Bezpečnosť a riziká elektronického bankovníctva

Laura Holotová

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Laura Holotová**
Osobní číslo:	**A11017**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost a rizika elektronického bankovnictví**
Téma anglicky:	**The Safety and Risks of Electronic Bankig**

Zásady pro vypracování:

1. **Vymezte pojem elektronické bankovnictví a analyzujte problematiku bezpečnosti elektronického bankovnictví.**
2. **Vyjmenujte nejvýznamnější průlomy bezpečnosti v oblasti e-bankingu.**
3. **Porovnejte elektronické krádeže na Slovensku a v Evropě.**
4. **Popište nové trendy v oblasti elektronického bankovnictví.**
5. **Navrhněte doporučení v problematice zneužití elektronického bankovnictví a zdůvodněte toto řešení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **JUŘÍK, Pavel. Svět platebních karet. Vyd. 1. Praha: Radix. ISBN 80-901-8531-2.**
2. **MÁČE, Miroslav. Platební styk: klasický a elektronický. 1. vyd. Praha: Grada, 2006, 125 s., [16] s. barev. il. a fot. ISBN 80-247-1725-5.**
3. **PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví: rady a tipy : vše o používání karet, banka po telefonu a v počítači, je to opravdu bezpečné, pohledy do zákulisí - jak to dělá banka, co nás čeká zítra?, praktické informace pro všechny případy. Vyd. 1. Praha: Computer Press, 2000, xii, 166 s. ISBN 80-722-6328-5.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management : BTSM 2007 : sborník mezinarodní konference, 12. a 13. 9. 2007, Zlín. Zlín: Univerzita Tomáše Bati, 2007. ISBN 9788073186050.**
5. **PROTIVINSKÝ, Miroslav. Bankovní loupeže :(přepadení bank, peněžních transportů a kriminalita v bankovnictví). Vyd. 1. Praha: Armex, 2001. 279 s. ISBN 80-86244-21-0**
6. **DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada, 2001. ISBN 8071694797.**

Vedoucí bakalářské práce: **doc. Ing. Jan Kunovský, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Prvá časť práce sa zaoberá vymedzením pojmu elektronické bankovníctvo, najčastejšími krádežami v oblasti elektronického bankovníctva, porovnaním elektronických krádeží na Slovensku a v Európe a novými trendmi, s ktorými sa v elektronickom bankovníctve môžeme stretnúť.

V druhej časti je navrhnutý model odporučenia pre elektronické bankovníctvo, konkrétne pre autentizáciu a autorizáciu klienta pomocou biometrických systémov.

Klíčová slova:

elektronické bankovníctvo, internetbanking, platobné karty, smartbanking, autentizácia, autorizácia, biometrické systémy, bezpečnosť

ABSTRACT

First part of this these deals with definition of electronic banking, most often cybercrimes, comparison between cybercrimes in Slovakia and cybercrimes in Europe and new trends we are facing in e-banking.

In second part, there is proposed model of recommendation for electronic systems of e-banking, especially for authorization and customers' authentication using biometrics systems.

Keywords:

electronic banking, internet banking, m-banking, payment card, authentication, authorization, biometric systems, safety

Poďakovanie

Touto cestou by som chcela veľmi pekne poďakovať pánovi doc. Ing. Jánovi Kunovskému, CSc. za cenné rady a pripomienky, ktoré som využila pri písaní tejto bakalárskej práce.

Takisto by som rada poďakovala mojim rodičom a priateľovi za ich podporu a trpezlivosť počas celého štúdia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Elektronické bankovníctvo je už dlhšiu dobu neodmysliteľnou súčasťou našich životov. Začiatky elektronického bankovníctva však siahajú až do polovice minulého storočia kedy začali vznikať prvé bankomatové karty a bankomaty. Odvtedy e-banking prešiel mnohými zmenami a pokrokmi a dostal sa až tam, kde je dnes.

S elektronickým bankovníctvom sa stretávajú milióny ľudí deň čo deň. Vyberajú peniaze z bankomatov, posielajú peniaze pomocou internetového bankovníctva z účtu na účet, či kontrolujú svoje zostatky pomocou mobilného telefónu alebo tabletu. Preto je potrebné, aby tieto služby boli dostatočne zabezpečené. Ochrana financií klienta by mala byť primárnou záležitosťou bánk kvôli udržaniu reputácie a vyhnutiu sa nepríjemnostiam, ktoré by krádeže mohli spôsobiť.

Cieľom práce bude na základe knižných a virtuálnych zdrojov zostaviť bezpečnostný model elektronického bankovníctva, ktorý bude spĺňať bezpečnostné požiadavky kladené na banku.

Teoretická časť práce sa bude v prvom bode venovať charakteristike elektronického bankovníctva. Elektronické bankovníctvo bude rozdelené na bankomaty a bankomatové karty, internetové bankovníctvo, homebanking a mobilné bankovníctvo. Ku každej časti bude písané o tom, ako funguje a bude tu spomenutá aj bezpečnosť. V druhom bode budú rozobrané elektronické zločiny, ktoré sú páchané v dnešnej dobe na bankomaty a internetové bankovníctvo. Bude tu spomenutý hlavne phishing, vishing, pharming, skimming, spying a tabnabbing. Ku každej podvodnej taktike bude opísané ako funguje. V druhej časti tohto bodu bude písané o hackeroch, ktorým sa podarilo uskutočniť veľké krádeže bánk pomocou internetu. V treťom bode bude porovnanie elektronických krádeží na Slovensku a v Európe a v poslednom bode teoretickej časti budú vymenované nové technológie s ktorými sa môžeme stretnúť v oblasti elektronického bankovníctva.

