БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

СЕКЦИЯ “СОФТУЕРНИ ТЕХНОЛОГИИ

И ИНФОРМАЦИОННИ СИСТЕМИ”

АВТОРЕФЕРАТ

на дисертация за присъждане на образователна и научна степен
“Доктор” по научна специалност 01.01.12. “Информатика”
на тема:

Оптимизация на сигурността при мобилното банкиране

Автор:
Бонимир Пенчев Пенчев

Научен ръководител:
доц. д-р Димитрина Полимирова

СОФИЯ, 2016

Дисертационният труд е обсъден и предложен за защита на разширено заседание на секция „Софтуерни технологии и информационни системи” към Института по математика и информатика – БАН, което се е състояло на 01.09.2016 г.

Дисертантът е докторант на свободна подготовка в секция „Софтуерни технологии и информационни системи“ към Института по математика и информатика – БАН.

Дисертационният труд е с обем от 147 страници и се състои от увод, 3 глави, заключение, списък на публикациите по дисертационния труд, декларация за оригиналност и списък с използвана литература, включваща 143 заглавия.

На свое заседание, проведено на 02.09.2016 г. Научният съвет на Института по математика и информатика - БАН избра Научно жури в състав: проф. Аврам Ескенази, доц. д-р Димитрина Полимирова, доц. д-р Веселина Жечева, проф. Владимир Сълов, доц. д-р Николай Стоянов.

Защитата на дисертационния труд ще се състои на разширено заседание на секция „Софтуерни технологии и информационни системи“ при Института по математика и информатика – БАН на ……2016 г. от ……. ч. в ……зала.

Материалите по защитата са на разположение на интересуващите се в библиотеката на Института по математика и информатика – БАН.

Автор: Бонимир Пенчев Пенчев

Заглавие: *„Оптимизация на сигурността при мобилното банкиране”*

Научен ръководител: доц. д-р Димитрина Полимирова

СЪДЪРЖАНИЕ

УВОД

В продължение на повече от 40 години една от основните цели на финансовите институции е свързана с осигуряването на лесен достъп и удобство за своите клиенти при реализирането на банкови операции. Въпреки че АТМ устройствата и интернет банкирането представляват ефективни канали за предоставяне на традиционни банкови продукти, един сравнително нов вид банкиране - мобилното банкиране - има значителен ефект върху пазара. За неговата актуалност и непрекъснато развитие свидетелстват проучвания, проведени в различни региони на света и обхващащи както развитите, така и развиващите се страни [1].

Постоянното развитие в посока по-широко разпространение на мобилното банкиране се дължи и на предимствата, които то предоставя както на банките, така и на техните клиенти [2]. Този канал позволява на потребителите да изпълняват финансови операции навсякъде, по всяко време, на по-ниска цена и без да е необходимо да посещават банков офис. От друга страна мобилното банкиране предлага стратегически предимства и на банките. То може да се използва като възможност за достигането до нови клиенти, може да подобри репутацията на организацията и нейните продукти или да послужи за провеждането на маркетингови кампании.

Въпреки тези предимства, използването на мобилни устройства с цел реализирането на банкови транзакции или получаването на достъп до финансова информация, не е толкова широко разпространено, както се очаква [3]. Това от своя страна свидетелства за съществуването на определени фактори, които оказват негативно влияние върху по-мащабното възприемане на мобилното банкиране.

АКТУАЛНОСТ

Установихме наличието на голям брой изследвания, които идентифицират различните пречки, оказващи влияние върху потребителя при вземане на решение относно използването на мобилно банкиране. След щателно проучване, резултатите не само ясно показаха, че в действителност съществуват различни фактори, които оказват негативно влияние върху потребителите при възприемане на мобилното банкиране, но и потвърдиха, че различните рискове, свързани с неговата сигурност, съществено въздействат при вземане на решение за неговото използване.

В своето проучване от 2014 г. Heggestuen [4] представя резултати, които показват, че потребителите имат желание да използват мобилното банкиране, но при условие, че те са уверени в неговата сигурност.

Като доказателство за продължаващата актуалност на посочения проблем са и резултатите от проучване, направено през 2015 [5] и представящо конкретни страхове на потребителите по отношение на сигурността на мобилното банкиране: страх от прихващане на данни, съдържащи финансова информация; възможност за компрометиране на мобилното устройство; вероятност от изгубване или кражба на мобилното устройство; опасения, че на мобилното устройство може да бъде инсталиран злонамерен софтуер.

ЦЕЛ И ЗАДАЧИ НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд има за цел да предложи някои подобрения, които едновременно да доведат до повишаване на сигурността при мобилното банкиране и до повишаване на доверието на потребителя при използването на тази услуга.

С оглед реализирането на целта са дефинирани следните задачи:

1. Да се изследва и анализира текущото състояние на информационната сигурност в процесите на мобилното банкиране.
   1.1. Да се определи същността на мобилното банкиране.
   1.2. Да се посочат проблемните области и свързаните с тях заплахи за потребителя като основен участник в процеса на мобилно банкиране.
   1.3. Да се изследват добрите практики и стратегии за защита, използвани за противодействие на съществуващите заплахи.
   1.4. Да се посочат подобрения, които могат да бъдат реализирани с цел противодействие на съществуващите заплахи.
2. Да се предложат нови или подобрени механизми за сигурност, които да внесат необходимите подобрения по отношение на сигурността при мобилното банкиране.
3. Да се реализира експериментално внедряване на предложените механизми за сигурност, като резултатите от него се използват за анализ на тяхната ефективност.

ОСНОВНИ ЕЛЕМЕНТИ НА ДИСЕРТАЦИОННИЯ ТРУД

Настоящият дисертационен труд се състои от увод, три глави, заключение, списък на публикациите по дисертационния труд, декларация за оригиналност и списък с използваната литература, включваща 143 заглавия.

В увода са формулирани целта и задачите на дисертационния труд и е обоснована необходимостта от повишаване на сигурността при мобилното банкиране, като са приведени данни от проучвания в областта.

Основната задача на първа глава е да се изследва и анализира текущото състояние на информационната сигурност в процесите на мобилното банкиране. Първоначално в нея представяме същността на мобилното банкиране, въз основа на което определяме и проблемните области, които съществуват за неговата сигурност, заедно със най-често реализираните атаки във всяка от тях. За всяка от дефинираните атаки изследваме текущо използваните добри практики и стратегии за защита, като установяваме необходимостта да бъдат внесени някои подобрения за сигурността във всяка една от проблемните области при потребителя.

Във втора глава разработваме концептуален модел за повишаване на сигурността при мобилното банкиране. Първоначално разглеждаме същността и обхвата на предложения модел и модулите, които той следва да включва. С цел да се добие по-пълна представа относно общата архитектура и функционалните възможности на представените модули, всеки от тях е допълнително разгледан като представяме съображенията за неговото проектиране, основните процеси, които следва да бъдат обхванати, както и входните и изходните параметри.

В трета глава оценяваме приложимостта на представения във втора глава концептуален модел за повишаване на сигурността при мобилното банкиране. Основната цел тук е да се изследва неговата ефективност. Тъй като в концептуалния модел участват пет различни модула, е необходимо да се изследва ефективността на всеки един от тях поотделно. Това е осъществено чрез реализирането на отделни експерименти за всеки модул, като за целта следваме обща методика на работа, включваща следните етапи: определяне на обхвата на експеримента, планиране на експеримента, провеждане на експеримента и представяне и анализ на резултатите.

