РЕЦЕНЗИЯ

от доц. д-р Веселина Господинова Жечева – Център по информатика и технически науки, Бургаски свободен университет
за дисертационен труд „Оптимизация на сигурността при мобилното банкиране“
на докторанта Бонимир Пенчев Пенчев,
разработен в секция „Софтуерни технологии и информационни системи“, Българска Академия на Науките
по конкурс за присъждане на образователната и научна степен "доктор",
професионално направление 4.6. "Информатика и компютърни науки"

Със Заповед № 239 / 08.09.2016 г. на Директора на Института по математика и информатика, Българска Академия на Науките съм определена за член на научното жури във връзка с конкурс за присъждане на образователната и научна степен "доктор", професионално направление 4.6. Информатика и компютърни науки.
Като член на научното жури получих следните документи:

1. Заявление (молба) до Директора на ИМИ-БАН за допускане до защита;
2. Професионална автобиография на ас. Бонимир Пенчев Пенчев;
3. Заповеди за зачисляване в докторантура и отчисляване с право на защита;
4. Протоколи за издържани изпити от докторантски минимум;
5. Информационни карти на НАЦИД – 2 бр.;
6. Списък и копия на публикациите за участие в конкурса – 7 броя;
7. Автореферат на ас. Бонимир Пенчев Пенчев на тема „Оптимизация на сигурността при мобилното банкиране“;
8. Дисертационен труд на ас. Бонимир Пенчев Пенчев на тема „Оптимизация на сигурността при мобилното банкиране“;
9. Справка за научните и научно-приложни приноси на докторанта в дисертацията и публикациите.
10. Копия на други документи от официалната документация по протичането на докторантурата на ас. Бонимир Пенчев.

Данни за дисертанта. Бонимир Пенчев Пенчев е роден в гр. Добрич. През 2007 г. завършва висшето си образование в ИУ - Варна с образователно-квалификационна степен Бакалавър по Информатика, а през 2008 г. – с образователно-квалификационна степен „Магистър“ по „Информатика“. От 2013 до 2016 г. е докторант на самостоятелна подготовка в Института по математика и информатика, откъдето е отчислен с право на защита поради изтичане срока на докторантурата със заповед 617 / 19.07.2016 г. Работил е като програмист, хоноруван асистент и асистент по информатика в Икономическия университет – Варна от 2008 г. досега. Преподава дисциплини, свързани с програмиране, проектиране и разработване на приложения, компютърни архитектури и др.

Данни за докторантурата. Бонимир Пенчев Пенчев е приет за докторант в самостоятелна подготовка към секция „Софтуерни технологии”, ИМИ – БАН на тема „Оптимизация на сигурността при мобилното банкиране”, област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6. Информатика и

компютърни науки, по научна специалност 01.01.12 Информатика за периода от 08.07.2013 г. до 08.07.2016 г. със заповед 466 / 25.07.2013 г. на Директора на ИМИ – БАН.
Със заповед 617 / 19.07.2016 г. на Директора на ИМИ – БАН докторантът Бонимир Пенчев Пенчев е отчислен с право на защита поради изтичане срока на докторантурата.
Дисертационният труд е насрочен за публична защита чрез Заповед 239 / 08.09.2016 г. на Директора на ИМИ – БАН при спазване на всички формални изисквания на действащата нормативна уредба.

Данни за дисертацията и автореферата. Кандидатът за заемане на образователната и научна степен "доктор" Бонимир Пенчев Пенчев е представил дисертационен труд и седем публикации по темата на дисертацията в научната периодика или в научни сборници.
Представеният дисертационен труд е с обем от 148 страници и се състои от увод, 3 глави, заключение, списък на публикациите по дисертационния труд, апробация, декларация за оригиналност и списък с използвана литература, включваща 143 заглавия.
Тематика на дисертационния труд. Представеният дисертационен труд е посветена на проблем от областта на информационната сигурност.
Методика. Използван е инструментариум, включващ методи от машинното обучение.