V praktickej časti bude zostavený model elektronického bankovníctva rozdelený na tri časti: bankomaty, internetbanking, smartbankig. Tento model bude zameraný na biometrické systémy a bude sa tu riešiť hlavne zvýšenie bezpečnosti autentizácie a autorizácie. Všetky časti budú zamerané na biometrický systém odtlačkov prstu. Na konci bude napísané zdôvodnenie tohto riešenia.

I. TEORETICKÁ ČÁST

1 POJEM ELEKTRONICKÉ BANKOVNÍCVO A PROBLEMATIKA BEZPEČNOSTI ELEKTRONICKÉHO BANKOVNÍCTVA

Elektronické bankovníctvo alebo aj priame bankovníctvo umožňuje klientom bánk kontakt so svojimi peniazmi 24 hodín denne. Toto sme dosiahli modernými technológiami. Dnes môžeme prostredníctvom elektronického bankovníctva zisťovať zostatky na účte, posielať peniaze z účtu na účet, platiť cez internet, objednávať si služby banky, atď. Najznámejšie formy elektronického bankovníctva sú Internetbanking; Mobilné bankovníctvo; Telebanking; Homebanking. [1]

Základná charakteristika elektronického bankovníctva:

- poskytovanie služieb prebieha výlučne pomocou elektroniky a internetu.
- na jednej strane je klient s potrebným technickým vybavením a na strane druhej je banka. Za banku môže systém pracovať samostatne, alebo je tu obsluhujúci pracovník.
- je treba jednoznačné identifikovanie a pri vykonávaní operácie sa musí identita overovať autorizačným mechanizmom [1]

Elektronické bankovníctvo zjednodušilo komunikáciu medzi bankou a klientom. Niekoľko storočí bola táto komunikácia možná len osobným stykom. Pokrok nastal vynájdením telefónu a neskôr rozšírením mobilných telefónov a internetu. Banky začali meniť ich služby. Hlavnými dôvodmi týchto zmien je úspora nákladov a zatraktívnenie služieb pre klientov. Úspora nákladov však nastáva až po relatívne dlhej dobe. Čo sa týka zatraktívnenia služieb ide hlavne o úsporu času a zrýchlenie. [2]

Možnosti komunikácie klienta a banky:

a) osobná návšteva
b) platobná karta
c) internetbanking
d) homebanking
e) mobilné bankovníctvo – SMS banking, GSM banking, WAP banking [2]

Rozvoj elektronického bankovníctva podmienil vznik platobných kariet.

1.1 Platobná karta

Platobná karta slúži ako prostriedok pre vyberanie peňažných prostriedkov alebo pre úhradu platby. Platobná karta je identifikačným dokladom, ktorej rozmery a fyzikálne vlastnosti stanovuje medzinárodná norma. Na lícovej strane sa nachádza číslo karty, obdobie jej platnosti a meno držiteľa. Na zadnej strane je magnetický prúžok a podpisový prúžok. Podľa čísla karty sa dá stanoviť druh karty (VISA, MasterCard) prvé dve číslice, vydavateľa karty (banka) ďalších 5 čísel a zvyšok slúži na identifikáciu konkrétneho držiteľa. Platobná karta je majetkom banky a nie majetkom držiteľa. [3]

Podľa medzinárodnej normy je stanovený rozmer karty 85,6 x 54,0 x 0,76 mm. Táto karta ďalej musí byť vyrobená z trojvrstvého PVC, ktorý splňuje tieto požiadavky:

a) je schopný elasticky vyrovnať deformácie vzniknuté bežným používaním;
b) je netoxický;
c) je odolný voči rôznym chemickým vplyvom pri bežnom používaní;
d) je použiteľný pri teplotách prostredia od -35 až do +50 stupňov Celzia a pri relatívnej vlhkosti vzduchu 5-95% pri 25 stupňoch Celzia;
e) je odolný voči zmačknutiu a skrúteniu.

Na prednú časť karty sú reliéfnym vyrazené nevyhnutné identifikačné údaje. Pre ne je určená dolná polovica prednej časti karty, ktorá obsahuje podľa normy tri riadky. Prvý riadok obsahuje 12 až 19 miestne číslo, ktoré udáva číslo karty. Druhý riadok uvádza obdobie platnosti karty a tretí riadok je určený pre meno držiteľa karty. Pre karty určené len pre elektronické transakcie sa v poslednej dobe nahradzuje reliéfne písmo hladkou tlačou alebo sú údaje zaznamenané laserovým paprskom. Pri niektorých kartách sa môžeme stretnúť na prednej strane s ochranným hologramom.

Zadná časť karty obsahuje:

a) magnetický prúžok – slúži ako médium pre záznam identifikačných údajov. Môže obsahovať dve alebo tri záznamové stopy.
b) podpisový prúžok – slúži ako záznam podpisového vzoru držiteľa karty.