В заключението са представени приносите на дисертационния труд и насоките за бъдеща работа.

ГЛАВА ПЪРВА: ИЗСЛЕДВАНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ПРОЦЕСИТЕ НА МОБИЛНОТО БАНКИРАНЕ

В настоящата глава изследваме и анализираме текущото състояние на информационната сигурност в процесите на мобилното банкиране, което е тясно свързано с целта на дисертационния труд.

1. Същност на мобилното банкиране.

Мобилното банкиране датира още от края на 1999 г., когато немската компания Paybox в сътрудничество с Deutsche Bank стартират първата такава услуга, като първоначално то е внедрено и тествано предимно в европейските страни – Германия, Испания, Швеция, Австрия и Великобритания.

В различните изследвания авторите често използват набор от термини, когато говорят за мобилното банкиране. С цел дефиниране на термина от гледна точка на настоящата разработка е необходимо да се разгледат различни негови определения, които са търпели изменение с течение на времето.

В резултат на направен анализ на наличните дефиниции, с цел да се определят техните сходства и различия и след изследване на текущото състояние на мобилното банкиране предлагаме следната работна дефиниция:

Мобилното банкиране е канал, предоставен от банкова или небанкова организация, който позволява на потребителя реализирането на активни и пасивни банкови транзакции и справки навсякъде и по всяко време с помощта на мобилно устройство, като мобилен телефон, смартфон или таблет.

Тези дефиниция е синтезирана за целите на дисертационния труд, но по същество има по-универсален характер и е много по-широко приложима. Като изхождаме от нея, на фиг. 1 представяме основните участници в процеса на мобилното банкиране.

Фиг. 1. Основни участници в процеса на мобилно банкиране

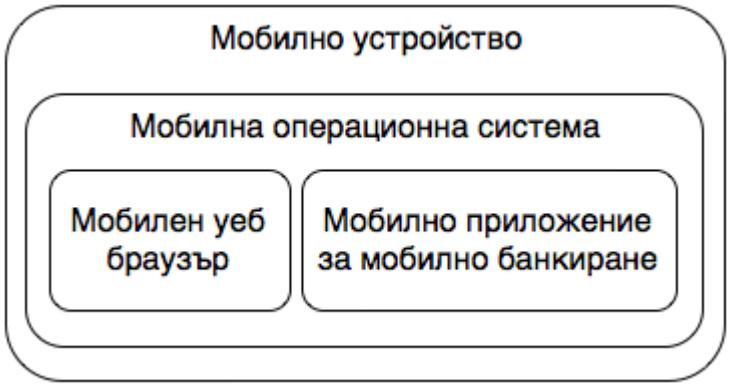
След като изследвахме същността на мобилното банкиране можем да пристъпим към определянето на проблемните области за неговата сигурност.

2. Проблемни области за сигурността при мобилното банкиране.

Сигурността при мобилното банкиране се определя като сложен процес поради наличието на различни участници при неговата реализация [6, 7]. Въпреки че проблеми, свързани със сигурността, могат да се наблюдават при всички основни участници в процеса на мобилно банкиране (вж. фиг. 1), необходимо е обхватът на настоящата разработка да се стесни, като избираме фокусът да е върху потребителя, тъй като той най-често се посочва като най-слабото звено по отношение на сигурността [8].

Това означава, че няма да изследваме проблеми, свързани със сигурността на банковите системи или услугите, които се изпълняват на техните сървъри, нито със сигурността на средата, служеща за пренос на информацията и предоставяна от мобилен оператор или доставчик на интернет услуги.

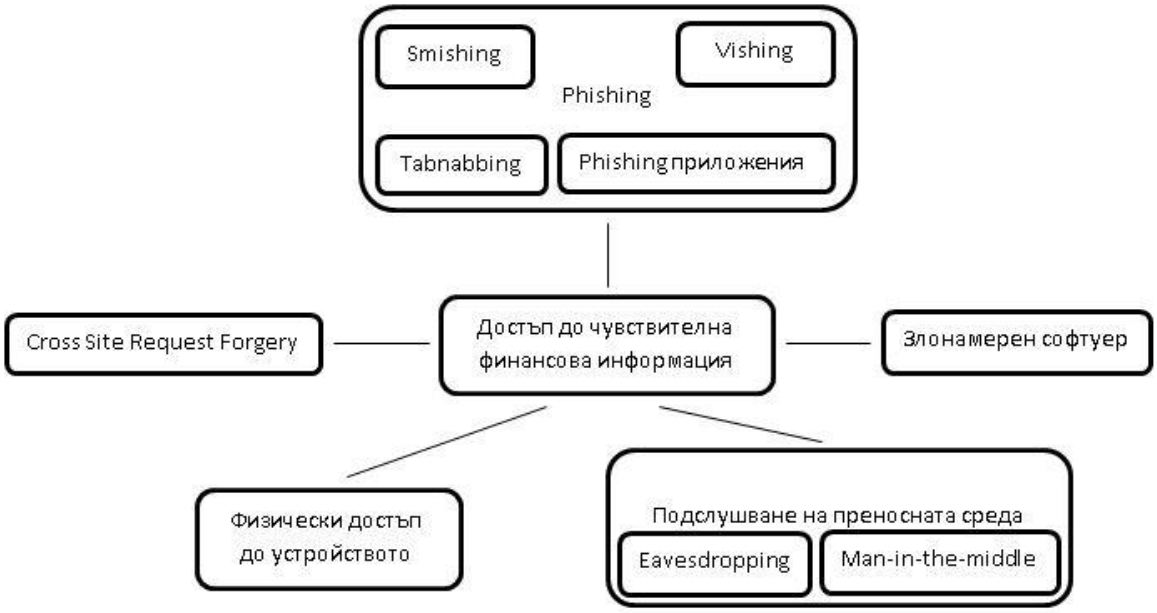
Въз основа на изследване на същността на мобилното банкиране могат да бъдат посочени четири основни проблемни области при потребителя по отношение на сигурността при мобилното банкиране (вж. фиг. 2): мобилно устройство, мобилен уеб браузър, мобилна операционна система и мобилно приложение за мобилно банкиране.



Фиг. 2. Проблемни области при потребителя по отношение на сигурността при мобилното банкиране

След като определихме основните проблемни области при потребителя за сигурността при мобилното банкиране, за всяка от тях е необходимо да изследваме съществуващите уязвимости и свързаните с тях заплахи.

В резултат на направения аналитичен обзор на съществуващите заплахи при четирите проблемни области за сигурността на мобилното банкиране при потребителя можем да представим най-често реализираните атаки (вж. фиг. 3): подслушване на преносната среда (eavesdropping, man-in-the-middle), Cross Site Request Forgery атака, неупълномощен физически достъп до устройството, phishing атака (vishing, smishing, tabnabbing, phishing приложения), злонамерен софтуер.



Фиг. 3. Най-често реализираните атаките, насочени към сигурността на мобилното банкиране при потребителя

След като определихме и систематизирахме най-често реализираните атаки, които съществуват за сигурността на мобилното банкиране при потребителя пристъпваме към изследване на различните практики, които понастоящем се използват за справяне с тях.

3. Стратегии за защита и добри практики за реализиране на сигурност при мобилното банкиране

В научната литература за всяка една от посочените на фиг. 3 атаки съществува широк набор от добри практики и стратегии за защита. Установихме обаче, че не всички от тях са достатъчно ефективни и това налага внасянето на някои подобрения, които да повишат сигурността на мобилното банкиране във всяка една от проблемните области при потребителя.