В ***Увода*** са формулирани целта и задачите на дисертационния труд. Разгледани са основните тенденции при онлайн банкирането и разплащанията, както и предимствата, които то носи за финансовите институции и клиентите. Идентифицирани са и проблемите пред потребителите при използване на мобилно банкиране – функционални, психологически, технически и др. Посочено е, че рисковете пред сигурността на разплащанията са сред най-важните условия за потребителите, обуславящи използването на мобилно банкиране. Обоснована е необходимостта от повишаване на сигурността при мобилните разплащания и банкиране, като са приведени данни от проучвания в областта. **Целта**, която се поставя в дисертационния труд, е: да се повиши сигурността на мобилното банкиране и респективно доверието на потребителите в тази услуга. **Задачите**, формулирани в увода на дисертационния труд, включват анализ на текущото състояние, заплахите и добрите практики в информационната сигурност при мобилното банкиране, предлагане на нови или подобрени механизми на сигурност и експериментално изследване и оценяване ефективността на предложените подобрения. Синтезирано е съдържанието на трите глави на дисертацията.

Глава 1, озаглавена Изследвания на информационната сигурност в процесите на мобилното банкиране, е обзорна. В нея са разгледани същността и основните понятия на мобилното банкиране, анализирани са проблемите, свързани с мобилното устройство, мобилната операционна система, мобилния браузър и приложението за мобилно банкиране. Направено е разграничение между мобилно банкиране и мобилни разплащания, като са разгледани характерните особености на двете услуги от гледна точка на сигурността. Изброени и анализирани са наличните в литературата дефиниции за мобилно банкиране, като е посочено разминаването в много от тях на основни понятия, което води до липсата на общоприета дефиниция. Разгледани са основните бизнес модели при мобилно банкиране, както и най-важните банкови услуги (активни и пасивни; справки и транзакции), които се предоставят на мобилните клиенти. Изследвано е предоставянето на мобилни банкови услуги в 3 региона на света: Далечният Изток и Китай, Европейският съюз (в частност Западна Европа) и Северна Америка, като е разгледано разпределението на тези услуги по вида на използваната технология: SMS

съобщения, мобилно приложение, сайт с мобилна версия. Установено е, че основната част от тези услуги се предоставя от мобилни приложения, което обосновава необходимостта от повишаване на сигурността на тези услуги. В резултат от направените изследвания е формулирана работна дефиниция на мобилното банкиране.
Формулирани са проблемните области в мобилното банкиране, свързани с всеки елемент в процеса: устройство, операционна система, браузър и приложение и е направен обзор на основните видове атаки, свързани с всеки елемент, както и добрите практики за защита от тези атаки. При атаки, свързани с използваното мобилно устройство, са отбелязани както такива, свързани със социален инженеринг (vishing, smishing и др.), така и технологични (SMS или MMS, съдържащ злонамерен код, например червей; уязвимости на използваните безжични технологии, например Wi-Fi, Bluetooth или NFC, при които се прилагат например man-in-the-middle, подслушване и др.). При атаки, свързани с мобилната операционна система, са изброени редица троянски коне и кийлогъри, които са мобилни версии на аналозите си за настолните операционни системи. При заплахите за сигурността, свързани с мобилния браузър, е посочено, че много от тях са близки до тези, свързани с браузърите за настолни операционни системи и включват фишинг, автоматично сваляне на злонамерен код и др.; докато други са специфични и са свързани с размерите на екрана и възможностите за автентификация на връзката. Анализирани са и основните заплахи, свързани с мобилните приложения.
Представени са основните атаки, както и добрите практики за тяхното противодействие – методи за криптиране на данните, за идентификация и автентификация, за сигурно съхранение на поверителни данни на мобилното устройство, както и повишаване информираността на потребителите за възможните рискове.

В ***Глава 2. Концептуален модел за повишаване сигурността на мобилното банкиране*** *е* обоснован и описан модел на система, повишаваща сигурността в процеса на мобилното банкиране. Формулирани са четири основни изисквания към проектирания модел като за всяко от тях е разработена обща методика, която съдържа последователните етапи (7 на брой), в които да бъдат дефинирани модулите. Освен това са формулирани предложения за подобрения, които да доведат до повишаване на нивото на сигурността, групирани по типове заплахи за сигурността, съгласно класификацията, въведена в Глава 1. Тъй като първите три етапа от формулираната методика са описани в Глава 1, то Глава 2 съдържа описанието на останалите 4 етапа за всеки от описаните пет модула както следва:

