Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

Security of Smart Banking Applications in Slovakia

Jozef Bucko

Technical University of Košice, Faculty of Economics, Department of Applied Mathematics and Business Informatics, Košice, Slovakia, jozef.bucko@tuke.sk

Received 28 July 2015; received in revised form 29 June 2016; accepted 1 July 2016

Abstract

High growth of smartphones and tablets usage has brought enormous rise in the use of newer form of electronic banking - Smart Banking, nowadays. This form of e-banking is suitable for small businessmen or private usage and its usage increases with the rise of popularity of mobile phones with operation systems. Transmitted information is more sensitive and related to financial transactions in e-commerce or communication between the client and the bank. There is an extremely important question of security hidden on the background of these applications. Is the security of distributed Smart Banking applications in Slovakia sufficient? How secure are these applications and which features may influence the security of these applications. The aim of the paper is to analyze the security of Smart Banking applications distributed by Slovak banks. The outcomes of our research are the specifications of parameters which affects the security of these applications. We also suggest a methodology for comparison of Smart banking applications depending on these parameters and for comparison of particular analyzed Smart Banking applications of Slovak banks which are used by the majority of Slovak clients.

Keywords: Smart banking applications, Security settings of smart phones, Criteria of security, Ranking of Slovak smart banking applications, Security coefficient

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

1 Introduction

Nowadays, in times of e-commerce and digital society, electronic banking is a part of everyday life not only in large enterprises, but also for small businesses and individual persons. In addition to the most common known form of direct banking-the Internet Banking, to the forefront gets its mobile equivalent- Smart Banking. This form of electronic banking is more suitable for smaller businesses or individuals that do not require the management of their accounts linked with the enterprise information system, or using this form for information purposes or one-time payments.

The sharp increase of Smart Banking usage is natural and related to the rapid development of smart mobile devices, especially increasingly popular Android operating system, which offers a variety of applications and possibilities. However, behind the convenient application there might be some security issues hidden. Is the internet connection secure in smart devices? Are security settings of our devices adequate? What are the threats of misuse or theft of sensitive data used to access our accounts? Which applications are authentic? Is the application of our bank really safe? How does the change of system settings required by another application during installation affect the current security settings of smart device?

Lots of users are unable to answer these questions. The aim of this paper is to analyze the security of Smart Banking applications in chosen Slovak banks and partly answer these questions. Furthermore, we also want to analyze issues of smart devices' security settings when using Smart Banking applications and specify parameters that affect the security of communication through smart devices when using these applications. The evaluation of these parameters introduce a security coefficient K_b on the basis of which we assess specific Smart Banking applications in the Slovak banks.

2 Development of Smart Banking

The term of mobile banking is however a broader concept and from historical perspective the development of electronic banking forms includes services such as banking via Global System for Mobile Communications (GSM banking), banking via Wireless Application Protocol (WAP banking), banking via Short Message Services (SMS banking), Subscriber Identification Module (SIM) Toolkit banking, etc. The definition of mobile banking can be found in Bucko and Mihók [2] or in Stair and Reynolds [30]. Currently, the mobile form of electronic banking is the most dynamically developing form of banking in the Slovak banks. Its specific form - Smart Banking is called according to the device for which it is intended. With increasing popularity of smartphones and tablets, Smart Banking seems like a convenient solution to handle the necessary transactions and transfer orders.

While using a smart phone, orders for payments or applications for loans can be placed. The development of mobile phones currently contributes to the improvement of other forms of electronic banking services, such as the Internet Banking, in which for example greater security is achieved by sending dynamically generated verification code via SMS.

The number of clients using the direct banking services initially rose slowly. The reason was high cost and lack of trust in these services due to low security perceived by customers [32]. Nevertheless, the number of users' forms of electronic banking since 2005 has increased several times. According to Eurostat, roughly a quarter of the EU population uses electronic banking. The most active in this aspect are the residents of the Scandinavian countries and in the opposite there is the south of Europe, where the percentage of e-banking users is the lowest. The leader in the use of e-banking is Norway. From the post-communist countries, the Baltic States (Lithuania, Latvia and Estonia) are at the forefront of e-banking usage.

Slovakia is in the lead of the V4 countries in electronic banking usage, but within the European Union in 2006 it was at 18th place. In 2014, Slovakia was at 21st place (EUROSTAT - [8]). Electronic banking is used at most in a group of young adults who are already actively using banking services and have experience with information technologies as digital natives [33]. Although traditional contact with the bank branch is still preferred by a significant percentage of the population, we can assume that the importance of traditional banking will gradually decline and will be replaced by electronic communication with the bank.

Client's communication with the bank via mobile banking uses a variety of distribution channels. It might be a communication via SMS, via mobile web or via native client applications. Each distribution channel has its strengths and weaknesses, and it is important to identify the best mode of information exchange for each banking service. According to the (Mobile Marketing Association (MMA) - [22]) the mobile banking distribution channels are compared (Table 1) in terms of usage, availability, security and functionality.

