Measurement of security of Smart banking applications – index of security

Jozef Bucko

Abstract:

Effective use of electronic communication is based on trust, which is built between communicating parties. A necessary condition for the formation of trust is a technology security of communication channels and experience, which is based on experience and knowledge of a communication environment and resources that mediate this communication. These general facts hold stronger if the transmitted information are more sensitive and are related to financial transactions in e-commerce or communications between the client and the bank. High growth of use of smart phones and tablets has been recorded in the use of new form of electronic banking – Smart banking, nowadays. Measure of level of security of such applications for suggested criteria and their comparison within the Slovak banks is subject of our paper.

Key words:

Smart banking, security, criteria of security, index of security, security recommendation

ACM Computing Classification System

*• **Information systems** ∼ **Online banking** • **Information systems** ∼ Secure online transactions • Security and privacy ∼ Mobile platform security • Security and privacy ∼ Mobile and wireless security*

Úvod

V súčasnej dobe elektronického obchodovania a digitálnej spoločnosti je elektronické bankovníctvo každodennou súčasťou nie len veľkých podnikateľských subjektov, ale aj malých živnostníkov a bežných súkromných osôb. Popri najbežnejšej známej forme priameho bankovníctva – Internet bankingu, sa do popredia dostáva jeho mobilná forma – Smart banking. Táto forma elektronického bankovníctva je svojím charakterom vhodnejšia pre menších podnikateľov, alebo súkromné osoby, ktoré nepožadujú prepojenie správy svojich účtov s firemným informačným systémom, alebo využívajú túto formu na informatívne účely, prípadne jednorazové platby. Prudký nárast používania tejto aplikácie je prirodzený a súvisí s prudkým rozvojom mobilných smart zariadení, najmä s čoraz populárnejším operačným systémom Android, ktorý ponúka množstvo aplikácií a možností. Na pozadí pohodlnej aplikácie sa však ukrýva rovnako aktuálna otázka bezpečnosti. Je internetové pripojenie smart zariadenia bezpečné? Je bezpečnostné nastavenie nášho zariadenia dostatočné? Aké sú hrozby zneužitia, alebo odcudzenia citlivých údajov, ktoré pri prístupe k svojim účtom používame? Ktoré aplikácie sú pravé? Aplikácia banky, v ktorej máme účet je naozaj bezpečná? Ako zmena nastavenia systému požadovaná inou aplikáciou pri inštalácií ovplyvní

aktuálne bezpečnostné nastavenie smart zariadenia? Množstvo používateľov nedokáže odpovedať na tieto otázky. Cieľom nášho príspevku je analyzovať bezpečnosť Smart bankingu na Slovensku a čiastočne odpovedať na stanovené otázky. Analyzovať problematiku bezpečnostného nastavenia smart zariadení pri používaní Smart bankingu a špecifikovať parametre, ktoré ovplyvňujú bezpečnosť komunikácie cez smart zariadenia pri používaní tejto aplikácie. Hodnotením týchto parametrov zavedieme koeficient bezpečnosti Kb na základe ktorého ohodnotíme konkrétne aplikácie Smart bankingu v slovenských bankách.

1 Vývoj Smart bankingu

V súčasnej dobe je Smart banking najdynamickejšie sa rozvíjajúcou formou elektronického bankovníctva v slovenských bankách. S narastajúcou obľubou smartfónov a tabletov sa Smart banking javí ako pohodlné riešenie pre vybavovanie potrebných transakcií či príkazov. Klienti sa nemusia nachádzať fyzicky v banke a predsa s ňou komunikujú. Je možné zadávať príkazy k platbe na iný účet, prijímať peňažné prostriedky na svoj účet či žiadajú o pôžičky. To všetko sa dá zabezpečiť cez Internet, stačí len vhodné zariadenie, počítač, notebook či mobilný telefón. Ak komunikácia s bankou prebieha prostredníctvom mobilného telefónu, môžeme hovoriť o mobilnom bankovníctve (Bucko, 2008).

Na Slovensku sa elektronické bankovníctvo začalo rozvíjať v 90. rokoch 20. storočia, keď viaceré banky na Slovensku začali poskytovať tieto služby a prvou formou sa stal Homebanking. Slovensko sa pomerne rýchlo dostalo v tejto oblasti na úroveň okolitých krajín. Dôvodom bola konkurencia bánk, príliv moderných už overených technológií zo zahraničia, ale čiastočne aj mentalita používateľov, vďaka ktorej elektronické bankovníctvo na Slovensku patrí medzi najlepšie zabezpečené systémy. Jednou z prvých bánk, ktoré na Slovensku začali ponúkať služby elektronického bankovníctva, bola Poľnobanka[1)]. Služba svojou finančnou náročnosťou bola určená hlavne pre firemných klientov. Pre súkromné osoby a drobných podnikateľov boli náklady príliš vysoké. Aj napriek tejto skutočnosti bol hlavným dôvodom rozvoja tejto služby väčší komfort. Z rozvojom foriem elektronického bankovníctva sa väčšina inovácií sústredila na pohodlie klientov, ale najmä bezpečnosť (zmena šifrovacích algoritmov, zlepšenie autentifikácie klientov, zavedenie GRID kariet). Práve kvalita používanie služby elektronického bankovníctva úzko súvisí s rovnováhou medzi týmito položkami. Prílišný komfort služby ide často na úkor bezpečnosti a príliš mnoho zabezpečovacích prvkov systému elektronického bankovníctva znižovali jeho komfortné použitie. S rastúcou dostupnosťou mobilných telefónov na Slovensku začali banky prirodzene s ich využívaním aj v tejto oblasti. Rozvoj mobilných telefón súčasne dobe prispieva aj k zvyšovaniu bezpečnosti iných foriem elektronického bankovníctva, akou je Internet banking, v ktorom sa teší veľkej obľube zasielanie overovacích kódov prostredníctvom SMS správ (Grajcar, 2012).

