ENHANCING THE SECURITY OF MOBILE BANKING THROUGH THE IMPLEMENTATION OF AUTOMATED CHECKS ON THE MOBILE DEVICE

Penchev Bonimir, University of Economics – Varna, PhD student at Institute of Mathematics and Informatics - Bulgarian Academy of Sciences, b.penchev@ue-varna.bg

Abstract: Despite the advantages that mobile banking has for both banks and customers, there are also certain barriers that have a negative influence on its large-scale adoption. One of these barriers is its security level. In our previous research we have identified a certain number of security attacks against mobile banking security. Along with them, we have found out that not all of the protection strategies and best practices are effective enough. In terms of mobile banking application an area of improvement is associated with the failure in training the user regarding certain recommended security actions offered by mobile banking service providers. Therefore the objective of the report is to design a tool to facilitate users by implementing a set of automated checks in order to examine certain parameters of the mobile device directly related to the mobile banking security.
Keywords: mobile banking, mobile security, mobile device, mobile applications

ПОВИШАВАНЕ НА СИГУРНОСТТА ПРИ МОБИЛНОТО БАНКИРАНЕ ЧРЕЗ РЕАЛИЗИРАНЕТО НА АВТОМАТИЗИРАНИ ПРОВЕРКИ НА МОБИЛНОТО УСТРОЙСТВО

Бонимир Пенчев, Икономически университет – Варна, докторант към институт по математика и информатика при БАН, b.penchev@ue-varna.bg

Абстракт: Въпреки предимствата, които мобилното банкиране предоставя на банките и на техните клиенти, съществуват определени фактори, които оказват негативно влияние при възприемане му. Един от тези фактори е нивото на неговата сигурност. По отношение на мобилното приложение за мобилно банкиране насока за подобрение на сигурността е справянето с неуспехите при обучение на потребителя, свързано с реализирането на определени препоръчителни действия, предлагани от доставчиците на услуги за мобилно банкиране. Затова и целта на настоящата разработка е да се проектира инструмент, който да улесни потребителите, като реализира набор от автоматизирани проверки, които да изследват определени параметри на мобилното устройство, пряко свързани със сигурността на мобилното банкиране.
Ключови думи: мобилно банкиране, мобилна сигурност, мобилни устройства, мобилни приложения

1. Въведение

В продължение на повече от 40 години една от основните цели на финансовите институции е свързана с осигуряването на лесен достъп и удобство за своите клиенти при реализирането на банкови операции. Въпреки че АТМ устройствата и интернет

банкирането представляват ефективни канали за предоставяне на традиционни банкови продукти, един сравнително нов вид банкиране - мобилното банкиране - има значителен ефект върху пазара. За неговата актуалност и непрекъснато развитие свидетелстват проучвания, проведени в различни региони на света и обхващащи както развитите, така и развиващите се страни [1].

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

Въпреки тези предимства, използването на мобилни устройства с цел реализирането на банкови транзакции или получаването на достъп до финансова информация, не е толкова широко разпространено, както се очаква [3]. Това от своя страна свидетелства за съществуването на определени фактори, които оказват негативно влияние върху по-мащабното възприемане на мобилното банкиране. С цел да идентифицираме кои са те, проведохме допълнително изследване. Неговите резултати не само ясно показаха, че в действителност съществуват различни фактори, които оказват негативно влияние върху потребителите при възприемане на мобилното банкиране, но и потвърдиха, че различните рискове, свързани с неговата сигурност, съществено въздействат при вземане на решение за неговото използване [4].

Представените по-горе резултати провокираха провеждането на следващо изследване, чиято основна цел беше да се проучат най-често проявяващите се уязвимости и заплахи за сигурността на мобилното банкиране. Фокусът на изследването беше насочен към потребителя, тъй като той много често се посочва като най-слабото звено по отношение на сигурността. В резултат на това, при него бяха идентифицирани четири основни проблемни области, засягащи сигурността - мобилно устройство, мобилен уеб браузър, мобилна операционна система и мобилно приложение за мобилно банкиране. Във всяка една от тях бяха проучени уязвимостите и произтичащите от тях заплахи, което доведе до определянето на най-често използваните атаки при мобилното банкиране: подслушване на преносната среда (eavesdropping атака, man in the middle атака), cross site request forgery атака, неупълномощен физически достъп до устройството, phishing атаки (vishing атака, smishing атака, tabnabbing атака и използване на phishing приложения) и злонамерен софтуер [5].