This comparison shows that a client application has the highest functionality and it is the most secure, but it requires active download of the application to the user's mobile phone. On the other hand, SMS distribution channel is the simplest, but it is insecure and has the least functionalities. Naturally, the best combination is to use the combination of distribution channels based on specific needs and activities of a user.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

Table 1: Comparison of mobile banking distribution channels

Type	Incidence	Ease of usage	Availability	Security	Functionality
SMS	5	5	5	2	1
Mobile web	3	3	3	3	4
Native client application	1	4	3	5	5
5 -Very good, 4 - Good, 3 -Average, 2 - Weak, 1- Very weak					

In this contribution, we focus on the evolving form of the direct banking, the Smart Banking, which is based on the existence of an application designed for smart mobile devices such as tablets and advanced (so called *smart*) phones using the Android operating system, Windows Phone, iOS or others.

3 Security of Smart Banking

Nowadays, the usage of smartphones has increased highly. Numerous new smart devices, mostly Android-based phones, revolutionized the market and the problem of smartphone applications' security became very important. Many articles about smartphone security and the potential risks of their usage were published in [17], [19], [20], [29]. Factors include less heterogeneity in operating systems, more penetration of smartphones and a greater incidence of users accepting downloads and sending executable files on mobile devices. It altogether caused that the risk of mobile attacks is much greater [1], [19]. With the increased processing power and memory of mobile devices, increased data transmission capabilities of the mobile phone networks and open with the third-party extensible operating systems, smart devices became an interesting target for the attackers. Many researchers and professionals are expecting a major security incident with mobile devices because of this increase in their performance and usage. Phones became an interesting target for the attackers and many studies have been performed to evaluate the security knowledge of the average user. Most of them show what the already well-known study of Whitten and Tygar [36] found out, that common users are not able to use security mechanisms correctly. The user studies regularly show that security mechanisms are neither understood nor correctly used by most of their users [10], [11]. In addition, some authors propose to embed security in products and in the development process [10] rather than having it stand-alone. Usability heuristics have been developed by Nielsen [24] and Shneiderman and Plaisant [29]. They are a good starting point for usability of security solutions.

Currently, there is no standard approach to the security of mobile banking. This fact is reflected by the diversity of solutions of mobile applications' activations and logging in. Smartphones, tablets and other devices supporting Smart Banking mobile applications are almost always online. They automatically connect to the network if the user does not disable it. These devices include Global Positioning System (GPS) modules and other equipment that may be susceptible to abuse by the attackers. However, the users of mobile banking are expecting at least the same level of application security as provided when using the Internet Banking. High level of security is important for both customers and the banks themselves because the bank is at the risk of losing its good reputation. This is the basis for building the trust in the services it offers, which is a precondition for the bank's successful operation.

The communication between a client and the bank as well as the data must be appropriately protected against interception by the third party. Therefore, it is necessary to provide encryption of the connection. The controlling of the application and data access is equally important. Before disclosure of sensitive information to the client, a certain degree of verification by appropriate combination of user authentication factors must be done. The data must be appropriately protected against unauthorized modification, accidental deletion or damage. It is also important to have an application designed in the way that in the case of device theft or loss the danger to the client and the bank is kept to a minimum. The solution may vary from classical blocking device by the Personal Identification Number (PIN) to biometric security elements.

Mobile banking applications tend to be natively developed for the most market dominant platform (iOS, Android, Windows Phone). The important factor is that the security of the application has a uniform solution for each platform. The basic element of the Smart Banking application's security is authentication, which consist of the checking and verification of the user who is trying to log into the application. Authentication can be based on knowledge of some information, ownership of special authentication element or on the basis of biometric characteristics of the user. When logging into the systems working with sensitive data, these methods combine authentication, and multifactor authentication is used.

In the case of combination of identification and password, and then dynamically generated code (e.g. One Time Password - OTP) delivered and notified by SMS message, we speak about two-factor authentication. This form of authentication is often used in Internet Banking. In the case of Smart Banking as the second factor a mobile phone is used. First, it is necessary to personalize and activate mobile banking via the Internet Banking by the exchange of service key between the bank system and the phone. Also biometrics begin to be used, usually in the form of logging in using fingerprints (e.g. in iPhone 5S) or user identification based on voice (Tatra banka). In the case of IT

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

technologies development and the price reduction, the identification based on DNA (Deoxyribonucleic acid) in mobile devices would be possible.

Another alternative to secure an access to the applications of Smart Banking might be the use of electronic (or digital) signature. However, in the Slovak conditions, unlike in some other EU countries, it remains unapplied for the authorization purposes in the case of mobile banking applications [34].