V roku 1981 sa prvý krát začali objavovať karty s elektronickým prvkom (mikropočítačom), ktorý postupne nahrádzajú magnetický prúžok, ktorého možnosti rozvoja sú dnes už vyčerpané. Dnes existuje mnoho druhov čipových kariet pre najrôznejšie oblasti použitia. V bankovníctve sa používajú tie najzložitejšie, so

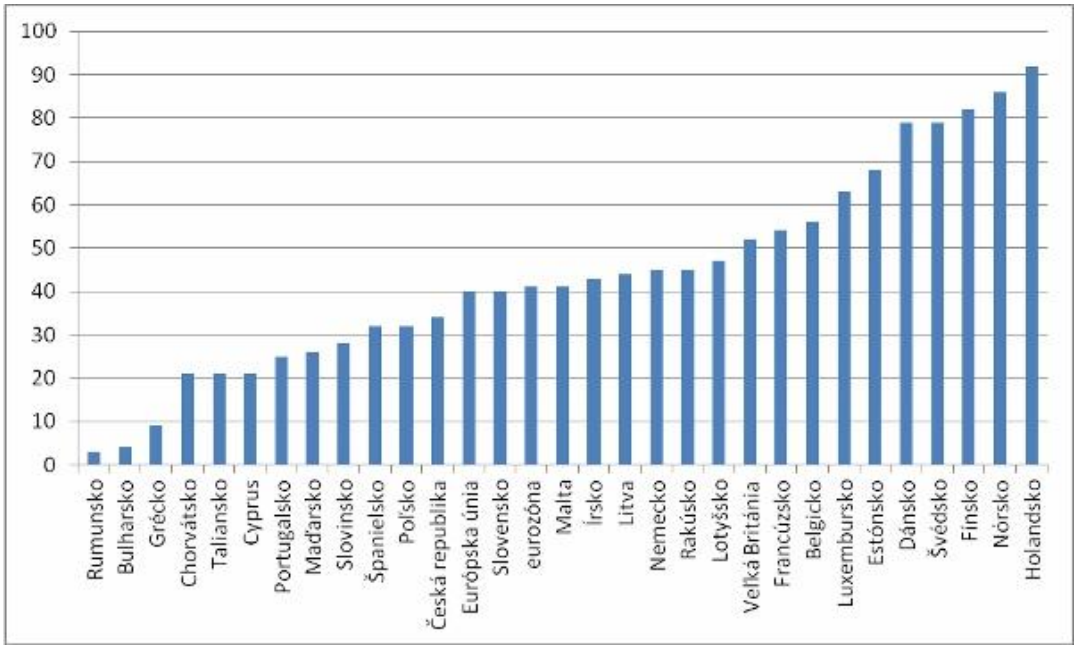
zabudovanými ochrannými prvkami. Konštrukcia i programové vybavenie mikroprocesoru umožňuje do karty bezpečne uložiť informácie potrebné k overeniu osobného kódu klienta PIN alebo iný verifikačný prvok (odtlačok prstu). [4]

Prvá organizácia, ktorá začala hromadne poskytovať platobné karty, ktoré boli príbuzné tým dnešným bol Diners Club. Táto organizácia vznikla v roku 1950. O osem rokov neskôr vytvorila jedna z najväčších bánk v USA vlastnú kartu, ktorá sa volala BankAmericard, z ktorej sa postupne stala dnes najznámejšia platobná karta Visa. Spoločnosť MasterCard vznikla v roku 1966 spojením niekoľkých menších bánk. Dnes existuje veľa spoločností, ktoré umožňujú ľuďom nosiť so sebou prakticky celý svoj majetok. Aj keď vo svete zažili najväčší rozvoj platobné karty v šesťdesiatych rokoch, u nás sa prvý bankomat objavil až v roku 1988. [5]

Ani platobné karty neunikli pozornosti páchateľov trestných činov a preto sa veľmi skoro objavili zneužitia kariet vlastnými aj cudzími osobami (stratené alebo odcudzené karty), dokonca aj napodobeniny kariet rôznej kvality. Všetky tieto prípady podvodov prispeli v priebehu posledných 30 rokov k neustálemu zdokonaľovaniu bezpečnostných techník ochrany karty i samotných platobných transakcii. Žiadny platobný systém nie je dnes schopný úplne zabrániť vzniku škôd, ktoré vznikajú zneužitím platobných kariet. Opatrenia pre zaistenie úplnej ochrany by boli také nákladné a náročné na organizáciu, že by sťažovali ich bežné používanie. [4]

1.2 Internetbanking

V dnešnej internetovej dobe má internetbankig stále väčší úspech. Je to veľmi jednoduchá, rýchla a pohodlná forma, ako sa bezpečne starať o svoje financie. [6]