Počet klientov využívajúcich služby priameho bankovníctva spočiatku stúpal iba pozvoľna (Tabuľka č.1), pretože stále boli poplatky veľmi vysoké a negatívne vplývala nedôvera v tieto služby z dôvodu nízkeho zabezpečenia a malého povedomia týchto služieb. Napriek tomu počet používateľov napr. služby Internet banking od roku 2005 vzrástol na štvornásobok.

Tabuľka 1: Nárast počtu používateľov služby internet banking

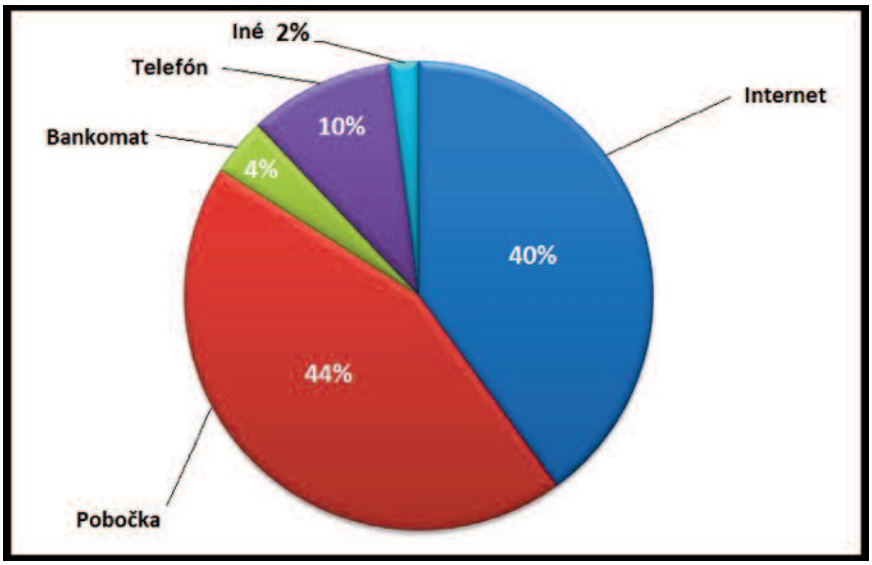
	2005	2006	2007	2010	2011	2012
Počet používateľov služby internet banking	10 %	13 %	15 %	30 %	34 %	40 %

Zdroj: SITA (SITA, 2012), Tlačová správa (Sagálová, 2011)

1) Poľnobanka – v roku 2002 zmenila názov na Unibanku a neskôr na Unicredit Bank

Podľa Eurostatu[2)] využíva elektronické bankovníctvo približne štvrtina obyvateľov Európskej únie. Najaktívnejší sú v tomto smere obyvatelia škandinávskych krajín, presne naopak je to na juhu Európy. Najvyššie využívanie priameho bankovníctva vykazuje Nórsko. Z krajín východnej Európy vynikajú pobaltské štáty Litva, Lotyšsko a Estónsko. Slovensko je na čele krajín V4, ale v Európskej únii mu patrí až 18. miesto (Kováčik, 2009).

Banky v Slovenskej Republike aj po celom svete sa snažia prispôsobiť novým trendom v smerovaní vzťahu banka-klient. Ide najmä o obmedzovanie návštev klienta akejkoľvek pobočky banky, a tak sa rozhodli o značnú podporu pre rozvoj produktov elektronického bankovníctva. Aj keď tradičný kontakt s bankou na pobočke stále preferuje značná časť populácie viac než novšie formy (viď Obr. 1) môžeme predpokladať, že jej význam bude postupne klesať a nahradí ju komunikácia z bankou cez internet (Horný, 2006).



Obrázok 1: *Uprednostňovaný spôsob kontaktu s bankou za rok 2012.*
Zdroj: Éra multikanálového bankovnictví na startu (Horný, 2006)

V klasifikácií foriem elektronického bankovníctva (Bucko, Mihók, 2008), patrí Smart banking k mobilným formám elektronického bankovníctva. Pojem Mobil banking je však širším pojmom a z historického hľadiska a vývoja foriem elektronického bankovníctva zahŕňa služby ako GSM bankovníctvo, WAP bankovníctvo, SMS bankovníctvo, SIM Toolkit bankovníctvo a pod. S vymedzením pojmu mobilné bankovníctvo sa môžeme stretnúť v (Bucko, Mihók, 2008, Stair, 2010). Najvšeobecnejšia definícia hovorí o mobilnom bankovníctve, ako o forme priameho bankovníctva, ktorou prostredníctvom mobilného telefónu klient môže spravovať svoj účet v danej banke. V slovenskej republike z pohľadu tejto definície ponúka plnohodnotné mobilné bankovníctvo šesť bánk, neplnohodnotné mobilné bankovníctvo ponúka jedna banka a šesť bánk ho neponúka vôbec.