The SSL (Secure Socket Layer) protocol is used to secure transfer of data between the user and the bank in mobile banking. SSL is cryptographic protocol designed to provide secure communication over a computer network. It creates a secure connection between banking applications and the server of the bank because symmetric cryptography is used to encrypt the transmitted data (3DES (Triple Data Encryption Algorithm), RC4 (Rivest Cipher 4), AES (Advanced Encryption Standard) and others.). The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiation in the beginning of the session (Handshake Protocol). The identity of the communicating parties can be authenticated using the public key cryptography. Message integrity control is ensured by using a hash algorithm (SHA (Secure Hash Algorithm), MD5 (Message Digest 5), etc.). At the present, an improved version of the protocol known by the acronym TLS (Transport Layer Security) is used. The user of a mobile phone is considered as the weakest link in the chain of security. Protecting the mobile phone from malware is just as important as in the case of a computer.

According to Westpac (Site 1), following ten security principles are recommended:

- Use a PIN to access the SIM card
- Lock your device by a password or by drawing a pattern.
- Use antivirus software to protect against malicious software.
- Connect through secure Wi-Fi network that is password protected.
- Turn off Bluetooth and use it only for short time and only with trusted devices.
- Logout from the application correctly.
- Install applications only from the web page of the bank or official application store.
- Regularly update the application and operating system installations.
- Delete all personal data and applications (in the case of sale of a device).
- Conceal personal information, PIN code and identification number.

In compliance with these principles it is possible to reduce the risk of mobile banking misuse to a minimum.

Some of security shortfalls, such as security problems with SMS and GPRS (General Packet Radio Service) protocols and security problems with the current bank's mobile banking solution were discussed in [3]. In [21] there were categorized application phishing attacks in mobile platforms and possible countermeasures and there was shown that personalized security indicators can help the users to detect phishing attacks and have very little deployment cost. The goal of paper [25] was to analyze the customer needs and expectations from the mobile applications' view in order to drive a defined set of requirements. They constructed the quantitative model based on standard operation research methods. In [4] there were presented the recommendations and opportunities for services that will help the users safely and confidently use mobile applications and platforms.

Increase of the security is inversely proportional to the comfort of mobile devices and applications' use. So it is a great challenge for developers of applications to find a solution that would sufficiently secure and also would be easy to use for often less digitally literate users. There is always a tradeoff between security and comfortable usability. The most secured system would be unusable. The users often really prefer simpler and more user friendly checks and procedures of applications, even though they risk losing their money. The level of knowledge and responsible behavior of users is inversely proportional to the need of stronger secure settings. The discussion about usability vs. security was provided in [14], [16], [37].

The security of applications depends on various sets of parameters and there are several points of view to problem of measuring and comparing features of these applications. Very important set of parameters depends on user behavior when using these applications. This point of view was discussed in several researches [28]. The level of user security and responsibility knowledge affects the general security of these applications. Quantification and measuring of such parameters is very difficult and require further research conducted by questionnaire surveys. On

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

the other hand, we can examine the security from the technological point of view. Quantification and measuring require setting up the relevant set of parameters or features of applications and finding the suitable methodology of evaluating these parameters or features. This way the comparison is based on statistical methods, which can help gain representative results of research. Authors of previous researches usually compare security of smartphone platforms [13], [23] or security of communications through communications protocols, encryption and privacy of communications [6]. Researches have proposed static and dynamic security analysis techniques for smartphone applications. Static analysis approaches scale to large numbers of applications, they do not capture runtime environment context such as configuration variables and user input as used in [5], [7]. On the other hand, dynamic analysis to capture runtime environment context, as used by TaintDroid [6]. Dynamic analysis was used for malware forensics or for quick system analysis and strategies to provide automatic code coverage [38]. AppsPlayground application was proposed for brevity, a framework for automated dynamic security analysis of Android applications in [26]. Suitable methods for the measuring of security for Smart Banking applications could be Multi Criteria Decision Making Methods, such as AHP (Analytic hierarchy process), ANP (Analytic network process), SMART (Specific Measurable Achievable Realistic Time), ELECTRE (ELimination Et Choix Traduisant la REalité), PROMETHEE (Preference Ranking Organization METHod for Enrichment of Evaluations). These were previously used in various research papers in the areas of Information technology (IT) security (network security, computing security, date security and information security) but there is a research gap in the field of application security [12].

Our point of view in measuring the security for Smart Banking applications is more specific and suitable for particular Smart Banking applications used in Slovak banks and the specifications of parameters are customized to set of features of such applications. We can merge all threats to one general threat that would mean that unauthorized person wants to use smart device with installation of Smart banking application. We didn´t consider the threat of *man-in-the-middle* attack because all banks have basically the same level of security of communications between the client and the bank. We also didn´t consider, the threats depending on behavior of users, because it's more less individual. We have focused on technical and technological features of compared applications and have specified particular parameters of security. Their descriptions are in chapter 4.