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

По отношение на мобилното приложение за мобилно банкиране една от насоките за подобрение е справяне с неуспехите при обучение на потребителя, което е свързано с реализирането на определени препоръчителни действия, предлагани от доставчиците на услуги за мобилно банкиране.

От тук можем да дефинираме и целта на настоящата разработка - да се проектира инструмент, който да улесни потребителите, като реализира набор от автоматизирани проверки, които да изследват определени параметри на мобилното устройство, пряко свързани със сигурността на мобилното банкиране.

2. Повишаване на сигурността при мобилното банкиране чрез реализирането на автоматизирани проверки на мобилното устройство.

За реализирането на целта сме проектирали софтуерен модул, който следва да се интегрира в мобилното приложение за мобилно банкиране. Въз основа на представените във въведението четири основни проблемни области за сигурността на мобилното банкиране сме съставили следния списък с автоматизирани проверки, които могат да бъдат включени в софтуерния модул:

- За реализиране на защита на мобилното устройство:
  - проверка за използването на некриптирана публична безжична мрежа;
  - проверка за реализирано криптиране на данните на мобилната операционна система;
  - проверка за използване на механизъм за удостоверяване преди използване на мобилното устройство;
  - проверка за включено автоматично заключване на мобилното устройство;
  - проверка за включена функция за изтриване на данните след определен брой пъти неуспешно удостоверяване;
  - проверка за включена функция 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:
  - проверка за определяне дали мобилната операционна система е актуализирана;
  - проверка за определяне дали мобилната операционна система е модифицирана;
  - проверка за определяне наличието на мобилно антивирусно приложение;
  - проверка за определяне успешното засичане на модифициран злонамерен софтуер.

- За реализиране на защита на мобилното приложение за мобилно банкиране:
  - 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.

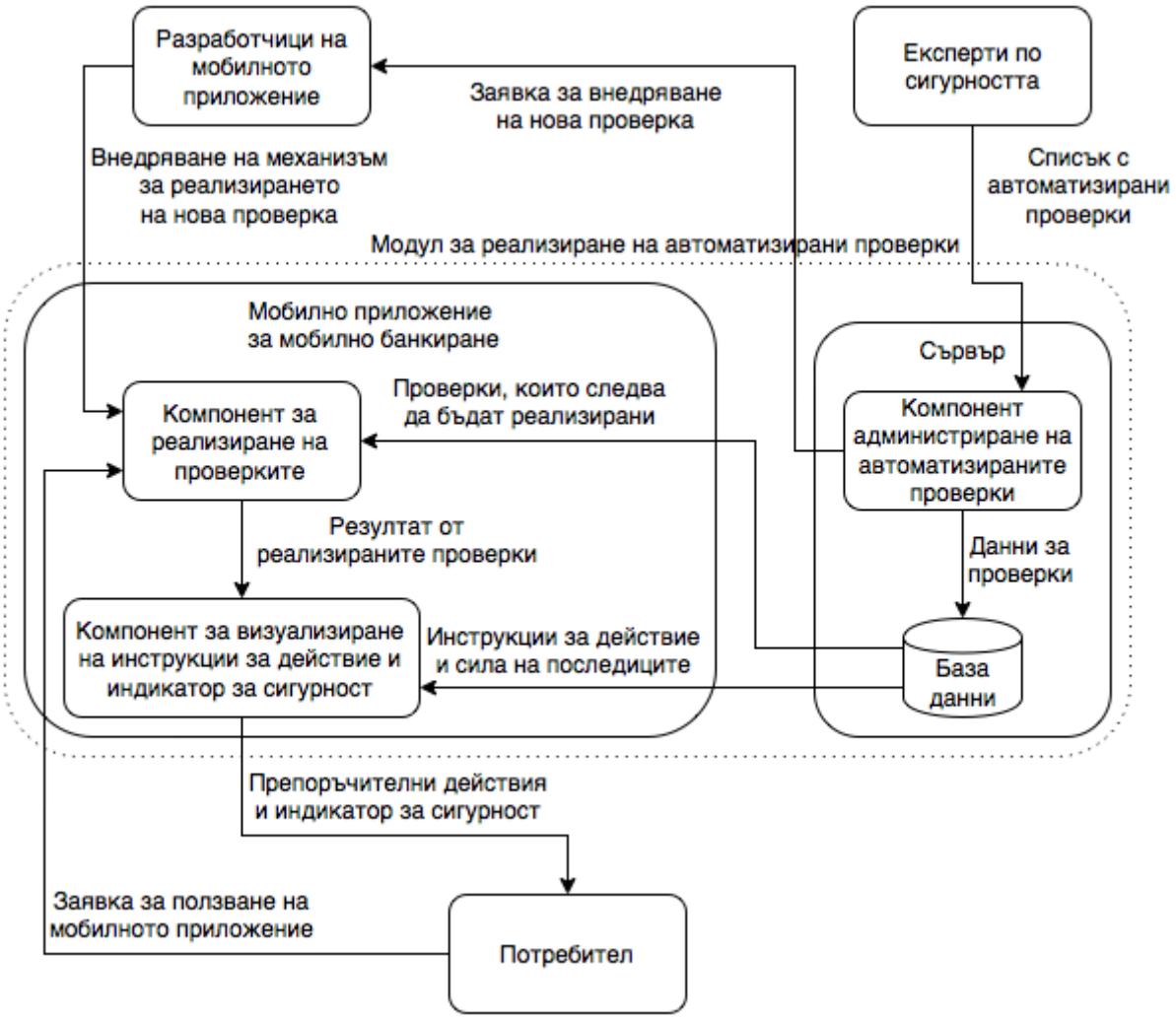
Представеният списък поражда някои съображения по отношение проектирането на софтуерния модул. Реализирането на толкова широк набор от проверки може да предизвика неудобство за потребителя, а това да доведе до отказ от използването на съответната услуга. От друга страна различните доставчици на тази услуга предоставят 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 представените съображения, може да дефинираме, че софтуерният модул 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 да помага на потребителите да предприемат определени действия, които да доведат до повишаване на нивото на сигурността при мобилното банкиране.
От архитектурна гледна точка софтуерния модул следва да бъде разделен на две основни части. Едната следва да бъде реализирана като компонент на мобилното приложението за мобилно банкиране, като по този начин в него следва да бъдат интегрирани допълнителни функционалности. Другата част следва да бъде разположена на сървър, където ще се поддържа базата от данни и където 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 модулът. 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 следва да се извърши от експертите по сигурността на доставчика на услуги за мобилно банкиране. Този процес следва да включва редица дейности и да 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 ще се определи 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 сървъра, от където ще се установи броят и видът на проверките, които следва да бъдат реализирани. Първоначално следва да се започне със задължителните проверки. Само ако те преминат успешно, ще се премине 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 тази стойност, е необходимо той да изпълни определени инструкции свързани с неуспешно преминалите препоръчителни проверки.
Въз основа на разгледаните процеси сме съставили следната архитектура на софтуерния модул за реализиране на автоматизирани проверки (вж. фиг. 1).