По отношение на мобилното устройство най-сериозно подобрение може да бъде направено при удостоверяването на потребителя. Основната цел е

отстраняването на недостатъците при използването на пароли и ПИН кодове при мобилните устройства [9].

По отношение на мобилната операционна система една от насоките за подобрение се свързва с техническата неспособност на потребителите да вземат решения, свързани с предоставянето на определени позволения по време на инсталация на дадено мобилно приложение [10]. Друга насока е отстраняване на невъзможността на антивирусния софтуер, използван при мобилните устройства, да засича модифициран злонамерен софтуер [11].

По отношение на мобилния уеб браузър също съществуват две насоки за подобрение. Първата се свързва с трудното реализиране на обучение на потребителя по отношение на phishing атаките и необходимостта от използването на автоматизирани инструменти за защита от този вид атака. Подобно подобрение може да бъде направено и за защита от CSRF атака, тъй като голяма част от наличните механизми за защита биват реализирани на сървър, а не при потребителя [12].

По отношение на мобилното приложение за мобилно банкиране съществуват три насоки за подобрение. Първата се свързва с проблема, който се наблюдава при TLS протокола. Той се прилага в една малка част от приложенията за мобилно банкиране. Нещо повече, там където се прилага, продължават да се използват старите и по-несигурни версии, дори след като бъдат представени новите [13]. Втората има за цел да се избегнат phishing атаки или достъп до мобилното приложение в следствие на реализиран неупълномощен достъп, като за това е необходимо подобряване на удостоверяването. Третата насока се свързва с неуспехите при обучение на потребителя по отношение на определени препоръчителни действия, предлагани от доставчиците на услуги за мобилно банкиране.

Резултатите от литературния обзор потвърждават необходимостта от внасянето на някои подобрения, които едновременно да доведат до повишаване на сигурността при мобилното банкиране и до повишаване на доверието на потребителя при използването на тази услуга.

ГЛАВА ВТОРА: КОНЦЕПТУАЛЕН МОДЕЛ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ

В настоящата глава разработваме концептуален модел за повишаване на сигурността при мобилното банкиране.

1. Същност и обхват на концептуалния модел за повишаване на сигурността при мобилното банкиране.

За създаването на концептуалния модел за повишаване на сигурността при мобилното банкиране е необходимо първоначално да бъдат дефинирани конкретните изисквания към нея. Въз основа на направения анализ в първа глава на настоящата разработка можем да дефинираме следните четири основни изисквания:

- Да се реализира защита на мобилното устройство.
- Да се реализира защита на мобилната операционна система.
- Да се реализира защита на мобилния уеб браузър.
- Да се реализира защита на мобилното приложение за мобилно банкиране.

Изготвянето на концептуалния модел изисква определянето на необходимите логически стъпки, които трябва да бъдат реализирани с цел да бъдат удовлетворени изискванията за сигурността. За всяко едно от тях следва да бъде приложена обща методика, която се състои от следните етапи:

1. Дефиниране на най-често реализираните атаки и използваните от тях уязвимости.
2. Определяне на най-често използваните стратегии за защита и добри практики за противодействие на дефинираните атаки.
3. Изследване на ефективността на най-често използваните стратегии за защита и добри практики.
4. Формулиране на предложения за подобрения, които да доведат до повишаване на нивото на сигурността.
5. Проектиране на формулираните подобрения.
6. Реализация на проектираните подобрения.
7. Измерване на ефективността на имплементираните подобрения.

В първа глава за всяко от четирите дефинирани изисквания за сигурността реализирахме първите три етапа от общата методика, като се позовахме на изследваната литература и резултатите, постигнати от други автори. Тъй като се оказва, че не всички от съществуващите добри практики и стратегии за защита са достатъчно ефективни, се налага формулирането на предложения за подобрения, които да доведат до повишаване на нивото на сигурността. Предлагаме те да са следните:

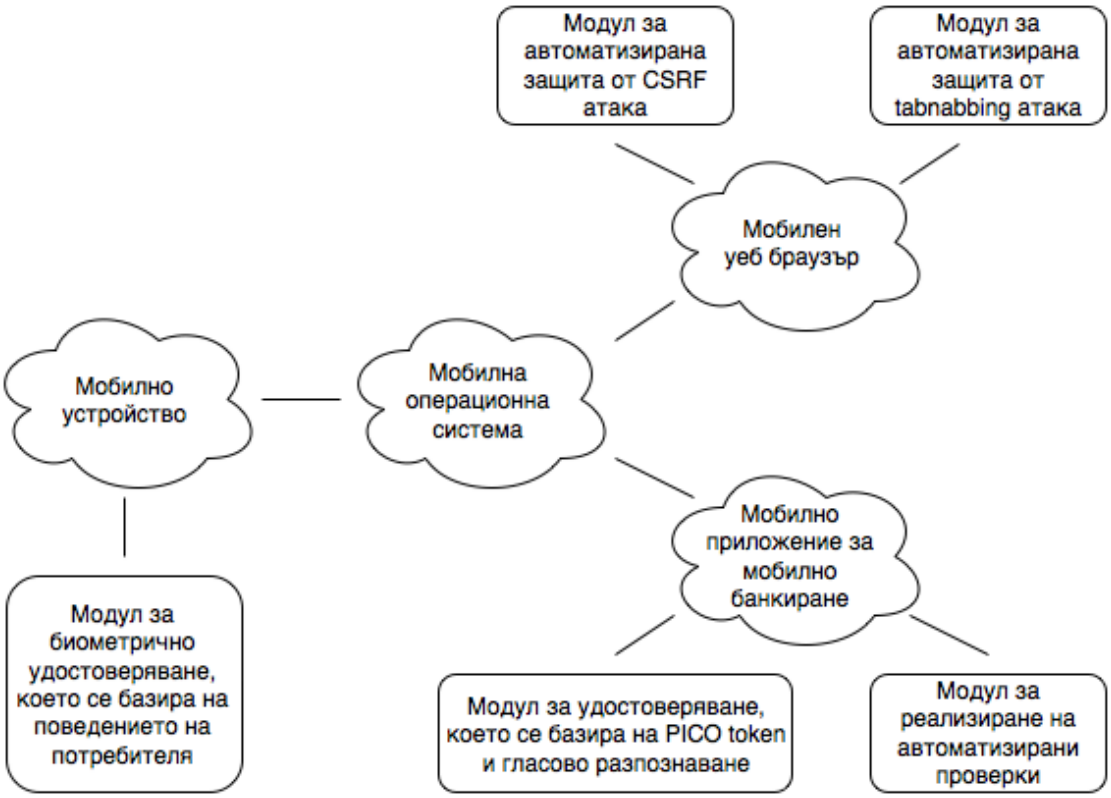
- За реализиране на защита на мобилното устройство:
  - метод за биометрично удостоверяване, който се базира на поведението на потребителя;
  - набор от автоматизирани проверки:
    - проверка за използването на некриптирана публична безжична мрежа;
    - проверка за включена функция за криптиране на данните на мобилната операционна система;
    - проверка за използване на механизъм за удостоверяване преди използване на мобилното устройство;
    - проверка за активирано автоматично заключване на мобилното устройството;
    - проверка за включена функция на мобилната операционна система, която да изтрива данните на мобилното устройство след реализирането на определен брой пъти неуспешно удостоверяване;
    - проверка за включена функция на мобилната операционна система за дистанционно заключване на мобилното устройство или за дистанционно изтриване на съдържанието му;
    - проверка за включените неизползваеми комуникационни интерфейси на мобилното устройство.
- За реализиране на защита на мобилната операционна система:
  - набор от автоматизирани проверки:
    - проверка за актуалността на версията на мобилната операционна система;
    - проверка за определяне дали мобилната операционна система е модифицирана;
    - проверка за инсталирано мобилно антивирусно приложение;
    - проверка за определяне успешното засичане на модифициран злонамерен софтуер от наличния антивирусен софтуер.