4 Methodology

The analysis of available Smart Banking applications in the Slovak banks was carried out. Based on this analysis, we have identified the parameters that are critical in term of security of the applications. We have considered the parameters in which given applications had partly different values. For example, applications have a different way of how clients log into it, the time after which the client is automatically logged off or amount limits on payments within the application, etc.

The basic method used for evaluation of the analysis and ranking of the applications is the method of multi-criteria decision making. This method is suitable to use in real situations, when the choice, in our case the choice of the safest Smart Banking application, depends on several parameters [9], [18]. Multi-criteria decision making is one of the most well-known branches of decision making. Multi-criteria decision making in general is divided into multi-objective decision making and multi-attribute decision making. The first of them studied continuous decision space, the second one focused on discrete decision space. Multi-criteria decision making methods may be widely diverse and there exists several alternatives, which represent the different choices of action available to the decision maker [31]. Each multi-criteria decision making problem is associated with multiple decision criteria, which may be arranged in hierarchical manner. In some cases different criteria may conflict with each other. Usually different criteria may be associated with different units of measure (this is our case) and it makes the problem hard to solve. Such type of multi-criteria decision making problem requires setting the weights of importance, which are normalized to add up to one. We simplified the situation in our study such that our specified criteria (parameters) are elementary, not multiple and we didn't consider conflicts with each other. Our identified parameters are incommensurable. It is very hard to set weights of importance of these criteria and for precision set of these weights is needed another more detailed research of this area. There are several methods to estimate weights of individual parameters [18]. For our research we chose the principle of scoring method the weights of individual parameters. For every identified parameter we have set scale of states and we have evaluated this scale by number. We have ordered the particular states on the scale from the most secure to the less secure. The most secure state was evaluated by numerical value of 1 and the less secure by 0. The states of the scale were evaluated in regular steps, from range <1, 0>. The overview of values is presented in Table 2.

Further, we used the method of transferring all the values of parameters for expression of single value, which we have called the security coefficient and denoted by symbol K_b. This process requires the computation of weights of individual parameters. We chose the principle of scoring method the weights of individual parameters. The resulting values were calculated according to the known equation (equation 1) [9]. The overview of these calculated values is in Table 4. We subsequently have computed security coefficient K_b as the sum of multiples of the value of individual applications and weights for a given parameter (equation 2). Based on the results, we sorted analyzed applications in order (Table 5) with the intention to express the quality assurance of Smart Banking applications. The quality assurance of applications is assessed to help the users to choose the appropriate application of Smart Banking.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

4.1 Analysis of Smart Banking Security Parameters

Based on the analysis of individual applications and experiences with electronic banking we specified 10 specific parameters and set values from the interval <0.1> of these parameters for individual products of the Slovak banks. Then we sorted applications by calculating the values of the security coefficient K_b. The values of each parameter and the resulting processing and order of the individual applications are indicated in the next part.

For evaluation process of analyzed applications, we have specified the parameters, according to which it is possible to compare these applications. These parameters affect the technological aspects of security. We did not consider other elements and techniques of security that may secondarily increase the security of Smart Banking, but they are not a direct part of the analyzed applications, such as strength-of-password assessment by the application, checking password duplication, keyboard simulations or similar utilities.

The first parameter is the *Activation of application* (P_1). It is the process following the successful installation of Smart Banking application. In this process, the Slovak banks largely use the same client's credentials as in the case of the Internet Banking (PID and password) and subsequent confirmation via SMS code or token. Application of mBank requires from the client to allow the particular device (Smart phone, or Tablet), on which this application is installed and user activation, too. Activation of the application is considered to be a highest level of security, because without the activation code anyone can (with knowledge of credentials to the Internet Banking) use the mobile application. If there is an additional activation provided, application receives the value of *1* for this parameter. On the other hand, *0* is set for this parameter.

Logging into the applications (P_2) can be analyzed through a fingerprint, token (hardware or software), predetermined PIN code (4 to 6 digits), passwords or logins from the Internet Banking (Personal ID + password). Despite the possibility to break fingerprint [15], it is not so easy [27]. The option logging in through a fingerprint is alternative choice for specific applications and we evaluate it by *1*. SMS/Token is more secure than PIN code (static password) [35]. Simple PIN code is less secure, but more secure than nothing. In case of passwords, we do not consider the differences in quality, which depends on user settings. The lists of all possibilities are in Table 2.

An important additional security parameter is represented by *limits of incorrect logins* (P_3). User may insert incorrect login elements 3-5 times in row depending on the application options.

Automatic check out (P_4) is a protective mechanism in case of inactivity. The application uses a variety of settings that range. Time-out is in the range of 1 minute and 20 minutes. Special possibility is to check out automatically when the device's screen darkens depending on user settings.