Komunikácia klienta s bankou prostredníctvom mobilného bankovníctva používa rôzne distribučné kanály. Jedná sa o komunikáciu prostredníctvom SMS, prostredníctvom mobilného webu, alebo prostredníctvom natívnych klientskych aplikácií. Každý distribučný kanál má svoje silné a slabé stránky, a je dôležité identifikovať najvhodnejší režim príjmu informácii pre každú bankovú službu. Tabuľka č. 2 nám poskytuje prehľadné porovnanie týchto kanálov (MMA, 2009):

2) Eurostat - Štatistický úrad Európskeho spoločenstva

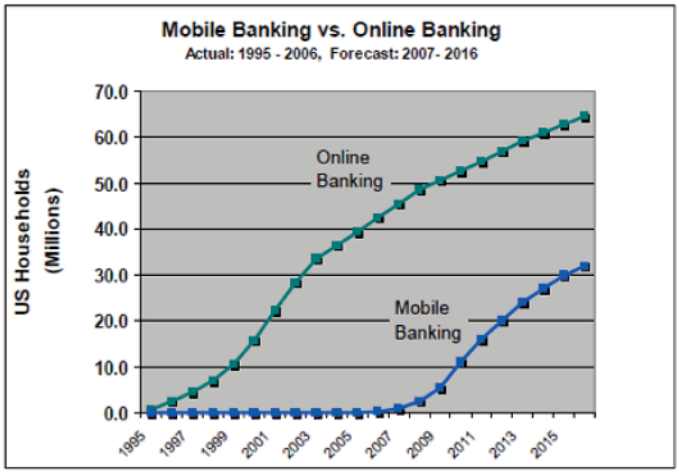
Tabuľka 2: Porovnanie distribučných kanálov mobilného bankovníctva (MMA, 2009)

Typ	Všeobecný výskyt	Jednoduchosť používania	Dostupnosť	Bezpečnosť	Funkcionalita
SMS	5	5	5	2	1
Mobilný web	3	3	3	3	4
Natívna klientska aplikácia	1	4	3	5	5
5 – Veľmi dobre, 4 – Dobre, 3 –Priemerné, 2 – Slabé, 1 – Veľmi slabé					

Zdroj: Mobile Banking Overview (MMA, 2009)

Teda distribučný kanál realizovaný SMS je dostupný všade, na každom mobilnom telefónnom zariadení, ľahko sa používa, ale má limitovanú funkcionalitu. SMS je ideálne médium pre upozornenia, notifikácie a zákaznícky orientované transakcie. Mobilný web poskytuje vyššiu funkcionalitu, ale vyžaduje na prístup špecifické mobilné zariadenie. Natívna klientska aplikácia poskytuje najvyššiu funkcionalitu, je najbezpečnejšia, ale vyžaduje aby si užívateľ stiahol aplikáciu do svojho telefónu. Je prirodzené, že najvhodnejšie je používanie kombinácie distribučných kanálov na základe konkrétnych požiadaviek a činností.

V našom príspevku sme sa zamerali na rozvíjajúcu sa formu priameho bankovníctva, Smart banking, ktorá je založená na existencii aplikácie určenej pre mobilné smart zariadenia, akými sú tablety a moderné telefóny používajúce operačný systém Android, Windows Phone, alebo iOS. Táto forma elektronického bankovníctva zaznamenáva progres, ktorý je možné porovnať s progresom využívania Internet bankingu. Priebeh nárastu používateľov týchto foriem elektronického bankovníctva od roku 1995 a predpoveď do roku 2016 znázorňuje nasledujúci graf (MMA, 2009).



Obrázok 2: *Porovnanie nárastu používateľov s predpovedaným vývojom (MMA, 2009)*
Zdroj: Mobile Banking Overview (MMA, 2009)

2 Bezpečnosť Smart bankingu

O bezpečnosť pri používaní mobilného bankovníctva pretrvávajú značné obavy. V súčasnosti neexistuje štandardný prístup k bezpečnosti pri mobilnom bankovníctve, čo sa prejavuje rôznorodosťou riešenia aktivácie mobilnej aplikácie a prihlasovania sa do nej. Prenosné zariadenia,