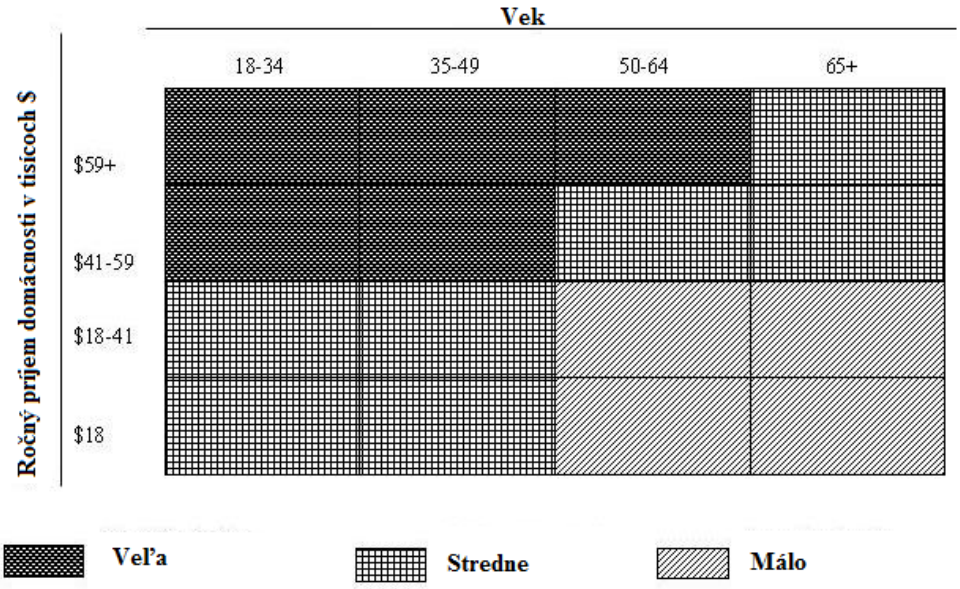
Obrázok 1 Využitie internetbankingu v rámci Európy [6]

Pri tejto službe nedochádza k presunu žiadnych fyzických objektov ale všetky transakcie, či už presun peňazí z účtu na účet, získanie zostatku na účte a podobne sú vykonávané elektronicky. Ak prihliadneme na riziká v elektronickom bankovníctve môžeme ho rozdeliť do troch častí:

- Informačná časť – banka uverejňuje informácie o produktoch a službách na svoje webové stránky. Tu je riziko, že tretia strana dokáže zmeniť informácie a teda treba zabezpečiť administrátorský prístup.
- Komunikačná časť – komunikácia medzi bankou a klientom. Odohráva sa už na internej úrovni a preto je treba zvýšiť stupeň ochrany. Môže to byť napríklad komunikácia o zostatku na účte pomocou mailov.
- Transakčná časť – tu treba najvyšší stupeň ochrany. Internetové bankovníctvo umožňuje manipulovať s peniazmi na účte, teda vykonávať transakcie medzi účtami napr. prevody finančných prostriedkov. [3]

Internetbanking je v najväčšom rozmachu a banky vymýšľajú stále nové a nové možnosti internetbankingu. Postupne dokonca vznikajú banky, ktoré nemajú kamenné pobočky ale

existujú len virtuálne. Internetbanking je hitom dnešnej rýchlej doby. Zameriava sa najviac na mladých a dobre zarábajúcich ľudí. [3]



Obrázok 2 Využívanie internetbankingu v USA podľa veku a ročného prímu [7]

Výhodou internetového bankovníctva je poskytovanie finančných služieb 24 hodín denne. Treba mať však prístup k internetu. Vďaka nemu majú zákazníci rýchlejšiu a lepšiu kontrolu nad svojimi účtami. A výhody internetového bankovníctva neplynú len pre zákazníkov, ale aj pre banky. Znižujú operatívne náklady, umožňujú lepšiu diverzifikáciu produktov a môžu poskytovať lepšie služby. Cena transakcie vykonanej internetovým bankovníctvom sa približne rovná:

- desatine ceny na pobočke
- pätine ceny transakcie pomocou telefónu
- tretine ceny výberu z bankomatu [3]

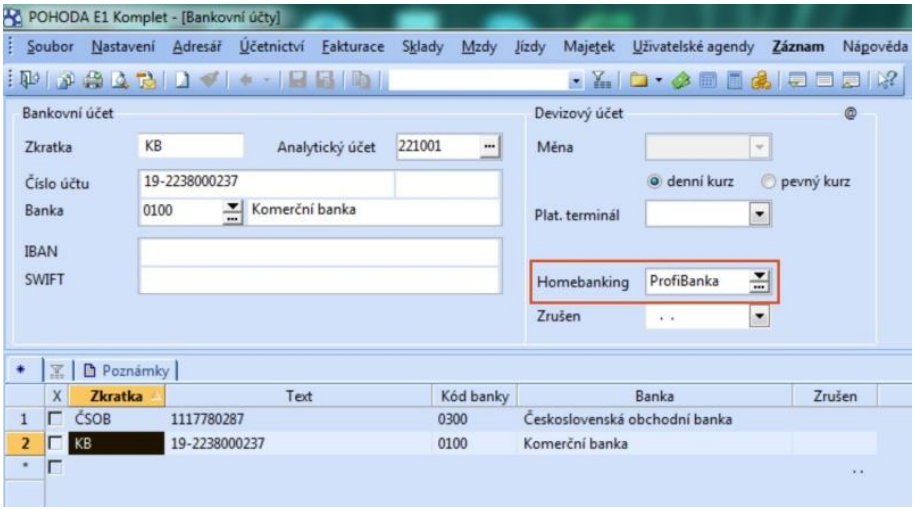
Pre bezpečnú komunikáciu banky s klientom používa banka SSL protokol. To je šifrovací protokol ležiaci medzi vrstvami TCP/IP a aplikačnými protokolmi http. Umožňuje komunikáciu medzi prehliadačom a bankovým serverom a taktiež dokáže určovať totožnosť serveru. SLL umožňuje autentizované prihlásenie bez toho, aby sa prenášalo heslo. Zabezpečuje šifrovanie a integritu prenášaných dát. Najbežnejšie využívanie SSL je pre protokol HTTPS, ktorého výhodou je, že hotová aplikácia v HTTP sa dá ľahko s minimálnymi úpravami preklopiť do HTTPS.[8]