Most applications of Smart Banking can be *minimized* (P_5). When switching to another application, Smart Banking application waits for the user's return for abovementioned time limit. Two applications (Peňaženka (Prima bank), Platby (SLSP - SLovenská SPoriteľňa) allow user to minimize the application but after returning to the application the client must log in again.

Authorization of payments (P_6) expresses authorization of executed payments. The analyzed applications for authorized payments required use of possible secure elements such as fingerprint, PIN, password or code sent by SMS to the client's phone number. In one particular application (Peňaženka (Prima bank)) it is not necessary to authorize the payment in application, what is considered to be an application's security weakness.

Daily limit (P_7) restricts financial loss to the user in the case of loss or theft of device and invasion of its security features. On the other hand, a daily limit can be certain restriction in respect of the higher amounts payments. Some applications have a monthly limit set, however that is irrelevant in the terms of security. Daily limits may be provided at the level of user account but we focused on additional restrictions of daily limits set specifically for Smart Banking applications. Assuming that Smart Banking is used in transactions with smaller amounts (if necessary to pay higher amounts the user might use the Internet Banking), we have rated with the highest value only the limit up to € 500.

Obfuscating code (P_8) means changing the source code so that it works, but it was unreadable and could not be easily imitated. The use of code obfuscation is considered safer than its absence.

Moving to the card (P_9) allows for example in Android application attribute android: *installLocation* and its value *auto* in the *manifest*. Moving to the SD (Secure Digital) card is recommended only for certain types of applications, because whenever a device is connected to the computer, all running applications on the card are stopped. Also the other applications have access to the data stored on the card, so the possibility of transferring to the card is considered less safe. Analyzed applications have 3 states. The most secure state is represented as no possibility to move application to the SD card and the value of 1 is assigned to this state. The less secure is possibility to move application to SD card and it is represented by value of 0. In the middle, there is possibility to move application to SD card but activation process is required again. Here, the value of 0,5 was assigned.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

Debug mode turned on (P_{10}) represents a risk for applications and at the time of the publication it should be turned off. All our applications analyzed had banned debug mode, so this parameter does not influence the overall ranking in evaluation of analyzed Smart Banking applications, even though we reported it, because from the perspective of applications' security assessment methodologies this parameter is essential.

We set (Table 2) the values $h_{ij} \in \langle 0,1 \rangle$ of each specified parameters states P_i, $i=\{1.2,\ldots,10\}$.

Table 2: Evaluation of specified parameters' states

Parameter	Value					
P_1	yes			No		
	1			0		
P_2	Fingerprint	SMS/Token	Limited Password	Password	PIN	Nothing
	1	0.8	0.6	0.4	0.2	0
P_3	3 trials		4-5 trials		No limit	
	1		0.9		0	
P_4	up to switching off the display	up to 2 min	up to 5 min	up to 10 min	up to 20 min	No limit
	1	0.8	0.6	0.4	0.2	0
P_5	no	yes up to 30 sec	yes up to 1 min	yes up to 2 min	yes up to 20 min	Yes, no limit
	1	0.8	0.6	0.4	0.2	0
P_6	Fingerprint	SMS/Token	Limited Password	Password	PIN	No authoriz.
	1	0.8	0.6	0.4	0.2	0
P_7	up to 500€	up to 1000€	up to 5000€	up to 10000€	up to 50000€	No limit
	1	0.8	0.6	0.4	0.2	0
P_8	yes			no		
	1			0		
P_9	no	yes, with reactivation process			yes	
	1	0.5			0	
P_{10}	no			yes		
	1			0		

4.2 Analysis of Smart Banking Applications in Slovak Bank Sector

Based on the specified parameters and the determination of their values, we analyzed Smart Banking applications in following banks in Slovakia: ČSOB (ČeskoSlovenská Obchodná Banka) (KBC Group (Kredietbank ABB Insurance CERA Bank)), SLSP (ERSTE Bank (Erste Deutsche Walfang Gesellschaft)), VUB (Všeobecná Úverová Banka) and Unicredit Bank Slovakia (Intesa Sanpaolo Group), Tatra banka and ZUNO (Raiffeisen Bank), mBank (Commerzbank), FIO (Financing and Insurance Operations) bank (FIO Financial Group), Sberbank (Sberbank of Russia) and Prima bank (Penta Investments). Selected banks belong to the most popular banks in Slovakia and possess cover the majority of Slovak banking market. Each Slovak bank is a part of international banking group that operates mainly in EU countries and at the same time they offer analyzed form of electronic banking. These banks are based in Slovakia but have foreign owners (as mentioned above). We omitted the applications of *Poštová banka* and *Slovenská sporiteľňa* because these provide only passive banking. World-renowned banks, such as CGB (Coconut Grove Bank), CA (Crédit Agricole bank), Satander or Nordic banks do not operate on Slovak market, so their Smart Banking applications are not used despite they belong to leaders among providers of this particular service with high level of security. Detailed values for different applications of compared banks are shown in the survey table (Table 3).

