

**БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ**  
**ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА**  
**СЕКЦИЯ “СОФТУЕРНИ ТЕХНОЛОГИИ**  
**И ИНФОРМАЦИОННИ СИСТЕМИ”**

# **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**

# СЪДЪРЖАНИЕ

<b>УВОД .....</b>	<b>3</b>
<b>ГЛАВА ПЪРВА: ИЗСЛЕДВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ПРОЦЕСИТЕ НА МОБИЛНОТО БАНКИРАНЕ.....</b>	<b>9</b>
1. Същност на мобилното банкиране.....	9
2. Проблемни области за сигурността при мобилното банкиране ....	18
2.1. Заплахи за сигурността при мобилното устройство .....	20
2.2. Заплахи за сигурността при мобилната операционна система ..	23
2.3. Заплахи за сигурността при мобилния уеб браузър.....	25
2.4. Заплахи за сигурността при мобилното приложение за мобилно банкиране.....	27
3. Стратегии за защита и добри практики за реализиране на сигурност при мобилното банкиране .....	30
3.1. Защита от Eavesdropping и Man-in-the-middle атаки.....	31
3.2. Защита от Cross Site Request Forgery (CSRF) атака.....	33
3.3. Защита от неупълномощен физически достъп.....	35
3.4. Защита от phishing атака.....	37
3.5. Защита от злонамерен софтуер.....	41
4. ЗАКЛЮЧЕНИЕ .....	43
<b>ГЛАВА ВТОРА: КОНЦЕПТУАЛЕН МОДЕЛ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ .....</b>	<b>48</b>
1. Същност и обхват на концептуалния модел за повишаване на сигурността при мобилното банкиране .....	48
2. Модул за биометрично удостоверяване, което се базира на поведението на потребителите .....	54
3. Модул за автоматизирана защита от TAVNABBINING АТАКА.....	58
4. Модул за автоматизирана защита от CSRF АТАКА.....	64
5. Модул за удостоверяване, който се базира на PICO TOKEN И ГЛАСОВО РАЗПОЗНАВАНЕ .....	70
6. Модул за реализиране на автоматизирани проверки .....	79
7. ЗАКЛЮЧЕНИЕ .....	84

<b>ГЛАВА ТРЕТА: ПРИЛОЖЕНИЕ НА КОНЦЕПТУАЛНИЯ МОДЕЛ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ .....</b>	<b>87</b>
1. Модул за биометрично удостоверяване, което се базира на поведението на потребителите.....	88
2. Модул за автоматизирана защита от TABNAVBING АТАКА.....	93
3. Модул за автоматизирана защита от CSRF АТАКА.....	100
4. Модул за удостоверяване, който се базира на PICO token и ГЛАСОВО РАЗПОЗНАВАНЕ .....	107
5. Модул за реализиране на автоматизирани проверки .....	115
6. ЗАКЛЮЧЕНИЕ .....	122
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>127</b>
<b>СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД.....</b>	<b>129</b>
<b>ДЕКЛАРАЦИЯ ЗА ОРИГИНАЛНОСТ .....</b>	<b>131</b>
<b>ИЗПОЛЗВАНА ЛИТЕРАТУРА.....</b>	<b>132</b>

## 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. Началото започва с въвеждането в експлоатация на АТМ<sup>1</sup> (Automated Teller Machine) устройствата през 1969 година. Тогава този вид машини са позволявали изпълнението на прости банкови операции като теглене на пари, докато в момента предоставят на клиентите по-широк набор от финансови услуги. В средата на 90-те години навлиза интернет банкирането, което позволява на потребителите по всяко време да имат достъп до обслужващата ги банка. По този начин те могат лесно и удобно да се възползват от различни банкови услуги като да получават информация за сметката си, да заявяват банкови извлечения или да осъществяват транзакции като прехвърляне на средства от една сметка в друга.

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 [1]. За неговата актуалност и непрекъснато развитие свидетелстват проучвания, проведени в различни региони на света и обхващащи както развитите, така и развиващите се страни [2, 3, 4, 5]. Търсенето на финансови услуги, предоставяни чрез мобилно банкиране, нараства и следствие на повсеместната употреба на смартфоните. Понастоящем броят на потребителите, които притежават такъв вид мобилен телефон, в световен мащаб е над 1.2 милиарда [6]. В

---

<sup>1</sup> Навсякъде в дисертационния труд където няма подходящ превод на български език са използвани оригиналните названия на термините в оригиналното им изписване на английски език.

резултат на това все повече банки предоставят мобилно банкиране, заедно с нов набор от продукти и приложения, разработени с цел да разширят достъпа си до клиенти, да подобрят начините за тяхното задържане, да повишат ефективността си и да разширят пазарния си дял [7].

Постоянното развитие в посока по-широко разпространение на мобилното банкиране се дължи и на редица предимства, които то предоставя както на банките, така и на техните клиенти. Този канал позволява на потребителите да изпълняват финансови операции (проверка на актуален баланс по сметка или проследяване на текущи транзакции) навсякъде, по всяко време, на по-ниска цена [8, 9] и без да е необходимо да посещават банков офис [10]. От друга страна мобилното банкиране предлага стратегически предимства и на банките. То може да се използва като възможност за достигането до нови клиенти [11, 12, 13], може да подобри репутацията на организацията и нейните продукти [14, 15] или да послужи за провеждането на маркетингови кампании [16].

Въпреки тези предимства, използването на мобилните телефони и таблети, с цел реализирането на банкови транзакции или получаването на достъп до финансова информация, не е толкова широко разпространено, както се очаква [17, 18, 19]. През 2013 г. Juniper Research [20] предсказва, че до 2017 г. се предполага 1 милиард потребители да използват мобилно банкиране, което представлява едва 15% от всички абонаменти за мобилни услуги [21]. Тази тенденция показва, не само че има значителни възможности за развитие по отношение на броя на потребителите, използващи мобилно банкиране, но също и че съществуват определени фактори, които оказват негативно влияние върху по-мощното му възприемане.

Съществуват голям брой изследвания, които идентифицират различните пречки, оказващи влияние върху потребителя при вземане на

решение относно използването на мобилно банкиране. Диференцират се два основни подхода, които се използват от различните автори. Едните се насочват към класифицирането на съществуващите фактори, влияещи негативно на мобилното банкиране, а другите си поставят за цел да изследват влиянието на конкретен фактор.

Първата група автори като Chemingui [22], Cruz, Laukkanen и Munoz [23], Laukkanen и Cruz [24], Laukkanen [25], Laukkanen и Kiviniemi [26] се обединяват около сравнително сходна класификация на факторите, въздействащи върху възприемането на мобилното банкиране. В нея Chemingui посочва, че от гледна точка на потребителите съществуват функционални и психологически фактори. Както Laukkanen [27], така и Cruz и Munoz [23] към функционалните бариери отнасят различни рискови фактори като финансов риск, икономическа загуба и рискове, свързани със сигурността на мобилното банкиране.

Въпреки че втората група автори изследват конкретно определени фактори, влияещи негативно върху възприемането на мобилното банкиране, те в голяма степен се доближават до класификацията, около която се обединява първата група. Jain [28], Lee и Chung [29], Lin [30] и Zhou [31] доказват, че нивото на доверие оказва значителен ефект върху нивото на удовлетвореност и затова е важен фактор при вземане на решение от страна на потребителите дали да използват мобилното банкиране.

Въпреки че посочените изследвания обхващат сравнително широк времеви обхват от 2007 до 2013 г. във всяко от тях присъства въпросът за сигурността на мобилното банкиране, като тя е един от основните фактори, които потребителите посочват като пречка при вземане на решение за използване на този канал. Като доказателство за продължаващата актуалност на посочения проблем са и резултатите от проучване, направено

през 2015 [2] 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.

В проучване от 2014 г. Heggstuen [32] показва, че запитани относно сигурността при мобилно банкиране, 31% от потребителите имат желание да платят за допълнителни функции за сигурност, 63% от тях желаят да сменят сметката си с друга, притежаваща по-добра сигурност, а 71% желаят да получат сметка, която гарантира, че евентуални загуби следва да бъдат възстановени. Това е индикатор, че потребителите имат желание да използват мобилното банкиране, но при условие, че те са уверени в неговата сигурност.

В резултат на всичко казано до тук е дефинирана **целта** на настоящата разработка. **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 поставената цел 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.

Настоящият дисертационен труд е структуриран в три глави.

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.

# **ГЛАВА ПЪРВА: ИЗСЛЕДВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ПРОЦЕСИТЕ НА МОБИЛНОТО БАНКИРАНЕ**

Основната задача на настоящата 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.

## **1. Същност на мобилното банкиране**

През последните две десетилетия се наблюдава непрекъснат подем в развитието и употребата на мобилните телефони. Тяхното бързо разпространение и развитие заражда идеята те да се използват не само за осъществяване на комуникация чрез глас и текстови съобщения. Изследователи и специалисти от практиката предлагат на потребителите услуги като банкиране, обучение и търговия, използвайки мобилните телефони като канал за разпространение. Сред тези услуги е и мобилното банкиране, което позволява на потребителите да използват мобилен телефон, за да манипулират с банковите си сметки.

Мобилното банкиране датира още от края на 1999 г., когато немската компания Paybox в сътрудничество с Deutsche Bank стартират първата такава услуга. Първоначално то е внедрено и тествано предимно в

европейските страни – Германия, Испания, Швеция, Австрия и Великобритания. Измежду развиващите се страни Кения е първата, която през 2007 г. започва предлагането на услуги за мобилно банкиране посредством SMS съобщения. Veijalainen и др. [33] твърдят, че основната причина за неговото бързо възприемане е способността на мобилните устройства да предлагат услуги по всяко време и на всяко място, включително и в движение.

В различните изследвания авторите често използват набор от термини, когато говорят за мобилното банкиране, например м-банкиране [34], безклоново банкиране [35], м-разплащания, м-трансфери, м-финанси [36] или джобно банкиране [37]. Въпреки че не е подходящо тези понятия да се използват като синоними, все пак между тях има обща черта и тя е, че всички те се свързват с предоставянето на услуга, която позволява реализирането на вид банкиране с помощта на мобилен телефон [38]. Тъй като често мобилното банкиране и мобилната търговия неправилно се използват като взаимнозаменяеми понятия, е важно да се внесе яснота по въпроса.

Мобилната търговия (m-Commerce) е подмножество на мобилния бизнес [39], който се свързва с възможностите за извършване на бизнес дейности независимо от времето и мястото на изпълнение [40]. Това е широко понятие, което обхваща всички форми на взаимодействие на потребителите както помежду си, така и с дадена бизнес организация с цел купуване или продаване на стоки и услуги с помощта на мобилно устройство [41]. Някои видове мобилна търговия са: мобилно забавление, мобилен маркетинг и реклама, мобилна информационна услуга и мобилно билетоиздаване [42].

В банковата индустрия, услуги, които са финансово обвързани и използват мобилни телекомуникационни технологии, са познати като

мобилни финансови услуги [43]. Те се класифицират в две основни категории: мобилни разплащания и мобилно банкиране. Cruz [44] идентифицира разликата между тях като твърди, че ако дадена банка не получава пряка финансова изгода от предлагането на дадена мобилна финансова услуга, то тя се определя като мобилно разплащане. Примери за такива услуги са плащания чрез SMS за получаване на продукт или услуга, несвързана с банката (например мелодии за звънене), зареждане на предплатени сметки или такси, начислявани към сметката за мобилни услуги, осъществяването на транзакции посредством безжична връзка, реализирана между терминал и чип в мобилно устройство.

Мобилното банкиране от друга страна най-общо може да се определи като предоставяне на банкови услуги посредством мобилен телефон [45]. 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 таблица 1 са представени малкото ясно изразени дефиниции на термина мобилно банкиране, налични в проучените литературни източници.

Дефиниция
Мобилното банкиране е приложение на м-търговията, което позволява на потребителите да получат достъп до банковите си сметки с помощта на мобилни устройства, с цел да реализират транзакции като проверка на баланс по сметка, прехвърляне на средства, реализиране на разплащания или продажба на акции. [46, 47, 29]
Мобилното банкиране е иновативен комуникационен канал, чрез който потребителят взаимодейства с банка с помощта на мобилно устройство. [48, 49, 19]

Мобилното банкиране предоставя възможност на потребителите да изпълняват банкови транзакции чрез мобилно устройство. [50]
Мобилното банкиране е финансова услуга, която се предоставя през мобилните комуникационни мрежи с помощта на мобилен телефон. [51]
Мобилното банкиране позволява на потребителите да получат достъп до банковите мрежи през телекомуникационните като използват мобилни телефони, пейджъри, персонални дигитални помощници или други подобни устройства. [52]
Мобилното банкиране е подмножество на системата за електронно банкиране, при което потребителите достъпват набор от банкови продукти с помощта на електронни устройства. [53]
Мобилното банкиране е система, която използва мобилните информационни и комуникационни технологии с цел да получи и предостави достъп до информационна система. [54]
Мобилните финансови приложения са наричат още мобилно банкиране. [55]
Мобилното банкиране е канал, при който потребителят взаимодейства с банка с помощта на мобилно устройство или PDA (персонален дигитален помощник) устройство. [15]
Мобилното банкиране е система, при която абонатът на мобилни услуги с помощта на мобилния си телефон може да изпълни парична транзакция по всяко време, от всяко място и с всеки. [56]

Таблица 1. Дефиниции на мобилно банкиране

Посочените дефиниции са анализирани с цел да се определят техните сходства и различия. Мобилното банкиране е представено като „система“, „канал“, „услуга“, „приложение на м-търговията“, „подсистема на

електронното банкиране“. Като функция, която то реализира, е посочено „реализиране на транзакции“, „взаимодействие с банка/банкова сметка“, „достъп до банкови продукти“. Най-подходящо е мобилното банкиране да бъде идентифицирано като „канал за предоставяне на банкови услуги“, тъй като с негова помощ потребителите получават достъп до определени банкови услуги. В тази връзка обаче е важно да се определи, кой и как предоставя услугите и какви точно могат да бъдат те.

Три са основните видове бизнес модели на мобилно банкиране - модел, фокусиран върху банката, модел с водеща роля на банката, модел с водеща роля на друга компания [53, 57]. Основната разлика между тези модели се изразява в начина на предоставяне на услуги до крайния потребител, т.е. кой стои в основата на модела, дали това е банката или някаква друга компания, отговаряща за предоставянето на банковите услуги. Първият модел по характер е допълващ и може да се разглежда като допълнение към традиционното банкиране, защото предоставя ограничени банкови услуги [53]. При модела с водеща роля на банката, на потребителя се предлага алтернатива на традиционното банкиране, като му се дава възможност да осъществява финансови операции, използвайки мобилно устройство, вместо да посещава офис на банката или да си взаимодейства с нейните служители. За разлика от този модел, при модела с водеща роля на друга компания банката не взема активно участие, разглежда се само като хранилище на средства, а всички функции се реализират от небанкова организация, като най-често това е телекомуникационна компания [58].

Банковите услуги, които се предоставят от мобилното банкиране, могат да се класифицират на база на информационния поток като активни и пасивни. Активните услуги са двупосочни, като при тях потребителят изисква услуга или информация от банката, а тя от своя страна трябва да

отговори или да предприеме някакво действие, свързано с искането на потребителя. При пасивните услуги банката изпраща информация въз основа на предварително зададени правила от потребителя. Според друга класификация банковите услуги се разграничават въз основа на същността на услугата като транзакции и справки. Транзакциите реализират движение на средства, а справките изпращат определена информация на потребителя. С цел предотвратяване на рискове за сигурността, някои банки предоставят на своите клиенти само справочни услуги, но този подход не може да се възприеме като осъществяване на напълно функциониращо мобилно банкиране.

	Пасивни	Активни
Транзакции		<ul style="list-style-type: none"> <li>- трансфер (вътрешнобанков и междубанков) на капитали;</li> <li>- плащане на задължения към различни търговци;</li> <li>- нареждане на чекове;</li> <li>- търговия на акции.</li> </ul>
Справки	<p>Различни видове известия:</p> <ul style="list-style-type: none"> <li>- за достигнат минимален баланс по сметка;</li> <li>- за задължения по кредит или към търговци;</li> <li>- за направени транзакции.</li> </ul>	<ul style="list-style-type: none"> <li>- проверка на баланс по сметка;</li> <li>- история на транзакции по сметка;</li> <li>- информация за статус на чек;</li> <li>- намиране на най-близкия АТМ или клон на банката.</li> </ul>

Таблица 2. Често предлагани услуги на мобилно банкиране

С цел да се установят най-често предлаганите услуги на мобилно банкиране в настоящия момент реализирахме отделно авторско проучване в следните три региона: Далечният Изток и Китай, Европейският съюз (в частност Западна Европа) и Северна Америка (САЩ и Канада). Изборът на тези региони се обуславя от факта, че според редица изследвания [59, 60, 61, 62] те са определяни като водещи в развитието на мобилното банкиране. Във всеки от посочените регион са изследвани по 20 банки, имащи развита система за мобилно банкиране, като необходимата информация е почерпена от техните уеб сайтове. В таблица 2 са представени най-често предлаганите услуги за мобилно банкиране, разграничени според двете по-горе разгледани класификации.

При изследването на най-често предлаганите услуги на мобилно банкиране установихме, че банките разположени както в развитите, така и в развиващите се страни, обикновено предлагат 3 основни начина за достъп до тези услуги (вж. табл. 3): текстови съобщения (SMS), мобилно приложение и уеб сайт за мобилно уеб приложение.

Регион	Текстови съобщения (SMS)	Мобилно приложение	Уеб сайт за мобилно уеб приложение
Далечен Изток и Китай	60%	80%	95%
Европейски съюз (Западна Европа)	95%	100%	75%
Северна Америка (САЩ и Канада)	60%	100%	85%
Общо	72%	93%	85%

Таблица 3. Процент от общия брой изследвани банки, предлагащи услуги за мобилно банкиране, по региони и по начин за достъп



Текстовите съобщения като начин за достъп до услугите на мобилното банкиране позволяват на потребителя да изпраща SMS съобщение до банката, изисквайки определена информация, като баланс по сметка или състоянието на определена транзакция. Банката от своя страна отговаря също със SMS съобщение, предоставяйки необходимите данни.

Мобилният уеб сайт е уеб сайт, който е оптимизиран за разглеждането му на ограничения като размер екран на мобилното устройство. Използването на този начин за достъп се доближава много до интернет банкирането, тъй като потребителят използва уеб браузър на мобилното устройство (или мобилния уеб браузър), за да получи достъп до уеб сайта за интернет банкиране на банката. Голяма част от банките използват този подход, тъй като той позволява намаляване на разходите, чрез използването на вече изградената инфраструктура и нейните компоненти.

Мобилните приложения са приложения, които могат да бъдат инсталирани на смартфон или таблет и работят в средата на мобилната операционна система. Първите мобилни приложения за мобилно банкиране изпълняват предимно информационни функции, но на настоящия етап, те могат да се използват за реализирането на активни транзакции. При изследването на най-често предлаганите услуги на мобилно банкиране установихме, че банките предлагат приложения за мобилно банкиране предимно за две от водещите операционни системи Android и iOS.

Както се вижда от данните в таблица 3 и разгледаните дефиниции (вж. табл. 1) по отношение на начина на достъп до услугите на мобилното банкиране присъстват термините „мобилен телефон“, „смартфон“, „таблет“, „мобилно устройство“. Затова те трябва да присъстват и при формирането на неговата дефиниция. Но тук трябва да се уточни, че независимо от това, че преносимите компютри се причисляват към

мобилните устройства, достъпът до банкови услуги реализиран чрез тях не трябва да се определя като мобилно банкиране, тъй като потребителският им интерфейс е много близък до този на настолните компютри. Затова този вид устройства се причисляват към една друга категория – тази на интернет банкирането.

В резултат на направения дотук анализ на наличните дефиниции и изследването 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**

Още през 2002 Claessens [63] забелязва, че съществуват съображения относно сигурността на мобилното банкиране, тъй като мобилните устройства, с помощта на които то се осъществява, са уязвими от заплахи, атаки и загуби. С течение на времето този канал започва да привлича все повече вниманието на кибер<sup>2</sup> престъпниците [64], като през последните 5 години се наблюдава непрекъснат ръст на разпространението и усъвършенстването на злонамерения софтуер, разработван за мобилни устройства и причиняващ различни вреди като кражба на чувствителна финансова информация, на финансови средства и на самоличност [65]. Тази тенденция е напълно нормална, тъй като тя е част от нарастването на кибер престъпленията, насочени въобще към институциите, предлагащи финансови услуги [66, 67, 68].

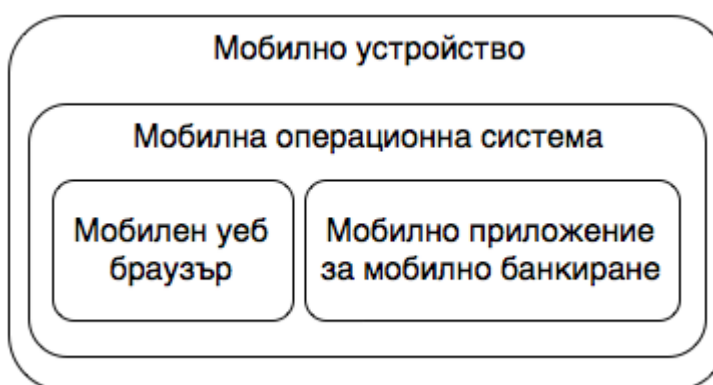
Сигурността при мобилното банкиране се определя като сложен процес поради наличието на различни участници при неговата реализация [69, 70]. Въпреки че проблеми, свързани със сигурността, могат да се наблюдават при всички основни участници в процеса на мобилно банкиране (вж. фиг. 1), необходимо е обхватът 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 [68].

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.

---

<sup>2</sup> Навсякъде в дисертационния труд думата „кибер“ е писана отделно от следващата дума, като се позоваваме на източник [68] - Национална стратегия за кибер сигурност „Кибер устойчива България 2020”

От дефиницията за мобилното банкиране, която изведохме в предходната точка, може да се определи, че минималното изискване към потребителя, за да използва неговите услуги, е той да разполага с мобилно устройство като мобилен телефон, смартфон или таблет. Като вземаме предвид основните начини, които се използват понастоящем за достъп до услугите на мобилно банкиране (вж. табл. 3), можем да определим и две допълнителни изисквания: наличие на мобилен уеб браузър или наличие на мобилно приложение за мобилно банкиране, работещи под мобилна операционна система. Тъй като текстовите съобщения се използват за предоставянето на справочни мобилни услуги, те не представляват интерес за настоящата разработка. Така, могат да бъдат посочени четири основни проблемни области при потребителя по отношение на сигурността при мобилното банкиране (вж. фиг. 2): мобилно устройство, мобилна операционна система, мобилен уеб браузър, 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.

## **2.1. Заплахи за сигурността при мобилното устройство**

Въпреки че мобилните устройства са малки като размер, те притежават множество функционалности [71], благодарение на вградените в тях технологии, които позволяват на потребителите им да реализират обаждания, да изпращат и приемат съобщения, да се свързват с други устройства, да осъществяват връзка с интернет, да четат информация от външни устройства. Според Cheng [71], колкото повече функционалности имат тези устройства, толкова повече те са податливи на заплахите, характерни за преносимите и настолните компютри.

Характерен тип атака за мобилните устройства по отношение на мобилното банкиране е vishing атака, при която потребителят получава обаждане, чиято основна цел е той да бъде измамен, че разговаря с банков служител и в резултат на това да предостави чувствителна финансова информация [72]. Под чувствителна финансова информация следва да се разбира потребителски имена и пароли, номера на банкови сметки или кредитни карти, както и временни пароли за достъп.

Подобен вид атака, може да бъде реализирана, чрез изпращането на SMS съобщение (позната като smishing атака), при която чувствителната финансова информация следва да бъде поискана под формата на текстово съобщение [72]. Възможностите на мобилните устройства за изпращане на съобщения, могат да се използват и като уязвими места за инсталирането на злонамерен софтуер, с чиято помощ може да бъде получен неупълномощен достъп до чувствителна финансова информация. Поради тази причина различните видове злонамерен софтуер за мобилни устройства представляват заплаха за сигурността при мобилното

банкиране. Като пример можем да посочим Worm.SymbOS.Comwar (компютърен червей), който е прикрепен като прикачен файл към MMS съобщение, с цел червеят да се прехвърли на мобилно устройство.

Уязвимости и заплахи за мобилното банкиране, които представляват канал за разпространението на различни форми на злонамерен софтуер или за реализирането на различни атаки, са действия като синхронизиране на мобилното устройство с настолен компютър, свързването му с външно запомнящо устройство или реализирането на безжична връзка, използваща технологиите Wi-Fi (Wireless Fidelity), Bluetooth, NFC (Near Field Communication).