akými sú chytré telefóny (smartphon), tablety a zariadenia, pre ktoré sú dané mobilné aplikácie určené, sú takmer stále on-line, automaticky sa prihlasujú na sieť, pokiaľ im to používateľ nezakáže, obsahujú senzory GPS a ďalšie vybavenie, ktoré môže byť náchylné k zneužitiu šikovným útočníkom. Používatelia mobilného bankovníctva pri tom očakávajú minimálne takú úroveň zabezpečenia aplikácie, aká je pri používaní príbuzného Internet bankingu. Vysoká úroveň bezpečnosti je dôležitá ako pre klientov, tak aj pre samotnú banku, pretože okrem zneužitia a reálnej krádeže je v ohrození povesť banky, ktorá je základom pri budovaní dôvery v služby, ktoré ponúka, čo je pre banku podmienkou existencie. Zabezpečený musí byť prenos údajov – vhodne chránený pred odchytením treťou osobou, preto je nevyhnutné zabezpečiť šifrovanú komunikáciu medzi klientom a bankou. Rovnako dôležité je, aby bola kontrolovaná aplikácia a prístup k dátam, pred sprístupnením citlivých informácií klientovi musí prebehnúť istý stupeň verifikácie používateľa vhodnou kombináciou autentifikačných faktorov. Údaje musia byť vhodné ochránené pred neoprávnenou modifikáciou, neúmyselným zmazaním, alebo poškodením. Dôležité je aj mať aplikáciu navrhnutú tak, aby v prípade straty zariadenia, možnosť ohrozenia klienta a banky bola čo najnižšia. Riešením môže byť od klasického blokovania zariadenia PINom, až po zabezpečenie biometrickým bezpečnostným prvkom (Dvořák, 2013).

Aplikácie mobilného bankovníctva bývajú zvyčajne natívne, napísané pre každú platformu zvlášť (iOS, Android, Windows Phone), pretože multiplatformové frameworky sa neosvedčili. Dôležitým faktorom je, aby bezpečnosť aplikácie bola pre každú platformu riešenia jednotne. Bezpečnostné prvky sú zvyčajne kódované v programovacom jazyku Objective-C (iOS) a v programovacom jazyku Java (Android) (Dvořák, 2013).

Základným prvkom bezpečnosti Smart banking aplikácií je autentifikácia, ktorej procesom je postup kontroly a overenia používateľa, ktorý sa snaží do aplikácie prihlásiť. Autentifikácia môže byť na základe znalosti nejakej informácie, vlastníctva špeciálneho autentifikačného predmetu, alebo na základe biometrických vlastnosti používateľa. Vo väčšine systémov bez požiadaviek kritickej bezpečnosti sa používa len prvý spôsob s využitím identifikačnej informácie a hesla. V prípade prihlasovania sa do systémov pracujúcich s citlivými údajmi sa tieto spôsoby autentifikácie kombinujú a používa sa viacfaktorová autentifikácia. V prípade kombinácia identifikácie a hesla a následne OTP[3)] kódu doručeného prostredníctvom SMS správy ide o dvojfaktorovú autentifikáciu, často využívanú v Internet bankingu. V prípade Smart bankingu sa ako druhý faktor využíva mobilný telefón. Ten je potrebné najprv personalizovať, aktivovať mobilné bankovníctvo cez službu Internet banking výmenou kľúčov medzi bankov a telefónom.

Rovnako, ako problém bezpečnej identifikácie a autentifikácie je dôležitý problém bezpečného prenosu údajov medzi používateľom a bankou. Na tento účel sa v mobilnom bankovníctve využíva protokol SSL (Secure Socket Layer). SSL Protokol poskytuje zabezpečenie komunikácie pomocou šifrovania a autentizácie oboch komunikujúcich strán. Jedná sa o protokol ktorý v našom prípade vytvára zabezpečené pripojenie medzi bankovou aplikáciou a serverom banky. Skladá sa z protokolov – SSL Record protocol a SSL Handshake protokol a funguje na princípe asymetrického šifrovania, kde každá z komunikujúcich strán má dvojicu šifrovacích kľúčov, verejný a súkromný. Na výmenu týchto kľúčov sa využíva najčastejšie algoritmus RSA alebo Diffie-Hellman. Pre šifrovanie samotných dát tu využívajú symetrické šifry (3DES, RC4 , AES a i.). Kontrolu integrity správ zabezpečuje kontrola pomocou hash algoritmov (SHA, MD5, ...). V súčasnosti sa využíva vylepšená verzia tohto protokolu známa pod skratkou TLS. Problém overenia platnosti používateľa, prenos citlivých údajov je dobre rozvinutý a riziko prelomenia „hrubou“ silou je menej pravdepodobný, ako útok na samotného používateľa a jeho návyky. Za najslabší článok v reťazi bezpečnosti je považovaný samotný používateľ mobilného telefónu. Ochrana mobilného telefónu

2) OTP – One Time Password – Jednorazové dočasné heslo

pred škodlivým softvérom je rovnako dôležitá ako v prípade počítača. Podľa (Westpac, 2013) sa odporúča používať tzv. bezpečnostné desatoro):

- Používať PIN pre prístup k SIM karte
- Uzamknúť svoje zariadenie – chrániť svoje osobné dáta heslom alebo nakreslením vzoru.
- Používať Antivírusový softvér – ten ochráni mobilné zariadenie pred škodlivým softvérom.
- Pripájať sa cez zabezpečené wifi – nepoužívať verejné wifi pripojenie ale použiť iba dôveryhodnú wifi sieť chránenú heslom.
- Vypínať Bluetooth – používať iba počas reálneho využívania a len pre dôveryhodné zariadenia.
- Odhlasovať sa korektne z aplikácie.
- Inštalovať aplikácie iba z web stránky banky alebo oficiálneho obchodu.
- Pravidelne aktualizovať aplikáciu alebo operačný systém kedykoľvek je to možné.
- Odstrániť osobné údaje – Zabezpečiť zmazanie údajov a aplikácií (napr. v prípade predaja mobilného zariadenia).
- Utajovať osobné informácie – žiadosti o PIN kód alebo identifikačné číslo je potrebné ignorovať.