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

Table 3: Smart banking applications and values of investigated parameters

	Activation	Logging in	Limit of logins	Automatic check out	Minimization of application	Authorization	Daily / monthly limit	Code obfuscation	Moving to the card	Debug mode turned on
Smartbanking (ČSOB)	Yes	PIN	3	5 min	Yes, waits1 min	SMS/Token	10 000€ / 68000 €	Yes	Yes	No
mBank Slovakia	Yes	PIN/fingerprint*	3	20 min	Yes	PIN	50€ /3 payments/ 1500€	Yes	Yes	No
Fio banka	Yes	PID+password IB/fingerprint*	5	By user settings	Yes	PIN/fingerprint*	none / none	Yes	Yes	No
Tatra banka	Yes	PIN	3	2 min	Yes, waits 2 min	PIN/Token	3000€ / 30000€	No	Yes with reactiv	No
VUB Mobil Banking	Yes	PIN/fingerprint*	5	5 min	Yes	SMS/Token	50 000€ / none	Yes	Yes	No
BankAir (UniCredit)	Yes	PIN/hardware token	3	3 min	Yes	None	3300€ / none	Yes	Yes	No
Zuno SK	Yes	PIN	5	5 min	Yes	PIN	1000€ / 30000€	Yes	No	No
Peňaženka (Prima banka)	Yes	Password	3	until display turns off	No	None	1000€ / 30000€	No	No	No
SmartBanking (Sberbank)	Yes	3 month limited password	3	1 min	Yes waits 30 seconds	3 month limited password	1000€ / 28000€	No	No	No
Platby (SLSP)	Yes	PIN	3	until display turns off	No	SMS, GRID	none / 170000€	No	No	No

* - Option fingerprint is available only for iPhone 5S, 6 and 6 Plus with iOS 8.1.1. for Androids devices, it is available for selected smartphone models of Samsung.

5 Evaluation of Analyzed Applications - Security Coefficient Kb

To evaluate the security of individual applications analyzed and selected order we chose a standard method of multi-criteria evaluation. Based on the setting of values range h_j for the different parameters, we calculated their weights v_{P_i} as a proportion of the variability of individual parameters and the sum of the variances of these parameters.

$$v_{P_i} = \frac{V_{P_i}}{\sum_i^j V_{P_i}}, \text{ for j = 1,2, ... ,10.,} \quad (1)$$

Where V_{P_i} is the coefficient of variation of the i-th parameter calculated as a ratio of standard deviation σ_i, of *i*-th parameter and the arithmetic average achieved values for parameter k_i. Weights of these parameters were calculated as follows:

Table 4: Calculated weights of specified parameters

Parameter	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
Weight v_{P_i}	0	0.1196	0.0099	0.0649	0.2121	0.1046	0.1261	0.1589	0.204	0

On the basis of individual parameters and calculated weights for each individual parameter we set the security coefficient K_b, as the sum of multiples of the value of individual applications and weights for a given parameter:

$$K_b = \sum_{1=1}^{10} v_{P_i} * h_{ij} \text{ for j = 1,2, ... ,10.,} \quad (2)$$

where h_{ij}, is a value of *i*-th parameter for *j*-th evaluated application.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 12 / ISSUE 1 / JANUARY 2017 / 42-52

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

The calculated factor of security is compared to the individual application and the ranking in terms of the coefficient is created (Table 5).

Table 5: Ranking of evaluated applications according to the coefficient value

Smart banking application	Security coefficient K_b	Final rank
SmartBanking (Sberbank)	0,6699	1
Peňaženka (Prima banka)	0,6396	2
Platby (SLSP)	0,5984	3
Zuno SK	0,5564	4
Smartbanking (ČSOB)	0,493	5
BankAir (Unikredit)	0,4627	6
Fio banka	0,4568	7
mBank SK	0,4484	8
VUB Mobil Banking	0,4352	9
Tatra banka	0,4319	10

6 Conclusion

This objective of this article was to compare and evaluate 10 Smart Banking applications provided by Slovak banks. The main aim of the article was to specify several parameters of Smart Banking applications that affect the security level of these applications. We have proposed a simple method for measuring the level of security of the Smart Banking applications based on evaluation of the parameters. The presented proposal is the first attempt to quantify the level of security of applications of that type in order to compare their quality from technological security point of view. We did not focus on the principles of user's behavior and its impact on the complex security when using Smart Banking. Our comparison is focused on Slovak banks and it is useful for clients of Slovak banks who are interested in security of Smart Banking applications. It can help them choose the more secure application. It can also help users decide how these applications are used. It would be interesting to use our proposed method of measuring the security of Smart Banking applications based on previous studied parameters in other countries and compare the results. The most secure application from this point of view is Smart Banking of Sberbank with security coefficient of K_b = 0,67. It would be interesting to compare this result with applications of world-renowned banks.