Bluetooth технологията предоставя възможност за свързване на устройства с цел размяна на информация. Проблемите за сигурността на тази технология са разгледани още през 2009 от Haataja [73]. BlueSnarfing е атака, при която кибер престъпникът се свързва към мобилно устройство през Bluetooth интерфейс, без знанието на потребителя. Така той може да получи неупълномощен достъп до различна информация, съхранена на устройството или да реализира инсталирането на злонамерен софтуер [74], чрез който да компрометира сигурността на мобилното банкиране. Първата проява на този вид атака е разпространението на компютърния вирус за мобилни устройства Cabir още през 2004.

През 2011 Gligoroski [75] сравнява Bluetooth атаките с Mobile Denial-of-Service (MDoS) атаките и определя вторите като по-сериозни, тъй като те могат да се използват срещу мобилното устройство с цел да се блокира нормалната му работа, чрез използване на критични за него ресурси като процесор, памет, мрежова пропускливост. По този начин потребителите няма да могат да използват нито една от функционалностите на засегнатото устройство, включително и мобилното банкиране.

Още през 2007 Ноерман и Siljee [76] описват различни проблеми свързани със сигурността на устройствата, използващи NFC технологията. Те посочват, че тя може да се използва като вход към мобилното устройство. Като доказателство за това през 2009 Mulliner [77] показва атака, при която NFC се използва с цел на смартфон да се инсталира компютърен червей. През 2012 Ries [78] отново потвърждава възможността за реализиране на такъв вид атака, а Bargaonkar [79] представя как NFC може да се използва за изпълнението на злонамерени команди на смартфон с мобилна операционна система Android 4.0.4.

При използването на Wi-Fi за реализиране на безжична комуникация една от съществуващите уязвимости е потребителят да свали на мобилното устройство файл, инфектиран със злонамерен софтуер [80]. Друга е свързана с компрометиране на поверителността и цялостността на комуникацията чрез атаки като eavesdropping или man-in-the-middle [81]. При eavesdropping атаката, кибер престъпниците използват различни инструменти с цел да подслушват данните, които се предават по мрежата [82]. При реализирането на man-in-the-middle атака предаваните данни могат дори да бъдат променени преди да пристигнат до легитимния получател [83]. Тези заплахи най-често съществуват при използването на некриптирани безжични мрежи, които обикновено са разположени на публични места като магазини, библиотеки, летища, хотели. Свързването на потребителите към тях крие опасности за реализирането на мобилно банкиране. Когато потребителите използват такива несигурни безжични мрежи, за да извършат проверка на баланса по сметка, да депозират чекове или да плащат сметки, кибер престъпниците могат лесно да подслушват мрежата и така да откраднат чувствителна финансова информация, която при публичните безжични мрежи се предава в некриптиран вид [84].

Малките размери и все още високата себестойност на мобилните устройства ги правят атрактивни за кражба [75]. Ако те бъдат загубени или откраднати, информацията, която се съхранява на тях може да остане незащитена [85], тъй като физическият достъп до устройството е пряко свързан с достъп до личните данни, съхранени на него. Достъп до съдържанието на тези устройства може да бъде получен и при тяхното изхвърляне или продаване [81], когато информация, която се съхранява на тях, не бъде правилно изтрита. От тук можем да определим, че получаването на неупълномощен достъп до мобилното устройство е уязвимост, която може да предостави възможност на кибер престъпниците да получат достъп до мобилното банкиране, в резултат на което да изпълнят неупълномощени транзакции.

## **2.2. Заплахи за сигурността при мобилната операционна система**

Основен проблем за сигурността на мобилното банкиране, свързан с мобилните операционни системи, е заплахата от инсталирането на различни видове злонамерен софтуер. Той може да използва определени уязвимости на мобилната операционна система с цел да се реализира достъп до чувствителна финансова информация. Често срещан злонамерен софтуер, насочен към потребителите на мобилно банкиране, е т.н. keylogger, който записва натисканите клавиши с цел да получи достъп до потребителски имена и пароли. Други познати прояви, които засягат приложенията за мобилното банкиране са: Zitmo, Banker, Perkel/Hesperbot, Wrob, Bankum, ZertSecurity, DroidDream. Голяма част от тях представляват разновидности на вече съществуващи версии, работещи при настолните компютри и системите за традиционно интернет банкиране [86, 19] и чиято



основна цел е получаване на достъп до чувствителна финансова информация.

Внасянето на злонамерен софтуер в мобилните операционни системи може да бъде реализирано по различни начини. В предходната подточка 2.1 разгледахме тези, свързани конкретно с функционалните характеристики на мобилното устройство. В настоящата подточка обръщаме внимание на уязвимостите, пряко свързани с мобилната операционна система, работеща на устройството.

Един от начините за инсталирането на злонамерен софтуер е използването на различните софтуерни пропуски и уязвимости за сигурността, които са налични в мобилните операционни системи. Положителното в този случай е, че производителите на тези операционни системи, постоянно ги проверяват и сравнително бързо пускат актуализации, които да поправят проблемните места. Проблемът, който възниква обаче е дали потребителят ще реагира достатъчно бързо и дали мобилната операционна система, която той използва, ще е последната налична версия с инсталирани всички пуснати актуализации.

Дори това да бъде реализирано, съществува и друг сериозен проблем за сигурността на мобилното банкиране. Някои от потребителите умишлено променят мобилната операционна система (известно като rooting за операционна система Android и jailbreaking за операционна система iOS) [85], като по този начин целят да получат допълнителни възможности. За съжаление с това не само се получава по-голям контрол над мобилната операционна система, но се премахват и някои от вградените ѝ механизми за сигурност. По този начин тя става по-податлива на злонамерен софтуер.

Проблеми за сигурността на мобилното банкиране могат да възникнат и в резултат на използвания приложен софтуер. Нерядко потребителите инсталират мобилни приложения, предоставяни от трети

страни, различни от официалните източници, на които се предполага, че може да се има доверие. След като бъдат инсталирани на мобилната операционна система, те могат тайно да получат достъп до мобилното приложение за мобилно банкиране и да откраднат от него чувствителна финансова информация.

Съвременните мобилни операционни системи дават възможност на потребителя да изпраща и получава различни видове съобщения като използва приложения за електронна поща (e-mail), за мигновени съобщения или за различни социални мрежи (Facebook, Twitter или LinkedIn). Съдържанието на тези съобщения крие заплахи за сигурността, тъй като то може да включва прикачени файлове или линкове към злонамерен софтуер или линкове към сайтове, реализиращи phishing атаки [87]. В допълнение ако дадено приложение, използвано за социална комуникация, бъде инфектирано със злонамерен софтуер, то може да се разпространи много бързо до други потребители, генерирайки автоматизирани съобщения до всички налични в списъка за контакти.

### **2.3. Заплахи за сигурността при мобилния уеб браузър**

Нарастващият брой на потребителите на мобилни устройства и техният постоянен достъп до интернет, прави мобилния браузър атрактивна мишена за хакерите и това се потвърждава от редица автори като Amrutkar и др. [88], Felt и Wagner [89], Niu и др. [90], Rieck и др. [91], Rydstedt и др. [92]. В следствие на това възникват определени заплахи за сигурността при реализирането на мобилното банкиране. В своя доклад Sujithra [93] твърди, че мобилният уеб браузър може да се използва за реализирането на атаки като phishing и автоматично сваляне на злонамерен софтуер.

Основната цел на phishing атаките е да измамат потребителя, за да могат кибер престъпниците да получат от него чувствителни данни [94], а в случая на мобилното банкиране – чувствителна финансова информация. Нейното получаване се реализира чрез линкове към сайтове, на които потребителите директно въвеждат чувствителните данни. Както показahme в подточка 2.2, линковете към phishing сайтове най-често се разпространяват с помощта на електронната поща или съобщения, изпращани през социалните мрежи.

Същият метод на разпространение може да се използва и за линкове към сайтове, при чието посещение се реализира автоматично сваляне на приложение, прикриващо злонамерен софтуер. В голяма част от случаите основна цел на този софтуер е да получи достъп до чувствителна финансова информация.

Повечето от съществуващите механизми за защита на уеб браузърите са насочени към настолните им версии. Заплахите за сигурността при тях обаче се различават от тези при мобилните уеб браузъри и затова е необходимо техните уязвимости да бъдат изследвани отделно [93].

Amrutkar и др. [95] посочват, че поради намаления размер на екрана на мобилното устройство се наблюдават проблеми при използването на идентификаторите за сигурност и за информация относно сертификатите, позволяващи на потребителите да идентифицират уеб сайтовете и да са сигурни в наличието на силни криптиращи алгоритми. World Wide Web Consortium (W3C) [96] предоставят ясни изисквания към потребителския уеб интерфейс по отношение на набора от механизми за сигурност. В своето изследване Amrutkar и др. [95] доказват, че почти всички стандартни уеб браузъри отговарят на тези изисквания, докато това не важи за голям брой от мобилните браузъри. Например, една от най-често срещаните

уязвимости е невъзможност да се разгледа целият линк в адресната лента, което веднага се свързва с успешната реализация на phishing атака.

Една от вариациите на phishing атаките, която може да бъде приложена през мобилните уеб браузъри е tabnabbing [97]. При този вид атака, ако потребителят посети phishing уеб сайт, остави го отворен и след това използва друг раздел (tab) на своя браузър, за да отвори друг уеб сайт, зареденият phishing сайт може да промени начина, по който изглежда и по този начин да заприлича на популярен уеб сайт (включително и на уеб сайт за мобилно банкиране). Тъй като мобилните уеб браузъри имат ограничен визуален достъп до разделите си, потребителят може да отвори раздел без да провери URL адреса (тъй като вече го е направил) и така да предостави чувствителна финансова информация. Този вид атака може да заблуди дори и потребители, които са запознати с традиционните phishing атаки.

Друг съществен проблем за мобилните уеб браузъри, който отново е представен в проучването на Amrutkar и др. [95], е успешната реализация на CSRF (Cross Site Request Forgery) атака. Този вид атака позволява на кибер престъпниците да изпращат заявки до уеб приложение, използвайки мобилния уеб браузър на даден потребител. Поради тази причина уеб приложението обработва тези заявки по същия начин, както би обработило истински заявки, изпратени от същия потребител. Така, успешните CSRF атаки могат да доведат до получаване на достъп до чувствителна финансова информация или направо до системите за мобилно банкиране [98], а от там и до изпълнението на неупълномощени транзакции.

#### **2.4. Заплахи за сигурността при мобилното приложение за мобилно банкиране**

Сигурността и неприкосновеността на чувствителната финансова информация е едно от основните съображения при възприемането на

приложенията за мобилно банкиране [99]. Ограниченият опит, свързан със защитата на личните данни и недостатъчните сведения от независими разработчици намалява ефективността на сигурността по отношение на приложенията за мобилното банкиране [100]. Затова е необходимо да представим различните актуални рискове, свързани с тяхната сигурност.

Въпреки че разработчиците на мобилните приложения за мобилно банкиране разбират колко важна е тяхната сигурност, често се случва те да правят компромис с нея, за да могат да спазят сроковете за разработка [101]. В резултат на това възникват различни уязвими места, които могат да се използват от злонамерения софтуер. След сериозен анализ на голям набор от мобилни приложения за мобилно банкиране, в своя доклад [102] ЮАActive (компания за кибер сигурност) посочва, че съществуват два основни проблема за тяхната сигурност.

За голяма част от изследваните мобилни приложения се установява, че липсва адекватна реализация на SSL или проверка на автентичността на сертификата. SSL (Secure Socket Layer) и TLS (Transport Layer Security) са най-важните протоколи за сигурност, които се използват да установят криптирани връзки при размяна на данни със сървъри и да потвърдят идентичността на сървъра. Тяхната липса води до успешната реализация на атаки като phishing, man-in-the-middle и eavesdropping.

В своето изследване Ante [103] доказва, че криптирането е необходимо не само при предаване на данни, а и при тяхното съхраняване. Обърнато е внимание на съществуването на мобилни приложения, които съхраняват в паметта на мобилното устройство некриптирана чувствителна финансова информация, до която може да бъде реализиран неупълномощен достъп.

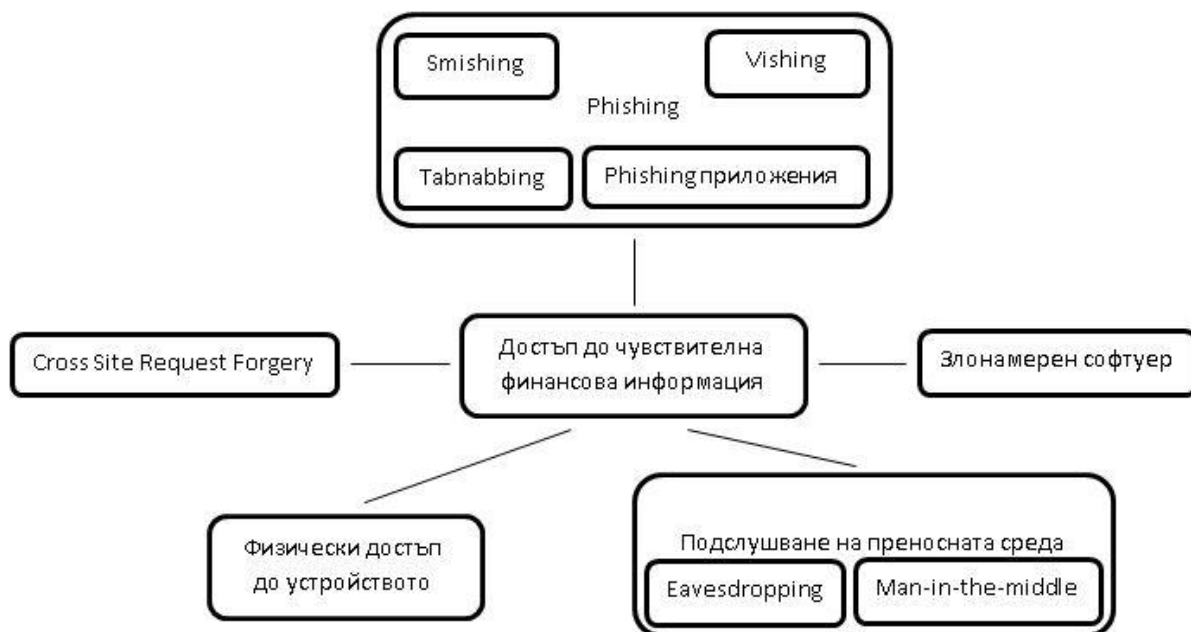
Като друг сериозен проблем при мобилните приложения за мобилно банкиране се посочва слабото и не гъвкаво удостоверяване, реализирано

чрез електронен подпис, ПИН код, парола или ОТР (еднократна парола). Най-често еднократната парола се предоставя на потребителя посредством допълнително хардуерно устройство или текстово съобщение. Слабото и не гъвкаво удостоверяване може да се използва като уязвимост при получаването на неупълномощен физически достъп до устройството или при успешната реализация на phishing атака, без значение дали през мобилния уеб браузър или чрез използването на измамни мобилни приложения, разработени от трети страни.

Заплахи за сигурността при мобилното банкиране в резултат на phishing атаки могат да възникнат и когато бъдат използвани измамни мобилни приложения или фалшиви актуализации на официално приложение, които кибер престъпниците пускат в магазините за мобилни приложения, предимно предлагани от трети страни. И в двата случая те могат да съдържат злонамерен код, който се използва с цел да се открадне чувствителна финансова информация [104].

В допълнение много от мобилните приложения за мобилно банкиране не притежават защита срещу реинженеринг (reverse engineering) на кода [105]. Това позволява на кибер престъпниците да анализират първичния програмен код (source code) и по този начин да открият начини за достъп до чувствителна финансова информация.

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).



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

С цел да предотвратят кибер измамите и да улеснят създаването на сигурна и здрава система за мобилно банкиране, много експерти по сигурността предлагат различни методи и практики, които да решават някои от съществуващите проблеми. Едновременно с това кибер престъпниците непрекъснато усъвършенстват атаките и техниките, които използват, за да атакуват мобилните устройства и в частност мобилното

банкиране. В настоящата точка са разгледани актуалните стратегии за защита и добри практики, които се използват за противодействие на всяка една от атаките представени на фиг. 3.

### **3.1. Защита от Eavesdropping и Man-in-the-middle атаки**

Реализирането на този вид атаки най-често се свързва с използването на некриптирани безжични мрежи, които са разположени на публични места. Затова и банките, предлагащи мобилно банкиране, препоръчват на потребителите да не използват такива мрежи. Въпреки че повечето от мобилните устройства, предоставящи възможност за Wi-Fi достъп, имат механизми, които показват дали мрежата е криптирана, много пъти тази възможност не се използва. Затова и един от основните подходи за защита от този вид атаки е да се прилагат протоколи за сигурност. Те ефективно защитават данните, които се предават по мрежата от мобилния уеб браузър или мобилното приложение, работещи на клиентското устройство, към сървърите на доставчика на услуги за мобилно банкиране.

Още през 2004 Pousttchi и Schurig [106] поставят като основно изискване за реализирането на мобилното банкиране използването на протоколи за сигурност. В последствие възникват различни изследвания, в които са представени и конкретни предложения за приложение на протоколите за сигурност. Например през 2012 Elkhodr и др. [99] предлагат комбинация на TLS протокола заедно с надежден метод за договаряне, който да удостоверява клиента, сървъра и мобилното устройство, използвано за реализирането на мобилно банкиране.

В тази връзка TLS протоколът традиционно намира сравнително широко приложение при защитата от eavesdropping и man-in-the-middle атаките [107]. В резултат на това той е подложен на постоянни проверки, а неговата сигурност е тема на различни изследвания в областта на



криптографията. Това определено е положително за неговото развитие, защото води до разработването на нови версии, които отстраняват откритите уязвимости за сигурността.

Проблемът, който обаче се наблюдава при TLS протокола, е, че той се прилага в една малка част от мобилните 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 [108]. Това от своя страна води до по-големи възможности за компрометиране на сигурността на мобилното банкиране.

В допълнение към използването на TLS протокола за подsigуряване на комуникацията между клиентското устройство и банковия сървър се прилагат различни подходи за проверка на използваните сертификати, с цел да се установи дали те са издадени от СА (Certification Authority) организация.

Един от подходите за реализирането на това е използване на отворения фреймуорк Certificate Transparency (СТ), чиято основна цел е да поддържа публичен отчет за всички издадени сертификати, като по този начин се предоставя възможност за засичане на подправените сертификати [109].

Друг подход се базира на техниката „certificate pinning“, която се използва с цел засичане на несъответствията между настоящия сертификат и предишно използвани сертификати. Въпреки че този подход изисква първоначално реализираната връзка да бъде сигурна, той се използва за ефективно засичане на всички следващи промени. В резултат на това той намира широко приложение, например в добавката за уеб браузър „Certificate Patrol“. Нещо повече, Google го използва за разработване на уникални отпечатъци на своите TLS сертификати, като това позволява на уеб браузъра Google Chrome да засече потенциална man-in-the-middle атака,

която може да използва подправен сертификат, който да е официално издаден от СА.

Въпреки наличието и на други подходи, използвани за проверка на сертификатите, посочените по-горе са оценени [110] като едни от най-често прилаганите и ползващи се с широка подкрепа.

### **3.2. Защита от Cross Site Request Forgery (CSRF) атака**

При появата на този вид атака са предложени няколко техники за противодействие, които обаче се оказват неефективни. Една от тях е при реализирането на операции, променящи състоянието, да се използват POST заявки, като се разчита на това, че те не са податливи на фалшификация. Доказано е обаче, че това не е така [111].

Друга техника за противодействие включва проверката на `referrer` (HTTP заглавно поле) при сървър. Операции, променящи състоянието, трябва да бъдат приети от уеб приложението само ако `referrer` полето съдържа предварително определена стойност. Тази техника би била ефективна срещу CSRF атаки, но присъствието на `referrer` поле не може да бъде подсигурано. Например уеб браузърите (както стандартните, така и мобилните) не добавят такова поле, когато HTTPS ресурс, който се счита за чувствителен, се опитва да се обърне към HTTP ресурс.

Като подобрение на `referrer` полето се предлага друго заглавно поле (`origin` поле), което предоставя на сървър по-малко чувствителна информация (само за произхода на заявката). Проблемът, който възниква тук е, че `origin` полето се определя като незадължително и поради тази причина може да се твърди, че при него се наблюдават същите недостатъци като при `referrer` полето [112].

Като алтернативни и по-ефективни техники за противодействие на CSRF атаките са подходите, базирани на `token` (обект, наличието на който

предоставя права за изпълнение на определена операция). При тях, когато уеб браузърът (стандартен или мобилен) генерира операция, променяща състоянието, автоматично се добавя уникален token, който следва да бъде проверен от сървъра. Успехът на този подход се крие в сигурността на token обекта, който трябва да не може лесно да бъде разпознат и да е валиден само за определен потребител. Затова и се реализират редица изследвания в областта, чиято основна цел е внасянето на подобрения в традиционно използваните token обекти.

Друг подход за противодействие на CSRF атаките, който е реализиран на ниво архитектура на уеб приложението, е свързан с ограничаване на точките за достъп до защитени ресурси. По този начин се елиминира CSRF атака срещу чувствителна информация, а в случая на мобилното банкиране срещу чувствителна финансова информация. Тези точки за достъп могат да бъдат подсилени както при сървъра, така и в комбинация с механизъм, реализиран в уеб браузъра [113].

Противодействие срещу CSRF атаките може да бъде осъществено и чрез изрично одобрение от страна на потребителя при реализирането на операции, променящи състоянието. Изискването на допълнително взаимодействие с потребителя затруднява успешното изпълнение на този вид атака на заден фон. Примери за осъществяването на този подход са използването на повторно удостоверяване или на допълнителни устройства, които генерират token обекти. Те често се използват при реализирането на онлайн банковите системи. Рискът, който обаче се крие при тази техника, е свързан с пренасочването на кибер престъпниците от CSRF атака към clickjacking атака.

До тук разгледаните техники се реализират при сървъра, където е разположено уеб приложението. Съществува малък брой решения, които работят на клиентското устройство и пряко защитават потребителя срещу

изпълнението на CSRF атака. Те могат да засичат потенциални несигурни заявки, в резултат на което или да ги блокират или да премахват от тях чувствителна информация. Едно от предизвикателствата за тези решения е свързано с поддържането на добър баланс между сигурност и ползваемост (usability), като тази нужда е в резултат на необходимостта от реализирането на съвместимост със всички възможни сайтове, които потребителя посещава.

### **3.3. Защита от неупълномощен физически достъп**

Получаването на неупълномощен физически достъп до мобилното устройство може да доведе до реализирането на достъп до данните на различните приложения, включително и тези за мобилното банкиране. Успешна техника за защита на информацията, която се използва и се предлага като възможност от мобилните операционни системи, е нейното криптиране. Основно предизвикателство при реализирането на това обаче е съхранението на криптиращия ключ. Той трябва да бъде наличен на самото устройство, защото в противен случай потребителят няма да може да получи достъп до собствените си данни. Решение на този проблем е използването на парола, която едновременно служи както за удостоверяване на потребителя, така и за генерирането на криптиращия ключ. По този начин той реално не се съхранява на устройството, а се създава в неговата памет при реализирането на успешно удостоверяване.

В тази връзка, най-широко прилаганите техники за удостоверяване при мобилните устройства са паролите и персоналните идентификационни номера (ПИН). Един от сериозните проблеми, който се наблюдава при тях е нежеланието на потребителите да ги използват [114]. Това се обуславя от факта, че потребителите използват мобилните устройства многократно, а това от своя страна води до необходимост от въвеждането на пароли всеки

път когато устройството или дадено мобилно приложение се използва. Като доказателство през 2014 в свое проучване Consumer Reports [115] посочват, че само 47% от анкетираните използват парола за достъп на техните мобилни устройства, като само половината от тях са активирали функцията за автоматично заключване на устройството.

Като решение на горепосочения проблем през 2013 Apple предлагат функционалността TouchID , като с нейна помощ не се налага въвеждането на ПИН, а потребителят се удостоверява посредством пръстов отпечатък. Две години по-късно през 2015 Google внедряват подобна функционалност в своята мобилна операционна система Android Marshmallows. Тук е важно да се отбележи, че това подобрение не е типично биометрично удостоверяване, а по-скоро е направено с цел удобство за потребителя, като сигурността на криптиращия ключ продължава да зависи от ПИН-а на устройството. Затова и е от съществено значение той да е достатъчно труден за разбиване.

Това насочва към друг проблем свързан с паролите, който се изразява в това, че дори да бъдат използвани при мобилните устройства, най-често те представляват 4 цифрен ПИН. Доказано е, че с помощта на brute-force атака този код може да бъде компрометиран за 14 часа [116]. В своята мобилна операционна система iOS 9, Apple въвежда използването на 6 цифрен ПИН, който може да удължи времето за неговото разбиване посредством brute-force атаката до 57 дена. Това естествено е максималното време, като в голяма степен то зависи и от сложността на съответния код.

За противодействие на този вид атака потребителят може да използва функция на операционната система, която да изтрие данните на мобилното устройство след въвеждането на определен брой пъти грешен ПИН код. Пробив, който се е наблюдавал при тази техника, е бил реализиран чрез

външно хардуерно устройство, което прекъсва захранването на устройството след всеки опит за въвеждане на ПИН код, а това от своя страна се изразява в незаписване на неуспешния опит и в нереализиране на функцията за изтриване на данните [117, 118].