Фиг. 1. Архитектура на модула за реализиране на автоматизирани проверки

Както се вижда от представената на фиг. 1 архитектура, за осъществяването на софтуерния модул за реализиране на автоматизирани проверки е необходимо изграждането на три основни софтуерни компонента: компонент за администриране на автоматизираните проверки, компонент за реализиране на проверките, компонент за визуализиране на инструкции за действие и индикатор за сигурност.

3. Заключение

В настоящата разработка представихме софтуерен модул за реализиране на автоматизирани проверки, чиято основна цел е повишаване на сигурността при мобилното банкиране. Акцентът беше поставен върху някои съображения, свързани с неговото проектиране, представяне на функционалните му възможности, както и общата му архитектура. Като насока за бъдеща работа може да очертаем внедряване на представения софтуерен модул в дадено приложение за мобилно банкиране, в следствие на което и реализирането на проверка на неговата приложимост и ефективност.

References

[1] Global Mobile Statistics 2014 Section G: Mobile Banking and M-money; Section H: Venture Capital (VC) Investment in Mobile. http://mobiforge.com/research-analysis/global-mobile-statistics-2014-section-g-mobile-banking-and-m-money-section-h-venture-capital-vc-inve. Достъп до данните: 31.03.2016.

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

[3] Mobile Banking Handset & Tablet Market Strategies 2013–2017. http://www.juniperresearch.com/reports/mobile_banking. Достъп до данните: 31.03.2016.

[4] Пенчев, Б. Фактори, оказващи негативно влияние върху потребителите при възприемане на мобилното банкиране. Известия на Съюза на учените – Варна, Серия „Икономически науки“, Варна, 2015, с. 150-155.

[5] Penchev, B. Security Issues in Mobile Banking. In: Proceedings of International Conference Human Systems Integration Approach to Cyber Security, Sofia, 2016, p. 135-144.