- За реализиране на защита на мобилния уеб браузър:
  - автоматизирана защита от CSRF атака;
  - автоматизирана защита от tabnabbing атака.
- За реализиране на защита на мобилното приложение за мобилно банкиране:
  - удобен метод за удостоверяване, който се базира на PICO token и гласово разпознаване;
  - набор от автоматизирани проверки:
    - проверка за определяне дали мобилното приложение използва TLS протокол за предаване на данните към сървъра и коя версия се използва;
    - проверка за актуалността на версията на мобилното приложението за мобилно банкиране.

След като са формулирани необходимите подобрения, можем да преминем към следващия етап - тяхното проектиране. На първо място е необходимо да вземем под внимание някои съображения, които да отговорят на основното предназначение на концептуалния модел - да позволи на доставчиците на услуги за мобилно банкиране да интегрират по-горе дефинираните подобрения в процеса по предоставянето му.

Тъй като реализирането на сигурността не е еднократен процес, е необходимо формулираните подобрения да бъдат организирани в относително независими единици (модули). По този начин се дава възможност при необходимост да могат да бъдат внесени допълнителни подобрения за сигурността, както под формата на нови модули, така и като допълнителни функционалности във всеки модул. Нещо повече, относителната независимост на отделните модули позволява промените или проблемите в някой от тях да имат минимален ефект върху състоянието на останалите. Естествено с цел реализирането на мащабируемост е необходимо да се реализира гъвкава връзка между независимите модули. В допълнение някои от подобренията могат да бъдат обединени в общ модул, където функционалността позволява.

Въз основа на казаното до тук предлагаме следната функционална структура на подобренията, които участват в концептуалния модел за повишаване на сигурността при мобилното банкиране (вж. фиг. 4).



Фиг. 4. Подобрения, участващи в концептуалния модел за повишаване на сигурността при мобилното банкиране

Всеки един от представените на фигурата модули следва да бъде допълнително разгледан, за да се добие по-пълна представа относно общата му архитектура и функционалните му възможности.

2. Модул за биометрично удостоверяване, което се базира на поведението на потребителя.

Настоящият модул следва да бъде реализиран като инструмент за идентифициране на потребителя на мобилното банкиране. Неговата основна функция следва да бъде осъществена на база на поведенчески характеристики, които се генерират в резултат на неговото взаимодействие със сензорния екран на мобилното устройство.

Основните процеси, които той следва да реализира, са:

- Събиране на определени входни данни (напр. вид движение при докосване, координати на точката на докосване, размер на точката на докосване, сила на натиск при докосване, време на реализиране на докосване) от сензорния екран на мобилното устройство.

- Извличане на отличителни белези от събраните входни данни, на база на които в последствие ще се създаде уникален подпис, който да се използва при удостоверяване на потребителя.

- Обучение на модула въз основа на извлечените отличителни белези, което да се състои от две фази – предварително обучение и последващо обучение. Когато потребителят използва устройството за първи път се активира предварителното обучение. След събиране на необходимите данни ще се активира последващото обучение, при което модулът ще продължава да се обучава за евентуални промени, който могат да настъпят в поведението на потребителя.

- Удостоверяване на потребителя, което се изразява в наблюдение на поведението му, като модулът следва да събира необходимите данни и да ги сравнява с изготвения по време на обучението уникален подпис.

3. Модул за автоматизирана защита от tabnabbing атака.

Преди проектирането на настоящия модул е проучен начина на функциониране на tabnabbing атаката, което е от значение при определянето на основните процеси, които трябва да участват в автоматизираната защита.

В резултат на това, **настоящият модул следва да представлява инструмент за засичане на възникналите промени на даден раздел на мобилния уеб браузър, когато той е бил извън фокуса на потребителя и за генериране на визуално предупреждение, което идентифицира промененото съдържание и помага на потребителя да разграничи легитимните промени от тези, използвани за реализиране на tabnabbing атака.**

Основните процеси, които той следва да реализира, са:

- Запомняне на начина, по който е изглеждал уеб сайтът, преди разделът, в който е зареден, да загуби фокус. За целта е необходимо да се направи снимка на съответния раздел, която да бъде съхранена и по-късно използвана.

- Сравняване с начина, по който ще изглежда разделът след възстановяване на фокуса, като тук е необходимо отново да се направи снимка, която да бъде сравнена с първоначално съхранената снимка.

- Представяне на засечените промени по подходящ начин на потребителя, за да може той ясно да идентифицира наличието на променено съдържание.

4. Модул за автоматизирана защита от CSRF атака.

Преди проектирането на настоящия модул е проучен начина на функциониране на CSRF атаката, което е от значение при определянето на основните процеси, които трябва да участват в автоматизираната защита.

В резултат на това, **настоящият модул следва да бъде реализиран като инструмент, който защитава нарушаването на цялостността на сесията за удостоверяване при изпращането на cross-site заявки. За осъществяване на това в мобилния уеб браузър на потребителя следва да се използва автоматичен алгоритъм за филтриране на заявките, който да реализира точно разграничаване между злонамерени и незлонамерени cross-site заявки и да отчита възможността за наличието на пренасочване.** Под автоматичен алгоритъм се разбира, че той не изисква никакво взаимодействие или конфигуриране от страна на потребителя.

Основните процеси, които той следва да реализира, са:

- Проверка на вида на генерираната заявка. Тук ще се определи дали източникът изисква от мобилния уеб браузър да реализира заявка за пренасочване към друг източник, а след това и дали генерираната заявка е стандартна или cross-site.

- Проверка на вида на cross-site заявката. Тук следва да се определи дали cross-site заявката е злонамерена или не.

- Определяне на състоянието на сесията, което мобилният уеб браузър трябва да прикрепи към генерираната заявка, като това следва да се реализира въз основа на предходно направените проверки.

5. Модул за удостоверяване, който се базира на PICO token и гласово разпознаване.

Настоящият модул следва да бъде реализиран като инструмент за идентифициране на потребителя пред мобилното приложение за мобилно банкиране на базата на комбиниране на PICO token, софтуерно вграден в мобилното устройство и биометричен механизъм за гласово разпознаване.

От архитектурна гледна точка настоящият модул следва да бъде реализиран като два основни компонента, предоставящи функционалности, които трябва да могат да бъдат интегрирани в мобилните приложения за мобилно банкиране.

Първият компонент следва да отговаря за удостоверяването на потребителя чрез софтуерен PICO token пред мобилното приложение за мобилно банкиране, в резултат на което той да получи възможност за работа с приложението и достъп до всички справочни услуги. При желание за реализиране на движение на парични средства е необходимо да бъде реализирано допълнително удостоверяване чрез гласово разпознаване, за което следва да отговаря вторият компонент.

Основните процеси, които следва да реализира първият компонент, са:

- Регистрация на потребителя, което се изразява в запомняне на потребителското име и паролата на потребителя в PICO token, тяхното криптиране със симетричен алгоритъм, разделяне на частния ключ на части и тяхното изпращане до допълнителни хардуерни устройства.