Друго решение за защита от неоторизиран физически достъп е използване на функцията на мобилната операционна система за дистанционно заключване на устройството или за дистанционно изтриване на съдържанието му. Тази функция е ефективна само ако се използва добър механизъм за удостоверяване, който би забавил кибер престъпниците и би дал нужното време на потребителите да я активират.

С цел да се избегнат разгледаните недостатъци при използването на пароли и ПИН кодове при мобилните устройства и да се реализира по-добър механизъм за удостоверяване, като нова тенденция се налагат изследвания в областта на биометричното удостоверяване, тъй като биометричните характеристики са уникални и могат по-трудно да бъдат дублирани или пренасяни.

Въпреки всички опити за противодействие в един момент все пак може да бъде получен неупълномощен физически достъп до мобилното устройство. С цел защита на мобилните приложения за мобилно банкиране е необходимо техните разработчици да са реализирали достатъчно сигурно удостоверяване. Тъй като това пряко се свързва с phishing атаките, то е разгледано по-подробно в подточка 3.4.

### **3.4. Защита от phishing атака**

Една от техниките, която се използва за противодействие на phishing атаките, е информиране на потребителите. Много от банките, предоставящи възможност за мобилно банкиране, декларират на уеб сайтовете си, че те никога не биха използвали непряк контакт (телефон,

текстово съобщение, електронна поща), за да поискат достъп до лични данни, а още повече номера на банкови сметки, кредитни карти или пароли за достъп. В допълнение финансовите институции предупреждават потребителите, че приложението за мобилно банкиране трябва да бъде изтеглено от официалния уеб сайт на банката, предоставяща услугата и че в никакъв случай не трябва да се използват приложения, които приличат на него и най-често се предлагат в магазините на трети страни.

Проблемът, който възниква при тази техника, е че малка част от потребителите достигат до тази информация, поради различни причини, включително и нежелание от тяхна страна. Това означава, че те по-лесно могат да станат жертва на phishing атака. Нещо повече, дори и тези, които са информирани, често пъти биват хванати в капана на кибер престъпниците. Затова е необходимо да се разгледат и други техники, които осигуряват допълнителна защита срещу успешното реализиране на phishing атаки.

Група от автори (Cognizant [119], Constantin [120], Lee и др. [70], Chandramohan и Tan [121], La Polla и др. [122], White [123]) предлагат използването на сходни механизми за сигурност като многофакторно удостоверяване, използване на SiteKey (уеб базирана система за сигурност) с въпроси и картинки за удостоверяване на потребители, удостоверяване на регистрирано мобилно устройство, които следва да бъдат приложени с цел да бъде повишена сигурността на мобилните приложения за мобилно банкиране.

При многофакторно удостоверяване не се използва само един единствен набор от данни за удостоверяване, а се изисква прилагането на допълнителни фактори [94]. Примери за такива фактори са: token, който се изпраща на мобилния телефон, чрез текстово съобщение, token, който се генерира на специализирано устройство, смарт карта, биометрична

информация и др. Целта на тяхното прилагане е поне един от допълнителните фактори за удостоверяване да се окаже извън контрола на кибер престъпниците.

Що се отнася до сигурността на мобилното банкиране при тази техника могат да възникнат някои съображения. Например не е подходящо мобилното устройство да се използва като втори фактор в процеса по удостоверяване, тъй като ако бъде получен физически достъп до него сигурността на втория фактор ще бъде компрометирана. Използването на допълнително устройство, на което да се получава информация за втория фактор, също се оказва проблем за потребителите на мобилното банкиране, тъй като носенето му представлява неудобство за тях [124].

Възможност за отстраняване на по-горе разгледания проблем е използването на интегрирани биометрики в мобилните приложения за мобилно банкиране с цел не само да се противодейства на phishing атаките, но и да се подобри удостоверяването на потребителите. През 2011 Fatima [125] представя сканирането на отпечатъци и разпознаването на глас като обещаващ начин за идентифициране и управление на достъпа. Въпреки че биометриките продължават да се смятат за добра алтернатива на удостоверяването посредством парола [126, 127], те имат и своите уязвимости. Отпечатъците, например, се оставят навсякъде, а четците могат да бъдат не толкова трудно компрометирани [128]. Затова е необходимо този вид удостоверяване да се комбинира и с друг метод като еднократна парола (OTP) или SiteKey, с цел да се постигне по-сигурно идентифициране и потвърждаване на самоличността.

Прилагането на SiteKey техниката, използваща картинки и въпроси за сигурност, най-често се реализира като част от процеса по удостоверяване на потребителите. Основната цел е предотвратяването на phishing атаки чрез добавянето на допълнителен слой за проверка на



самоличността. Оказва се, обаче, че тази техника не е достатъчно ефективна. В своето проучване Lee и Bauer [129] показват, че 75% от тестваните потребители въвеждат данните за удостоверяване, въпреки липсата на картинката, гарантираща, че те не предоставят информацията на phishing уеб сайт.

Като допълнение към многофакторното удостоверяване, доставчиците на услуги за мобилно банкиране подобряват процедурите по удостоверяване като използват допълнителни проверки за сигурност. Те проверяват дали се осъществява влизане в системата от нерегистрирано мобилно устройство по същия начин както се реализира защитата от кражба на кредитни карти, чрез подход базиран на аномалии. Банките позволяват регистрирането на доверени устройства, от където може да се използва традиционното удостоверяване, което се базира на потребителско име и парола. При използването на други устройства от потребителите се изисква многофакторно удостоверяване.

Друг подход за справянето с phishing атаките е използването на софтуер (уеб браузъри, e-mail клиенти, антивирусни програми), който да засече поведение характерно за phishing e-mail или уеб сайт. За съжаление приложението на автоматизирани подходи не е лесна задача. Понастоящем механизмите за противодействие на phishing атаки, разработени за популярните уеб браузъри се базират на „черните“ списъци [130]. Те от своя страна се изграждат или автоматично чрез използването на автоматизирани работи за обхождане, които търсят phishing сайтове [131] или чрез набиране на сигнали за такива сайтове [132]. Не рядко и финансовите институции наемат фирми за сигурност, които ръчно търсят phishing сайтове с цел по-бързото отстраняване на възникващите заплахи.

### **3.5. Защита от злонамерен софтуер**

Подобно на phishing атаките, за противодействие на злонамерения софтуер се прилага информиране на потребителите. Доставчиците на услуги за мобилно банкиране се опитват да запознаят своите клиенти с необходимите действия, които те трябва да предприемат, за да се предпазят от този вид атака. Например препоръчва им се да изключват всички комуникационни интерфейси, които не използват; да актуализират мобилната операционна система; да не използват приложението за мобилно банкиране на смартфон с модифицирана операционна система; да актуализират приложението за мобилно банкиране и да не използват негови стари версии, които могат да съдържат различни уязвимости; да използват мобилно антивирусно приложение. Проблемът, който възниква при тази практика е, че не е сигурно дали потребителите са запознати и едновременно с това дали прилагат тези препоръчителни действия.

Тъй като злонамереният софтуер най-често работи под формата на приложения в мобилните операционни системи, техните производители също прилагат различни техники за защита. Apple използват централизиран модел за предоставяне на мобилни приложения до потребителите, като те могат да бъдат инсталирани само посредством техния официален магазин AppStore. Единственият начин за инсталиране на мобилни приложения от трети страни е чрез реализиране на модификация на мобилната операционна система (jailbreaking). Използвайки този централизиран подход Apple прилагат по-строги политики при контролиране на съдържанието на мобилните приложения и по този начин предоставят по-голяма сигурност на крайния потребител.

При разпространението на своите мобилни приложения Google прилагат алтернативен подход, който се базира на отворения модел. Така компанията позволява на разработчиците да разработват мобилни

приложения с по-малко ограничения, а потребителите да ги инсталират от различни източници, не само от официалния им магазин GooglePlay. В резултат на това, въпреки всички функции за сигурност на операционната система Android, възникват много повече възможности за внасяне на злонамерен софтуер. Например кибер престъпниците могат да инжектират злонамерен код в официално мобилно приложение, след което да го разпространят подписвайки го с анонимен сертификат. Поради тази причина е необходимо използването на допълнителни механизми за подобряване на сигурността на крайния потребител.

Характерна особеност за мобилните операционни системи е, че техните приложения работят в изолирана среда („sandbox“) и по този начин нямат директен достъп помежду си. Този принцип е в основата на тяхната сигурност. Поради естествената нужда от обмяната на данни между мобилните приложения, тя се реализира с помощта на споделени услуги и място за съхранение. Затова в допълнение към използването на изолирана среда, се прилагат и т.н. разрешения (permissions), чрез които се реализира контрол над достъпа до услуги и сензори на устройството. По този начин всяко едно мобилно приложение трябва изрично да заяви желание за достъп до определени услуги и ресурси.

В тази връзка популярна област на изследване е засичане дали дадено мобилно приложение използва разрешения извън разрешените му и как това оказва въздействие върху личните данни на потребителите, а от там и на сигурността на мобилното банкиране. Enck и др. [133] декомпилират Android приложения с цел да проучат какви разрешения те имат над операционната система и установяват, че голяма част от мобилните приложения злоупотребяват с предоставените им разрешения. Макар чрез използване на други методи, тези резултати се подкрепят и от автори като Felt [134] и Feinstein [135]. Освен това с помощта на системата TaintDroid

[136] се установява, че има изтичане на лични данни през Android приложенията. Този проблем се наблюдава и при iOS операционната система, но в значително по-малка степен [137].

Като друг проблем на системата за разрешения на Android се посочва, че по време на инсталиране на дадено мобилно приложение тя разчита потребителят да вземе решение дали да предостави съответните разрешения. За съжаление много от потребителите не са технически способни да вземат такива решения и това често води до инсталирането на злонамерен софтуер.

За справяне със злонамерения софтуер се използват и софтуерни продукти, които могат да се инсталират на мобилното устройство и които служат за откриване на мобилен злонамерен софтуер [138]. За неговото засичане комерсиалните антивирусни приложения най-често прилагат подход, който се базира на сигнатури. При него дадена програма се класифицира като злонамерен софтуер ако тя съдържа последователност от инструкции, които съвпадат с предварително зададен модел. Основната положителна черта на този подход е точното засичане на вече познат злонамерен софтуер. Оказва се, обаче, че приложенията за засичане, които го използват, имат сериозен недостатък. Те могат да бъдат лесно заобиколени, когато се приложат техники за модифициране на злонамереното приложение [139, 140].

## **4. Заключение**

В настоящата глава изследвахме и анализирахме текущото състояние на информационната сигурност в процесите на мобилното банкиране, което е тясно свързано с целта на дисертационния труд. Въз основа на това могат да бъдат направени следните важни заключения. По отношение на същността на мобилното банкиране това са:

- В изследваната литература се прави ясно разграничение между двете основни категории мобилни финансови услуги: мобилно банкиране и мобилно разплащане. В допълнение ясно се посочва мястото на мобилното банкиране като част от мобилната търговия, а тя от своя страна като част от мобилния бизнес.
- На базата на проучените литературни източници предлагаме нова дефиниция за мобилно банкиране: *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.*
- При изследване на услугите, които се предоставят посредством мобилното банкиране е установено, че банките, разположени както в развитите, така и в развиващите се страни, обикновено предлагат 3 основни начина за достъп на потребителя до този канал: текстови съобщения (SMS), уеб сайт за мобилно уеб приложение и мобилно приложение.
- Предложената дефиниция ясно определя основните участници в процеса на мобилното банкиране. Това са потребителят, доставчикът на услуги за мобилно банкиране и преносната среда, служеща за предаване на информацията между тях. Те са пряко свързани с проблемните области за неговата сигурност.

Не по-малко важни заключения могат да бъдат направени и по отношение на проблемните области:

- Сигурността при мобилното банкиране се определя като много сложен процес поради наличието на различни участници при неговата реализация. Тази сложност води до необходимостта

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.

- Идентифицирахме четири основни проблемни области при потребителя по отношение на сигурността при мобилното банкиране - мобилно устройство, мобилна операционна система, мобилен уеб браузър и мобилно приложение за мобилно банкиране.
- В резултат на изследване на уязвимостите и произтичащите от тях заплахи във всяка една от дефинираните проблемни области определихме най-често реализираните атаки, насочени към сигурността на мобилното банкиране: 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.

Що се отнася до прилаганите практики и стратегии за защита, най-важните заключения са:

- В изследваната литература за всяка една от най-често реализираните атаки съществува широк набор от добри практики и стратегии за защита. Установихме обаче, че не всички от тях са достатъчно ефективни и това налага да бъдат внесени 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 чрез реализирането на механизъм, предоставящ едновременно по-добро удостоверяване и необходимото удобство при използването му от потребителя.

- По отношение на мобилната операционна система една от насоките за подобрене се свързва с техническата неспособност на потребителите да вземат решения, свързани с предоставянето на определени разрешения по време на инсталация на дадено мобилно приложение. Друга насока е подобряване на антивирусния софтуер, използван при мобилните устройства, като целта е да се преодолее невъзможността му да засича модифициран злонамерен софтуер.
- По отношение на мобилния уеб браузър също съществуват две насоки за подобрене. 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 подобрене може да бъде направено и за защита от CSRF атака, тъй като голяма част от наличните механизми за защита биват реализирани на сървъра, а не при потребителя.
- По отношение на мобилното приложение за мобилно банкиране съществуват три насоки за подобрене. Първата се свързва с реализирането на контрол на качеството от страна на разработчиците на тези приложения, при който да се проверява дали се използва актуална версия на TLS протокола и дали се реализира проверка на сертификата на сървъра. Втората има за цел да се избегнат phishing атаки или достъп до мобилното приложение в следствие на реализиран неупълномощен достъп –

за това е необходимо подобряване на удостоверяването на мобилното приложение. 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. 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.

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

Реализацията на сигурността на информационните системи, автоматизиращи даден бизнес процес, започва с дефинирането на определени директиви от най-високо ниво, които представляват фундаментални цели от гледна точка на сигурността, насочени както към цялата система, така и към изграждащите я компоненти. Тези цели определят политиката за сигурност, която представлява стратегически инструмент за дефиниране на управлението и защитата на чувствителни ресурси и информация. Въз основа на дефинираните цели следва да се изготвят конкретните изисквания за сигурността. Те от своя страна се използват за създаването на модел за сигурност, който представлява символично и формализирано в рамките на възможното представяне на

политиката за сигурност и който осигурява необходимата логическа структура, която трябва да се следва за реализирането на крайната цел. Едва след дефинирането на модела за сигурност се пристъпва към определяне на спецификите за разработване на определени компоненти и механизми за сигурност.

Тъй като мобилното банкиране не е нов процес, управленският персонал на всяка организация, която го прилага, разполага с фундаментални цели от гледна точка на неговата сигурност. От друга страна обаче, за да бъдат дефинирани актуалните изисквания по отношение на неговата сигурност, е нужно да бъдат идентифицирани съществуващите проблемни области. Това направихме във втора точка на първа глава на настоящата разработка. Там сигурността при мобилното банкиране се определя като много сложен процес и това обуславя необходимостта обхватът на нейната реализация в настоящата разработка да бъде стеснен и насочен към потребителя, тъй като той най-често се посочва като най-слабото звено за сигурността. В резултат на направения анализ идентифицирахме четири основни проблемни области при потребителя по отношение на сигурността при мобилното банкиране, въз основа на които 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.

На база на дефинираните по-горе изисквания следва да изготвим **концептуален модел за повишаване на сигурността при мобилното банкиране**. Неговото изготвянето изисква определянето на необходимите логически стъпки, които трябва да бъдат реализирани с цел да бъдат

удовлетворени изискванията за сигурността. За всяко едно от четирите изисквания 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 реализираните подобрения.

Представените етапи следва да бъдат изпълнени в представената по-горе последователност, тъй като те са взаимосвързани и резултатите получени след осъществяването на всеки предходен задават входните параметри за всеки следващ. В допълнение за изпълнението на всеки от тях могат да бъдат използвани различни подходи, както автоматизирани, така и неавтоматизирани.

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. В резултат на това последователно определихме най-често реализираните атаки, насочени към сигурността на мобилното банкиране, най-често използваните стратегии за защита и добри практики, както и тяхната ефективност. 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 устройство;
    - 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;

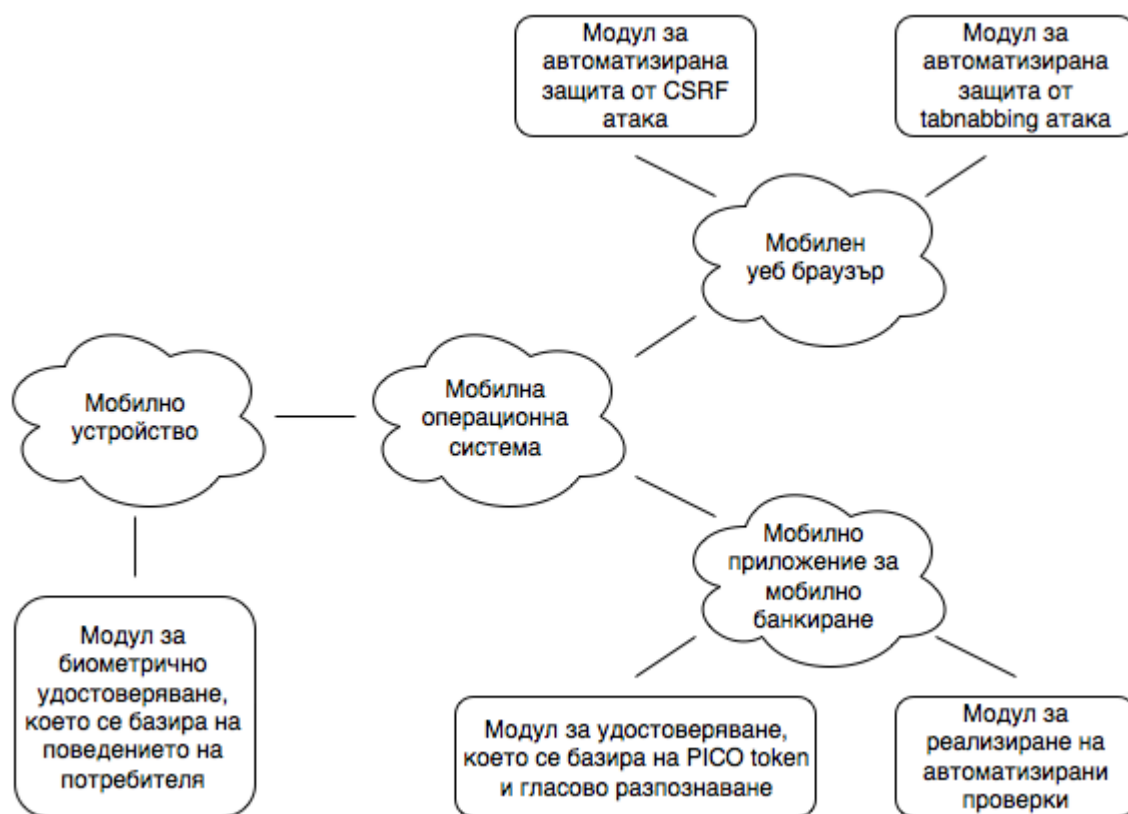
- проверка за определяне дали мобилната операционна система е модифицирана;
  - проверка за инсталирано мобилно антивирусно приложение;
  - проверка за определяне успешното засичане на модифициран злонамерен софтуер от наличния антивирусен софтуер.
- За реализиране на защита на мобилния уеб браузър:
    - 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 приложение 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 внасяни 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 и 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 функционалната структура на подобренията, които участват в концептуалния модел за повишаване на сигурността при мобилното банкиране (вж. фиг. 4).



Фиг. 4. Подобренията, които участват в концептуалния модел за повишаване на сигурността при мобилното банкиране

Всеки един от представените модули на фиг. 4 следва да бъде допълнително разгледан, за да се добие по-пълна представа относно общата му архитектура и функционалните възможности, които той предоставя. Под архитектура следва да разбираме не само структурата на модула, но и процесите, които той изпълнява, тъй като основната цел тук е всеки модул да се представи в разбираем за разработчиците вид. За реализирането на това може да се следва общ подход, като при него е необходимо последователно да бъдат определени някои съображения и изисквания за неговото проектиране, основните процеси, които следва да бъдат обхванати, входните и изходните параметри за всеки един от тях, а въз основа на това и архитектурата на модула.

## **2. Модул за биометрично удостоверяване, което се базира на поведението на потребителите**

Биометричното удостоверяване при мобилните устройства може да се базира на два вида характеристики - физически (пръстов отпечатък, ирис, геометрия на ръката и др.) или поведенчески (начин на натискане на клавишите, начин на подписване, начин на докосване на сензорния екран (touchscreen) на устройство).

Тук можем да дефинираме, че **настоящият модул за биометрично удостоверяване 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.**

За да осъществим неговата основна функционалност е необходимо да определим основните процеси, които трябва да реализира модулът. Те са:

- събиране на входни данни и тяхното съхранение;
- извличане на отличителни белези от събраните входни данни;
- обучение на модула въз основа на извлечените отличителни белези;
- удостоверяване на потребителя.

При реализиране на събирането на входните данни е необходимо от сензорния екран на мобилното устройство да бъдат получени следните входни параметри:

- вид движение при докосване – натискане, отпускане, придвижване, превъртане;
- координати на точката на докосване – определят мястото на докосване на сензорния екран;
- размер на точката на докосване;
- сила на натиск при докосване;
- време на реализиране на докосване – на база на това може да бъде изчислена продължителността на докосване.

Те от своя страна ще служат като входяща информация при реализиране на извличането на отличителните белези или при реализиране на процеса по удостоверяване на потребителя.

В допълнение към дефинираните по-горе входни параметри причисляваме и дефинирането на шаблон за заключване, който да се използва за допълнително удостоверяване на потребителя.

Основната задача при извличането на отличителните белези е да бъдат извлечени определени характеристики на докосване, на база на които да се създаде уникален подпис, който да се използва при удостоверяване на потребителя. Следва да бъдат извлечени следните характеристики:



- брой движения при докосване за определено време;
- брой докосвания с няколко пръста за определено време;
- брой докосвания с един пръст за определено време;
- средна продължителност на движение при докосване за определено време;
- средна продължителност на докосване с няколко пръста за определено време;
- средна продължителност на докосване с един пръст за определено време;
- среден размер на докосваната област от един пръст;
- приблизително най-често докосвана област от сензорния екран;
- стандартно отклонение от приблизително най-често докосвана област – използва се за по-точно дефиниране на предходната характеристика;
- средна скорост на движение при докосване;
- средна сила на натиск при докосване.

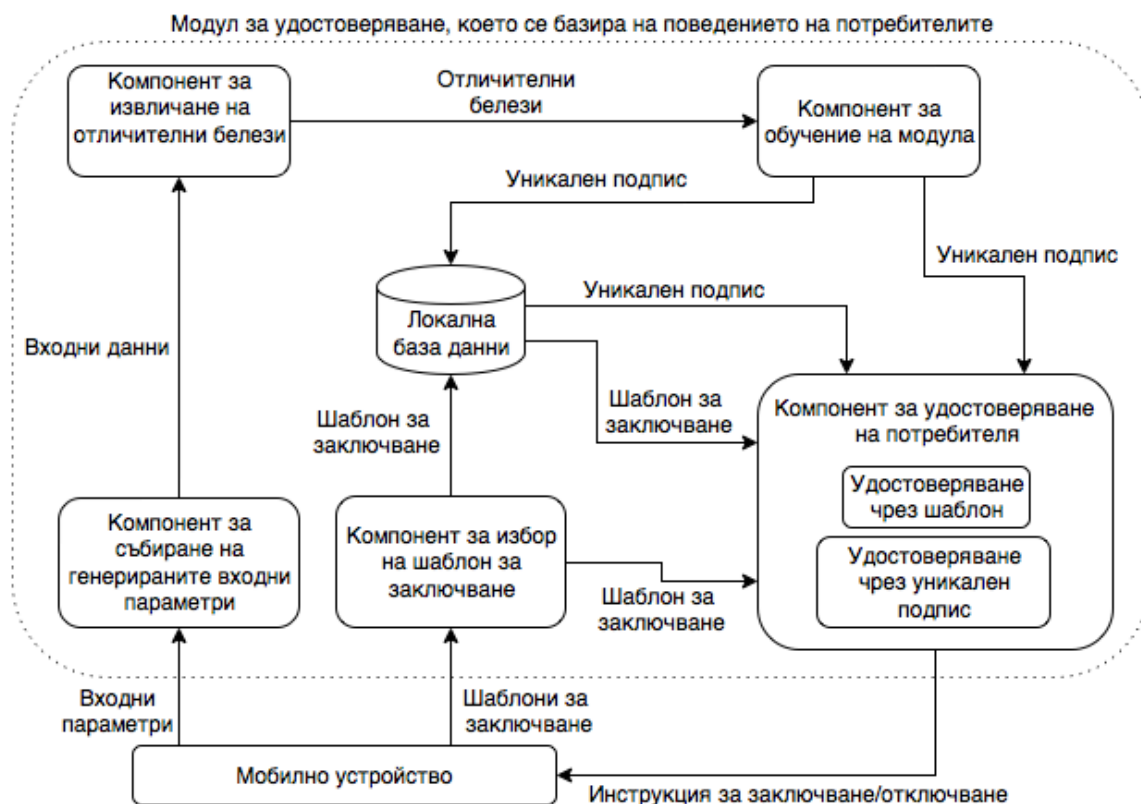
Процесът по обучение на модула въз основа на извлечените отличителни белези се състои в създаването на уникален подпис, който да се използва при удостоверяване на потребителя. Това следва да се реализира с използването на алгоритъм за машинно обучение. Неговият избор не е лесна задача, тъй като съществуват различни алгоритми за машинно обучение, които са подходящи за различни цели. Затова е необходимо да бъде направено допълнително изследване, при което да се направи оценка на ефективността на различните алгоритми.