1.3 Homebanking

Homebanking bol obľúbený hlavne do konca 90. rokov, kedy internetové bankovníctvo nebolo ešte také rozšírené a bola k nemu nedôvera. Neskôr však internetové bankovníctvo homebanking skoro nahradilo. Stále však zostáva doménou firiem. Je aj riešením pre banky, ktoré nemajú svoje internetové bankovníctvo lebo sa im vzhľadom k počtu klientov nevyplatí. Program homebankingu je licenčne viazaný na jeden počítač poprípade sieť počítačov. To je jeho nevýhoda oproti internetbankingu. [9]

Homebanking umožňuje takmer všetky bezhotovostné operácie – zisťovanie zostatku na účte, podanie príkazu k úhrade, sledovanie toku platieb, zakladanie terminovaných účtov, zahraničné platby atď. Ponúka aj prístup do databázy banky, kde sa dajú vyhľadávať kurzové lístky, úrokové sadzby, ponuka služieb a pod. Tento program sa dá pripojiť na vlastný ekonomický systém a umožňuje automatické zadávanie platobných príkazov a výpisov z účtov. [9]

Ako zabezpečenie používajú programy homebankingu pre potvrdenie operácie podpisový certifikát. Dáta bývajú prenášané internetom cez šifrované SSL spojenie alebo priamym spojením na modem banky, spravidla priamym vytočením telefónneho čísla. [7]



Obrázok 3 Ukážka ako vyzerá homebanking - Homebanking POHODA [10]

1.4 Mobilné bankovníctvo

V dnešnej dobe je vlastníkom smartfónu takmer každý. Banky preto začali majiteľom smartfónov dávať možnosť si stiahnuť aplikácie pre smartbanking. Vo vyspelejších štátoch je smartbanking bežnou súčasťou života. Na Slovensku a v Čechách túto službu využíva zatiaľ veľmi malé percento ľudí. [11]

Každá banka ponúka iné služby mobilného bankovníctva. Zatiaľ čo niektoré podporujú len rozosielanie zostatku na účte, u iných možno dávať aj príkazy k úhrade či zakladať termínované účty. [11]

Formy mobilného bankovníctva:

- SMS
- GSM
- WAP

1.4.1 SMS banking

Je to forma bankovníctva, ktorá je založená na tom, že banka rozosiela nezaheslované správy. Delia sa na push a pull správy.

Push správy sú rozosielané bez toho aby si ich zákazník vyžiadal. Môže to byť napríklad:

- periodické informácie o stave účtu
- pripísanie alebo odpísanie peňazí z účtu
- nedostatok prostriedkov
- neúspešná/úspešná platba šeku
- jednorázové heslo OTP atď.

OTP (one time password) je heslo, ktoré sa zasiela klientovi pri prihlasovaní do internetbankingu alebo pri posielaní platby na účet. Je to určitá forma ochrany pred zneužitím konta. Toto heslo je platné iba jeden krát a potom expiruje.

Ďalším druhom SMS sú pull SMS. Tie si vyžiada zákazník a banka na ne odpovedá. Môžu to byť :

- vyžiadanie o informácii zostatku na účte
- žiadosť o zrušenie platby
- žiadosť o zablokovanie karty
- aktuálny kurzový lístok

1.4.2 GSM banking

Je to softvérové rozhranie, ktoré pomocou mobilného telefónu umožňuje komunikáciu klienta s bankou. Robí sa to pomocou technológie GSM SIM Toolkit. Pri GSM SIM Toolkite je potrebné splniť niekoľko predpokladov. Treba mať telefón podporujúci technológiu GSM Toolkit, špeciálnu SIM kartu a nakoniec samozrejme banku, ktorá túto službu umožňuje. Pri prihlasovaní je treba zadávať BPIN. [2]

1.4.3 WAP banking

Je to veľmi ojedinelá forma mobilného bankovníctva. Dnes je už o veľkom nahrádzaná aplikáciami v smart mobilných telefónoch. Využíva sa pri nej WAP (wireless aplication protocol) a slúži hlavne na zisťovanie zostatku na účtoch, na príkaz k úhrade a k zisteniu aktuálnych kurzov. [12]