- Удостоверяване на потребителя, което се изразява в проверка за наличие на допълнителните хардуерни устройства, сглобяване на частния ключ и предоставяне на достъп до справочни услуги за мобилно банкиране.

Основните процеси, които следва да реализира вторият компонент, са:

- Получаване на гласов сигнал, като от потребителя се изисква да прочете динамично генерирана фраза, която се визуализира на екрана на мобилното устройство.

- Извличане на отличителни белези от получения гласов сигнал, като това следва да се реализира на сървър, до който се изпраща записаният гласов сигнал.

- Моделиране на профил на потребителя въз основа на извлечените отличителни белези, като за целта следва да се реализира обучение, което да се осъществи на сървъра.

- Сравнение на предварително съхранения моделиран профил с новосъздаден профил при постъпване на заявка за удостоверяване.

- Удостоверяване на потребителя, въз основа на резултата, получен при сравняването на гласовите профили.

6. Модул за реализиране на автоматизирани проверки.

Настоящият модул следва да бъде реализиран като инструмент, който осъществява определен набор от автоматизирани проверки, дефинирани от доставчиците на услуги за мобилно банкиране. Така той следва да помогне на потребителите да предприемат определени действия, които да доведат до повишаване на нивото на сигурността при мобилното банкиране.

От архитектурна гледна точка, модулът следва да бъде разделен на две основни части. Едната част следва да бъде реализирана като компонент на мобилното приложението за мобилно банкиране, като по този начин в него следва да бъдат интегрирани допълнителни функционалности. Другата част следва да бъде разположена на сървър, където ще се поддържа базата от данни и където следва да бъдат дефинирани проверките, които следва да бъдат реализирани.

Основните процеси, които следва да реализира модулът, са:

- Съставяне на списък от автоматизирани проверки в резултат на извършване на анализ на сигурността и оценка на риска, както и определяне на вида на съответната проверка - задължителна или препоръчителна.

- Съхраняване на дефинирания списък в база от данни, което ще позволи повторното използване и ефективното управление на автоматизираните проверки.

- Реализиране на дефинираните автоматизирани проверки, като за целта следва да се осъществи връзка с базата от данни, която се намира на сървъра и от където се установява броя и вида на проверките, които следва да бъдат реализирани. Първоначално следва да се започне със задължителните проверки. Само ако те преминат успешно се преминава към препоръчителните проверки.

- Представяне на резултатите на потребителя, като той получава достъп до услугите за мобилно банкиране, само ако задължителните проверки са преминали успешно.

ГЛАВА ТРЕТА: ПРИЛОЖЕНИЕ НА КОНЦЕПТУАЛНИЯ МОДЕЛ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ

В настоящата глава оценяваме приложимостта на представения във втора глава концептуален модел за повишаване на сигурността при мобилното банкиране. За реализирането на това осъществихме 5 експеримента, по един за всеки от представените във втора глава модули.

1. Модул за биометрично удостоверяване, което се базира на поведението на потребителите.

Настоящият експеримент има за цел да изследва ефективността и да определи най-подходящия алгоритъм за машинно обучение, който може да бъде използван в

модула за биометрично удостоверяване, което се базира на поведението на потребителите.

На всеки от участниците в експеримента последователно предоставихме мобилно устройство LG Nexus 5. На него предварително инсталирахме разработено от нас мобилно приложение, което използвахме да съберем входни данни (свързани с докосване) от сензорния екран на мобилното устройство. При работа с приложението на потребителя се даде възможност да сърфира в интернет и да реализира стандартни действия. Междувременно докато той си взаимодейства с разработеното мобилно приложение, то събира входните данни и ги записва в log файла на устройството.

Въз основа на данните от log файла ръчно изготвихме два файла във формат .arff, подходящи за софтуерния продукт KNIME. Първият .arff файл представлява тренировъчен набор, който се използва за реализиране на предварително обучение, което въз основа на входните данни класифицира потребителите на базата на избран алгоритъм. Вторият .arff файл служи за тестови набор, с чиято помощ определихме до колко избраният алгоритъм за машинно обучение правилно определя, че тестовите данни се класифицират към даден потребител.

Алгоритъм	Процент на грешка
Back-Propagation Neural Networks	5.32%
C4.5	19.5%
Naive Bayes	17.16%
Particle Swarm Optimization Radial Basis Function Network	1.8%
Radial Basis Function Network	8.9%
Repeated Incremental Pruning to Produce Error Reduction (RIPPER)	7.84%

Таблица 1. Резултати от тестване на алгоритмите за машинно обучение

Резултатите от експеримента (вж. табл. 1) показват, че грешката, която се постига при използването на алгоритъма Particle Swarm Optimization Radial Basis Function Network е 1.8%, което ни дава основание да заключим, че съответният алгоритъм за машинно обучение е подходящ за съответната задача. Представеният в таблица 1 процент на грешка е осреднена стойност от процентите на верните данни, погрешно оценени като неверни (false negatives) и на грешните данни, погрешно

оценени като верни (false positives). От тук на свой ред смятаме, че модулът за биометрично удостоверяване, което се базира на поведението на потребителите, следва да изпълни успешно своите функции по защита на мобилното устройство от неоторизиран достъп.

2. Модул за автоматизирана защита от tabnabbing атака

Настоящият експеримент има за цел да измери производителността на алгоритъма за засичане, участващ в модула за автоматизирана защита от tabnabbing атака. Под производителност ще разбираме необходимото време както за обработка на информацията, така и за предупреждаване на потребителя относно реализираните промени. За реализирането на целта последователно осъществихме измерване на времето необходимо за: прихващане на снимка на даден раздел на мобилния уеб браузър, разделяне на прихванатата снимка на части, сравнение между две снимки, представяне на разликите между двете снимки.

За да измерим времето, което е необходимо за прихващане на снимка на даден раздел на мобилния уеб браузър трябваше да създадем добавка за Firefox Mobile. Избрахме този мобилен уеб браузър, тъй като измежду най-широко използваните на този етап единствено той позволява инсталирането на добавки. Поради ограниченията на Add-on SDK (комплект за разработка на добавки за Firefox Mobile) избрахме и инсталирахме 6 добавки на стандартен уеб браузър Firefox (46.0.1), които предоставят възможност за прихващане на снимка на даден раздел на мобилния уеб браузър.

Резултатите от това измерване (вж. табл. 2) показаха, че средното време за изпълнение на тази операция е 113 мс.

Easy Screenshot	Awesome Screenshot Plus	Screengrab	Nimbus Screen Capture	Lightshot	Abduction
133 мс	107 мс	122 мс	103 мс	111 мс	100 мс

Таблица 2. Време в милисекунди (мс) за прихващане на снимка

За да измерим времето, което е необходимо за разделяне на прихванатата снимка на части разработихме JavaScript функция, която получава като входен параметър предварително изготвена снимка, разделя я на части и ги съхранява в масив. За нейни входни параметри изготвихме 8 различни снимки с помощта на

инсталираната по-рано добавка Easy Screenshot. Изготвените снимки се различават по следните критерии: съдържание на снимката (на два различни уеб сайта), разделителна способност (тествано е на 2 различни устройства – LG Nexus 5 и Vonino Sirius QS), размер на една част (10x10 пиксела и 15x15 пиксела).