The final evaluation and a detailed overview of the evaluation of applications are shown in the Table 3. Based on the analysis of each application, we specified parameters that affect the security of these applications. We set the value of individual states of specified parameters, defined and calculated coefficient of security K_b. We quantified the weights of specified criteria by multi-criteria evaluation method (Table 4). By using the calculated index security, we ranked all of the analyzed applications from the safest to least safe (Table 5). All applications after their installation in Smart Phone require process of activation. The activation process is executed through Internet banking of particular bank. Logging into the application is implemented mostly via PIN or password, but in three applications, the client can log into with biometry fingerprints. For some clients, this method is inconvenient; on the other hand, the login via simple PIN is practical, but less secure. Payments in one of evaluated application don't have to be authorized, so it reduces the level of security and safety again. In combination with a long time limit to automatic sign off when user is inactive, it could be very dangerous. In the case of application Peňaženka (Prima bank), it was not the security issue because the application is not allowed to minimize and when display turns off the user is automatically logged out.

In case of Unikredit bank, Fio bank, mBank, VUB and Zuno (Slovakia) bank Smart Banking, the application can be minimized. These applications logged off automatically after particular time period. This in case of lost or stolen phone while banking application is still logged in, this might result in possible abuse. Obfuscation of source code at least partly avoids the possibility that potential attacker identifies possible weaknesses and shortcomings in the application and should therefore be used in all applications. However, it is not applied in the four examined applications. The banks with applications with security coefficient K_b below 50% should analyze why it reached a lower score and take steps to its increase. The development of Smart Banking applications is very quick and progressive. Banks include new secure methods and secure elements on day-to-day basis. Analysis of Smart Banking applications in Slovakia was two times updated during preparation of this paper. During this period, all banks have included activation process of applications. Some of them have started to use biometric fingerprint, daily limits were decreased and time of inactivity was set to the shorter period.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

Websites List

Site 1: Westpac, Mobile Banking - Top 10 mobile security tips
http://www.westpac.com.au/security/how-to-protect-yourself/mobile-banking-security/

References

[1] M. Becher, C. Felix, J. Hoffmann, T. Holz, S. Uellenbeck, and CH. Wolf, Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices, in Proceedings IEEE Symposium on Security and Privacy, Barkeley, CA, 2011, pp. 96-111.
[2] J. Bucko and P. Mihók, Elektronické Služby v Bankovníctve. Košice. Košice : Technical University of Košice, 2008.
[3] K. Chikomo, M.K. Chong, A. Arnab, and A. Hutchison. (2006, November) Security of mobile banking. University of Cape Town, South Africa, Tech. Rep. [Online]. Available: http://pubs.cs.uct.ac.za/archive/00000347/01/Security_of_Mobile_Banking_paper.pdf.
[4] E. Chin, P. A. Felt, V. Sekar, and D. Wagner, Measuring user confidence in smartphone security and privacy, in Proceedings Eighth Symposium On Usable Privacy and Security SOUPS, Washington, DC, 2012, pp. 1-16.
[5] M. Egele, Ch. Kruegel, E. Kirda, and G. Vigna, PiOS: Detecting privacy leaks in iOS applications, in Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, 2011, pp. 1-15.
[6] W. Enck, P. Gilbert, B. P. Chun, L. Cox, J. Jung, P. N. McDaniel, and A. Sheth, TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones, in Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), Vancouver, BC, 2010, pp. 393-408.
[7] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, A study of android application security, in Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, 2011, pp. 315-330.
[8] Eurostat. (2015, September) Individuals using the internet for internet banking (Table). Eurostat. [Online]. Available:http://ec.europa.eu/eurostat/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tin00099&language=en
[9] P. Fiala, J. Jablonský and M. Maňas, Modely a Metody Rozhodování. Praha: Nakladatelství Oeconomica, 2008.
[10] S. Furnell, Making security usable: Are things improving? Computers & Security, vol. 26, no. 6, pp. 434-443, 2007.
[11] S. Furnell, et al.: The challenges of understanding and using security: A survey of end-users, Computers & Security, vol. 25, no. 1, pp. 27-35, 2006.
[12] P.K. Gade and M. Osuri, Evaluation of multicritera decission making methods for potential use in application security, M. S. Thesis Electrical Enginnering, School of Computing Blekinge Institute of Technology ,Karlskrona, Sweden, 2014.
[13] J. Han, et al., Comparing mobile privacy protection through cross-platform applications, in Proceedings 20th Annual Network & Distributed System Security Symposium (NDSS 2013), San Diego, USA, 2013, [Online]. Available at: http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=2697&context=sis_research
[14] A. Josang and G. Sanderud, Security in mobile communications: Challenges and opportunities, in Proceedings of the Australasian Information Security Workshop Conference on ACSW frontiers, 2003, pp. 43-48.
[15] Y.H. Jo, S.Y. Jeon, J.H. Im, and M.K. Lee. (2016) Security analysis and improvement of fingerprint authentication for smartphones. Hindawi. [Online]. Available at: http://dx.doi.org/10.1155/2016/8973828.
[16] A. Josang, M.A. Zomai and S. Suriadi, Usability and privacy in identity management architectures, ACSW '07, in Proceedings of the Fifth Australasian Symposium on ACSW Frontiers, Australian Computer Society, Inc., Darlinghurst, Australia, Australia, 2007, pp. 143-152.
[17] J. Kleinberg, The wireless epidemic, Nature, vol. 449, no. 20, 2007.
[18] K. Kočišová, Multi-criteria evaluation of mortages. (2014) Aplikácie informačných technológií. E.S.R. [Online]. Available: http://www.e-s-r.org/sites/default/files/archive_ita/2014-02_articles_ita.pdf.
[19] P. Kuper, The state of security, IEEE Security & Privacy, vol. 3, no. 5, pp. 51-53, 2005.
[20] N. Leavitt, Mobile phones: The next frontier for hackers?, IEEE Computer, vol. 38, no. 4, pp. 20-23, 2005.
[21] C. Marforio, M.R. Jayaram, C. Soriente, K. Kostiainen, and S. Capkun. (2015) Personalized security indicators to detect application phishing attacks in mobile platforms, CoRR, abs/1502.06824, 2015. DBLP. [Online]. Available: http://dblp.uni-trier.de/rec/bib/journals/corr/MarforioMSKC15
[22] MMA-Mobile. (2009, January) Marketing Association: Mobile Banking Overview (NA). Mmglobal. [Online]. Available: www.mmaglobal.com/files/mbankingoverview.pdf
[23] R.M. Nabi, R.A. Mohammed and R.M. Nabi, Smartphones platform security a comparison study, International Journal, vol. 5, no.11, 2015.
[24] J. Nielsen. (1995, January) Ten usability heuristics. Useit. [Online]. Available: http://www.useit.com/papers/heuristic/heuristic list.html
[25] K. Pousttchi and M. Schurig, Assessment of today's mobile banking applications from the view of customer requirements, in Proceedings System Sciences, 2004, of the 37th Annual Hawaii International Conference on, Big Island, Hawaii, 2004, pp. 10.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762017000100004