2 NAJVÝZNAMNEJŠIE PRIELOMY BEZPEČNOSTI V RÁMCI E-BANKINGU

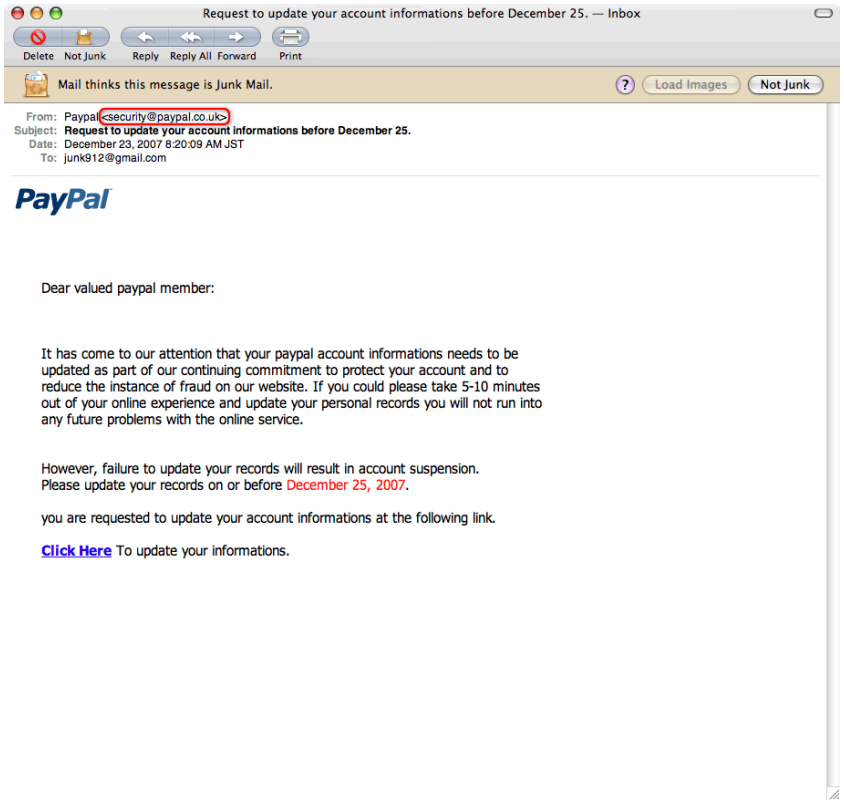
Inovácie v technologickej oblasti a konkurencia bank prináša stále viac bankových služieb. S rýchlim rozvojom sa však spájajú aj riziká, ktoré sa týkajú hlavne zabezpečenia účtov a prevádzania transakcií proti zneužitiu treťou osobou. V tejto časti práce budú analyzované často vyskytujúce sa útoky na citlivé údaje.

Najčastejšími formami zneužitia sú:

- phishing
- pharming
- vishing
- skimmnig
- spying
- tabnabbing

2.1 Phishing

Skratka je odvodená od **P**assword **H**arvest Fi**shing** čo v doslovnom preklade znamená zberanie hesiel rybárčením. Je to jeden z najstarších spôsobov klamania užívateľa. Sú to vlastne podvodné správy, ktoré sa snažia vytiahnuť z ľudí informácie o ich citlivých informáciách. Robí sa to za pomoci sociálneho inžinierstva. Sociálne inžinierstvo je metóda, pri ktorej útočník manipuluje osobu za účelom získania údajov alebo sa snaží osobu zmanipulovať k určitej činnosti. Pri tomto útoku klienti dostávajú falošné emaily, ktoré vyzerajú ako z ich banky alebo iných inštitúcii, kde dochádza k manipulácii s peniazmi. Príkladom je PayPal, eBay, Skype, atď. Tieto emaily bývajú vo veľmi dobrom prevedení. Môžu oznamovať neprevedenie platobného príkazu, bezpečnostnú hrozbu kvôli ktorej je treba previesť zmenu prihlasovacích údajov alebo sa môžu tváriť ako prieskum verejnej mienky o konkrétnej inštitúcii. V texte správy spravidla býva link, ktorý vyzerá, že nás presmeruje na stránky organizácie, ale v skutočnosti nás presmeruje na falošné stránky. Tieto stránky sa na prvý pohľad nelíšia od originálnych stránok. Keď sa však pozrieme bližšie, tak adresa stránky je iná a väčšinou začína nezabezpečeným protokolom (http://).[13]

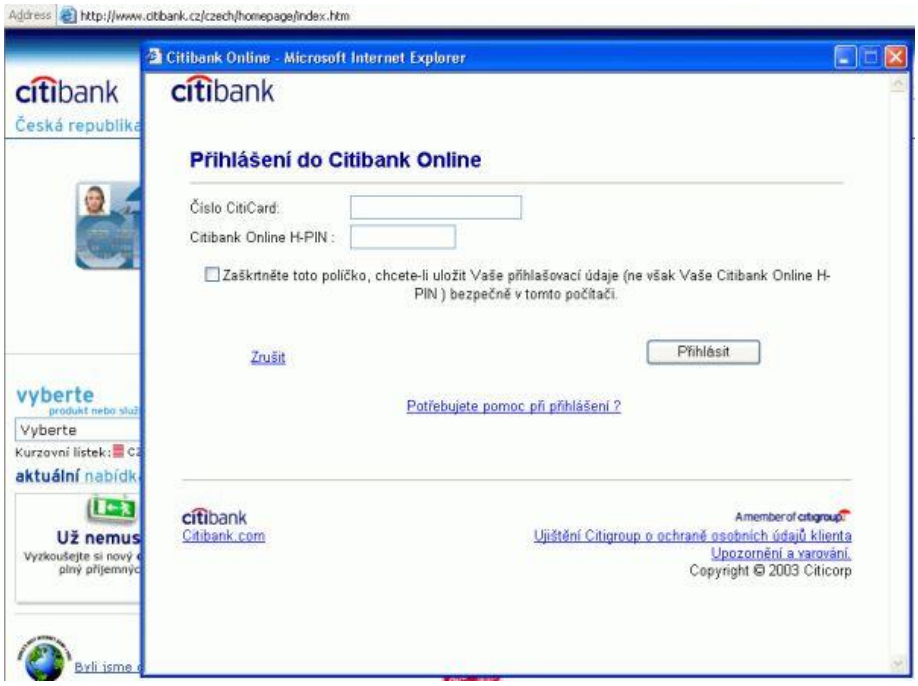


Obrázok 4 Príklad phishingového mailu, ktorý vyzerá ako zo spoločnosti PayPal [14]