Самото обучение трябва да се състои от две фази – предварително обучение и последващо обучение. Когато потребителят използва устройството за първи път се активира предварителното обучение, при което от потребителя трябва да се поиска да нарисува определен брой

шаблони, като по този начин модулът събира данни за поведенчески биометрични характеристики като размер на пръста, сила на натиск, координация и др. Преди преминаването към следващата фаза потребителят трябва да избере един от шаблоните за заключване, който да използва при своето удостоверяване. След това е необходимо реализирането на последващо обучение за определен период от време, при което модулът продължава да се обучава за евентуални промени, които могат да настъпят в поведението на потребителя.

Когато потребителят иска да отключи устройството, той трябва да се удостовери посредством по-рано избрания шаблон. При успех модулът трябва да продължи да наблюдава поведението на потребителя, като събира необходимите данни и ги сравнява с изготвения по време на обучението уникален подпис. Ако в даден момент се получи несъответствие между сравняваните стойности към мобилното устройство трябва да се изпрати инструкция то да се заключи. При минимални различия от уникалния подпис може да се реализира допълнително обучение, в резултат на което да се създаде нов такъв.

Въз основа на разгледаните процеси на фиг. 5 предлагаме архитектурата на модула за биометрично удостоверяване. Както се вижда от представената на фигурата архитектура, за реализиране на модула за биометрично удостоверяване, който се базира на поведението на потребителите е необходимо изграждането на шест софтуерни компонента: компонент за събиране на генерираните входни параметри, компонент за избор на шаблон за заключване, локална база данни, компонент за извличане на отличителни белези, компонент за обучение на модула и компонент за удостоверяване на потребителя.



Фиг. 5. Архитектура на модула за биометрично удостоверяване

### 3. Модул за автоматизирана защита от tabnabbing атака

Преди да пристъпим към изграждането на настоящия модул е необходимо да разгледаме начина на функциониране на tabnabbing атаката, което ще ни помогне за определяне на някои изисквания към проектирането и на основните процеси, които трябва да участват в автоматизираната защита.

Този вид атака разчита на способността на съвременните браузъри, както за персонални компютри, така и за мобилни устройства, да предоставят възможност за отваряне на нов уеб сайт в нов раздел (tab). Тя протича в следната последователност от действия:

1. Даден кибер престъпник убеждава даден потребител да посети злонамерен уеб сайт, който на пръв поглед изглежда като безвреден. Основната идея е този уеб сайт да остане зареден в раздел на уеб браузъра,

при което потребителят да отвори нов раздел. За реализирането на това кибер престъпникът често използва атрактивни хипервръзки, при избора на които се генерира пренасочване към нов уеб сайт, която се зарежда в нов раздел.

2. При изгубване на фокуса върху раздела, в който е зареден уеб сайтът, генериращ tabnabbing атаката, се стартира JavaScript код. Неговата задача е след известно изчакване (за да е сигурно, че потребителят в настоящия момент използва друг раздел на уеб браузъра) да се извършват промени със съдържанието на уеб сайта. Променят се заглавието, favicon (иконата, която се изобразява в раздела до името на уеб сайта) и цялостният изглед, по такъв начин, че уеб сайтът да заприлича на форма за удостоверяване на дадено уеб приложение. Изборът кое уеб приложение да се имитира може да е предварително дефиниран или да се базира на статистиката на уеб браузъра за най-често зарежданите уеб приложения от потребителя. Междувременно потребителят използва друг раздел на уеб браузъра и нищо не подозира за реализираните промени.

3. На един по-късен етап, когато потребителят реши да разгледа отворените раздели на уеб браузъра, той може да разпознае някой с позната favicon и несъзнателно да отвори раздела, съдържащ контролирания от кибер престъпника уеб сайт. На този етап е малко вероятно потребителят да провери адреса на уеб сайта в адресната лента, тъй като той разчита на доверието, което има в предишно отворените раздели и заредените в тях уеб сайтове. След предоставянето на убедителна форма за удостоверяване потребителят продължава като въвежда чувствителна информация, която се изпраща на кибер престъпника и с това tabnabbing атаката приключва.

Въз основа на начина на функциониране на този вид атака можем да дефинираме, че **настоящият модул за автоматизирана защита от tabnabbing атака 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.**

От архитектурна гледна точка модулът за автоматизирана защита от tabnabbing атака може да бъде реализиран като добавка за мобилен уеб браузър, защото по този начин неговата функционалност ще може да бъде добавена към всеки мобилен уеб браузър, който има система за добавяне на допълнителни софтуерни компоненти и функционалности.

За да осъществим неговата основна функционалност е необходимо да определим основните процеси, които трябва да реализира модулът. Те са:

- запомняне на начина, по който е изглеждал уеб сайтът, преди разделът, в който е зареден, да загуби фокус;
- сравняване с начина, по който ще изглежда разделът след възстановяване на фокуса;
- представяне на потребителя на засечените промени.

За запомняне на начина, по който е изглеждал уеб сайтът, преди разделът, в който е зареден, да загуби фокус, следва да използваме подход, който се базира на видимото съдържание на дадения раздел, точно по начина по който потребителят го възприема. Това води до няколко предимства в сравнение с техники, които анализират структурата и съдържанието на дадена страница и при които се наблюдава заобикаляне на превантивните мерки срещу tabnabbing атаката. За реализацията на този първи процес е необходимо да се използва помощта на приложно програмния интерфейс (API) на съответния мобилен уеб браузър с цел да бъдат получени следните входни параметри:

- favicon на заредения уеб сайт;

- снимка на настоящо отворения раздел точно преди да бъде загубен фокусът.

В случай, че приложният програмен интерфейс на съответния мобилен уеб браузър не позволява реализирането на снимка точно в този момент, като алтернативно решение може да се предложи нейното реализиране през определени интервали от време, когато разделът е бил на фокус, като в локален файл или база от данни следва да се поддържа информация за нейната последна версия.

Тази снимка ще се използва като основа за сравнение, когато разделът получи обратно фокус. Тя и favicon трябва да бъдат съхранени и изпратени като входяща информация към следващия процес.

Когато даден раздел бъде възстановен на фокус, модулът трябва отново да използва приложно програмния интерфейс на съответния мобилен уеб браузър и да получи същите входни параметри като при предходния процес.

След това трябва да се направи сравнение между съхранените данни при изгубване на фокуса върху дадения раздел и тези след неговото възстановяване, в резултат на което да бъдат засечени разликите. Сравнението на favicon следва да се реализира по първичния програмен код, а снимката да се сравнява напълно визуално. За целта е необходимо всяка снимка да бъде разделена на растерни изображения с фиксиран размер. Размерът трябва да бъде така определен, че да се постигне максимален баланс между производителност и прецизност. Всяко изображение, което е част от едната снимка, се сравнява със съвпадащото му от другата снимка. От съществено значение тук е изборът на алгоритмите, които ще послужат както за разделяне на снимката на растерните изображения, така и за реализиране на тяхното сравнение.

Ако се окаже, че няма точно съвпадение между сравняваните изображения, от настоящия процес трябва да бъдат изпратена информация, определяща кои части от общата снимка следва да бъдат маркирани като променени.

Веднъж след като различията за фокусирувания раздел са изчислени, модулът следва да покрие напълно уеб сайта с допълнителен слой, който е прозрачен, с изключение на различията, които следва да се покажат в полупрозрачен червен цвят. Този допълнителен слой не трябва да причинява никакви нежелани взаимодействия и едновременно с това да позволява през него към оригиналното съдържание на уеб сайта да преминават събития, генерирани от мишката или клавиатурата.

От съображения за сигурност при реализиране на този процес е необходимо да се извършва засичане, при което да се проверява дали злонамереният уеб сайт не се опитва да отстрани този допълнителен слой с цел да заблуди потребителя и ако е така трябва да се използва подходящ механизъм за известяване.

Затова като решение на представения проблем в допълнение към слоя, който отбелязва промените на уеб сайта, модулът може да използва допълнителен индикатор за сигурност, който да е част от мобилния уеб браузър и който да дава информация за настоящия статус на сайта. При него могат да се разграничат следните нива:

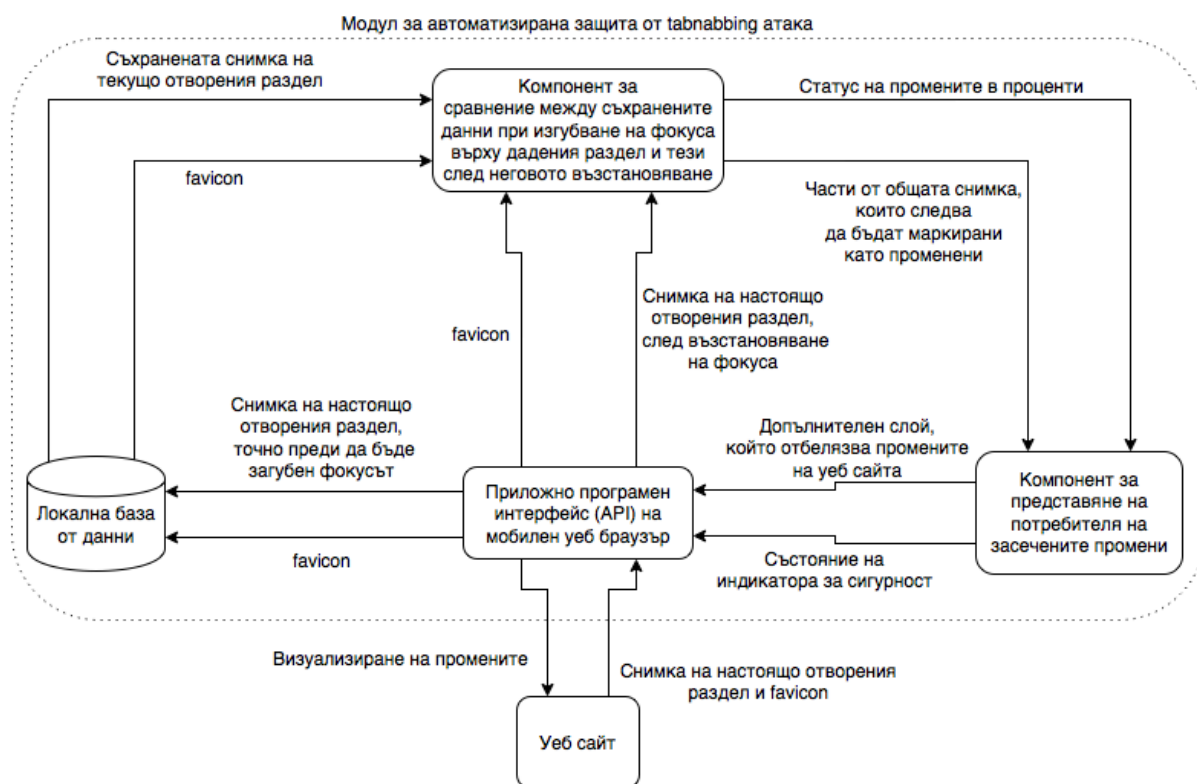
- минимална промяна – до 15 % от съдържанието на сайта;
- умерена промяна – до 50 % от съдържанието на сайта;
- съществена промяна – над 50 % от съдържанието на сайта.

Наличието на представения индикатор за сигурност като част от средата на мобилния уеб браузър, подсигурява, че дори злонамереният уеб сайт да успее по някакъв начин да премахне слоя, визуализиращ

промените, потребителят може да разчита на друг механизъм, показващ достоверността на сайта.

Този механизъм за известяване може да бъде реализиран подобно на други широко възприети и внедрени механизми за известяване, каквито например са изобразяването на „катианар“ когато се използва сигурна връзка или визуализирането на съобщение, съдържащо предупреждение за невалиден SSL сертификат.

Въз основа на разгледаните процеси предлагаме следната архитектура на модула за автоматизирана защита от tabnabbing атака (вж. фиг. 6).



Фиг. 6. Архитектура на модула за автоматизирана защита от tabnabbing атака

Както се вижда от представената на фиг. 6 архитектура, за реализиране на модула за автоматизирана защита от tabnabbing атака е



необходимо изграждането на два софтуерни компонента: компонент за сравнение между съхранените данни при изгубване на фокуса върху дадения раздел и тези след неговото възстановяване и компонент за представяне на потребителя на засечените промени.

#### **4. Модул за автоматизирана защита от CSRF атака**

Преди да пристъпим към изграждането на настоящия модул е необходимо да разгледаме начина на функциониране на CSRF атаката, което ще ни помогне за определяне на някои изисквания към проектирането и на основните процеси, които трябва да участват в автоматизираната защита.

Класическата CSRF атака протича в следната последователност от действия:

1. Потребителят създава сесия за удостоверяване, която се използва от дадено уеб приложение. В това се включва въвеждането от негова страна на информация за удостоверяване посредством уеб браузър, нейното изпращане до уеб приложението и връщането на потвърждение или отказ за успешното създаване на сесията. Предварителното създаването на сесия за удостоверяване се определя като задължително условие за успешното реализиране на атаката.

2. На един по-късен етап потребителят решава да зареди нов уеб сайт в друг раздел на уеб браузър, който се оказва злонамерен уеб сайт. Вероятността за успех при реализиране на атаката може да бъде повишена, ако съдържанието на злонамерения уеб сайт е пряко свързан с атакуваното уеб приложение. Например при атакуването на мобилен сайт за мобилно банкиране, кибер престъпникът може да използва уеб сайт, който предоставя финансови съвети на потребителите. Друг вариант за повишаване на успеваемостта на атаката е вмъкването на хипервръзки в

уеб приложението от действие 1, които водят до зареждането на злонамерения сайт.

3. Злонамереният сайт създава скрита заявка, която изпраща към уеб приложението от действие 1, като при това уеб браузърът предполага, че заявката е част от по-рано създадената сесия за удостоверяване и автоматично добавя към нея информация за сесията, в която се включват и данните за удостоверяване на потребителя.

Казаното до тук определя CSRF атаката като реализирането на cross-site заявки докато е активна дадена сесия за удостоверяване. Cross-site заявка е заявка, която се обръща към източник (домейн), който е различен от този, към който се предполага, че тя се обръща.

Следователно тяхното забраняване предполага осигуряването на надежден начин за противодействие на CSRF атаките. Това обаче не е съвсем така, тъй като cross-site заявки се използват и при реализирането на незлонамерени функционалности. Те намират приложение при доставчиците на интернет разплащания и при реализирането на централизирано удостоверяване. Например когато даден потребител иска да използва PayPal за реализиране на разплащане, уеб браузърът препраща потребителя от онлайн магазина към уеб сайта на доставчика. След като потребителят се удостовери и приеме разплащането, уеб браузърът препраща обратно към уеб сайта, от който е иницирано разплащането. Тук имаме cross-site заявка от PayPal към онлайн магазина по време на неговата сесия за удостоверяване.

Допълнителното усложняване за реализирането на настоящия механизъм за защита от CSRF атака е съществуването на HTTP пренасочване. Когато уеб сървърът получи заявка, той може да върне отговор, който изисква от уеб браузъра да реализира пренасочване поради различни причини, например защото ресурсът, който трябва да се достъпи

е преместен. Уеб браузърът ще реализира това пренасочване автоматично, без да изисква взаимодействие от страна на потребителя. Поради широката приложимост на механизма за пренасочване, проблемите свързани с него няма как да бъдат игнорирани. Нещо повече злонамерените сайтове могат да го използват с цел да заобиколят защитата от CSRF атака при клиента. Следователно, правилното справяне с HTTP пренасочването е ключово изискване за сигурността.

В резултат на това като две основни предизвикателства при реализирането на механизъм за защита от CSRF атака на ниво потребител можем да посочим реализирането на ясно разграничаване между злонамерени и незлонамерени cross-site заявки и вземането предвид възможността за възникване на заявка генерираща пренасочване.

Въз основа на горните съображения, можем да дефинираме, че **настоящият модул за автоматизирана защита от CSRF атака, следва да бъде реализиран като инструмент, който защитава нарушаването на цялостността на сесията за удостоверяване, при изпращането на cross-site заявки. За осъществяването 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.

От архитектурна гледна точка модулът за автоматизирана защита от CSRF атака може да бъде реализиран като добавка за мобилен уеб браузър, защото по този начин неговата функционалност ще може да бъде добавена към всеки мобилен уеб браузър, който има система за добавяне на допълнителни софтуерни компоненти и функционалности.

За да осъществим неговата основна функционалност е необходимо да определим основните процеси, които трябва да реализира модулът. Те са:

- проверка на вида на генерираната заявка;
- проверка на вида на cross-site заявката;
- определяне на състоянието на сесията (cookies и authentication headers), което мобилният уеб браузър трябва да прикрепи към генерираната заявка.

При първия процес първоначално следва да се провери дали след изпращане на заявката до източника, той връща отговор, с който изисква от мобилния уеб браузър да реализира пренасочване към друг източник или не. Без значение от резултата е необходимо да се направи втора проверка, при която да се определи дали генерираната заявка е стандартна заявка (обръща се към същия източник, който е наличен в сесията за удостоверяване) или cross-site заявка (по-горе вече определихме какво представлява тя).

При реализирането на процеса по проверка на вида на cross-site заявката следва да приложим следното правило: дадена cross-site заявка може да се смята за незлонамерена, тогава и само тогава когато по-рано в рамките на сесията на уеб браузъра, един източник изрично е упълномощил друг по специфичен начин да реализира този вид заявка. След като бъде реализирано упълномощаване между два източника е необходимо то да бъде съхранено в хранилище за упълномощаване. Тук е важно да уточним, че даден източник следва да реализира такъв вид упълномощавания само за източници, на които вярва. С други думи, даден източник остава уязвим на CSRF атаки, ако са реализирани от източници, на които той има доверие.

Важно е също да определим в какво се състои упълномощаването между два източника – източник А упълномощава източник Б, когато

източник А създава и изпраща POST заявка към източник Б или когато източник А реализира препращане към източник Б с помощта на URL, съдържащо параметри.

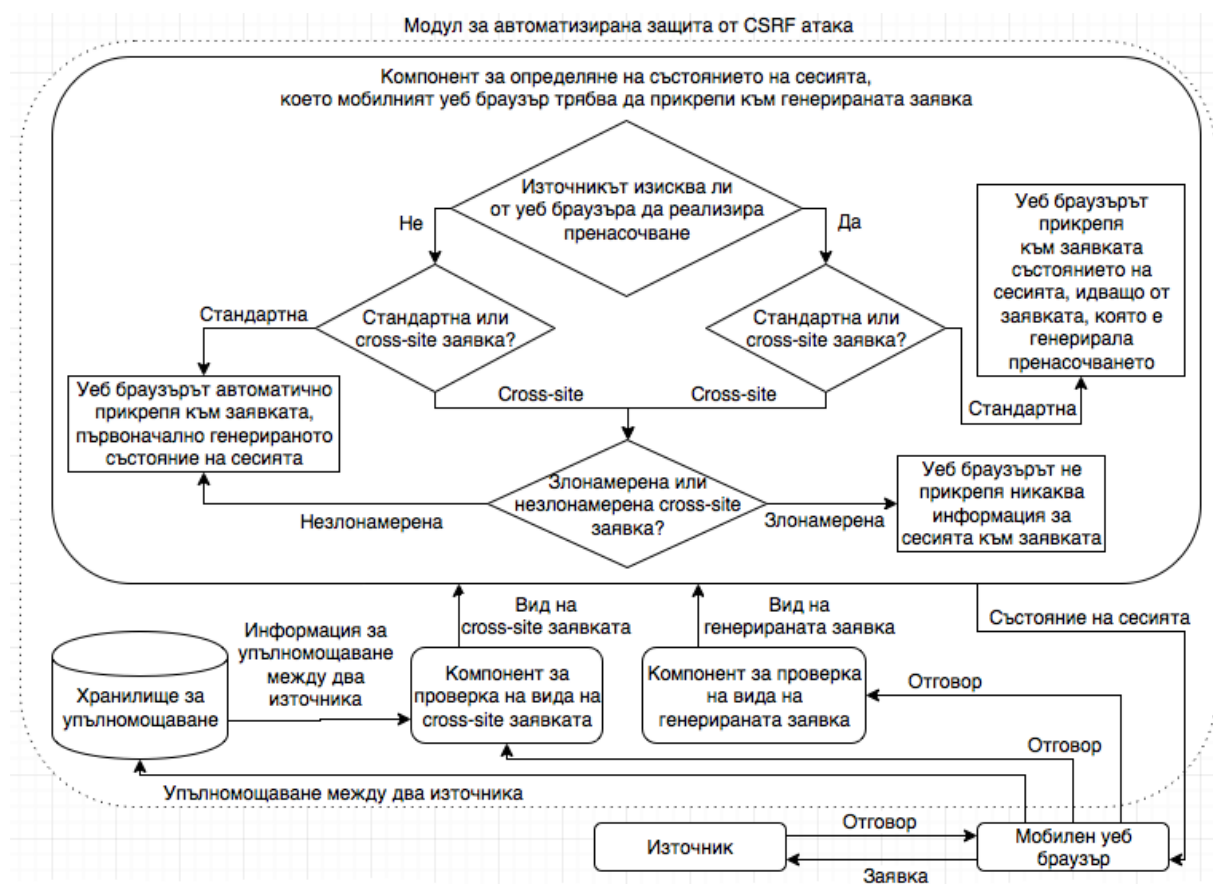
Начинът на упълномощаване е реализиран на базата на това правило поради две причини. Първата е, че незлонамерените cross-site заявки функционират чрез представения механизъм, а втората, че е доста трудно кибер престъпникът да накара даден източник да изпрати POST заявка или URL, съдържащо параметри, към неговия злонамерен сайт. Ако това бъде реализирано, то даденият източник има по-сериозни проблеми за сигурността като cross-site scripting (XSS) уязвимост или неупълномощено проникване в неговия сървър.

Реализирането на GET заявка между два източника не се приема за сигурно упълномощаване, тъй като в даден уеб сайт могат да бъдат инжектирани хипервръзки, водещи към злонамерени уеб сайтове, чиято цел е реализирането на CSRF атака. Например в уеб сайтовете на социалните мрежи потребителите имат възможност за генериране на съдържание, което да се показва на другите потребители. В това съдържание могат да бъдат внедрени хипервръзки към злонамерен уеб сайт, които даден потребител може да отвори след като е извършил успешно удостоверяване, в резултат на което да се стартира CSRF атака.

Последният процес се свързва с определяне на състоянието на сесията, което мобилният уеб браузър трябва да прикрепи към генерираната заявка. Нека първоначално разгледаме ситуацията, при която източникът, до когото е генерираната заявка, не връща отговор, с който изисква от уеб браузъра да реализира пренасочване към друг източник. Ако в този случай имаме стандартна заявка или незлонамерена cross-site заявка, те се управляват по същия начин както се управляват понастоящем от незащитен уеб браузър. Уеб браузърът автоматично прикрепя към заявката,

първоначално генерираното състояние на сесията. Ако уеб браузърът установи, че заявката е злонамерена cross-site заявка, той не прикрепя никаква информация за сесията към нея.

Сега да разгледаме другата ситуация, при която източникът, до когото е генерираната заявка, връща отговор, с който изисква от мобилния уеб браузър да реализира пренасочване към друг източник. Ако в този случай имаме стандартна заявка, състоянието на сесията се ограничава до познатото състояние на предходната заявка, т.е. заявката, която е генерирала пренасочването. Ако заявката е незлонамерена cross-site заявка, уеб браузърът прикрепя към заявката състоянието на сесията, а ако установи, че заявката е злонамерена, той не прикрепя никаква информация за сесията към нея.



Фиг. 7. Архитектура на модула за автоматизирана защита от CSRF атака

Въз основа на разгледаните процеси на фиг. 7 предлагаме архитектурата на модула за автоматизирана защита от CSRF атака. Както се вижда от представената на фигурата архитектура, за реализиране на модула за автоматизирана защита от CSRF атака е необходимо изграждането на три софтуерни компонента: компонент за проверка на вида на генерираната заявка, компонент за проверка на вида на cross-site заявката и компонент за определяне на състоянието на сесията, което мобилният уеб браузър трябва да прикрепи към генерираната заявка.