Резултатите от това измерване (вж. табл. 3) показват, че средното време за изпълнение на функцията по разделяне на снимката на части е 50 мс. От тях установихме, че времето за реализирането на тази операция зависи от една страна от разделителната способност, а от друга от размерите на една част и не зависи от съдържанието на снимката или от хардуерните характеристики на устройството.

Снимка	Разделителна способност	Размер на една част	Време
Снимка 1	1024 x 768	10x10 пиксела	59 мс
Снимка 1	1366 x 768	10x10 пиксела	67 мс
Снимка 1	1366 x 768	15x15 пиксела	39 мс
Снимка 1	1024 x 768	15x15 пиксела	29 мс
Снимка 2	1024 x 768	10x10 пиксела	63 мс
Снимка 2	1366 x 768	10x10 пиксела	71 мс
Снимка 2	1366 x 768	15x15 пиксела	42 мс
Снимка 2	1024 x 768	15x15 пиксела	31 мс

Таблица 3. Време в милисекунди (мс) за разделяне на снимка на части

За да измерим времето за сравнение между две снимки разработихме JavaScript функция, която получава като входни параметри две снимки и реализира сравнение между всеки пиксел от едната снимка с всеки от другата. За нейни входни параметри изготвихме 5 различни снимки. Те се различават единствено по процента на промените, които са направени върху оригиналната снимка (0%, 25%, 50%, 75%, 100%).

Резултатите от това измерване (вж. табл. 4) показват, че не малко количество от време е консумирано от алгоритъма, реализиращ сравнението пиксел по пиксел на всяка част на снимката. Времето използвано от него е тясно свързано с броя на промените, които са настъпили на страницата. Това е така, тъй като реализирахме алгоритъма по такъв начин, че ако засече различие още на първия пиксел, да не проверява останалите пиксели. Следователно, при осъществяване на tabnabbing атака, ще има налични повече промени, които да бъдат засечени и алгоритъмът за сравнение следва да се реализира дори по-бързо.

Процент на промени спрямо оригиналната снимка	Милисекунди, изразходени за сравнение
0 %	119
25 %	90
50 %	58
75 %	29
100 %	5

Таблица 4. Зависимост между количеството на промените на оригиналната снимка и времето необходимо на алгоритъма за сравнение

За да измерим времето за визуализирането на разликите между две снимки трябваше да създадем добавка, която визуално ги представя на потребителя. Поради ограниченията на Add-on SDK, създадената от нас добавка, визуализира единствено съобщение, представящо процента на реализираните промени. Резултатите от това измерване показват, че информирането на потребителя се реализира бързо – за 1 мс.

Въз основа на резултатите получени при реализиране на четирите измервания можем да определим, че средното време необходимо на алгоритъма е 230 мс. От тях почти половината 113 мс се използва от приложно програмния интерфейс(API) на браузъра, което е извън нашия контрол. Измерването на производителността при така описаните ограничения ни дава основание да твърдим, че модулът успява достатъчно бързо да обработи информацията и да предупреди потребителя за реализираните промени. Това определя и неговата ефективност по отношение на tabnabbing атаката.

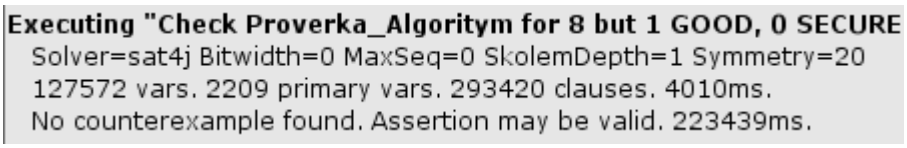
3. Модул за автоматизирана защита от CSRF атака

Настоящият експеримент има за цел да изследва ефективността на предложения от нас алгоритъм за филтриране при осъществяване на автоматизирана защита от CSRF атака.

За реализирането на това първоначално изготвихме формално описание на алгоритъма за филтриране. Като основа за формалното описание използвахме разработения от Akhawe [14] модел на уеб инфраструктурата, като за целите на експеримента внесохме нужните допълнения в модела. Въз основа на същия модел изготвихме и формално описание на CSRF атаката.

На база на изготвените формални описания реализирахме проверка на алгоритъма за филтриране по отношение на неговата ефективност при защита от

CSRF атака. За целта използвахме софтуерния инструмент за проверка на модели Alloy Analyzer, който позволява автоматизирано да се нарушат някои от свойствата на сигурността и така да се докаже или отхвърли валидността на даден модел.



Фиг. 5. Резултат от проверка на формалния модел на алгоритъма за засичане на tabnabbing атака

Резултатът от експеримента (вж. фиг. 5) показва, че не са открити примери (No counterexample found), които да свидетелстват, че злонамерен потребител може да генерира злонамерена cross-site заявка, като използва уеб браузъра на потребителя. Това от своя страна показва ефективността на предложения от нас алгоритъм за филтриране и възможността за използването му в модула за осъществяване на автоматизирана защита от CSRF атака.

4. Модул за удостоверяване, който се базира на PICO token и гласово разпознаване

Настоящият експеримент има за цел да направи оценка на модула за удостоверяване, който се базира на PICO token и гласово разпознаване.

Като основа за осъществяването на целта използвахме подход за оценка на уеб базирани механизми за удостоверяване, който е разработен от Bonneau [15]. Той се нарича UDS и се състои от 25 свойства, които са разделени в 3 основни категории: ползваемост (usability), разпространяемост (deployability) и сигурност (security). При него оценяването на даден механизъм за удостоверяване се реализира чрез проверка дали определените свойства са удовлетворени, като се използва тристепенна скала за оценка – да, почти и не.

Тъй като подходът на Bonneau не беше напълно съвместим с представения от нас модул за удостоверяване, сметнахме за необходимо той да бъде модифициран с цел по-добрата му приложимост. Поради тази причина дефинирахме нов подход за оценяване, в който включихме подмножество на свойствата дефинирани в UDS подхода. Към подмножеството добавихме и две допълнителни свойства, които са тясно свързани с token базираните механизми за удостоверяване:

- Продължително удостоверяване

- Различни нива на позволения

Последното, което реализирахме в настоящия експеримент беше да сравним модула с резултатите на алтернативни механизми (ПИН, парола, биометрики и token устройства), чиито оценки определихме на база публикацията на Bonneau [15].

Свойство	Модул	Token	ПИН	Биометрики	Парола
Липса на необходимост от запомняне	**да**	**да**	-	**да**	-
Липса на необходимост от физическо притежание	*почти*	-	**да**	**да**	-
Ефикасност при употреба	*почти*	*почти*	**да**	**да**	**да**
Безгрешно удостоверяване	*почти*	*почти*	*почти*	-	-
Лесно възстановяване при загуба	*почти*	-	**да**	**да**	**да**
Незначителна цена за потребител	*почти*	-	**да**	**да**	**да**
Добро развитие	-	**да**	**да**	*почти*	**да**
Устойчивост срещу физическо наблюдение	**да**	**да**	-	**да**	-
Устойчивост срещу измама	**да**	**да**	*почти*	-	*почти*
Устойчивост срещу налучкване	**да**	**да**	**да**	**да**	-
Устойчивост срещу phishing атака	**да**	**да**	**да**	-	-
Устойчивост срещу кражба	**да**	*почти*	**да**	**да**	**да**
Невъзможност за асоцииране	-	**да**	**да**	-	**да**
Продължително удостоверяване	**да**	*почти*	-	-	-
Различни нива на позволения	**да**	-	-	-	-

Таблица 5. Сравнение на различните механизми за удостоверяване

От резултатите представени в таблица 5 установяваме, че предложеният механизъм за удостоверяване, който се базира на PICO token и гласово разпознаване, по отношение на свойствата от категории („ползваемост“ и „разпространяемост“) отстъпва на алтернативните механизми. Въпреки това по отношение на свойствата от категория „сигурност“ той има най-висока оценка. В допълнение той удовлетворява свойството „липса на необходимост от запомняне“ и почти удовлетворява „липса на необходимост от физическо притежание“, които в първа глава посочихме като едни от основните проблеми, които потребителите изпитват, по отношение на удобството на удостоверяване. Затова считаме, че предложеният

метод за удостоверяване води до повишаване на сигурността при мобилното банкиране.