Dodržiavaním týchto doporučení zvyšuje bezpečnosť používania mobilného bankovníctva a znižuje riziko jeho zneužitia. Budúcnosť vidíme v najnovších trendoch v oblasti IT technológie. Udomácňovať sa začína biometria, najčastejšie prihlasovanie sa pomocou odtlačkov prsta (iPhone 5S) či identifikácia užívateľa na základe hlasu (Tatra banka). V prípade rozvoja IT technológií a znižovania ich cien je možné využitie identifikácie na základe DNA už v bežných mobilných zariadení. Zvýšenie bezpečnosti je nepriamo úmerne komfortnosti používania mobilných zariadení a aplikácií, preto je veľkou výzvou pre tvorcov aplikácií nájsť také riešenie, ktoré by bolo dostatočne bezpečné a zároveň ľahko použiteľné aj pre bežných často menej IT zdatných používateľov.

3 Analýza parametrov bezpečnosti Smart bankingu v SR

Cieľom nášho príspevku je porovnanie Smart banking aplikácií slovenských bánk. Každá aplikácia má rozdielny spôsob akým sa aktivuje, ako sa do nej klienti prihlasujú, dobu po ktorej klienta automaticky odhlási či limity na platby prostredníctvom tejto aplikácie. Na základe tejto skutočnosti sme špecifikovali 10 konkrétnych parametrov a skúmali sme ich hodnoty pre 10 rôznych aplikácií Smart bankingu v slovenských bankách. V tejto analýze sme tieto parametre identifikovali, porovnali a vyhodnotili v prehľadovej tabuľke. Jedna sa aplikácie ČSOB, SLSP, VÚB, ZUNO, mBank, FIO banky, Tatra banky, Prima banky, Sberbank Slovensko a UniCredit Bank. Neuvažovali sme s aplikáciou Pošta a banka od Poštovej banky a Účty od Slovenskej Sporiteľne pretože tieto aplikácie poskytujú iba pasívne bankovníctvo.

3.1 Analyzované parametre

Pre proces hodnotenia analyzovaných aplikácií sme vyšpecifikovali nasledujúce kritéria. Tie sme pre ďalšie spracovanie s účelom zoradiť aplikácie na základe splnenia daných kritérií označili indexmi k1 až k10 (Polák, 20014).

- Aktivácia aplikácie k_1
- Prihlásenie do aplikácie k_2
- Počet chybných pokusov pri prihlasovaní sa do aplikácie k_3
- Čas do odhlásenia aplikáciou pri nečinnosti používateľa k_4
- Minimalizácia aplikácie k_5
- Autorizácia platieb v aplikácii k_6
- Denný / Mesačný limit na platby v aplikácii k_7
- Obfuskácia kódu aplikácie k_8
- Presun aplikácie na kartu k_9
- Zapnutý ladiaci mód k_{10}

Prvým parametrom je *Aktivácia aplikácie.* Analyzované aplikácie využívajú rôzne spôsoby aktivácie. Väčšinou sa ale jedná o prihlásenie z údajmi od Internet bankingu a následné potvrdenie cez SMS kód. Dve aplikácie (mBank SK, VÚB Mobil Banking) nevyžadujú po klientoch žiadnu aktiváciu, na prihlásenie im stačia údaje z Internet bankingu. Aktivácia aplikácie považujeme za dôležitý bezpečnostný prvok, bez nej sa môže hocikto kto zistí nejakým spôsobom prihlasovanie údaje od Internet bankingu prihlásiť aj do mobilnej aplikácie. Jednotlivé stavy sme ohodnotili nasledovne:

Kritérium 1: Aktivácia aplikácie

Aktivácia aplikácie	Bodové hodnotenie
Áno	1
Nie	0,4

Prihlásenie sa do aplikácie u analyzovaných aplikácií sa dá zadať prostredníctvom prihlasovacích údajov z Internet bankingu (PID + heslo), pomocou vopred určeného PIN kódu (4 až 6-miestny), alebo pomocou hesla. Prvý spôsob je pre klientov menej pohodlný, i keď rovnako bezpečný. Jednotlivým možnostiam sme priradili nasledujúce hodnoty:

Kritérium 2: Prihlásenie sa do aplikácie

Prihlasovanie do aplikácie	Bodové hodnotenie
PIN	1
Heslo	1
PID+heslo z IB	0,9

Dôležitým doplnkovým bezpečnostným prvkom sú limity pri prihlasovaní sa. V aplikáciách je možné chybne zadať PIN/heslo 3 až 5 krát v závislosti od danej aplikácie.