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

Както вече споменахме в заключението на първа глава, с цел да се избегнат phishing атаки или достъп до мобилното приложение за мобилно банкиране в следствие на реализиран неупълномощен достъп, е необходимо да се реализира подобряване на удостоверяването и на ниво мобилно приложение.

Като основа за разработването на настоящия модул следва да използваме PICO token, който е разработен от Frank Stajano [141] с основната задача да замени механизмите за удостоверяване, които се базират на пароли. По този начин следва да се реши както проблемът, свързан с неудобството, което потребителят изпитва от необходимостта да помни пароли, така и този, свързан с използването на така наречените слаби пароли, които са податливи на атаки.

В настоящия момент PICO token се реализира като хардуерно устройство, което генерира и управлява данните за удостоверяване на потребителя. За осъществяване на удостоверяване е необходимо потребителят да носи това устройство постоянно. Като допълнителни

съображения за сигурност, за да се реализира удостоверяване с PICO token е необходимо той да осъществи комуникация с малки допълнителни устройства, които са проектирани да бъдат закрепени към всекидневни предмети, които потребителите носят със себе си. Всяко от тези допълнителни устройства предава поредица от тайни. Когато всички необходими тайни се съберат PICO се отключва и може да се използва от своя собственик.

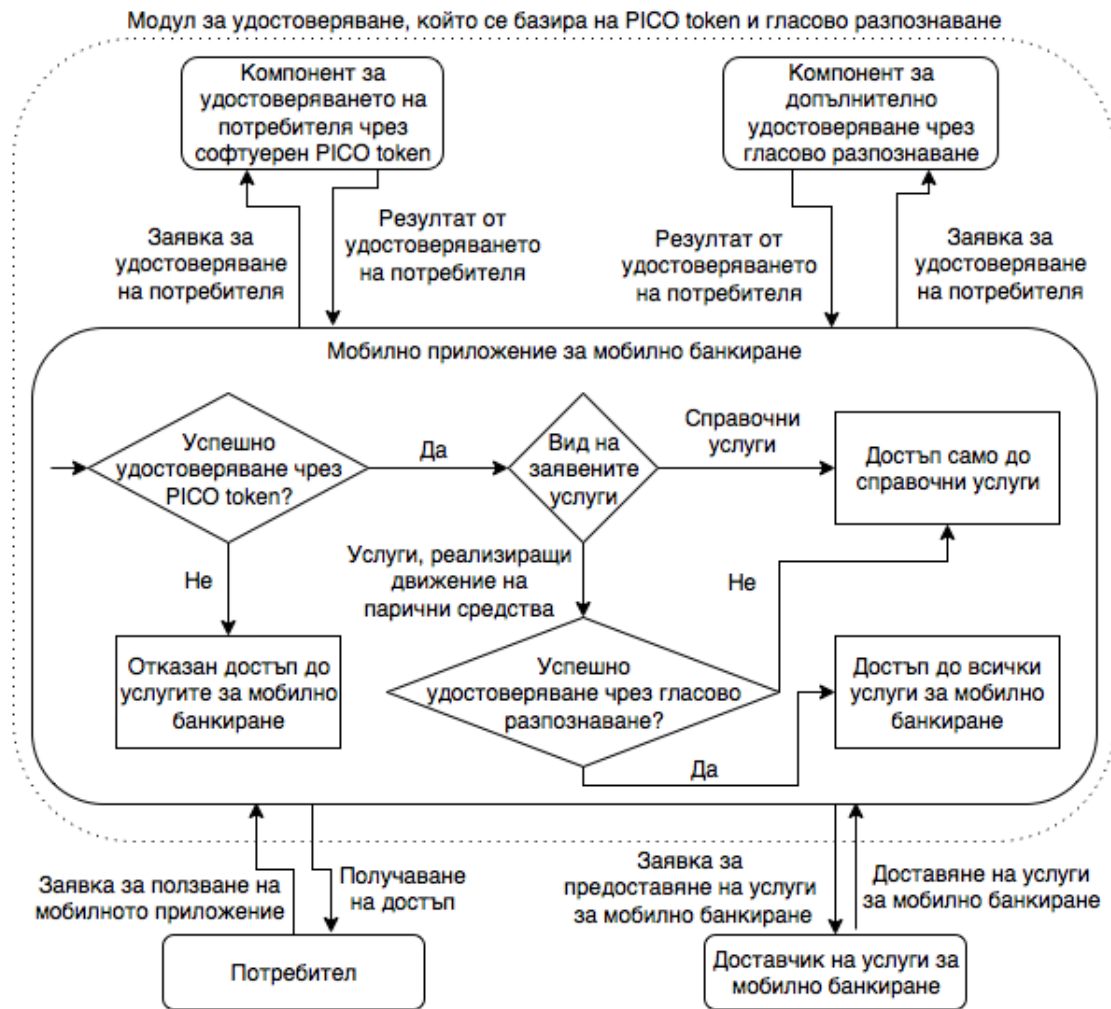
От казаното до тук възникват два основни проблема с прилагането на този механизъм за удостоверяване при използване на приложението за мобилно банкиране. Първият проблем беше разгледан в първа глава на настоящата разработка и се свързва с нежеланието на потребителите да носят допълнителни устройства, тъй като това представлява неудобство за тях. Като решение предлагаме самото мобилно устройство да бъде използвано като PICO token, тъй като настоящите смартфони и таблети могат да предоставя всички необходими хардуерни изисквания за реализирането на това. Естествено, за да се запази необходимото ниво на сигурност, потребителите ще трябва да носят едно или няколко от малките допълнителни устройства. Техните малки размери и лесното им прикрепяне към всекидневни предмети (например ключове) би предоставило необходимото ниво на удобство за потребителите.

Вторият проблем, който възниква, се свързва с факта, че всеки, който притежава PICO token (без значение как е реализиран - дали като хардуерно устройство или е софтуерно вграден в мобилното устройство) и малките допълнителни устройства, може да има пълен достъп до акаунта на потребителя за определен период от време. Затова тук следва да бъдат приложени допълнителни средства за сигурност, които обаче не трябва да изискват от потребителя да помни каквато и да е информация. Като допълнителен фактор за удостоверяване и решение, отговарящо на това



изискване, може да се използва биометричен механизъм за гласово разпознаване. Това е подходящ начин за подобряване на сигурността на достъпа, тъй като понастоящем съвременните мобилни устройства разполагат с високочувствителни микрофони.

Въз основа на горните съображения, можем да дефинираме, че **настоящия модул за удостоверяване 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.**



Фиг. 8. Архитектура на модула за удостоверяване, който се базира на PICO token и гласово разпознаване

От архитектурна гледна точка модулът за удостоверяване, който се базира на PICO token и гласово разпознаване следва да бъде реализиран като два основни компонента (вж. фиг. 8), предоставящи функционалности, които трябва да могат да бъдат интегрирани в мобилните приложения за мобилно банкиране, разработени от доставчиците на тази услуга.

Първият компонент трябва 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 от негова страна да бъде реализирано движение на парични средства е необходимо да бъде реализирано допълнително удостоверяване чрез гласово разпознаване, за което следва да отговаря вторият компонент.

За да осъществим основната функционалност на първия компонент е необходимо да определим основните процеси, които той трябва да реализира. Те са:

- регистрация на потребителя;
- удостоверяване на потребителя.

При стартиране на мобилното приложение за мобилно банкиране се изпраща заявка към софтуерния PICO token, която проверява дали в него са съхранени данни за удостоверяване на потребителя на мобилното устройство. Ако това е така, се преминава към неговото удостоверяване. В противен случай следва да се реализира процес на регистрация.

Процесът на регистрация започва с въвеждането на код, предоставен от банката, което ще доведе до отключване на екрана на мобилното приложение за въвеждане на потребителското име и парола, които също са предоставени от банката. Това е еднократен процес, тъй като от този момент за удостоверяването на потребителя ще се грижи софтуерния PICO token.

След успешното удостоверяване пред сървъра на банката, въведените потребителско име и парола следва да се запазят, след което да се криптират с помощта на симетричен алгоритъм, в резултат на което да се генерира частен ключ, който в последствие ще е необходим за декриптирането им. Създаденият частен ключ не се съхранява в паметта на PICO token, а следва да се раздели на части в зависимост от бройката на малките допълнителни устройства, като всяка част се криптира с несиметричен алгоритъм и посредством радио комуникация се изпраща до всяко устройство.

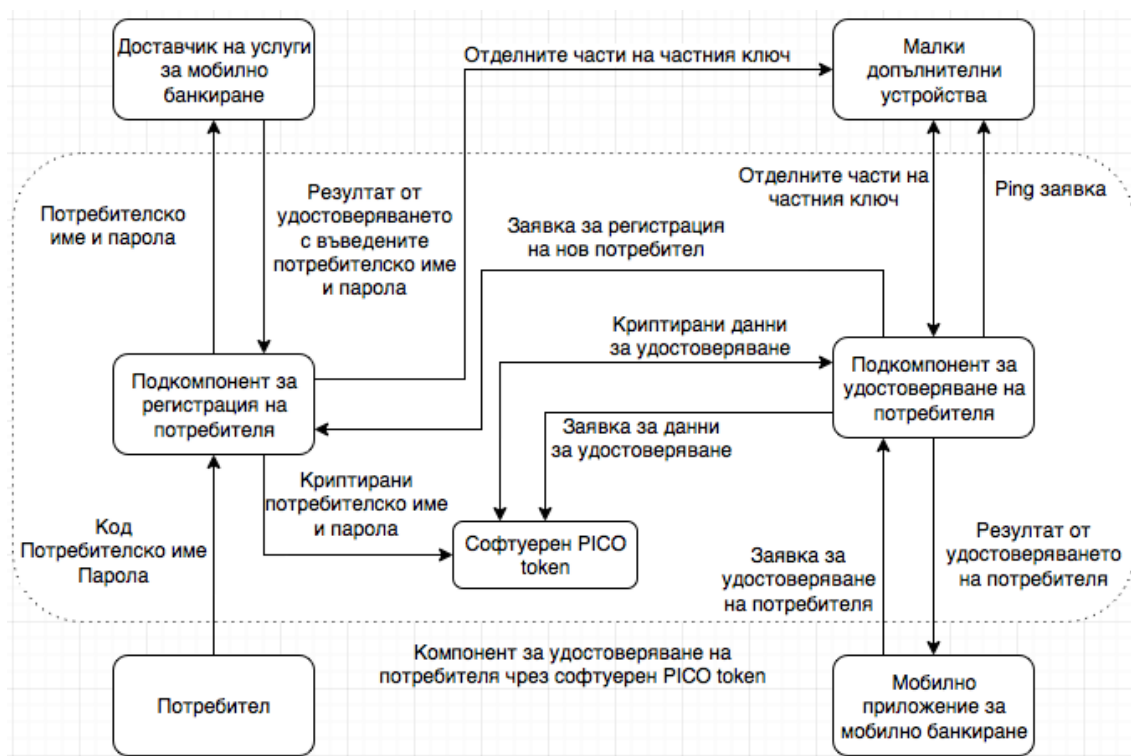
При реализирането на процеса по удостоверяване на потребителя първоначално мобилното приложение за мобилно банкиране изпраща заявка до PICO token, в която изразява желание да получи достъп до потребителското име и паролата. За да може да му ги предостави PICO трябва първо да получи достъп до частния ключ, с чиято помощ да ги декриптира. За да реализира това е необходимо PICO да провери дали в близост до мобилното устройство са налични малките допълнителни устройства. Това се осъществява чрез изпращането на ring заявки, на които те трябва да отговорят. При успешен ring с всяко от тях, към PICO се изпращат частите на частния ключ. Когато всички те бъдат събрани, той се реконструира и в резултат на това се отключват данните за удостоверяване на мобилното приложение и се получава достъп до неговите функционалности (на този етап справочни услуги). Потребителят получава възможност за реализирането на банкови услуги за определен период от време, след което ще е необходимо предходният процес да се повтори.

Веднага след успешното удостоверяване следва потребителското име и паролата на потребителя да бъдат отново симетрично криптирани, като се генерира нов частен ключ, който се разделя на части, всяка от тях се

криптира несиметрично и отново чрез радио комуникация се изпраща до малките допълнителни устройства.

От съображения за сигурност е необходимо да се състави изискване към малките допълнителни устройства да поддържат две основни състояния – начално (фабрично, изчистено) състояние и състояние зададено от потребителя. Към тях е необходимо да се добави и правило, с което се гарантира, че второто състояние не може да повлияе на първото и изискване кога да се преминава в първото състояние. По този начин може да се позволи дистанционното заключване на PICO, както и задаване на начално състояние на малките допълнителни устройства, което ще гарантира невъзможност за достъп до частния ключ.

Въз основа на разгледаните процеси предлагаме следната архитектура на компонента за удостоверяване на потребителя чрез софтуерен PICO token (вж. фиг. 9).



Фиг. 9. Архитектура на компонента за удостоверяване на потребителя чрез софтуерен PICO token.

Както се вижда от представената на фиг. 9 архитектура, за реализиране на компонента за удостоверяване на потребителя чрез софтуерен PICO token е необходимо изграждането на три софтуерни подкомпонента: подкомпонент за регистрация на потребителя, софтуерен PICO token и подкомпонент за удостоверяване на потребителя.

За да осъществим основна функционалност на втория компонент е необходимо да определим основните процеси, които той трябва да реализира. Те са:

- получаване на гласов сигнал;
- извличане на отличителни белези от получения гласов сигнал;
- моделиране на профил на потребителя въз основа на извлечените отличителни белези;
- сравнение на моделираните профили;
- удостоверяване на потребителя.

Получаването на гласов сигнал следва да се реализира с помощта на микрофона на мобилното устройство. Този процес се осъществява в два случая – при добавянето на нов потребител или при удостоверяването на вече съществуващ. И в двата случая от потребителя се изисква да прочете динамично генерирана фраза, която се визуализира на екрана на мобилното устройство. В резултат на това като входяща информация към следващия процес се изпраща записаният гласов сигнал.

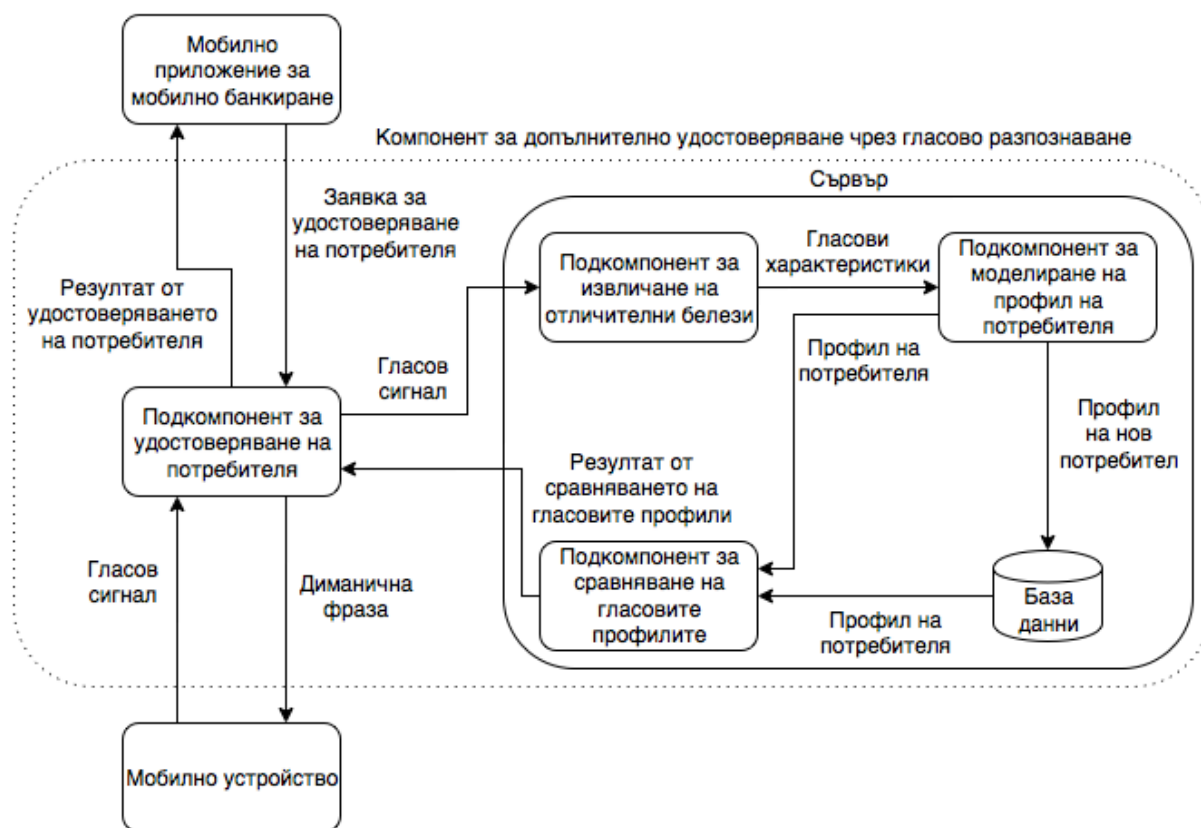
Основната задача при извличането на отличителните белези е записаният гласов сигнал да бъде изпратен на сървър, където от него да бъдат извлечени определени гласови характеристики, които ще послужат за моделиране на профил на потребителя, който ще се използва при неговото удостоверяване. Въпреки че има различни методи за реализиране на този процес, най-често използваната техника е MFCC (Mel-Frequency Cepstral

Coefficient), която дава форма на отличителните белези като вектори в равнината.

След извличане на отличителните белези е необходимо съввърът да реализира обучение над тях, в резултат на което да бъде моделиран профил на потребителя, който да се съхрани в базата данни. Съхранението на моделирания профил следва да се реализира само и единствено когато потребителят използва мобилното приложение за мобилно банкиране за първи път, в резултат на което се осъществява процес по регистрация. В противен случай новият моделиран профил се използва за удостоверяване на потребителя. И в двата случая профилът следва да съдържа MFCC векторите от предходния процес, от които да се извлекат отличителните белези. Самото моделиране на профила може да се реализира чрез използването на алгоритъм LBG (Linde–Buzo–Gray) за векторно квантуване, което е стандартна техника за групиране на приблизително сходни вектори в равнината.

При реализиране на удостоверяване на потребителя, трябва отново да бъде прихванат гласов сигнал. Последователно да се премине през стъпките по извличане на отличителни белези и моделиране на профил. След това следва да бъде реализирано сравнение между профила, генериран при процеса на удостоверяването и този, съхранен при регистрацията на потребителя. За осъществяването на процеса по сравнение между профилите може да се използва измерване на разстояние в евклидовото пространство. Ако дотук всичко премине успешно, следва да бъде реализирано и сравнение дали потребителят е произнесъл динамично генерираната фраза, като по този начин се цели да се избегне използването на предварително записан глас.

Въз основа на разгледаните процеси предлагаме следната архитектура на компонента за допълнително удостоверяване чрез гласово разпознаване (вж. фиг. 10).



Фиг. 10. Архитектура на компонента за допълнително удостоверяване чрез гласово разпознаване.

Както се вижда от представената на фиг. 10 архитектура, за реализиране на компонента за допълнително удостоверяване чрез гласово разпознаване е необходимо изграждането на четири софтуерни компонента: подкомпонент за извличане на отличителните белези, подкомпонент за моделиране на профил на потребителя, подкомпонент за сравняване на гласовите профили и подкомпонент за удостоверяване на потребителя.

## **6. Модул за реализиране на автоматизирани проверки**

Разработването на настоящия модул се свързва пряко с неуспехите при обучение на потребителя по отношение на определени препоръчителни действия, предлагани от доставчиците на услуги за мобилно банкиране. Неговата основна задача е да улесни потребителите, като реализира набор от автоматизирани проверки, които да изследват определени параметри на мобилното устройство, пряко свързани със сигурността на мобилното банкиране.

В първа точка на настоящата глава ясно бяха дефинирани четири основни изисквания по отношение на сигурността на мобилното банкиране. В процеса по формулиране на подобренията за три от изискванията е определена необходимостта от използването на различни автоматизирани проверки. Тъй като функционалността позволява, този вид подобрения следва да бъдат обединени в настоящия модул, като той следва да включва следните проверки:

- проверка за използване 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 устройство;
- проверка за включена функция на мобилната операционната 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;
- 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;
- 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 приложение за мобилно банкиране.

Представеният по-горе списък поражда някои съображения по отношение проектирането на настоящия модул. Реализирането на толкова широк набор от проверки може да предизвика неудобство за потребителя, а това да доведе до отказ от използването на съответната услуга. От друга страна различните доставчици на тази услуга представят различни препоръчителни действия, които изискват от своите потребители. Затова при проектирането на модула е необходимо на банките, предоставящи мобилно банкиране да се даде възможност да определят кои проверки следва да бъдат задължителни, кои препоръчителни, както и възможност на един по-късен етап да се реализират промени като добавяне, премахване или модифициране на съответната проверка.

Въз основа на горните съображения, можем да дефинираме, че **настоящия модул за реализиране на автоматизирани проверки следва да бъде разработен като инструмент, който осъществява определен набор от автоматизирани проверки, дефинирани от доставчиците на услуги за мобилно банкиране, в резултат на което помага на потребителите да предприемат определени действия, които да доведат до повишаване на нивото на сигурността при мобилното банкиране.**

От архитектурна гледна точка модулет за реализиране на автоматизирани проверки следва да бъде разделен на две основни части. Едната следва да бъде реализирана като компонент на мобилното приложение 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 ще бъдат дефинирани проверките, които следва да бъдат реализирани.

За да осъществим неговата основна функционалност е необходимо да определим основните процеси, които трябва да реализира модулет. Те са:

- съставяне на списък от автоматизирани проверки;
- съхраняване на дефинирания списък в база от данни;
- реализиране на дефинираните автоматизирани проверки;
- представяне на резултатите на потребителя.

Процесът по съставяне на списъка от автоматизирани проверки се извършва от експертите по сигурността на доставчика на услуги за мобилно банкиране. Този процес включва редица дейности и започва с анализ на сигурността, въз основа на който могат да бъдат определени съответните автоматизирани проверки, които следва да реализира модула. Следващата стъпка е свързана с реализирането на оценка на риска и по-специално дефиниране на силата на последиците ако някоя от

определените проверки не бъде реализирана. По този начин се определя кои от тях са ключови и следва да бъдат задължителни и кои ще бъдат само препоръчителни.

След съставянето на списъка с автоматизирани проверки, те следва да бъдат въведени в база от данни, като основната цел тук е да се осигури тяхното повторно използване и ефективно управление. При реализирането на това за всяка проверка е необходимо да бъде съхранена информация за нейното име, нейния вид (задължителна или препоръчителна), инструкциите за действие, както и силата на последиците, ако тя не премине успешно. За всяка от нововъведените проверки е необходимо да се изпрати заявка до разработчиците на мобилното приложение, тъй като те трябва да интегрират нужната функционалност.

Процесът по реализиране на дефинираните автоматизирани проверки следва да се осъществи, когато потребителят стартира мобилното приложение за мобилно банкиране. При това ще се осъществи връзка с базата от данни, която се намира на сървър, от където се установява броят и видът на проверките, които следва да бъдат реализирани. Първоначално се започва със задължителните проверки. Само ако те преминат успешно, се преминава към реализирането на препоръчителните проверки. За осъществяването на проверките е необходимо да се използва помощта на приложно програмния интерфейс (API) на съответната мобилна операционна система. Резултатите от всички проверки следва да бъдат предадени към следващия процес, който следва да ги представи на потребителя.

Ако резултатът от всяка от задължителните проверки е положителен потребителят следва да получи достъп до услугите за мобилно банкиране. В противен случай той ще получи инструкции какво трябва да направи, за да използва функционалностите на мобилното приложение. По отношение

на препоръчителните проверки, както говори името им, отрицателният им резултат не следва да задължава по никакъв начин потребителя да реализира определени действия. От друга страна тяхното състояние следва да участва във формирането на стойност на индикатор на сигурността на мобилното устройство по отношение на мобилното банкиране. Ако потребителят желае да повиши неговата стойност, е необходимо той да изпълни определени инструкции свързани с неуспешно преминалите препоръчителни проверки.

Въз основа на разгледаните процеси предлагаме следната архитектура на модула за реализиране на автоматизирани проверки (вж. фиг. 11).



Фиг. 11. Архитектура на модула за реализиране на автоматизирани проверки

Както се вижда от представената на фиг. 11 архитектура, за реализиране на модула за реализиране на автоматизирани проверки е необходимо изграждането на три софтуерни компонента: компонент за администриране на автоматизираните проверки, компонент за реализиране на проверките, компонент за визуализиране на инструкции за действие и индикатор за сигурност.

## **7. Заключение**

В настоящата глава предложихме концептуален модел за повишаване на сигурността при мобилното банкиране. Неговата 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 нови или подобрени механизми за сигурност. В този смисъл предложеният концептуален модел реализира втората задача и е един от основните приноси на настоящия дисертационен труд.