- *модул за биометрично удостоверяване, който се базира на поведението на потребителите* – целта му е идентификация на потребителя чрез поведенчески анализ на неговите действия. За целта се изграждат профили на потребителските действия, събрани в резултат на работата му със сензорния екран и групирани по отличителни белези. След това е извършено обучение на модула, след което е реализирано и самото разпознаване;
- *модул за автоматизирана защита от tabnabbing атака* – описани са основните характеристики на този вид атака, след което е формулирана основната цел на модула – да открива промените в раздели на мобилния браузър когато той е извън фокуса на потребителя, както и да извежда съобщение при откриване на значителни промени в съдържанието, които се третират като нарушение. Това се реализира на базата на сравняване на начина, по който е изглеждал разделът преди и след възстановяване на фокуса на потребителските действия;
- *модул за автоматизирана защита от CSRF атака* – описан е начинът на изпълнение и целите на такава атака, като е предложен метод за нейното

неутрализиране. Той включва следене и филтриране на заявките от браузъра като неоторизираните заявки (т.е. не към сайта, за който са предназначени) се блокират автоматично. Освен това алгоритъмът отчита възможността за пренасочване на легитимни заявки;

- *модул за удостоверяване, който се базира на PICO токен и гласово разпознаване* – целта на този модул е да извършва идентификация по удобен за потребителя начин без да е необходимо да използва пароли. Той се състои от две основни части, които реализират основните функционалности – регистрация и удостоверяване на потребителя за първия подмодул и анализ и разпознаване на гласовия сигнал чрез сравнение с предварително зададени образци за втория подмодул;
- *модул за реализиране на автоматизирани проверки* – този модул реализира помощни функции като проверки за използване на некриптирана мрежа, за използване на механизми за удостоверяване, за заключване на устройството, за актуалност на версията на използвания софтуер и др. с цел да се повиши общото ниво на сигурността на мобилното устройство и в частност на приложението за мобилно банкиране.

За всеки от изброените модули са описани и обосновани неговата архитектура, основните му функции, данните, които ще обработва и очакваните резултати. Представена е и принципна схема, показваща взаимодействието му с другите модули и мястото в цялостната архитектура на модела.

Предложена е и функционална структура на описаните модули, дефинираща мястото му спрямо останалите елементи на системата за мобилно банкиране.

В ***Глава 3. Приложение на концептуалния модел за повишаване сигурността на мобилното банкиране*** са представени симулационните изследвания и получените резултати от реализацията на предложения модел. За всеки от предложените пет модула са описани обхватът, планирането, провеждането на експериментите и анализ на получените резултати. Освен това са описани подробно използваните алгоритми, реализирани с различни средства и технологии. За всеки модул са представени и анализирани получените резултати под формата на процент на грешките. Описана е и обратната връзка от страна на потребителите по отношение на използването на разработените модули.

- *модул за биометрично удостоверяване, който се базира на поведението на потребителите.* Подбрана е целева група, като експериментът се провежда контролирано под ръководството на експерти с мобилно устройство, на което е инсталиран софтуер, събиращ данни за начина на работа на потребителя с устройството. Към събраните данни са приложени 6 избрани алгоритми за машинно обучение и класифициране и са представени резултатите от всеки от тях;
- *модул за автоматизирана защита от tabnabbing атака.* Целта на този експеримент е да се оцени производителността на модула като време за обработка и предупреждение на потребителя при наличие на установено нарушение. Модулът се основава на сравнение на изображенията от екрана (screenshot) на браузъра преди и след разглеждането му от потребителя. Представени и анализирани са времената за обработване в зависимост от процента на изменение на съдържанието на страницата спрямо началното;
- *модул за автоматизирана защита от CSRF атака.* Чрез езика за моделиране Alloy са описани алгоритъмът за филтриране на заявките и CSRF атака, след което е формално проверено чрез софтуерна симулация, че алгоритъмът ефективно

предпазва от атаките. Представените резултати показват, че не са открити примери, които да доведат до нарушаване на политиката на сигурност;

- *модул за удостоверяване, който се базира на PICO токен и гласово разпознаване.* За оценка на модула е използвана модифицирана версия на подхода UDS (usability, deployability, security), при който се оценява автентификацията на потребителя по множество критерии;
- *модул за реализиране на автоматизирани проверки.* Подбрана е целева група, като експериментът се провежда контролирано под ръководството на експерти с мобилно устройство, на което работи прототип на реализирания модул. Проверките са разделени в групи по важност. Представени и анализирани са резултатите от обратната връзка от потребителите и от ефективността на разработения модул.