[26] V. Rastogi, Y. Chen and W. Enck, Appsplayground: Automatic security analysis of smartphone applications, in Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, TX, 2013.
[27] M. Roger. (2014, September) Why I hacked touchID (again) and still think it's awesome. Lookout. [Online]. Available: https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/.
[28] S. Rosen, Z. Qian and Z.M. Mao, Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users, in Proceedings of the third ACM Conference on Data and Application Security and Privacy. ACM, 2013, pp. 221-223.
[29] B. Shneiderman and C. Plaisant, Designing the User Interface: Strategies for Effective Human-Computer Interaction, 4th ed. Pearson Addison Wesley, 2004.
[30] R.M. Stair and G.W. Reynolds, Principles of Information Systems. 9. Vydanie Boston: Cengage Learning, 2010.
[31] E. Triantaphyllou, Multi-criteria Decision Making Methods: A Comparative Study. Dordrecht, The Netherlands: Kluwer Academic Publishers, 2000.
[32] M. Vejačka, Customer acceptance of electronic banking: Evidence from Slovakia, Journal of Applied Economic Sciences, vol. 9, no. 3, pp. 514-522, 2014.
[33] M. Vejačka, Electronic banking acceptance among young adult internet users in Slovakia, Journal of Economy, Business and Financing, vol. 1, no. 1, pp. 1-7, 2013.
[34] M. Vejačka, Utilization of electronic signature in Slovak banks, ICTIC 2013, in Proceedings in Conference of Informatics and Management Sciences: The 2nd International Conference, Žilina, EDIS, 2013, pp. 200-204.
[35] S.C. Weir, G. Douglas, T. Richardson, and M. Jack, Usable security: User preferences for authentication methods in eBanking and the effects of experience, Interacting with Computers, vol. 22, no. 3, pp. 153-164, 2010.
[36] A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, in USENIX Security Symposium, 1999.
[37] M. Wu, S. Garfinkel and R. Miller. (2004, July) Secure web authentication with mobile phones. Dimacs. [Online]. Available: http://dimacs.rutgers.edu/Workshops/Tools/abstract-wu-garfinkel-miller.pdf.
[38] L-K Yan and H. Yin, DroidScope. (2009, April) Seamlessly reconstructing the OS and dalvik. ACM. [Online]. Available: http://portal.acm.org/citation.cfm?id=1558977.1558997.