Реализирането на концептуалния модел преминава през няколко основни етапа. Първият етап е свързан с анализ на сигурността при четирите основни проблемни области при потребителя по отношение на сигурността при мобилното банкиране – мобилно устройство, мобилна операционна система, мобилен уеб браузър и мобилно приложение за мобилно банкиране. При всяка една от тях реализирахме дефиниране на атаките и използваните от тях уязвимости, определяне на най-често използваните стратегии за защита и добри практики за противодействие на дефинираните атаки, изследване на ефективността на използваните стратегии за защита и добри практики.

В първа глава на настоящата разработка реализирахме описания първи етап като се позовахме на изследваната литература и резултатите

постигнати от други автори. Направените там изводи, свързани със неефективността на някои от съществуващите практики и стратегии за защита, обуславят формулирането на предложения за подобрения, които да доведат до повишаване на нивото на сигурността.

Вторият етап от изграждането на концептуалния модел се свързва с проектирането на формулираните подобрения, където е и акцентът на настоящата глава. Този етап започва със съставянето на функционална структура на подобренията, които участват в концептуалния модел за повишаване на сигурността при мобилното банкиране. В резултат на това дефинирахме пет основни модула:

- Модул за биометрично удостоверяване, което се базира на поведението на потребителя - Представлява инструмент за идентифициране на потребителя на мобилното банкиране на база на поведенчески характеристики, които се генерират в резултат на неговото взаимодействие със сензорния екран на мобилното устройство.
- Модул за автоматизирана защита от tabnabbing атака - 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.
- Модул за автоматизирана защита от CSRF атака - Представлява инструмент, който защитава нарушаването на цялостността на сесията за удостоверяване, при изпращането на cross-site заявки, като в мобилния уеб браузър на потребителя 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.

- Модул за удостоверяване, който се базира на PICO token и гласово разпознаване - Представлява 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.
- Модул за реализиране на автоматизирани проверки - Представлява инструмент, който осъществява определен набор от автоматизирани проверки, дефинирани от доставчиците на услуги за мобилно банкиране, в резултат на което помага на потребителите да предприемат определени действия, които да доведат до повишаване на нивото на сигурността при мобилното банкиране.

С цел да се добие по-пълна представа относно общата архитектура и функционалните възможности на представените модули, всеки от тях е допълнително разгледан като са представени съображенията за неговото проектиране, основните процеси, които следва да бъдат обхванати, както и входните и изходните параметри.

Въпреки представеното детайлно проектиране на формулираните подобрения остава въпросът доколко те са ефективни и приложими в практиката. Именно това е и фокусът на следващата, трета глава от дисертационния труд.

## **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. 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 при всеки следваме обща методика на работа, включваща следните етапи:

- Обхват на експеримента – на този етап следва да поставим основите на експерименталното изследване, като определим неговите цел и задачи;
- Планиране на експеримента – на този етап следва да определим избора на експерименталната среда (индустриална, лабораторна, академична, контролирана среда), подбора на участниците (експерти, студенти, стажанти) и избора на инструменти и материали (необходим хардуер и софтуер);
- Провеждане на експеримента – на този етап следва да опишем стъпките при провеждане на експеримента.
- Представяне и анализ на резултатите – на този етап следва да представим получените резултати във вид на таблици, фигури, които да интерпретираме по отношение на целта и задачите на експеримента.



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

Целта на настоящия експеримент е да се изследва ефективността и да се определи най-подходящия алгоритъм за машинно обучение, който може да бъде използван в модула за биометрично удостоверяване, което се базира на поведението на потребителите.

За осъществяването на целта е необходимо да бъдат реализирани следните задачи:

- събиране на входни данни от сензорния екран на мобилното устройство;
- извличане на отличителни белези от събраните входни данни;
- използване на извлечените отличителни белези за тестване на различни алгоритми за машинно обучение (класификация).

Подготвихме провеждането на експеримента да се реализира в контролирана среда, т.е. под контрол на експерти, които следят за правилното му изпълнение и при необходимост дават насоки на участниците.

За реализиране на експеримента избрахме 30 участника (17 мъже и 13 жени) на възраст от 18 до 50 години. Избрахме тази възрастова група, тъй като това е частта от населението, която най-активно работи с мобилни устройства със сензорен екран. От участниците 1 е с основно образование, 8 са със средно, а 21 с висше. Всички от тях имат собствено мобилно устройство със сензорен екран, както и необходимите познания за базова работа с него.

При подбора на участниците за експеримента използвахме стохастичния (или случаен) метод на подбор. При него всички единици на генералната съвкупност имат равен шанс да попаднат в извадката на

изследването. По този начин структурата на извадката възпроизвежда с определена точност структурата на цялата генерална съвкупност. Така се осигурява представителност (репрезентативност) на информацията, която е получена за извадката.

За реализиране на първата задача на експеримента (събиране на входни данни от сензорния екран на мобилното устройство) предварително разработихме мобилно приложение, което инсталирахме на смартфон LG Nexus 5, работещ с най-широко разпространената мобилна операционна система Android и нейната най-използвана версия KitKat 4.4.

За реализиране на мобилното приложение използвахме средата за разработка Visual Studio Community 2015 с допълнително инсталирано разширение, даващо възможност за работа със средата за разработка Xamarin. Последната позволява разработването на native мобилни приложения с помощта на програмния език C#, който е използван и тук. За първоначално тестване на приложението използвахме симулатора Xamarin Android Player.

Разработихме мобилното приложение така, че през него потребителят да получи достъп до интернет. За целта използвахме WebView елемент на интерфейса, който позволява разглеждането на уеб сайтове в самото приложение. Така докато потребителят сърфира в интернет следва да бъдат събирани следните входни данни:

- вид движение при докосване – натискане, отпускане, придвижване, превъртане;
- координати на точката на докосване – определят мястото на докосване на сензорния екран;
- размер на точката на докосване;
- сила на натиск при докосване;

- време на реализиране на докосване – на база на това може да бъде изчислена продължителността на докосване.

За осъществяване на събирането на посочените данни използвахме интерфейса `Android.Views.View.OnTouchListener`, който позволява при реализиране на докосване от потребителя върху сензорния екран да бъде направено обръщение към метода `OnTouch(View, MotionEvent) : Boolean`. Благодарение на използвания в него обект от класа `Android.Views.MotionEvent` се получава достъп до посочените по-горе данни, генерирани от докосването.

Последното, което следва да реализира мобилното приложение, е съхранението на събраните входни данни. За целта използвахме възможността на Android устройствата да водят отчет на изпълняваните операции и да ги записват в т.н. log файл. Записването и прочитането на данните от този файл осъществихме с помощта на класа `Android.Util.Log`, който предоставя необходимите функционалности.

За осъществяването на третата задача на настоящия експеримент (тестване на различни алгоритми за машинно обучение) решихме да използваме софтуерния продукт KNIME. Алгоритмите за машинно обучение, които избрахме да бъдат тествани са следните:

- Back-Propagation Neural Networks;
- C4.5;
- Naive Bayes;
- Particle Swarm Optimization Radial Basis Function Network
- Radial Basis Function Network;
- Repeated Incremental Pruning to Produce Error Reduction (RIPPER).

След планирането на експеримента можем да пристъпим към описание на неговото провеждане.

На всеки от участниците последователно предоставихме мобилното устройство LG Nexus 5. След това направихме предварителен инструктаж за действията, които всеки от тях следва да реализира. Първоначално потребителят стартира мобилното приложение, което ще се използва за събирането на входните данни представени по-горе. След това въвежда уникален код, който се състои от най-малко 4 символа и трябва да представлява комбинация от букви и цифри. След натискането на бутон за започване в WebView елемента на интерфейса се зарежда търсачката google.com. След това на потребителя се предоставя възможност да сърфира в интернет и да реализира стандартни действия, все едно работи на своя смартфон. Например могат да се използват докосвания с един или с няколко пръста, да се работи в портретен или в пейзажен изглед. Междувременно докато потребителят взаимодейства с разработеното мобилно приложение, то събира входните данни и ги записва в log файла на устройството. След период от 5 минути потребителят бива информиран, че необходимите данни са събрани и че приложението ще се затвори.

След като всички потребители преминават през описаните по-горе стъпки реализирахме втората задача на експеримента (извличане на отличителните белези). На база на данните от log файла ръчно изготвихме два файла във формат .arff, които са подходящи за софтуерния продукт KNIME. В тях включихме следните отличителни белези:

- брой движения при докосване за определено време;
- брой докосвания с няколко пръста за определено време;
- брой докосвания с един пръст за определено време;
- средна продължителност на движение при докосване за определено време;
- средна продължителност на докосване с няколко пръста за определено време;

- средна продължителност на докосване с един пръст за определено време;
- среден размер на докосваната област от един пръст;
- приблизително най-често докосвана област от сензорния екран;
- стандартно отклонение от приблизително най-често докосвана област – използва се за по-точно дефиниране на предходната характеристика;
- средна скорост на движение при докосване;
- средна сила на натиск при докосване.

Първият .arff файл представлява тренировъчен набор, който се използва от софтуерния продукт KNIME за реализиране на предварително обучение, което въз основа на отличителните белези ясно 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.

След провеждане на необходимите тестове получихме резултатите представени в таблица 4. Те 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 4 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. Нещо повече, считаме, че след комбиниране с

предвидения в модула шаблон за заключване, процентът на грешното удостоверяване ще бъде сведен до минимум.

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 4. Резултати от тестване на алгоритмите за машинно обучение

## 2. Модул за автоматизирана защита от tabnabbing атака

Начинът, по който проектирахме модула за автоматизирана защита от tabnabbing атака го отличава с три основни характеристики, които стоят в основата на неговата ефективност по отношение на сигурността. Те са следните: безпогрешно засичане на tabnabbing атака, удобно и ясно представяне на резултатите за потребителя и наличието на индикатор за сигурност, вграден в мобилния уеб браузър.

Безпогрешното засичане на tabnabbing атаки се свързва с начина на тяхното откриване от страна на модула. Както вече определихме във втора глава това следва да се реализира чрез прихващането на визуална снимка на даден раздел при възникване на събитията загуба и възстановяване на фокуса на съответния раздел. За да остане tabnabbing атаката незасечена е необходимо при визуалното сравнение на тези две снимки да се окаже, че те са напълно идентични. Това може да се случи само ако уеб сайтът не се е

променил докато е бил извън фокус или в случай, че е реализирана класическа phishing атака. Тъй като засичането на този вид атака не е цел на настоящия модул ние можем само да очертаем включването на подобна функционалност към него като насока за бъдеща работа.

Втората характеристика, която е също свързана с ефективността на модула, е удобното и ясно представяне на резултатите за потребителя. С помощта на допълнителен слой, който се добавя върху раздела, който е на фокус, на потребителя следва да се покаже кои части от уеб сайта са променени след като той е бил последно на фокус. В допълнение проектирахме модулет така, че да засича дали злонамереният уеб сайт активно се опитва да премахне слоя, който информира потребителя, и ако е така да предупреди потребителя чрез подходящо съобщение.

По отношение на третата характеристика, модулет следва да добави икона на индикатора за сигурност в лентата с инструменти на мобилния уеб браузър. Използването на подобен начин за известяване, позволява на потребителя да се предостави информация за настъпилите промени по съответния раздел. Положителната черта на този индикатор е, че той работи в рамките на добавката и няма връзка с кода, използван за визуализиране на съответния уеб сайт. Това ефективно предотвратява реализирането на манипулации от страна на злонамерен уеб сайт.

За да е още по-ефективна защитата от tabnabbing атака е необходимо модулет да е способен да предупреди потребителя за каквито и да е промени преди той да успее да въведе чувствителна информация. Нещо повече, тъй като алгоритъмът се реализира когато потребителят превключи между разделите е от съществено значение да няма някакво забележимо влияние върху производителността.

От тук можем да дефинираме целта на настоящия експеримент, а именно да се 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 е необходимо да бъдат осъществени следните задачи:

- да се определи производителността, свързана с прихващането на снимка на даден раздел;
- да се определи производителността, свързана с разделяне на снимките на части;
- да се определи производителността при реализиране на сравнение на двете снимки;
- да се определи производителността при визуализиране на промените и индикатора за сигурност.

За реализиране на първата и четвъртата задача на експеримента предварително проучихме възможностите на мобилните уеб браузъри за поддръжка на добавки. Оказва се, че от най-широко използваните от тях на този етап единствено Firefox Mobile позволява инсталирането на добавки. За разработването на добавки за този мобилен уеб браузър е необходимо да се използва следният комплект за разработка на софтуер - Add-on SDK. Той включва широк набор от приложно програмни интерфейси (APIs), които са написани на програмния език JavaScript и се използват за разработване на добавки за всички версии на браузъра Firefox. За съжаление в официалната документация на Add-on SDK е посочено, че към настоящия момент не всички модули са напълно функционални за Firefox Mobile. Това обуславя някои от ограниченията, които възникнаха и следва да опишем при реализирането на настоящия експеримент.



За провеждане на задачите на експеримента използвахме таблет Vonino Sirius QS (CPU: quad-core, 1.3 GHz, RAM: 1 GB DDR3), работещ с най-широко разпространената мобилна операционна система Android и нейната най-използвана версия KitKat 4.4. Допълнително инсталирахме и последната версия на Firefox Mobile (46.0.1). При реализирането на третата задача използвахме и смартфон LG Nexus 5 (CPU: quad-core, 2.3 GHz, RAM: 2 GB DDR3), който има същите настройки като таблета.

За реализиране на първата задача на експеримента (да се определи производителността, свързана с прихващането на снимка на даден раздел) трябваше да създадем добавка, която осъществява прихващане на снимка на активния раздел в два момента – при загуба и при възстановяване на фокус върху него. Прихващането на загубата и възстановяването на фокуса беше успешно постигнато като използвахме свойството `deck` на обект от класа `BrowserApp` на приложно програмния интерфейс. Проблем възникна при прихващането на снимката, тъй като в настоящия момент Add-on SDK не поддържа тази функционалност (достъп до `window` елемента) за мобилни уеб браузъри. Като решение на проблема избрахме и инсталирахме 6 добавки за последната версия на стандартен уеб браузър Firefox, които реализират посочената функционалност. Целта на това наше решение е въпреки наложените ограничения да получим ориентиrowъчен резултат за времето, което е необходимо да се прихване снимка на даден раздел. Тъй като Add-on SDK търпи непрекъснато развитие в бъдеще се очаква посочената функционалност да се поддържа.

За реализиране на втората задача на експеримента (да се определи производителността, свързана с разделяне на снимките на части) разработихме JavaScript функция, която получава като входен параметър предварително изготвена снимка под формата на `canvas` елемент, разделя

я на части и ги съхранява в масив. За настоящата и следващата задача не използвахме Add-on SDK, тъй като съответните функционалности могат да бъдат реализирани чрез стандартен JavaScript код и по този начин не се ограничаваме от поддръжката, която осигурява комплектът за разработване на добавки за уеб браузър.

За реализиране на третата задача на експеримента (да се определи производителността при реализиране на сравнение на двете снимки) разработихме JavaScript функция, която получава като входни параметри две снимки под формата на `canvas` елементи. Тук използвахме метода `getImageData()`, който връща обект от `ImageData`, в който се съхранява информацията (под формата на масив) за всеки пиксел на снимката. Така на един по-късен етап функцията реализира сравнение между всеки пиксел от едната снимка с всеки от другата.

За реализиране на четвъртата задача на експеримента (да се определи производителността при визуализиране на промените и индикатора за сигурност) трябваше да създадем добавка, която симулира оцветяване на части (настъпилите промени) от уеб сайта и която визуализира индикатора за сигурност. Тъй като на този етап Add-on SDK не поддържа нито промяна на съдържанието на визуализираните страници, нито създаването на икона за индикатора за сигурност, единственото, което реализира създадената от нас добавка е да визуализира съобщение, представящо процента на реализираните промени. За целта използвахме обект от класа `Snackbars` на приложно програмния интерфейс.

След планирането на експеримента можем да пристъпим към описание на неговото провеждане и представяне на получените резултати.

При реализиране на първата задача измерихме времето, което е необходимо на всяка от 6-те добавки, за да се реализира прихващане на снимка на един и същ уеб сайт. Резултатите са представени в таблица 5.

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

Таблица 5. Време в милисекунди (мс) за прихващане на снимка

Въз основа на резултатите от таблица 5 изчислихме, че средното време за изпълнение на тази операция е 113 мс. Това време се използва от приложно програмния интерфейс на брауъра.

При реализиране на втората задача измерихме времето, за което създадената JavaScript функция извършва разделянето на снимката на части. За целта като входен параметър 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), размер на една част (10x10 пиксела и 15x15 пиксела). Резултатите, които получихме, са представени в таблица 6.

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

Въз основа на резултатите от таблица 6 изчислихме, че средното време за изпълнение на функцията по разделяне на снимката на части е 50 мс. Освен това установихме, че времето за реализирането на тази операция зависи от една страна от разделителната способност, а от друга от размерите на една част. То не е зависимо нито от съдържанието на снимката, нито от хардуерните характеристики на устройството.

При реализиране на третата задача измерихме времето, за което създадената JavaScript функция извършва сравнение между две зададени снимки. За целта като 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%). Получените от нас резултати са представени в таблица 7.

Процент на промените спрямо оригиналната снимка	Време, необходимо на алгоритъма за сравнение
0 %	119 мс
25 %	90 мс
50 %	58 мс
75 %	29 мс
100 %	5 мс

Таблица 7. Зависимост между количеството на промените на оригиналната снимка и времето необходимо на алгоритъма за сравнение.

Въз основа на резултатите в таблица 7 установяваме, 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.

При реализирането на четвъртата задача измерихме времето, за което създадената добавка визуализира съобщение, представящо процента на реализираните промени. Резултатите показват, че това се реализира за 1 мс. Поради наложените ограничения на Add-on SDK не успяхме да измерим времето за оцветяване на настъпилите промени по уеб сайта. Това може да бъде очертано като насока за бъдеща работа.

Въз основа на резултатите получени при реализиране на четирите задачи 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. Като насока за бъдеща работа можем да посочим, че съответните измервания следва да бъдат повторени при отстраняване на ограниченията, свързани с неговото цялостно реализиране.

### **3. Модул за автоматизирана защита от CSRF атака**

Целта на настоящия експеримент е да се изследва ефективността на предложения от нас в точка 4 на втора глава алгоритъм за филтриране при осъществяване на автоматизирана защита от CSRF атака.

За реализирането на целта е необходимо да бъдат реализирани следните задачи:

- формално описание на алгоритъма за филтриране с помощта на езика за моделиране Alloy;
- формално описание на CSRF атака с помощта на езика за моделиране Alloy;
- на база на формалните описания да се реализира проверка дали алгоритъмът за филтриране ефективно предпазва от CSRF атака.

Като основа за реализиране на първата задача на експеримента (формално описание на алгоритъма за филтриране с помощта на езика за моделиране Alloy) ще използваме разработения от Akhawe [142] модел на уеб инфраструктурата. За неговото формално описание също е използван езикът за моделиране Alloy. С негова помощ са представени както основните характеристики на уеб браузърите, уеб сървърите, управлението на сесиите и HTTP протокола, така и колекция от модели на атаки за уеб. Именно затова този модел е подходящ при реализиране на по-точна оценка на ефективността на нови предложения за подобряване на сигурността при различните уеб механизми.

За да реализираме успешно формалното описание както на алгоритъма за филтриране, така и на CSRF атаката (втората задача на експеримента), беше необходимо да се запознаем обстойно с модела на Akhawe. Поради немалкия му обем няма да го представяме в настоящата разработка, а по-скоро ще обърнем внимание само някои негови особености, които са тясно свързани с провеждането на настоящия експеримент. При необходимост допълнителна информация може да бъде намерена в следния източник Akhawe [142].

За осъществяването на третата последна задача (на база на формалните описания да се реализира проверка дали алгоритъмът за

филтриране ефективно предпазва от CSRF атака) използвахме последната стабилна версия 4.2 на 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.

След планирането на експеримента можем да пристъпим към описание на неговото провеждане.

За да изготвим формално описание на алгоритъма за филтриране се оказва необходимо да разширим модела на Akhawe като включим в него информация за достъп до състоянието на сесията и за начина, по който се реализира упълномощаване между два източника.

На фиг. 12 е представена дефиницията на новата сигнатура `SystoyanieSesiya`, която предоставя възможност за достъп до състоянието на сесията.

```
sig SystoyanieSesiya {  
  iztochnik: Origin,  
  cookies: set Cookie  
}
```

Фиг. 12. Дефиниция на сигнатура за достъп до състоянието на сесията

На фиг. 12 се вижда, че в сигнатурата дефинираме две полета. Полето `iztochnik` е от тип `Origin`. Тип `Origin` е дефиниран в модела на Akhawe и се използва за различаване на различни източници (уеб сървъри), които отговарят на домейни от реалния свят. Полето `cookies` е множество от тип `Cookie`, което съдържа информация, която се изпраща от източника към мобилния уеб браузър.

За определяне състоянието на сесията в следствие на заявка или отговор се налага да създадем нова сигнатура `SesiyaHTTPTransaction` (вж. фиг. 13), която разширява оригиналната сигнатура

HTTPTransaction като добавя две нови полета – z\_systoyanie (състоянието на сесията в момента на изпращане на заявката) и o\_systoyanie (състоянието в момента на получаване на отговор).

```
sig SesiyaHTTPTransaction extends HTTPTransaction {
  z_systoyanie : SystoyanieSesiya,
  o_systoyanie : SystoyanieSesiya
} {
  z_systoyanie.iztochnik = o_systoyanie.iztochnik
  o_systoyanie.cookies = z_systoyanie.cookies + (resp.headers & SetCookieHeader).thecookie
  z_systoyanie.iztochnik = req.host
}
```

Фиг. 13. Дефиниция на сигнатура SesiyaHTTPTransaction.

От дефиницията се вижда, че състоянието на сесията трябва да е едно и също както преди реализиране на заявката, така и след получаване на отговора. Може да бъде добавена нова информация единствено под формата на поле (thecookie) от тип Cookie, която се генерира (SetCookieHeader) при реализиране на отговор (resp) от страна на сървъра.

Следващата стъпка, която реализирахме, беше да определим какви са ограниченията за реализиране на упълномощаване между два източника (вж. фиг. 14).

```
fact Upylnomoshtavane {
  all z : HTTPRequest | {
    (some (req.z).cause & SesiyaHTTPTransaction || z.method = POST)
    &&
    (getPrincipalFromOrigin[transactions.(req.z).owner] in GOOD ||
     getPrincipalFromOrigin[(req.z).cause.req.host] in GOOD &&
     (some (req.z).cause & SesiyaHTTPTransaction))
    implies
    getPrincipalFromOrigin[z.host] not in WEBATTACKER
  }
}
```

Фиг. 14. Ограничения при упълномощаване между два източника.



Участниците GOOD и WEBATTACKER са дефинирани в модела на Akhawe. Първият представлява участник, който следва наложените правила. Вторият е злонамерен потребител, който може да контролира злонамерени уеб сървъри, но няма други разширени мрежови възможности.

След като дефинирахме необходимите допълнения към модела на Akhawe преминахме към изготвянето на формалното описание на алгоритъма за филтриране. То реално представлява символна реализация на представения в точка 4 на втора глава алгоритъм.

Първото, което трябва да проверим, е дали източникът изисква от мобилния уеб браузър да реализира пренасочване. За целта използвахме функцията `sameOrigin[o1:Origin, o2:Origin2]` от модела на Akhawe. Като аргументи на функцията се подават източникът, към който е отправена заявката (`trans.req.host`) и източникът, от който е получен отговор (`((transactions.trans).owner)`). Полето `trans` е от дефинирания от нас тип `SesiyaTransaction`, което по-късно ще ни позволи да следим какво е състоянието на сесията преди изпращане на заявката и след получаване на отговор. Другите полета са дефинирани в модела на Akhawe.

Следващата стъпка при реализиране на алгоритъма е да проверим дали заявката е стандартна или `cross-site`. Тук отново използвахме `sameOrigin` функцията, като разликата е в аргументите, които и се предават. Първият отново е източникът, към който е отправена заявката (`trans.req.host`), а вторият е полето `trans.z_systoyanie.iztochnik`, което е дефинирано в сигнатурата `SesiyaTransaction`. По този начин проверяваме дали няма различие между наличния източник в сесията и този, към който е отправена новата заявка.

Последната проверка, която трябва да реализира алгоритъмът за филтриране е да установи дали cross-site заявката е злонамерена или незлонамерена. Тази проверка се базира на по-рано представените ограничения, свързани с успешното упълномощаване между два източника, тъй като то ще гарантира за вида на cross-site заявката.

Следва да представим и трите резултата, които се получават в следствие на реализираните проверки:

- мобилният уеб браузър автоматично прикрепя към заявката (trans.z\_systoyanie.cookies) първоначално генерираното състояние на сесията (ss: SystoyanieSesiya, ss.cookies);
- мобилният уеб браузър прикрепя към заявката (trans.z\_systoyanie.cookies) състоянието на сесията, идващо от заявката, която е генерирала пренасочването (resp.headers.thecookie);
- мобилният уеб браузър не прикрепя никаква информация за сесията към заявката (ss: SystoyanieSesiya, no ss.cookies).