5. Модул за реализиране на автоматизирани проверки

Настоящият експеримент има за цел да определи как потребителите възприемат модула за реализиране на автоматизирани проверки.

На всеки от участниците в експеримента последователно предоставихме мобилно устройство LG Nexus 5. На него предварително инсталирахме разработено от нас мобилно приложение, което използвахме да реализира следните автоматизирани проверки:

- НБМ – проверка за използване на некриптирана публична безжична мрежа.
- КОС – проверка за включена функция за криптиране на данните на мобилната операционна система.
- МУ - проверка за използване на механизъм за удостоверяване преди използване на мобилното устройство.
- АЗ - проверка за активирано автоматично заключване на мобилното устройство.
- БТ - проверка за включен Bluetooth интерфейс на мобилното устройството.
- АОС - проверка за актуалността на версията на мобилната операционна система.
- МОС - проверка дали мобилната операционна система на потребителя е модифицирана.
- АВ - проверка за инсталирано мобилно антивирусно приложение.

След стартиране на приложението, резултатът, който получава всеки потребител е, че нито една от автоматизираните проверки не е преминала успешно, той вижда кои от тях са задължителни (МБ, АЗ, АОС) и кои препоръчителни (останалите), както и стойността на индикатора за сигурност, която е „0 от 11“. Индикаторът за сигурността се изчислява на базата на следната система за оценка:

- Ако проверката е задължителна и е преминала успешно – 2т.
- Ако проверката е препоръчителна и е преминала успешно – 1т.
- Ако проверката не е преминала успешно – 0 т.

След това на потребителите, които желаят да удовлетворят неуспешно преминалите проверки предоставихме възможност да го направят без или с получаване на допълнителни инструкции, в зависимост от тяхната компетентност и желание. Инструкциите, които всеки потребител следва да предприеме, за да удовлетвори някоя от проверките, подготвихме предварително в хартиен вариант.

На всеки от потребителите осигурихме необходимото време за работа като междувременно наблюдавахме взаимодействието им с модула и реализирахме следните наблюдения:

- Опитва ли се потребителят да удовлетвори неуспешно преминалите проверки или се отказва да използва приложението за мобилно банкиране.
- Знае ли потребителят как да удовлетвори неуспешно преминалите проверки без да получава допълнителни инструкции.
- Предоставените от нас инструкции подпомагат ли за по-лесното удовлетворяване на неуспешно преминалите проверки.
- Склонен ли е потребителят да пренебрегне препоръчителните проверки.
- До каква степен потребителят подобрява индикатора за сигурност в края на експеримента.

След провеждането на експеримента получихме описаните по-долу резултати.

От тестваните 30 потребители още в самото начало на експеримента 5 заявиха, че предпочитат да ползват мобилния уеб браузър, за да реализират мобилно банкиране, след като разбират, че за да използват мобилното приложение за мобилното банкиране е необходимо да удовлетворят определени изисквания. Като причина те посочват, че извършват само справочни операции и затова смятат, че не е нужно да отделят време за удовлетворяване на изискванията.

В таблица 6 са представени резултатите на останалите 25.

Проверка	**Брой потребители, реализирали проверката**		**Общ брой потребители**		
	***без* инструкции**	***с* инструкции**	***реализирали*** **проверката**	***не са реализирали*** **проверката**	***опитали да реализират*** **проверката**
НБМ	1	4	5	3	8
КОС	2	4	6	2	8
МУ	**12**	**10**	**22**	**3**	**25**
АЗ	**6**	**16**	**22**	**3**	**25**
БТ	5	2	7	1	8
АОС	**8**	**14**	**22**	**3**	**25**
МОС	0	0	0	8	8
АВ	1	2	3	5	8

Таблица 6. Резултати от действията на потребителите

От таблица 6 установяваме, че 22-ма (88%) от потребителите успяха да реализират и трите задължителни проверки, а 3-ма от тях не можаха да реализират нито една от проверките, дори и след предоставянето на необходимите инструкции. Като причина посочиха, че инструкциите не са достатъчно ясни. От тук можем да направим извод, че предоставените инструкции имат нужда от допълнително подобрение.

Нещо друго, което прави впечатление е броят на потребителите опитали да реализират препоръчителните проверки. Те са само 8 тъй като останалите открито заявиха, че ще се опитат да изпълнят само задължителните проверки. От тук можем да направим извод, че потребителят по-успешно реагира на задължителните проверки и затова те могат да бъдат по-успешно прилагани в настоящия модул.

На фиг. 6 представяме резултатите отразяващи процента на удовлетворените проверки като е разграничено, кои от тях са направени без или с допълнителни инструкции.

Фиг. 6. Процент на удовлетворените проверки

От фиг. 6 установяваме, че 75% от проверките са реализирани от над 60% от заявилите желание да го направят. Една част от потребителите имат необходимите знания, за да удовлетворят неуспешно преминалите проверки. Въпреки това, при 63% от проверките се вижда, че успеваемостта се дължи на предоставените допълнителни инструкции. Това показва както необходимостта от изготвянето им, така и тяхната полза за потребителите.

Сериозно различие наблюдаваме при проверката за модифицирана операционна система. Във връзка с това, потребителите заявиха, че техните системи са модифицирани и затова са решили да не удовлетворят съответната проверка.

Резултатите от експеримента показват, че 74% от всичките потребители (30 души) подобряват с най-малко 55% индикатора си за сигурност, тъй като това е процентът на тези, които са реализирали задължителните проверки. При тези заявили желание да удовлетворят и препоръчителните проверки този процент е дори с по-висока стойност. Това ни дава основание да твърдим, че ако модулът за автоматизирани проверки бъде разработен в пълната си функционалност би повишил нивото на сигурността при мобилното банкиране.

ЗАКЛЮЧЕНИЕ

В дисертационния труд са разгледани актуални въпроси, свързани с начините да се повиши сигурността на мобилното банкиране, което да повлияе положително на потребителите при възприемането на този вид банкиране.

Предложили сме концептуален модел за повишаване на сигурността при мобилното банкиране. Акцентът е поставен върху идентифицирането на най-често реализираните атаки свързани със сигурността на мобилното банкиране, анализ на ефективността на най-често използваните стратегии за защита и добри практики, формулирането на конкретни подобрения, обособяването им в модули и представяне на общата архитектура и функционалните възможности на всеки от тях.

С цел да се изследва ефективността на всеки от модулите участващи в по-рано представения концептуален модел сме провели експериментално изследване. Резултатите от него потвърждават приложимостта на концептуалния модел и в частност тази на всеки един от представените модули.