Kritérium 3: Počet dovolených chybných pokusov

Limity pokusov	Bodové hodnotenie
3 pokusy	1
4 a 5 pokusov	0,9
bez limitu	0

Automatické odhlasovanie predstavuje ochranný mechanizmus v prípade nečinnosti používateľa. Aplikácie využívajú rôzne nastavenia dĺžky tohto intervalu. Automatické odhlásenie je v rozmedzí od 1 minúty až po 20 minút. Špeciálnou možnosťou je automatické odhlásenie na základe zhasnutia displeja zariadenia, čo závisí na nastavení používateľa.

Kritérium 4: Čas automatického odhlasovania

Odhlásenie po čase inaktivity	Bodové hodnotenie
po zhasnutie displeja	1
po 1 minúte	1
3 až 5 minút	0,8
10 a 15 minút	0,5
20 minút	0,3

Väčšinu aplikácií Smart bankingu je možné minimalizovať. V prípade prepnutia sa do inej aplikácie, Smart banking aplikácia čaká na návrat užívateľ po dobu spomenutú vyššie alebo do jednej minúty. Dve aplikácie (Tatra banka, Zuno SK) neumožňujú minimalizáciu aplikácie alebo zhasnutie displeja, po návrate do aplikácie sa musí klient znova prihlásiť.

Kritérium 5: Minimalizácia aplikácie

Minimalizácia aplikácie	Bodové hodnotenie
Nie	1
Áno, čaká do 1 minúty na návrat	1
Áno	0,5

Autorizácia platieb hovorí o spôsobe akým sa potvrdzujú vykonávané platby v aplikácií. V analyzovaných aplikáciách bolo pre autorizáciu platby potrebné zadať PIN, heslo alebo SMS kód zaslaný na klientove telefónne číslo. Pri troch aplikáciách (Tatra banka, BankAir, Peňaženka) nie je potrebné platby v aplikácii autorizovať, čo pokladáme za bezpečnostnú slabinu aplikácie. Taktiež autorizácia SMS kódom zaslaným na to isté telefónne číslo pokladáme za menej bezpečné.

Kritérium 6: Autorizácia platieb

Autorizácia platieb	Bodové hodnotenie
PIN	1
Heslo	1
SMS kód	0,7
žiadná	0,5

Denný limit môže používateľovi zmierniť možnú stratu v prípade prelomenia aplikácie a jej zneužitiu. U iných používateľov môže byť denný limit určitým obmedzením v prípade potreby platiť vyššie čiastky. Niektoré aplikácie majú stanovený aj mesačný limit, ten však z hľadiska bezpečnosti nie je taký určujúci. Keďže predpokladáme, že Smart banking aplikácie sa vo väčšej miere používajú pri menších finančných transakciách a v prípade potreby platenia väčšej finančnej čiastky používateľ siahne po Internet bankingu sme limit do 1000 € hodnotili najvyšším bodovým ziskom.

Kritérium 7: Denný limit na platby v aplikácií

Denný limit	Bodové hodnotenie
do 1000 €	1
do 2000 €	0,9
do 3300 €	0,8
do 10 000 €	0,7
do 50 000 €	0,6
žiadny	0,5

Aplikácia Fio banka nemá žiadny limit pre platby, jediné obmedzenie je len disponibilný zostatok na účte a aplikácia Platby (SLSP) nemá žiadny denný limit.

Obfuskácia kódu znamená zmenu zdrojového kódu tak, aby fungoval, ale bol nečitateľný a nedal sa ľahko odkopírovať. Zisťovali sme teda, či je kód ľahko čitateľný a zrozumiteľný. Použitie obfuskácie kódu pokladáme za bezpečnejšie, ako jeho absenciu.

Kritérium 8: Obfuskácia kódu aplikácie

Obfuskácia kódu	Bodové hodnotenie
Áno	1
Nie	0,4

Štyri aplikácie z desiatich nevyužívali obfuskáciu kódu.

Presun na kartu umožňuje napr. pri android aplikáciách atribút android:installLocation a jeho hodnota „auto“ v elemente <manifest>. Presun na SD kartu sa odporúča iba niektorým typom aplikácií, pretože pri pripojení zariadenia k počítaču sú všetky bežiace aplikácie na karte zastavené. K údajom uloženým na karte majú prístup aj iné aplikácie, preto možnosť presunu na kartu pokladáme za menej bezpečnú.

Kritérium 9: Povolenie presunu na pamäťovú kartu

Presun na kartu	Bodové hodnotenie
Nie	1
Áno	0,7

Možnosť presunu na kartu nemali povolené aplikácie Tatra banka, Zuno SK, Peňaženka a Sberbank Smart Banking.

Zapnutý ladiaci debug mód predstavuje pre aplikácie riziko a pri jej publikovaní by mal byt vypnutý.

Kritérium 10: Zapnutý ladiaci kód

Debug kód	Bodové hodnotenie
Nie	1
Áno	0

Všetky nami analyzované aplikácie mali zakázaný ladiaci mód, takže tento parameter nemal vplyv na celkové poradie hodnotenia analyzovaných aplikácií Smart bankingu, napriek tomu sme ho uvádzali, pretože z pohľadu hodnotenia bezpečnosti aplikácií je tento parameter podstatný.