За реализиране на втора задача изготвихме следното формално описание на CSRF атаката (вж. фиг. 15).

```

pred CSRF_ataka[z : HTTPRequest] {
  some getPrincipalFromOrigin[z.host]
  getPrincipalFromOrigin[z.host] in GOOD

  some (WEBATTACKER.servers & involvedServers[req.z]) ||
    (some getPrincipalFromOrigin[(transactions.(req.z)).owner]
    && getPrincipalFromOrigin[(transactions.(req.z)).owner] in WEBATTACKER)

  some brow : (z.headers & CookieHeader).thecookie | {
    not brow in ((req.z).*cause.resp.headers & SetCookieHeader).thecookie
  }
}

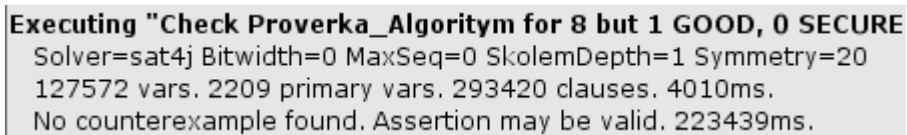
```

Фиг. 15. Формално описание на CSRF атака.

Атаката дефинира възможността на злонамерен потребител (WEBATTACKER) да генерира злонамерена заявка ( $z : \text{HTTPRequest}$ ), към която да прикрепи информация за сесията ( $\text{thecookie}$ ), която е създадена между мобилният уеб браузър на даден потребител ( $\text{brow}$ ) и незлонамерен сървър ( $z.\text{host}$ ).

Последната задача от експеримента реализирахме чрез създаването на функция за проверка на ефективността на алгоритъма за филтриране (`check Proverka_Algorithm`). В нея с помощта на функцията `CorrectWebModel` от модела на Akhawe симулирахме изпълнението на всички включени в неговия модел HTTP събития, с което се проверява дали някое от тях води до резултат, дефиниран в `pred CSRF_ataka`.

С помощта на инструмента Alloy Analyzer е изпълнена функцията `check Proverka_Algorithm`, в следствие на което получихме резултата представен на фиг. 16.



```
Executing "Check Proverka_Algorithm for 8 but 1 GOOD, 0 SECURE
Solver=sat4j Bitwidth=0 MaxSeq=0 SkolemDepth=1 Symmetry=20
127572 vars. 2209 primary vars. 293420 clauses. 4010ms.
No counterexample found. Assertion may be valid. 223439ms.
```

Фиг. 16. Резултат от изпълнението на функцията `check Proverka_Algorithm`.

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

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

Целта на настоящия експеримент е да се направи оценка на модула за удостоверяване, който се базира на PICO token и гласово разпознаване.

За осъществяването на целта е необходимо да бъдат реализирани следните задачи:

- дефиниране на подход за реализиране на оценяването;
- оценяване на модула за удостоверяване и сравняване с резултатите на алтернативни механизми – ПИН, парола, биометрики и token устройства.

За реализиране на първата задача на експеримента проучихме научната литература и открихме, че подобен подход за оценка на уеб базирани механизми за удостоверяване е разработен от Bonneau [143]. Той се нарича UDS и се състои от 25 свойства, които са разделени в 3 основни категории: ползваемост (usability), разпространяемост (deployability) и сигурност (security). 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.

За изчисляване на общата оценка при използване на UDS подхода е определено, че всяко от свойствата от различните категории има различна тежест в зависимост от целта на оценяването. Например ако се търси най-сигурният механизъм за удостоверяване (какъвто е и нашият случай), свойствата свързани със сигурността следва да имат по-голяма тежест в общата оценка.

Bonneau споменава възможност за комбинирането на механизми като част от двуфакторно удостоверяване. По отношение на свойствата от категориите ползваемост и разпространяемост двуфакторното

удостоверяване предлага дадено свойство тогава и само тогава, когато то присъства и в двата механизма за удостоверяване. По отношение на свойствата от категория сигурност двуфакторното удостоверяване предлага дадено свойство тогава и само тогава, когато то присъства поне при един от двата механизма за удостоверяване.

Тъй като подходът на Vonneau не е 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. Тези от тях, които са неприложими по отношение на token устройствата или приложими за всички сравнявани механизми са премахнати. В резултат на това подмножеството на UDS подхода, което ще участва в нашия подход за оценяване следва да включва следните свойства:

✓ Категория „ползваемост“

- Липса на необходимост от запомняне – свойството е удовлетворено ако потребителите не трябва да помнят никаква тайна. Оценка „почти“ се дава в случаите когато една тайна ще се използва за различни видове удостоверяване.
- Липса на необходимост от физическо притежание – свойството е удовлетворено ако не се изисква носенето на допълнителни физически предмети (хардуер). Оценка „почти“ се дава в случай, че физическият предмет е по всяко време в потребителя.
- Ефикасност при употреба – свойството е удовлетворено ако времето, което потребителят трябва да изчака, за да бъде реализирано удостоверяване, е приемливо кратко.
- Безгрешно удостоверяване – свойството е удовлетворено, когато правилният потребител успешно се идентифицира пред механизма

за удостоверяване, без наличието на чести грешки. Всяко забавяне (правописни грешки, грешно биометрично удостоверяване) определя механизма като неудовлетворяващ свойството.

- Лесно възстановяване при загуба – свойството е удовлетворено ако потребителят може лесно да възстанови възможността за удостоверяване в следствие на загуба например на допълнителни хардуерни устройства, забравени данни за удостоверяване или различие в биометричните характеристики.

✓ Категория „разпространяемост“

- Незначителна цена за потребител – свойството е удовлетворено, когато механизмът за удостоверяване предлага незначителна цена за неговото използване както от страна на потребителя, така и на този, пред който се реализира удостоверяването.
- Добро развитие – свойството е удовлетворено, когато голям брой потребители са използвали успешно механизма за удостоверяване.

✓ Категория „сигурност“

- Устойчивост срещу физическо наблюдение – свойството е удовлетворено, ако злонамерен потребител не може да получи достъп до данните за удостоверяване в следствие на наблюдаване на начина, по който легитимните потребители се удостоверяват.
- Устойчивост срещу измама - свойството е удовлетворено, когато злонамерен потребител не може да получи достъп до данните за удостоверяване в следствие на изучаване на лични данни за легитимния потребител като дата на раждане, имена, детайли за семейството или друга чувствителна информация.
- Устойчивост срещу налучкване – свойството е удовлетворено, ако механизмът за удостоверяване ограничава възможността за налучкване на данните за удостоверяване.

- Устойчивост срещу phishing атака – свойството е удовлетворено, ако злонамерен потребител не може да използва тази атака, за да получи достъп до чувствителна информация, която по-късно да се използва за компрометиране на сигурността.
- Устойчивост срещу кражба – свойството се отнася за удостоверяване, при което се използва допълнителен хардуер. То е удовлетворено ако не е достатъчно кражбата на допълнителния хардуер да компрометира механизма за удостоверяване.
- Невъзможност за асоцииране – свойството е удовлетворено ако не може да се направи пряка връзка между механизма за удостоверяване и идентичността на потребителя.

Към представеното подмножество добавихме две допълнителни свойства, които са тясно свързани с token базираните механизми за удостоверяване. Това е и нашият принос към дефинирания от нас подход за оценка. Свойствата са класифицирани към категорията „сигурност“ и са следните:

- Продължително удостоверяване – свойството е удовлетворено, когато механизмът за удостоверяване предлага периодична проверка за самоличността на потребителя. Този процес не е задължително да бъде скрит от потребителя, но не трябва да представлява неудобство за него.
- Различни нива на позволения – свойството е удовлетворено ако механизмът за удостоверяване предлага достъп до различни функционалности в зависимост от степента на доверие, която определя, че потребителят е този, за който се представя.

След дефинирането на подхода, който ще използваме за реализиране на оценяването пристъпихме към самото оценяване на модула за удостоверяване, който се базира на PICO token и гласово разпознаване. За

всяко от свойствата, налични в подхода, следва да обосновем поставените от нас оценки.

Свойството „липса на необходимост от запомняне“ определяме като удовлетворено, тъй като нито при PICO token, нито при гласовото разпознаване от потребителя се изисква да помни някаква тайна за удостоверяване.

На свойството „липса на необходимост от физическо притежание“ даваме оценка „почти“. Въпреки че PICO token ще е реализиран софтуерно, все пак потребителите трябва да носят малки допълнителни устройства, които ще бъдат прикрепени към ежедневни предмети, които те така или иначе носят със себе си.

На свойството „ефикасност при употреба“ даваме оценка „почти“, поради факта, че при реализирането на гласово разпознаване на отдалечен сървър може да има известно забавяне за потребителя.

На свойството „безгрешно удостоверяване“ даваме оценка „почти“, поради факта, че при използването на биометрични характеристики, какъвто е случаят с гласовото разпознаване, в зависимост от използвания алгоритъм може да има вариация в процента на грешно удостоверяване.

На свойството „лесно възстановяване при загуба“ даваме оценка „почти“, поради факта, че при загуба на някое от малките допълнителни устройства, възстановяването става сравнително бързо, но потребителят трябва да се свърже с доставчика на услуги за мобилно банкиране, който му ги е предоставил.

На свойството „незначителна цена за потребител“ даваме оценка „почти“, поради факта, че доставчикът на услуги за мобилно банкиране следва да има определени разходи по отношение на малките допълнителни устройства.



Свойството „добро развитие“ определяме като неудовлетворено, тъй като предложеният от нас механизъм за удостоверяване е представен на идейно ниво и не е тестван от потребителите.

Свойството „устойчивост срещу физическо наблюдение“ определяме като удовлетворено, тъй като дори злонамерен потребител да наблюдава начина, по който легитимните потребители се удостоверяват, той няма как да получи достъп до данните за удостоверяване.

Свойството „устойчивост срещу измама“ определяме като удовлетворено, тъй като при гласовото разпознаване се използва динамично генерирана фраза, която предотвратява възможността за реализиране на replay атаки, които се базират на предварително изготвени записи.

Свойството „устойчивост срещу налучкване“ определяме като удовлетворено, тъй като при гласовото разпознаване, което се реализира на сървър, може да се реализира противодействие, което да ограничава този вид атака.

Свойството „устойчивост срещу phishing атака“ определяме като удовлетворено, тъй като при този механизъм за удостоверяване от потребителя никъде не се изисква въвеждането на данни за удостоверяване.

Свойството „устойчивост срещу кражба“ определяме като удовлетворено, тъй като дори и злонамереният потребител да получи физически достъп до мобилното устройство или малките допълнителни устройства, това не е достатъчно, за да се компрометира механизма за удостоверяване.

Свойството „невъзможност за асоцииране“ определяме като неудовлетворено, тъй като при използването на гласовото разпознаване може да се направи пряка връзка между механизма за удостоверяване и идентичността на потребителя.

Свойството „продължително удостоверяване“ определяме като удовлетворено, тъй като от една страна PICO token реализира периодична проверка за самоличността на потребителя, а от друга всеки път при желание да бъде реализирано парично движение на средства потребителят трябва да премине през задължително гласово разпознаване.

Свойството „различни нива на позволения“ определяме като удовлетворено, тъй като в зависимост дали потребителят е използвал PICO token, гласово разпознаване или и двете на него му се предоставя различен достъп до услугите за мобилно банкиране.

Представените резултати от оценката обобщаваме в таблица 8, като едновременно с това правим сравнение с представените по-рано алтернативни механизми, чиито оценки определихме на база публикацията на Vonneau [143].

От резултатите, представени в таблица 8, установяваме, че предложеният механизъм за удостоверяване, който се базира на PICO token и гласово разпознаване, по отношение на свойствата от категория „сигурност“ има най-висока оценка. От друга страна по отношение свойствата от другите две категории той отстъпва на алтернативните механизми. Като положителен момент можем да подчертаем, че той има по-висока оценка от token удостоверяването, което е на второ място по отношение на свойствата от категория „сигурност“. 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.

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

Таблица 8. Сравнение на различните механизми за удостоверяване

От казаното до тук може да направим извод, че предложеният механизъм за удостоверяване води до повишаване на сигурността при

мобилното банкиране. Като насока за бъдещото му подобрене е необходимо да се работи в посока за повишаване на стойностите на свойствата от категориите „ползваемост“ и „разпространяемост“.

## **5. Модул за реализиране на автоматизирани проверки**

Целта на настоящия експеримент е да се определи как потребителите възприемат модула за реализиране на автоматизирани проверки.

За реализирането на целта е необходимо да бъдат изпълнени следните задачи:

- реализиране на определени автоматизирани проверки;
- представяне на резултатите (индикатор за сигурност и инструкции за действие) на всеки потребител;
- наблюдаване на поведението на всеки потребител при взаимодействие с модула.

Подготвихме провеждането на експеримента да се реализира в контролирана среда, т.е. под контрол на експерти, които следят за правилното му изпълнение и при необходимост дават насоки на участниците.

За реализиране на експеримента избрахме 30 участника (17 мъже и 13 жени) на възраст от 18 до 50 години. Избрахме тази възрастова група, тъй като това е частта от населението, която най-активно работи с мобилни устройства със сензорен екран. От участниците 1 е с основно образование, 8 са със средно, а 21 с висше. Всички от тях имат собствено мобилно устройство със сензорен екран, както и необходимите познания за базова работа с него.

При подбора на участниците за експеримента използвахме стохастичния (или случаен) метод на подбор. При него всички единици на генералната съвкупност имат равен шанс да попаднат в извадката на

изследването. По този начин структурата на извадката възпроизвежда с определена точност структурата на цялата генерална съвкупност. Така се осигурява представителност (репрезентативност) на информацията, която е получена за извадката.

За осъществяване на първата задача на експеримента (реализиране на определени автоматизирани проверки) предварително разработихме мобилно приложение, което е инсталирано на смартфон LG Nexus 5, работещ с най-широко разпространената мобилна операционна система Android и нейната най-използвана версия KitKat 4.4.

За реализиране на мобилното приложение използвахме средата за разработка Visual Studio Community 2015 с допълнително инсталирано разширение, даващо възможност за работа със средата за разработка Xamarin. Последната позволява разработването на native мобилни приложения с помощта на програмния език C#, който е използван и тук. За първоначално тестване на приложението използвахме симулаторът Xamarin Android Player.

Разработихме мобилното приложение така, че да реализира следните автоматизирани проверки:

- НБМ – проверка за използване на некриптирана публична безжична мрежа. За целта използваме класа `WifiManager`, който предоставя API за управление на всички аспекти на Wi-Fi връзката. Благодарение на неговия метод `StartScan()` осъществяваме сканиране на активната безжична мрежа и от свойството `Capabilities` на класа `ScanResult` получаваме информация за използвания протокол за защита на достъпа до мрежата.
- КОС – проверка за включена функция за криптиране на данните на мобилната операционна система. За целта използваме

свойството `StorageEncryptionStatus` на класа `DevicePolicyManager`, което определя статуса на криптиране на данните на устройството.

- МУ - проверка за използване на механизъм за удостоверяване преди използване на мобилното устройство. За целта използваме свойството `IsKeyGuardSecure` на класа `KeyguardManager`, което дава информация дали се използва ПИН код, шаблон за заключване или парола за удостоверяване.
- АЗ - проверка за активирано автоматично заключване на мобилното устройство. За целта използваме свойството `LockPatternEnabled` на класа `Settings.Secure`, което дава информация дали автоматичното заключване е активирано.
- БТ - проверка за включен Bluetooth интерфейс на мобилното устройство. За целта използваме свойството `Adapter` на класа `BluetoothManager`, което дава информация дали има активиран Bluetooth интерфейс.
- АОС - проверка за актуалността на версията на мобилната операционна система. За целта използваме свойството `Release` на класа `Build.VERSION`, което дава информация за настоящо инсталираната версия на операционната система Android.
- МОС - проверка за определяне дали мобилната операционна система на потребителя е модифицирана. За целта правим проверка за наличието на файла `„/system/app/Superuser.apk“`.
- АВ - проверка за инсталирано мобилно антивирусно приложение. За целта използваме метода `GetInstalledPackages()` на класа `PackageManager`, който позволява да се направи проверка за наличието на различни мобилни антивирусни приложения. В

нашия случай проверяваме за продукта Avast Mobile Security. (В предишно авторско изследване той е оценен най-високо).

Последното, което реализира мобилното приложение е показване на резултата от всяка проверка, както и индикатор за сигурността на устройството. 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.

От представените проверки като задължителни определихме следните:

- МБ - проверка за използване на механизъм за удостоверяване преди използване на мобилното устройство;
- АЗ - проверка за активирано автоматично заключване на мобилното устройство;
- АОС - проверка за актуалността на версията на мобилната операционна система.

Останалите проверки са препоръчителни.

Инструкциите, които всеки потребител следва да предприеме, за да удовлетвори някоя от проверките, предварително подготвихме в хартиен вариант и ги предоставихме на тези от потребителите, които заявиха желание.

За осъществяване на третата задача на настоящия експеримент (наблюдаване на поведението на всеки потребител при взаимодействие с модула) определихме да бъдат реализирани следните наблюдения:

- Опитва ли се потребителят да удовлетвори неуспешно преминалите проверки или се отказва да използва мобилното приложение 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 планирането на експеримента можем да пристъпим към описание на неговото провеждане.

На всеки от участниците последователно предоставихме мобилното устройство LG Nexus 5. След това направихме предварителен инструктаж за действията, които всеки от тях следва да реализира. Първоначално потребителят стартира мобилното приложение, което се използва за реализиране на представените автоматизирани проверки. Резултатът, който получава всеки потребител е, че нито една от автоматизираните проверки не е преминала успешно, той вижда кои от тях са задължителни и кои препоръчителни, както и стойността на индикатора за сигурност, която е „0 от 11“. 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. На всеки от потребителите осигурихме необходимото време за работа. След като някой от тях заяви, че е приключил с поставената задача направихме проверка до каква степен са удовлетворени проверките и каква е стойността на индикатора за сигурност.



По време на реализиране на различните етапи на експеримента осъществихме представените по-горе наблюдения. В следствие на това може да преминем към представяне на получените 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 разбраха, че за да използват мобилното приложение за мобилното банкиране е необходимо да удовлетворят определени изисквания. Като причина те посочиха, че извършват само справочни операции и затова смятат, че не е нужно да отделят време за удовлетворяване на изискванията.

В таблица 9 са представени резултатите на останалите 25.

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

Таблица 9. Резултати от действията на потребителите

От таблица 9 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 тях, 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 подобрене.

Нещо друго, което ни 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. 17 представяме резултатите отразяващи процента на удовлетворените проверки като е разграничено, кои от тях са направени без или с допълнителни инструкции.



Фиг. 17. Процент на удовлетворените проверки

От фиг. 17 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 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.

## **6. Заключение**

В настоящата глава оценихме приложимостта на представения във втора глава концептуален модел за повишаване на сигурността при мобилното банкиране. Основната цел тук беше да се изследва ефективността на всеки един от петте модула, които участват в него. За осъществяването на това реализирахме експерименти за всеки модул, като следвахме обща методика на работа, включваща следните етапи: определяне на обхват на експеримента, планиране на експеримента, провеждане на експеримента и представяне и анализ на резултатите.

Целта на първия проведен експеримент беше да се изследва ефективността и да се определи най-подходящият алгоритъм за машинно обучение, който може да бъде използван в модула за биометрично удостоверяване, което се базира на поведението на потребителите. Първоначално на всеки от участниците в експеримента предоставихме мобилното устройство LG Nexus 5. На него беше инсталирано разработено от нас мобилно приложение, което се използва за събиране на входни данни от сензорния екран на мобилното устройство. На база на събраните входни данни изготвихме два файла в подходящ формат за софтуерния продукт KNIME. С негова помощ реализирахме тестване на различни алгоритми за машинно обучение. Резултатите от експеримента показаха, че грешката, която се постига при използването на алгоритъма Particle Swarm Optimization Radial Basis Function Network е 1.8%, което ни дава основание да направим извод, че съответният алгоритъм за машинно обучение е подходящ за съответната задача. От тук на свой ред смятаме, че модулет за биометрично удостоверяване, който се базира на поведението на потребителите, следва да изпълни успешно своите функции по защита на мобилното устройство от неоторизиран достъп.

Целта на втория проведен експеримент беше да се измери производителността на алгоритъма за засичане, участващ в модула за автоматизирана защита от tabnabbing атака. Под производителност разбираме необходимото време както за обработка на информацията, така и за предупреждаване на потребителя относно реализираните промени. За реализиране на целта последователно осъществихме измерване на:

- времето, което е необходимо, за да се реализира прихващане на снимка на един и същ уеб сайт;
- времето, за което се извършва разделянето на снимката на части;

- времето, за което се извършва сравнение между две зададени снимки;
- времето, за което се визуализира съобщение, представящо процента на реализираните промени.

Резултатите от експеримента показаха, че средното време необходимо за изпълнение на алгоритъма е 230 мс, като от тях 113 мс се използват от приложно програмния интерфейс (API) на браузъра, което е извън нашия контрол. По време на провеждане на експеримента възникнаха и някои ограничения. Като ги вземем предвид, можем да направим извод, 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.

Целта на третия проведен експеримент беше да се изследва ефективността на предложението от нас алгоритъм за филтриране при осъществяване на автоматизирана защита от CSRF атака. Това беше реализирано с помощта на софтуерния инструмент за проверка на модели Alloy Analyzer, като предварително изготвихме формално описание на алгоритъма и на CSRF атаката. Като основа за формалното описание използвахме разработения от Akhawe [142] модел на уеб инфраструктурата, като за целите на експеримента внесохме някои допълнения в модела. Резултатът от проверката на модела показва, че не са открити примери, които да свидетелстват, че злонамерен потребител може да генерира злонамерена cross-site заявка, като използва мобилния уеб браузър на потребителя. Това от своя страна показва ефективността на предложението от нас алгоритъм за филтриране и възможността за използването му при осъществяване на автоматизирана защита от CSRF атака.

Целта на четвъртия проведен експеримент беше да се направи оценка на модула за удостоверяване, който се базира на PICO token и гласово

разпознаване. Като основа използвахме подход за оценка на уеб базирани механизми за удостоверяване, който е разработен от Bonneau [143]. Тъй като този подход не беше напълно съвместим с представения от нас модул за удостоверяване беше необходимо да го модифицираме 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 две допълнителни свойства, които са тясно свързани с token базираните механизми за удостоверяване. Последното, което реализирахме беше да оценим модула за удостоверяване и да го сравним с резултатите на алтернативни механизми – ПИН, парола, биометрики и token устройства. Резултатите показаха, 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. Затова считаме, че предложеният метод за удостоверяване води до повишаване на сигурността при мобилното банкиране.

Целта на петия проведен експеримент беше да се определи как потребителите възприемат модула за реализиране на автоматизирани проверки. Първоначално на всеки от участниците в експеримента предоставихме мобилното устройство LG Nexus 5. На него беше инсталирано разработено от нас мобилно приложение, което се използва за реализиране на определени автоматизирани проверки и представяне на резултатите от тях. След това на потребителите, които пожелаха да удовлетворят неуспешно преминалите проверки предоставихме възможност да го направят без или с получаване на допълнителни инструкции, в зависимост от тяхната компетентност и желание. Междувременно наблюдавахме всеки потребител при взаимодействието му

с модула. От резултатите, получени от експеримента, могат да бъдат направени следните заключения:

- съществува група потребители, които не са склонни въобще да опитат да удовлетворят автоматизирани проверки;
- съществува необходимост от предоставяне на допълнителни инструкции, тъй като при 63% от проверките успеваемостта се дължи на тях;
- необходимо е да се направи подобрене на предоставените инструкции, тъй като за някои от потребителите те не са достатъчно разбираеми;
- потребителят по-успешно реагира на задължителните проверки и затова те могат да бъдат по-успешно прилагани в настоящия модул.
- Потребителите подобряват индикатора за сигурност – 74% от всичките потребители (30 души) го подобряват с най-малко 55%.

Тези изводи ни дават основание да твърдим, че ако модулът за автоматизирани проверки бъде разработен в пълната си функционалност би повишил нивото на сигурността при мобилното банкиране.

Проведеното в рамките на настоящата глава експериментално изследване потвърждава ефективността и приложимостта на предложението във втора глава концептуален модел. Въпреки това получените резултати имат само предварителен характер и е необходимо да бъдат направени допълнителни по-широкообхватни изследвания, които да осигурят статистически значими резултати. Това може да бъде очертано като насока за развитието на настоящата разработка.

## ЗАКЛЮЧЕНИЕ

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

1. На базата на анализиранияте 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)



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.

# СПИСЪК НА ПУБЛИКАЦИИТЕ ПО 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 следните:

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.

## **ДЕКЛАРАЦИЯ ЗА ОРИГИНАЛНОСТ**

С настоящото декларирам, че резултатите и приносите, представени в дисертационния ми труд на тема "Оптимизация на сигурността при мобилното банкиране" са оригинални.

Бонимир Пенчев Пенчев

Подпис:

## ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Safeena, R., H. Date, A. Kammani, N. Hundewale. Technology Adoption and Indian consumers: Study on Mobile Banking. International Journal of Computer Theory and Engineering, 2012, 4(6), p. 1020-1024.