Приноси. Авторът на настоящата рецензия приема дефинираните от докторанта приноси, а именно:

1. На базата на анализираните литературни източници е синтезирана нова дефиниция за мобилно банкиране, която е широко приложима и има универсален характер.
2. Определени и систематизирани са най-често реализираните атаки и използваните от тях уязвимости във всяка една от проблемните области за сигурността при потребителя на мобилното банкиране.
3. Установено е какви подобрения могат да бъдат внесени, за да се повиши сигурността на мобилното банкиране във всяка една от проблемните области при потребителя.
4. Предложен е концептуален модел за повишаване на сигурността при мобилното банкиране, чиято основна цел е да подпомогне доставчиците на услуги за мобилно банкиране да повишат нивото на сигурността във всяка една от дефинираните проблемни области при потребителя чрез интегрирането на пет нови или подобрени механизми за сигурност.
5. Доказана е ефективността на всеки един от предложените механизми за сигурност, присъстващ в предложения концептуален модел за повишаване на сигурността при мобилното банкиране.

Описани са и насоки за бъдещо развитие на работата и подобряване на получените резултати.

Във връзка с дисертационния труд могат да се отправят следните **въпроси, критични забележки и коментари:**

1. Модулът за биометрично удостоверяване на базата на потребителското поведение се базира на данни, получени от взаимодействието на потребителя с мобилното устройство. Тези данни са силно зависими от приложението, от работата с което са събирани. За кои приложения са събирани данни (в дисертацията на стр. 91 е посочено само, че се зарежда google) и как са усреднени те спрямо броя и вида на приложенията?
2. Защо при реализиране на модула за автоматизирана защита от tabnabbing атака е избрано сравняване на изображения на екрана (screenshot) вместо сравняване на кода на двете страници или части от него, което би работило по-бързо? В дисертацията не е посочена каква е точността на избрания метод и устойчивостта му на грешки.
3. От предложените модули са реализирани софтуерно и тествани с реални данни първият, вторият и петият, докато третият е описан и тестван формално чрез език

за моделиране, а четвъртият е оценен по множество критерии, без да е описано потребителско тестване. Кое налага разликата в прилаганите методи и защо не е използвана унифицирана методология?

4. Един от най-често използваните методи за биометрично удостоверяване е разпознаването на лице. Защо този метод не е използван съвместно или вместо метода за разпознаване на глас?
5. Представените резултати в глава 3 включват оценка на точността на метода чрез процент на грешката. Каква част от грешките са верни данни, погрешно оценени като неверни или обратно (false positives и false negatives)?
6. Стр. 49, ред 2 отдолу, текстът „Неговото изготвянето" трябва да се замени с „Неговото изготвяне".
7. Докторантът не е представил справка за цитирания на неговите публикации.

Цялостното впечатление на рецензента от дисертационния труд на кандидата е положително, като приема всички приноси съгласно представената ми справка. Направените по-горе забележки и коментари нямат за цел да омаловажат неговите постижения, които имат главно научно-приложен характер и трябва да се възприемат по-скоро като препоръка за бъдещата му работа.

Публикации и участия в научни форуми. Представени са седем публикации, от които 3 са статии в списания в България и 4 – доклади на конференции, като един от тях е изнесен на специализиран форум - международната научна конференция „Human Systems Integration Approach to Cyber Security" в София, един на конференция във Велико Търново и два – на конференции във Варна.

Заключение

Въз основа на изложеното по-горе считам, че кандидатът Бонимир Пенчев Пенчев изпълнява всички критерии и изисквания по Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в Българската академия на науките. Посочените приноси и положителни страни на дисертационния труд ми дават основание убедено да препоръчам на членовете на уважаемото Научно жури да присъди на Бонимир Пенчев Пенчев образователната и научна степен "доктор", професионално направление 4.6. "Информатика и компютърни науки".

Подпис:

/доц. д-р В.Жечева/

24.10.2016 г.
Гр. Бургас