Prvý phishingový útok bol zaznamenaný v roku 1995. Cieľom bola americká spoločnosť America Online (AOL) a účelom bolo získať prihlasovacie údaje užívateľov. Vtedy sa im podarilo ovládnuť emailové adresy užívateľov a posielať z nich nevyžiadanú poštu. [15]

Phishers za krátku dobu zistili, že sa schránky dajú využiť k získaniu informácii o kreditných kartách, bankových účtov a pod. 11. 9. 2001 využili hackeri chaos a pokúsili sa zaútočiť na platobné účty E-gold. Tento útok bol zaistený a zlikvidovaný. Ďalší významnejší útoky prebehli v roku 2003, a to na finančné inštitúcie E-loan, E-gold, Wells Fargo a Citibank. [16]

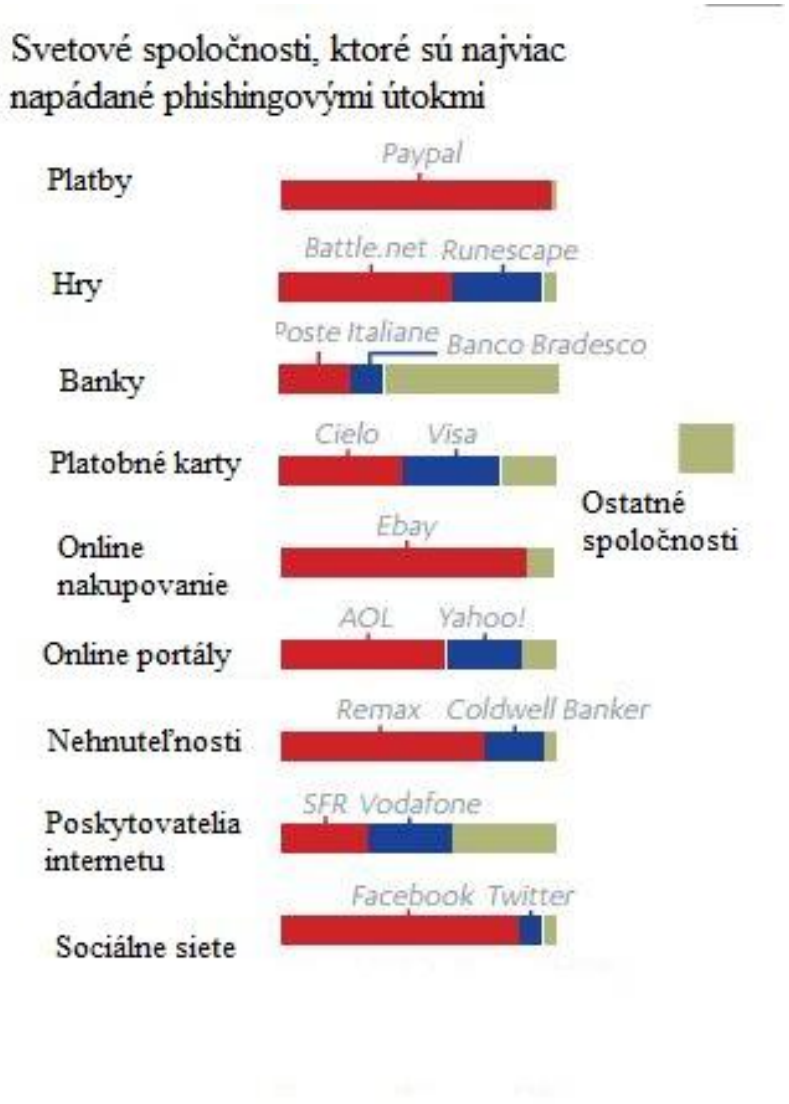
V roku 2003 bola behom útoku na Citibank po prvýkrát použitá technika vyskakovacích okien, takzvané pop up okná. Klient obdržal email s odkazom na stránky Citibank a kliknutím na odkaz sa otvorila skutočná stránka Citibank a vyskakovacie okno, ktoré vyžadovalo zadanie čísla karty a PIN kódu. Informácie boli následne posielané útočníkovi. [17]



Obrázok 5 Pop up okná pri phishingovom útoku na Citibank [18]

V rokoch 2006 a 2007 sa obeťami phishingu v rámci USA stalo 3 600 000 ľudí. V roku 2006 boli celkové straty 2,3 miliardy dolárov a to znamená, že na každého poškodeného pripadá strata 866 dolárov. V roku 2007 boli straty vyššie, konkrétne 3,2 miliardy dolárov. [19]