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

[3] 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.

[4] Mobile Banking Penetration in Selected European Countries in 2013 and 2014. <http://www.statista.com/statistics/310402/mobile-banking-penetration-europe/>. 14.05.2015.

[5] Frequency of Mobile Banking Usage in United Kingdom (UK) from 2011 to 2014. <http://www.statista.com/statistics/318596/uk-mobile-banking-frequency/>. 14.05.2015.

[6] There Will Soon Be One Smartphone For Every Five People In The World. [www.businessinsider.in/There-Will-Soon-Be-One-Smartphone-For-Every-Five-People-In-The-World/articleshow/21375608.cms](http://www.businessinsider.in/There-Will-Soon-Be-One-Smartphone-For-Every-Five-People-In-The-World/articleshow/21375608.cms). 14.05.2015.

[7] Shaikh, A. A. Mobile Banking Adoption Issues in Pakistan and Challenges Ahead. Journal of the Institute of Bankers Pakistan, 2013, 80(3), p. 12-15.

[8] 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.

- [9] Suoranta, M. Adoption of Mobile Banking in Finland. <http://urn.fi/URN:ISBN:951-39-1654-5>. 14.07.2015.
- [10] Medhi, I., A. Ratan, K. Toyama. Mobile-Banking Adoption and Usage by Low-Literate, Low-Income Users in the Developing World. Proceedings of the 3rd International Conference on Internationalization, Design and Global Development: Held as Part of HCI International, 2009, p. 485-494.
- [11] Kim, G., B. S. Shin, H. G. Lee. Understanding Dynamics between Initial Trust and Usage Intentions of Mobile Banking. Information Systems Journal, 2009, 19(3), p. 283-311.
- [12] Scornavacca, E., H. Hoehle. Mobile Banking in Germany: a Strategic Perspective. International Journal of Electronic Finance, 2006, 1(3), p. 304-320.
- [13] Tiwari, R., S. Buse, C. Herstatt. Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage. Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management, 2007, p. 886-894.
- [14] Liou, D. Four Scenario Analysis for Mobile Banking Development Contextualized to Taiwan. Proceedings of the Portland International Conference on Management of Engineering & Technology, 2008, p. 2634-2643.
- [15] Barnes, S. J., B. Corbitt. Mobile Banking: Concept and Potential. International Journal of Mobile Communications, 2003, 1(3), p. 273-288.
- [16] Riivari, J. Mobile Banking: A Powerful New Marketing and CRM Tool for Financial Services Companies All over the Europe. Journal of Financial Services Marketing, 2005, 10(1), p. 11-20.
- [17] Dineshwar, R., M. Steven. An Investigation on Mobile Banking Adoption and Usage: a Case Study of Mauritius. Proceedings of the 3rd Asia-Pacific Business Research Conference, 2013, 3(3), p. 197-217.

- [18] Luarn, P., H. Lin. Toward an Understanding of the Behavioral Intention to Use Mobile Banking. *Computers in Human Behavior*. 2005, 21(6), p. 873-891.
- [19] Shih, K., H. Hung, B. Lin. Assessing User Experiences and Usage Intentions of m-Banking Service. *International Journal of Mobile Communications*, 2010, 8(3), p. 257 – 277.
- [20] Mobile Banking Handset & Tablet Market Strategies 2013–2017. [http://www.juniperresearch.com/reports/mobile\\_banking](http://www.juniperresearch.com/reports/mobile_banking). 05.07.2015.
- [21] ICT Facts and Figures: The World in 2015. [www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf](http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf). 05.07.2015.
- [22] Chemingui, H., H. B. Iallouna. Resistance, Motivations, Trust and Intention to Use Mobile Financial Services. *International Journal of Bank Marketing*, 2013, 31(7), p. 574-592.
- [23] Cruz, P., T. Laukkanen, P. Muñoz. Exploring the Factors behind the Resistance to Mobile Banking in Portugal. *International Journal of E-Services and Mobile Applications*, 2009, 1(4), p. 16-35.
- [24] Laukkanen, T., P. Cruz. Cultural, Individual and Device-Specific Antecedents on Mobile Banking Adoption: a Cross-National Study. *Proceeding of the 45th International Conference on System Science (HICSS)*, 2012, p. 3170-3179.
- [25] Laukkanen, T. Determinants of Mobile Banking Resistance: a Preliminary Model. *Proceedings of ANZMAC (Australian and New Zealand Marketing Academy) Conference*, 2008, p. 1-3.
- [26] Laukkanen, T., V. Kiviniemi. The Role of Information in Mobile Banking Resistance. *International Journal of Bank Marketing*, 2010, 28(5), p. 372-388.

[27] Laukkanen, T., S. Sinkkonen, M. Kivijarvi, P. Laukkanen. Innovation Resistance among Mature Consumers. *Journal of Consumer Marketing*, 2007, 24(7), p. 419-427.

[28] Jain, Y. Mobile Banking: a Study on Adoption & Challenges in Southern Rajasthan, India. *International Journal of Innovative Research & Development* 2(4), p. 902-914.

[29] Lee, K. C., N. Chung. Understanding Factors Affecting Trust in and Satisfaction with Mobile Banking in Korea: a Modified DeLone and McLean's Model Perspective. *Interacting with Computers*, 2009, 21(5-6), p. 385 – 392.

[30] Lin, H. An Empirical Investigation of Mobile Banking Adoption: the Effect of Innovation Attributes and Knowledge-based Trust. *International Journal of Information Management*, 2011, 31(3), p. 252 – 260.

[31] Zhou, T. An Empirical Examination of Initial Trust in Mobile Banking. *Internet Research*, 2011, 21(5), p. 527 – 540.

[32] Heggstuen, 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.

[33] Veijalainen, J., V. Terziyan, H. Tirri. Transaction Management for m-Commerce at a Mobile Terminal. *Electronic Commerce Research and Applications*, 2006, 5(3), p. 229-245.

[34] Liu, Z., Q. Min, S. Ji. An Empirical Study on Mobile Banking Adoption: the Role of Trust. *Proceedings of the 2nd International Symposium on Electronic Commerce and Security*, 2009, 2, p. 7-13.

[35] Ivatury, G., I. Mas. The Early Experience with Branchless Banking. CGAP Focus Note, 2008, 46, <http://ssrn.com/abstract=1655257>, 05.07.2015.

[36] Donner, J., C. A. Tellez. Mobile Banking and Economic Development: Linking adoption, Impact, and Use. *Asian Journal of Communication*, 2008, 18(4), p. 318-332.



- [37] Amin, H., M. R. A. Hamid, G. H. Tanakinjal, S. Lada. Undergraduate Attitudes and Expectations for Mobile Banking. *Journal of Internet Banking and Commerce*, 2006, 11(3), p. 1-10.
- [38] Brown, I., Z. Cajee, D. Davies, S. Stroebe. Cell Phone Banking: Predictors of Adoption in South Africa - an Exploratory Study. *International Journal of Information Management*, 2003, 23(5), p. 381-394.
- [39] Cronin, M. J. Mobile Commerce. *The Internet Encyclopedia*, Volume 2, New Jersey, John Wiley & Sons, 2004, p. 614-626.
- [40] Stanoevska-Slabeva, K. Towards a Reference Model for m-Commerce Applications. *Proceedings of the 11th European Conference on Information Systems*, 2003, p. 1-13.
- [41] Alex, K. Is it Finally Time for m-Commerce, [http://ovum.com/wp-content/uploads/2011/10/ST\\_IT\\_Q2\\_2010.pdf](http://ovum.com/wp-content/uploads/2011/10/ST_IT_Q2_2010.pdf). 10.07.2015.
- [42] Tiwari, R., S. Buse. *The Mobile Commerce Prospects: a Strategic Analysis of Opportunities in the Banking Sector*. Hamburg, Hamburg University Press, 2007.
- [43] Върбанов, Р., К. Шишманов, В. Краева, Е. Денчев, К. Стефанова, С. Парушева, П. Петров. *Информационни технологии в бизнеса*. Велико Търново, Фабер, 2009.
- [44] Cruz, P., L. B. F. Neto, P. Muñoz-Gallego, T. Laukkanen. Mobile Banking Rollout in Emerging Markets: Evidence from Brazil. *International Journal of Bank Marketing*, 2010, 28(5), p. 342-371.
- [45] Stair, R. M., G. Reynolds. *Fundamentals of Information Systems*. 5th Edition, USA, Course Technology, 2009.
- [46] Alafeef, M., D. Singh, K. Ahmad. The Influence of Demographic Factors and User Interface on Mobile Banking Adoption: a Review. *Journal of Applied Sciences*, 2012, 12(20), p. 2082-2095.

- [47] Harma, M. K., R. Dubey. Prospects of Technological Advancements in Banking Sector using Mobile Banking and Position of India. Proceedings of the International Association of Computer Science and Information Technology Spring Conference, 2009, p. 291-295.
- [48] Akturan, U., N. Tezcan. Mobile Banking Adoption of the Youth Market: Perceptions and Intentions. Marketing Intelligence and Planning, 2012, 30(4), p. 444-459.
- [49] Masrek, M. N., N. B. Omar, N.A. Uzir, I. E. Khairuddin. The Impact of Technology Trust on Mobile Banking Utilization. Science Series Data Report, 2012, 4(12), p. 27-36.
- [50] Punithavathi, R., K. Duraiswamy. Secured Authenticated Mobile Agent Based Mobile Banking System. European Journal of Scientific Research, 2011, 57(3), p. 494-501.
- [51] Bångens, Dr. L., B. Söderberg. Mobile Banking - Financial Services for the Unbanked. The Swedish Program for ICT in Developing Regions, SPIDER, 2008.
- [52] Kondabagil, J. Risk Management in Electronic Banking: Concept and Best Practices. Singapore, John Wiley & Sons, 2007.
- [53] Porteous, D. The Enabling Environment for Mobile Banking in Africa. Boston, Department for International Development, 2006.
- [54] Borreguero F. J. M., J. C. Pelaez. Spanish Mobile Banking Services: an Adoption Study. Proceedings of the International Conference on Mobile Business, 2005, p. 274-280.
- [55] Mallat, N., M. Rossi, V. K. Tuunainen. Mobile Banking Services. Communications of the ACM, 2004, 47(5), p. 42-46.
- [56] Salvi, A. B., S. Sahai, S. Dial M for Money. Proceedings of the 2nd ACM International Workshop on Mobile Commerce, 2002, p. 95-99.

[57] Anyasi, F. I., P. A. Otubu. Mobile Phone Technology in Banking System: Its Economic Effect. Research Journal of Information Technology, 2009, 1(1), p. 1-5.

[58] Arguirre, E., D. Dias, K. Prochaska. Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Colombia. Washington, CGAP, 2008.

[59] Customer Loyalty in Retail Banking. [http://www.bain.com/Images/BAIN\\_REPORT\\_Customer\\_loyalty\\_in\\_retail\\_banking.pdf](http://www.bain.com/Images/BAIN_REPORT_Customer_loyalty_in_retail_banking.pdf). 10.07.2015.

[60] Winning through customer experience [http://www.ey.com/Publication/vwLUAssets/EY\\_-\\_Global\\_Consumer\\_Banking\\_Survey\\_2014/\\$FILE/EY-Global-Consumer-Banking-Survey-2014.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_Global_Consumer_Banking_Survey_2014/$FILE/EY-Global-Consumer-Banking-Survey-2014.pdf). 10.07.2015.

[61] Banking Anytime and Anywhere. <http://www.mobile-money-gateway.com/sites/default/files/Banking%20anytime%20anywhere.pdf>. 10.07.2015.

[62] Total Mobile Phone Users Who Use Mobile Banking Services Split by 8 key regions. <http://www.africatelecomsonline.co.za/statistics/statistics/total-mobile-phone-users-m-who-use-mobile-banking-services-split-by-8-key-regions-2010-2013>. 10.07.2015.

[63] Claessens, J., V. Dem, D. De Cock, B. Preneel, J. Vandewalle. On the Security of Today's Online Electronic Banking Systems. Computers & Security, 2002, 21(3), p. 253-265.

[64] Panja, B., D. Fattaleh, M. Mercado, A. Robinson, P. Meharia. Cybersecurity in Banking and Financial Sector: Security Analysis of a Mobile Banking Application. Proceedings of the International Conference on Collaboration Technologies and Systems (CTS), 2013, p. 397-403.

[65] He, W. A Survey of Security Risks of Mobile Social Media through Blog Mining and an Extensive Literature Search. Information Management & Computer Security, 2013, 21(5), p. 381-400.

[66] Report on Cyber Security in the Banking Sector. [http://www.dfs.ny.gov/reportpub/dfs\\_cyber\\_banking\\_report\\_052014.pdf](http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf). 17.07.2015.

[67] The Cybersecurity 101: A Resource Guide for Bank Executives: Executive Leadership of Cybersecurity. Conference of State Bank Supervisors. <https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf>. 17.07.2015.

[68] 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

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

[70] 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.

[71] Cheng, Z. Mobile Malware: Threats and Prevention. Santa Clara, McAfee Avert, 2007.

[72] Dunham K. Mobile Malware Attacks and Defense. Rockland, Syngress Publishing, 2008.

[73] Haataja, K. Security Threats and Countermeasures in Bluetooth-enabled Systems. Ph.D. dissertation, Department of Computer Science, University of Kuopio, 2009

[74] Franklin, C., J. Layton. How Bluetooth Works. <http://electronics.howstuffworks.com/bluetooth1.htm>. 23.07.2015.

[75] Gligoroski D., P. Stephanow, G. Maguire. Security as a Service in Cloud for Smartphones. <http://www.diva-portal.org/smash/get/diva2:446114/FULLTEXT01.pdf>. 23.07.2015.

[76] Hoepman, J., J. Siljee. Beyond RFID: the NFC Security Landscape. Whitepaper, TNO, 2007.

[77] Mulliner, C. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones, Proceedings of the Fourth International Conference on Availability, Reliability and Security, 2009, p. 695– 700.

[78] Ries, U. Phishing via NFC. The H Security, <http://www.webcitation.org/6BzrM8Qmp>. 23.07.2015.

[79] Borgaonkar, R. USSD/Android Dailer Vulnerability. <http://www.webcitation.org/6DW71H3uK>. 23.07.2015.

[80] Makhoul, A., N. Boudriga. Intrusion and Anomaly Detection in Wireless Networks. Handbook of Research on Wireless Security, New York, Information Science Publishing, 2008, p. 78-94.

[81] A Framework for Auditing Mobile Devices. [http://www.bakertilly.com/uploads/auditing-mobile-devices\\_2014.pdf](http://www.bakertilly.com/uploads/auditing-mobile-devices_2014.pdf). 23.07.2015.

[82] Nickolov, E. Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations. Information & Security, 2005, 17, p. 105-119.

[83] Nickolova, M., E. Nickolov. Threat Model for User Security in E-Learning Systems. International Journal “Information Technologies and Knowledge”, 2007, 1, p. 341-347.

[84] Legnitto, J. Mobile Banking on Unsecure Wireless Networks is Risky Business. <http://www.privatewifi.com/title-mobile-banking-on-unsecure-wireless-networks-is-risky-business/>. 17.07.2015.

[85] Jeon, W., J. Kim, Y. Lee, D. Won. A Practical Analysis of Smartphone Security. Proceedings of the International Conference Human Interface and the Management of Information, 2011, p. 311-320.

[86] The Risks & Rewards of Mobile Banking Apps. Webroot. [http://www.brightcloud.com/pdf/RisksRewardsofMobileBankingAppsWhitepaper\\_20140619115948\\_311111.pdf](http://www.brightcloud.com/pdf/RisksRewardsofMobileBankingAppsWhitepaper_20140619115948_311111.pdf). 17.07.2015.

[87] Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO-12-757. <http://www.gao.gov/assets/650/648519.pdf>. 24.07.2015.

[88] Amrutkar, C., K. Singh, A. Verma, P. Traynor. VulnerableMe: Measuring Systematic Weaknesses in Mobile Browser Security. Proceedings of the International Conference on Information System Security, 2012, p. 16-34.

[89] Felt, A. P., D. Wagner. Phishing on Mobile Devices. Proceedings of the IEEE Web 2.0 Security and Privacy Workshop, 2011, p. 1-10.

[90] Niu, Y., F. Hsu, H. Chen. iPhish: Phishing Vulnerabilities on Consumer Electronics. Proceedings of the 1st Conference on Usability, Psychology, and Security, 2008, 10, p. 1-8.

[91] Rieck, K., T. Krueger, A. Dewald. Cujo: Efficient Detection and Prevention of Drive-by-download Attacks. Proceedings of the 26th Annual Computer Security Applications Conference, 2010, p. 31-39.

[92] Rydstedt, G., B. Gourdin, E. Bursztein, D. Boneh. Framing Attacks on Smart Phones and Dumb Routers: Tap-jacking and Geo-localization Attacks. Proceedings of the USENIX Workshop on Offensive Technology, 2010, p. 1-8.

[93] Sujithra, M. Mobile Device Security: a Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications, 2012, 56(14), p. 24-29.

[94] Парушева, С. Кражбите на самоличност и защитата на интернет банкирането. Икономически алтернативи, 2009, 2, с. 84-96.

[95] Amrutkar, C. , P. Traynor, P. Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. IEEE Transactions on Mobile Computing, 2015, 14(5), p. 889-903.

[96] W3C. Web Security Context: User Interface Guidelines. [www.w3.org/TR/2010/WD-wsc-ui-20100309/](http://www.w3.org/TR/2010/WD-wsc-ui-20100309/). 30.07/2015.

[97] Raskin, A. Tabnabbing: A New Type of Phishing Attack. <http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/>. 30.07.2015.

[98] Zeller, W. Cross-site Request Forgeries: Exploitation and Prevention. [http://www.cs.utexas.edu/~shmat/courses/cs378\\_spring09/zeller.pdf](http://www.cs.utexas.edu/~shmat/courses/cs378_spring09/zeller.pdf). 30.07.2015.

[99] Elkhodr, M., S. Shahrestani, K. Kourouche. A Proposal to Improve the Security of Mobile Banking Applications. Proceedings of the 10th International Conference on ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012, p. 260-265.

[100] Balebako, R., L. Cranor. Improving App Privacy: Nudging App Developers to Protect User Privacy. IEEE Security & Privacy, 12(4), p. 55-58.

[101] Study Finds Seven out of Ten Retail and Finance Applications Vulnerable to Heartbleed-style Attacks. <http://www.castsoftware.com/news-events/press-release/press-releases/download/study-finds-seven-out-of-ten-retail-and-finance-applications-vulnerable-to-heartbleed-style-attacks>. 30.07.2015.

[102] Sanchez, A. Personal Banking Apps Leak Info Through Phone. <http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html>. 30.07.2015.

[103] Ante, S. E. Banks Rush to Fix Security Flaws in Wireless Apps. <http://online.wsj.com/article/SB10001424052748703805704575594581203248658.html#printMode>. 22.07.2015.

[104] Huang, S. The South Korean Fake Banking App Scam. <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-south-korean-fake-banking-app-scam.pdf>. 17.07.2015.

[105] whiteCryption Introduces New Level of Security for Mobile Payment Applications. <http://www.prweb.com/releases/2014/01/prweb11531529.htm>. 17.07.2015.

[106] Pousttchi, K., M. Schurig. Assessment of Today's Mobile Banking Applications from the View of Customer Requirements. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004, 7, p. 10.

[107] Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. <https://trac.tools.ietf.org/id/draft-ietf-tls-tls13-12.html>. 17.07.2015.

[108] Survey of the SSL Implementation of the Most Popular Web Sites. <https://www.trustworthyinternet.org/ssl-pulse/>. 17.07.2015.

[109] Laurie, B., A. Langley, E. Kasper, Certificate transparency. <https://tools.ietf.org/html/rfc6962>. 17.07.2015.

[110] Grant, A. C. Search for Trust: an Analysis and Comparison of CA System Alternatives and Enhancements. Dartmouth Computer Science. <http://www.cs.dartmouth.edu/reports/TR2012-716.pdf>. 17.07.2015.

[111] Zeller, W., E. W. Felten. Cross-site Request Forgeries: Exploitation and Prevention. Princeton University, 2008.

[112] Barth, A., C. Jackson, J. C. Mitchell. Robust Defenses for Cross-site Request Forgery. Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, p. 75–88.

[113] 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.

[114] Ben-Asher, N., N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, S. Möller. On the Need for Different Security Methods on Mobile Phones. Proceedings of 13th International Conference on Human Computer Interaction with Mobile Devices and Services, 2011, p. 465-473.



[115] 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.

[116] Elenkov, N. Revisiting Android Disk Encryption. <http://nelenkov.blogspot.com/2014/10/revisiting-android-disk-encryption.html?view=sidebar>. 17.07.2015.

[117] Chell, D. Apple iOS Hardware Assisted Screenlock Bruteforce. <http://blog.mdsec.co.uk/2015/03/bruteforcing-ios-screenlock.html>. 17.07.2015.

[118] Ryan, S. CVE-2014-4451 – Apple iOS Bug Allowing Unlimited Incorrect Pin Attempts. <http://technicalnotebook.com/software-bugs/apple-ios-bug-allowing-unlimited-incorrect-pin-attempts/>. 17.07.2015.

[119] Mobile Banking Security: Challenges, Solutions. Cognizant. <http://www.cognizant.com/InsightsWhitepapers/Mobile-Banking-Security-Challenges-Solutions-codex898.pdf>. 17.07.2015.

[120] Constantin, L. Security Analysis of Mobile Banking Apps Reveals Significant Weaknesses. <http://www.pcworld.com/article/2086320/security-analysis-of-mobile-banking-apps-reveals-significant-weaknesses.html>. 17.07.2015.

[121] Chandramohan, M., H. B. K. Tan. Detection of Mobile Malware in the Wild. *Computer*, 2012, 45(9), p. 65-71.

[122] La Polla, M., F. Martinelli, D. Sgandurra. A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 2013, 15(1), p. 446-471.

[123] White, A. Six Main Rules Of Safe Mobile Banking. Where, When And How? <http://blog.jammer-store.com/2013/05/six-main-rules-of-safe-mobile-banking-where-when-and-how/>. 17.07.2015.

[124] Edge, M. E., P. R. F. Sampaio. A Survey of Signature Based Methods for Financial Fraud Detection. *Computers and Security*, 2009, 28(6), p. 381-394.

[125] Fatima, A. E-banking Security Issues – Is There a Solution in Biometrics. *Journal of Internet Banking and Commerce*, 2011, 16(2), p. 1-9.

[126] About Touch ID Security on iPhone and iPad. <https://support.apple.com/bg-bg/HT204587>. 17.07.2015.

[127] Berg, D. How to use your fingerprint reader. <http://www.laptopmag.com/articles/how-to-use-your-fingerprint-reader>. 17.07.2015.

[128] Roberts, P. F. 7 Ways to Beat Fingerprint Biometrics. <http://www.itworld.com/article/2823742/security/120606-10-ways-to-beat-fingerprint-biometrics.html>. 17.07.2015.

[129] Lee, J., L. Bauer, M. L. Mazurek. The Effectiveness of Security Images in Internet Banking. *IEEE Internet Computing*, 2015, 19(1), p. 54-62.

[130] Safe Browsing API. Google. <https://developers.google.com/safe-browsing/>. 17.07.2015.

[131] Wenyin, L., G. Huang, L. Xiaoyue, Z. Min, X. Deng. Detection of Phishing Webpages Based on Visual Similarity. *Proceedings of the 14th International Conference on World Wide Special Interest Tracks and Posters*, 2005, p. 1060-1061.

[132] PhishTank. <http://www.phishtank.com/>. 17.07.2015.

[133] Enck, W., D. Ocateau, P. McDaniel, S. Chaudhuri. A Study of Android Application Security. *Proceedings of the 20th USENIX conference on Security*, 2011, p. 21-21.

[134] 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.

[135] Feinstein, B., D. Peck. Caffeine Monkey: Automated Collection, Detection and Analysis of Malicious JavaScript. [https://www.blackhat.com/presentations/bh-usa-07/Feinstein\\_and\\_Peck/Whitepaper/bh-usa-07-feinstein\\_and\\_peck-WP.pdf](https://www.blackhat.com/presentations/bh-usa-07/Feinstein_and_Peck/Whitepaper/bh-usa-07-feinstein_and_peck-WP.pdf). 17.07.2015.

[136] Enck, W., P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, A. N. Sheth. TaintDroid: an Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation, 2010, p. 393-407.

[137] Egele, M., C. Kruegel, E. Kirda, G. Vigna. PiOS: Detecting Privacy Leaks in iOS Applications. Proceedings of the 18th Annual Networking and Distributed Systems Security Symposium, 2011.

[138] Polimirova, D., E. Nickolov. Real-Time System for Assessing the Information Security of Computer Networks. Open Research Problems in Network Security, 2010, p. 123-133.

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

[140] Sikorski, M., A. Honig. Practical Maleware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco, No Starch Press, 2012.

[141] Stajano, F. Pico: No More Passwords! Proceedings of the 19th International Conference on Security Protocols, 2011, p. 49-81.

[142] 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.

[143] 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.