Podrobné hodnoty pre jednotlivé aplikácie bank sú uvedená v prehľadovej tabuľke.

4 Hodnotenie analyzovaných aplikácií – bezpečnostný koeficient Kb

Na vyhodnotenie bezpečnosti jednotlivých analyzovaných aplikácií a zvolenie poradia sme si zvolili štandardnú metódu multikriteriálneho hodnotenia. Na základe stanovania škály hodnôt pre jednotlivé kritéria sme vypočítali váhy jednotlivých kritérií v_{k_i}, ako podiel variabilít jednotlivých kritérií a súčtu variabilít týchto kritérií.

$$v_{k_i} = \frac{V_{k_i}}{\sum_i^j V_{k_i}}, \text{ pre } j = 1, 2, \ldots, 10.,$$

Tabuľka 3: Smart banking aplikácie a hodnoty skúmaných parametrov

	Aktivácia	Prihlásenie	Počet pokusov	Čas inaktivity	Minimalizácia aplikácie	Autorizácia	Denný / mesačný limit	Obfuskácia kódu	Presun na kartu	Zapnutý debug kód	Hodnotenie
Smartbanking (ČSOB)	Áno	PIN	5	5 minút	Áno, čaká 1 minútu	PIN	10 000 € / 68000 €	Áno	Áno	Nie	0,8942
mBank SK	Nie	PID+heslo z IB	3	20 minút	Áno	SMS, okrem preddefin.	2000 € / žiadny	Áno	Áno	Nie	0,6328
Fio banka	Áno	PID+heslo z IB	5	5, 10, 15, 30 minút	Áno	PIN	žiadny / žiadny	Áno	Áno	Nie	0,734
Tatra banka	Áno	PIN	3	Do zhasnutia displeja	Nie	nie je	3000 € / 30000 €	Nie	Nie	Nie	0,839
VUB Mobil Banking	Nie	PID+heslo z IB	5	10 minút	Áno	SMS/Token	50 000 € / žiadny	Áno	Áno	Nie	0,6413
BankAir (Unikredit)	Áno	PIN	3	3 minúty	Áno	nie je	3300 € / žiadny	Áno	Áno	Nie	0,7587
Zuno SK	Áno	PIN	4	Do zhasnutia displeja	Nie	PIN	1000 € / žiadny	Áno	Nie	Nie	0,9975
Peňaženka (Prima banka)	Áno	heslo	3	Do zhasnutia displeja	Áno, čaká 5 sekúnd	nie je	1000 € / žiadny	Nie	Nie	Nie	0,8622
SmartBanking (Sberbank)	Áno	heslo	3	1 minúta	Áno čaká 30 sekúnd	heslo	1000 € / 28000 €	Nie	Nie	Nie	0,9265
Platby (SLSP)	Áno	PIN	3	15 minút	Áno, čaká 1 minútu	SMS, GRID	žiadny / 170 000 €	Nie	Áno	Nie	0,713

Zdroj: Bezpečnosť mobilných služieb elektronického bankovníctva (Polák, 20014), vlastné spracovanie

Kde V_{k_i} je variačný koeficient *i*-teho kritéria vypočítaný ako podiel smerodajnej odchýlky σ_i, i-teho kritéria a aritmetického priemeru dosiahnutých hodnôt pre kritérium k_i. Váhy jednotlivých kritérií boli nasledovné:

Tabuľka 4: Vypočítaná váha jednotlivých kritérií

Kritérium	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
Váha v_{k_i}	0,131	0,0227	0,0245	0,1647	0,147	0,1285	0,1161	0,147	0,1185	0

Zdroj: vlastné spracovanie

Na základe hodnôt jednotlivých kritérií a vypočítanej váhy pre jednotlivé kritérium sme si stanovili koeficient bezpečnosti K_b, ako súčet násobkov hodnôt jednotlivých aplikácií a váh pre dané kritérium:

$$K_b = \sum_{1=1}^{10} v_{k_i} * h_{ij} \text{ pre } j = 1, ..., 10,$$

kde h_{ij}, je hodnota *i*-tého kritéria pre *j*-tu hodnotenú aplikáciu.