Считаме, че работата по темата може да бъде продължена поне в следните няколко насоки:

- Реализиране на подобрения по отношение на сигурността на мобилното банкиране, които не са включени в предложения концептуален модел във втора глава.
- Повтаряне на експеримента по отношение на модула за автоматизирана защита от tabnabbing атака, след като бъдат отстранени наличните в момента ограничения, свързани с реализирането му.

- Подобряване на модула за удостоверяване, който се базира на PICO token и гласово разпознаване с цел повишаване на оценката му спрямо алтернативните механизми, чрез повишаване на стойностите на свойствата от категориите „ползваемост“ и „разпространяемост“.
- Реализиране на допълнителни по-широкообхватни изследвания за всеки от предложените модули, които да осигурят статистически значими резултати.
- Разработване и тестване на пълната функционалност на предложения модел за повишаване на сигурността при мобилното банкиране.

НАУЧНИ И НАУЧНО-ПРИЛОЖНИ ПРИНОСИ

В резултат на проведеното изследване в настоящия дисертационен труд са постигнати следните научни и приложни приноси:

1. На базата на анализираните литературни източници синтезирахме нова дефиниция за мобилно банкиране, която е широко приложима и има универсален характер. (Задача 1.1)
2. Определихме и систематизирахме най-често реализираните атаки и използваните от тях уязвимости във всяка една от проблемните области за сигурността при потребителя на мобилното банкиране. (Задача 1.2)
3. Установихме какви подобрения могат да бъдат внесени, за да се повиши сигурността на мобилното банкиране във всяка една от проблемните области при потребителя. (Задача 1.3 и задача 1.4)
4. Предложихме 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. (Задача 2)
5. Доказахме ефективността на всеки един от предложените механизми за сигурност, присъстващ в предложения концептуален модел за повишаване на сигурността при мобилното банкиране. (Задача 3)

ПУБЛИКАЦИИ ВЪВ ВРЪЗКА С ДИСЕРТАЦИОННИЯ ТРУД

Публикациите, свързани с дисертационния труд, са следните:

1. Penchev, B. Effectiveness of a Conceptual Model for Increased Mobile Banking Security. Serdica Journal of Computing, 2016. (под печат). Публикацията е свързана с принос 5.
2. Пенчев, Б. Повишаване на сигурността при мобилното банкиране чрез реализирането на автоматизирани проверки на мобилното устройство. Компютърни науки и комуникации, 2016, 5(1), ISSN: 1314-7846, с. 3-8. Публикацията е свързана с принос 4.
3. Пенчев, Б. Концептуален модел за повишаване на сигурността при мобилното банкиране. Сборник с доклади от четвърта международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново, 2016, 2, ISSN: 1310-3946, с. 50-53. Публикацията е свързана с принос 4.
4. Penchev, B. Security Issues in Mobile Banking. Proceedings of International Conference „Human Systems Integration Approach to Cyber Security“, Sofia, 2016, ISBN: 978-954-9348-77-4, p. 135-144. Публикацията е свързана с принос 3.
5. Penchev, B. Mobile Banking Security Practices for Android Users. International Journal "Information Technologies & Knowledge", 2015, 9(3), ISSN: 1313-0455, p. 237-246. Публикацията е свързана с принос 2.
6. Пенчев, Б. Фактори, оказващи негативно влияние върху потребителите при възприемане на мобилното банкиране. Известия на Съюза на учените – Варна, Серия „Икономически науки“, Варна, 2015, ISSN: 1314-7390, с. 150-155. Публикацията е свързана с принос 3.
7. Пенчев, Б. Приоритетни канали за реализация на мобилно банкиране. Сборник с доклади от международна научна конференция, посветена на 45 годишнината от създаването на катедра „Информатика“ в Икономически университет – Варна, Варна, 2014, ISBN: 978-954-21-0780-4, с. 150-157. Публикацията е свързана с принос 1.

Изнесените доклади, свързани с дисертационния труд, са:

1. Доклад на тема „Концептуален модел за повишаване на сигурността при мобилното банкиране“, представен на четвъртата международна научна

конференция „Техника. Технологии. Образование. Сигурност“, проведена на 01-03.06.2016 във Велико Търново.

2. Доклад на тема “Фактори, оказващи негативно влияние върху потребителите при възприемане на мобилното банкиране“, представен на научна конференция „Науката в служба на обществото“, проведена на 30.10.2015 във Варна.
3. Доклад на тема „Security Issues in Mobile Banking“, представен на международната научна конференция „Human Systems Integration Approach to Cyber Security“, проведена на 28-29.09.2015 в София.
4. Доклад на тема „Приоритетни канали за реализация на мобилно банкиране“, представен на международна научна конференция „Информационните технологии в бизнеса и образованието“, проведена на 17.10.2014 във Варна..

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Global Mobile Statistics 2014 Section G: Mobile Banking and m-money; Section H: Venture Capital (VC) Investment in Mobile. https://mobiforge.com/research-analysis/global-mobile-statistics-2014-section-g-mobile-banking-and-m-money-section-h-venture-capital-vc-inve. 14.05.2015.

[2] Esmaili, E., M. I. Desa, H. Moradi, A. Hemmati. The Role of Trust and Other Behavioral Intention Determinants on Intention toward Using Internet Banking. International Journal of Innovation, Management and Technology, 2011, 2(1), p. 95-100.

[3] Mobile Banking Handset & Tablet Market Strategies 2013–2017. http://www.juniperresearch.com/reports/mobile_banking. 05.07.2015.

[4] Heggestuen, J. The Future Of Mobile And Online Banking: 2014. http://www.businessinsider.com/the-future-of-mobile-and-online-banking-2014-slide-deck-2014-10. 17.07.2015.

[5] Consumers and Mobile Financial Services 2015. http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf. 14.05.2015.

[6] He, W. A Review of Social Media Security Risks and Mitigation Techniques. Journal of Systems and Information Technology, 2012, 14(2), p. 171-180.

[7] Lee, H., Y. Zhang, K. L. Chen. An Investigation of Features and Security in Mobile Banking Strategy. Journal of International Technology and Information Management, 2013, 22(4), p. 23-46.

[8] Министерство на отбраната. Национална стратегия за кибер сигурност "Кибер устойчива България 2020". http://www.cyberbg.eu/doc/Cyber%20Security%20Strategy%20BG%20-%20final%20draft%20%205%203.pdf. 15.07.2016

[9] Consumer Reports. Smart Phone Thefts Rose to 3.1 Million in 2013. http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm. 17.07.2015.

[10] Felt, A. P., K. Greenwood, D. Wagner. The Effectiveness of Application Permissions. Proceedings of the USENIX Conference on Web Application Development, 2011, p. 1-12.

[11] Rastogi V., Y. Chen, X. Jiang. DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013, p. 329-334.

[12] Czeskis, A., A. Moshchuk, T. Kohno, H. J. Wang. Lightweight Server Support for Browser-based CSRF protection. Proceedings of the 22nd International Conference on World Wide Web, 2013, p. 273–284.

[13] Qualys. Trustworthy internet movement - SSL pulse. https://www.trustworthyinternet.org/ssl-pulse. 31.03.2016.

[14] Akhawe, D., A. Barth, P. E. Lam, J. C. Mitchell, D. Song. Towards a Formal Foundation of Web Security. Proceedings of the 23rd IEEE Computer Security Foundations Symposium, 2010, p. 290–304.

[15] Bonneau, J., C. Herley, P. Oorschot, F. Stajano. The Quest to Replace Passwords: a Framework for Comparative Evaluation of Web Authentication Schemes. Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012, p. 553-567.