава 3 уводи теоријске основе истраживања које су релевантне за присутуп предложен у овом раду. Оне укључују криптографију са јавним кључевима, генераторе псеудослучајних бројева, заштитне кодере, интерливере и неинвертибилне трансформације.

У глави 4 предложен је један нови приступ криптографски заштићеној биометијској аутентификацији, заснован на криптографији са јавним кључевима, генератору псеудослучајних бројева и опозивој биометрији. На основу тога, изложен је и предлог једног система за проверу идентитета корисника услуга мобилног банкарства базирана на биометрији дужице људског ока, уз дефинисање алгоритама за упис и верификацију корисника.

Систем који имплементира предлог из главе 4, анализиран је у глави 5. Прво је размотрен проблем издвајања обележја дужице и верификације идентитета особе. Потом су изложени резултати анализе перформанси предложеног система на реалном скупу података. Коначно, презентовани су резултати испитивања случајности шифрованих опозивих шаблона и података који се преносе преко мреже.

Закључак и преглед могућих смерова даљег истраживања дати су у глави 6.

6. Постигнути резултати и научни допринос докторске дисертације

Потврђени доприноси овог рада су следећи:

- предложена је нова метода за проверу идентитета корисника помоћу шифрованих опозивих биометријских шаблона;
- предложено решење је модуларно у погледу примењених криптографских механизама, и независно од тога да ли се примењују шифарски алгоритми са симетричним или јавним кључем;
- предложена је својеврсна шема за верификацију дужице у којој се, за разлику од познатих система, не користе кодове за корекцију грешака, а верификација корисника се не заснива на поређењу хеш кодних речи које носе минималну количину информације о биометријском узорку;
- предложени систем за проверу идентитета је погодан за примену у сценарију мобилног банкарства, будући да је грешка лажног прихватања занемарљива, а величина биометријског узорка је прикладна за смештање на мобилним уређајима (за разлику од биометријских узорака добијених хомоморфним шифровањем, који су знатно већи);

- предложено решење је применљиво у технологији облака због релативно ниске процесорске захтевности, за разлику од других шифарских алгоритама који су знатно захтевнији по питању процесорских ресурса.

7. Мишљење и предлог Комисије о докторској дисертацији

На основу свега изложеног Комисија је мишљења да докторска дисертација кандидата Милоша Јовановића 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 Милоша Јовановића под називом "**Једна класа криптографски заштићене аутентификације клијената заснована на опозивој биометрији**", предлажемо Већу департмана за последипломске студије и Сенату Универзитета Сингидунум да прихвати напред наведену докторску дисертацију и одобри њену јавну одбрану.

Београд, 11/06/2020

Чланови комисије:

проф. др Милан М. Милосављевић, редовни професор, ментор

проф. др Младен Веиновић, редовни професор, председник

проф. др Бошко Николић, редовни професор, члан
Електротехнички факултет Универзитета у Београду