Záver

Predmetom článku bolo porovnanie a zhodnotenie 10 aplikácií Smart bankingu ponúkaných slovenskými bankami. Výsledné hodnotenie a detailný prehľad hodnotených aplikácií sa nachádza v tabuľke č. 3. Na základe vyšpecifikovaných kritérií sme zaviedli hodnotiace kritéria pre stavy jednotlivých aplikácií a zaviedli a vypočítali index bezpečnosti K_b hodnotenej aplikácie. Použili sme metódu multikritreriálneho hodnotenia, na základe ktorého sme vyčíslili jednotlivé váhy špecifikovaných kritérií (Tabuľka č. 4). Výsledný index bol vo všetkých prípadoch nad 60 %, čo je možné hodnotiť veľmi kladne a súhlasí so všeobecným tvrdením, že stav bezpečnosti elektronického bankovníctva na Slovensku je na vysokej úrovni. Za nedostatok u aplikácií mBank a VUB môžeme považovať absenciu procesu aktivácie. Pre banky by bolo dobré zvážiť využitie tejto ochrannej metódy. Prihlasovanie do aplikácie je realizované väčšinou prostredníctvom PIN alebo hesla, v 3 aplikáciách sa klient prihlasuje za pomoci bezpečnostných údajov z Internet bankingu. Pre niektorých klientov je tento spôsob nepohodlný, na druhej strane jednotnosť prihlasovacích údajov je praktické, avšak nie bezpečnejšie. Platby v troch aplikáciách nie je potrebné autorizovať, čo opäť znižuje úroveň bezpečnosti. V kombinácií s dlhou dobou automatického odhlasovania sa po inaktivite by to bolo veľmi nebezpečné. V prípade aplikácií od Tatra banky a Prima banky je to v poriadku, lebo aplikácia nemá povolenú možnosť minimalizácie a pri zhasnutí displeja je používateľ automaticky odhlásený. V prípade BankAir od Unicredit banky sa minimalizovaná aplikácia odhlási až po 3 minútach, čo v prípade krádeže alebo straty telefónu s prihlásenou bankovou aplikáciou je teoreticky možné zneužiť. Obfuskácia zdrojového kódu aspoň čiastočne predchádza možnosti zistiť prípadnému útočníkovi zistiť možné slabiny a nedostatky v aplikácii, preto by mala byť použitá v každej aplikácií, čomu tak v štyroch prípadoch nie je. Bankám, ktorých aplikácie mali index bezpečnosti K_b pod 80 % by mali analyzovať prečo dosiahli nízke skóre a prijať opatrenia na jeho zvýšenie.

Literatúra

[1] BUCKO, J., MIHÓK, P.: *Elektronické služby v bankovníctve.* 1. vyd. Košice : TU, EkF, 2008. 125 s. ISBN 978-80-553-0052-8

[2] DVOŘÁK, Petr – *Zabezpečení mobilních bankovnictví* [online]. 2013 [cit. 2013-12-09]. Dostupné na internete: < http://www.smartcardforum.cz/files/06.pdf >.
[3] GRAJCAR, M.: *Internet banking prešiel počas rokov od faxov k mobilným telefónom* [online]. 2012 [cit. 2013-10-10]. Dostupné na internete: < http://openiazoch.zoznam.sk/cl/116846/Internet-banking-presiel-pocas-rokov-od-faxov-k-mobilnym-telefonom
[4] HORNÝ, Patrik: *Éra multikanálového bankovnictví na startu* [online]. 2006 [cit. 2013-10-15]. Dostupné na internete: < http://bankovnictvi.ihned.cz/c1-19353670-era-multikanaloveho-bankovnictvi-na-startu >.
[5] KOVÁČIK, Martin: *Internet banking: Väčšiemu pohodliu klientov bráni strach* [online]. 2009 [cit. 2013-10-14]. Dostupné na internete: < http://www.investujeme.sk/internet-banking-vacsiemu-pohodliu-klientov-brani-strach/#poll >.
[6] MMA-MOBILE MARKETING ASSOCIATION: *Mobile Banking Overview (NA)* [online]. 2009 [cit. 2013-12-10]. Dostupné na internete: < www.mmaglobal.com/files/mbankingoverview.pdf >.
[7] POLÁK, T. – Bezpečnosť mobilných služieb elektronického bankovníctva, Diplomová práca, 2014.
[8] SAGÁLOVÁ, Eva: *Tlačova správa – K Internet bankingu si sadáme najmä v čase výplat* [online]. 2011 [cit. 2013-10-14]. Dostupné na internete: < http://www.postovabanka.sk/_img/Documents/Tlacove spravy/2011/K Internet bankingu si sadame najma v case vyplat.pdf >.
[9] SITA: *Internet banking využíva zhruba tretina Slovákov* [online]. 2012 [cit. 2013-10-13]. Dostupné na internete: < http://www.zive.sk/internet-banking-vyuziva-zhruba-tretina-slovakov/sc-4-a-300407/default.aspx >.
[10] SITA: *Svoje financie spravuje cez internet banking 40 percent Slovákov* [online]. 2013 [cit. 2013-10-14]. Dostupné na internete: < http://www.zive.sk/svoje-financie-spravuje-cez-internet-banking-40-percent-slovakov/sc-4-a-308227/default.aspx >.
[11] STAIR, Ralph M. – REYNOLDS, George W. : *Principles of Information Systems*. 9. Vydanie Boston: Cengage Learning, 2010. 658 s. ISBN 978–0-324–66528–4
[12] WESTPAC, *Mobile Banking – Top 10 mobile security tips | Westpac* [online]. [cit. 2013-12-21]. Dostupné na internete: < http://www.westpac.com.au/personal-banking/mobile-banking/mobile-security/mobile-security-tips>.

Meranie bezpečnosti Smart banking aplikácií – index bezpečnosti

doc. RNDr. Jozef Bucko, PhD.
Katedra aplikovanej matematiky a hospodárskej informatiky,
Ekonomická fakulta, Technická univerzita v Košiciach,
Nemcovej 32, 04001 Košice.
jozef.bucko@tuke.sk