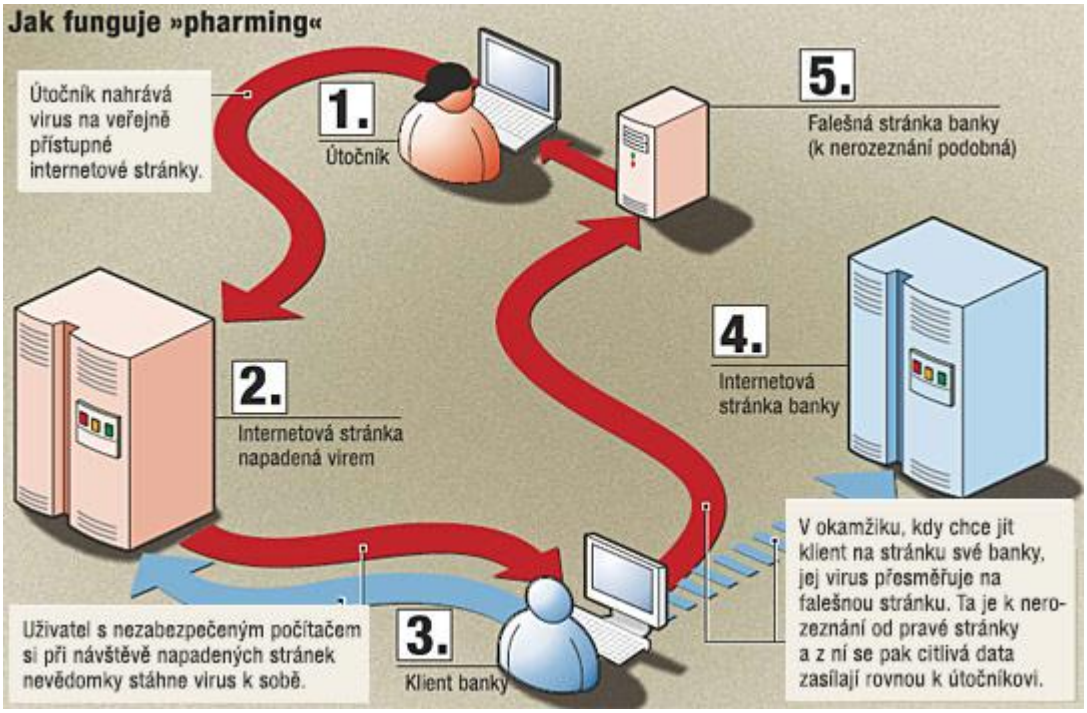
V roku 2011 odhalila spoločnosť ESET phishingový útok na klientov Latin American bank. Klientom prišli emaily so správou, že ich karta je zablokovaná a žiadali po nich potvrdenie údajov do odkazu, ktorý bol v maily uvedený. Tento útok trval približne 5 hodín a falošnú stránku stihlo za tento čas navštíviť 164 užívateľov, Citlivé údaje pritom zadalo 35 ľudí a to je 21% z celkového počtu. [20]



Obrázok 6 Spoločnosti, ktoré sú najviac napádané phishingovými útokmi podľa kategórii [21]

2.2 Pharming

Pharming je automatizovaná forma phishingu. Táto metóda nie je súčasťou sociálneho inžinierstva. Útočníci napádajú DNS servery alebo počítače. V prípade zle zabezpečených DNS serverov potom všetci užívatelia, ktorý sú na tento server pripojený, zadávajú správnu adresu, ale sú presmerovaní na falošnú stránku. V prípade napadnutia jednotlivých počítačov útočníci napádajú PC s operačným systémom Windows, ktoré obsahujú takzvané hosts súbory, ktoré fungujú podobne ako DNS server. Ak sa útočníkom podarí zapísať do tohto súboru svoju adresu podvodnej stránky, tak je efekt rovnaký ako v predchádzajúcom prípade. [22]



Obrázok 7 Ako funguje pharming [22]

2.3 Vishing

Skratka slov voice-over a phishing, čo znamená lovenie hesiel cez telefón. Táto metóda sa prevádza za pomoci sociálneho inžinierstva. Útočníci sa snažia dostať z klientov informácie o prístupe k internetbankingu prostredníctvom telefónneho rozhovoru. Útočníci pomocou malware získajú autorizačné údaje. Útočník sa do internetbankingu prihlási, ale pre úplné prihlásenie potrebuje autorizačný kód. Preto pošle klientovi varovnú SMS napríklad: *„Zaznamenali sme pokus o podvodnú transakciu na Vašom účte. Pre overenie Vás budeme kontaktovať z telefónneho čísla xxxx xxxx. Banka xxx.“* Následne útočník zavolá menom banky klientovi a aby získal jeho dôveru povie mu napríklad jeho užívateľské meno alebo niekoľko znakov z hesla. Ďalej mu oznámi, že bol zachytený pokus o podozrivú transakciu a pre jej zrušenie si vypýta transakčný kód a môže manipulovať s napadnutým účtom. [23]

2.4 Skimming

Výraz je odvodený od anglického slova to skim, čo znamená zbierať, sťahovať. Je to trestná činnosť spojená s bankomatovými kartami. Páchatelia pomocou špeciálneho zariadenia nasadeného na bankomat kopírujú dáta z magnetického prúžku. Pomocou týchto dát následne vytvárajú nové falšované karty. Okrem údajov z magnetického prúžku je ďalším dôležitým údajom PIN kód. Na jeho získanie používajú páchatelia bankomatové kamery, mobilné telefóny alebo špeciálnu klávesnicu, ktorá sa umiestňuje miesto klávesnice pôvodnej alebo na ňu. Prvé skimmovacie zariadenie v ČR bolo odhalené v roku 2001. Banky nezverejňujú počet skopírovaných kariet ani objemy peňazí, ktoré takto boli ukradnuté, ale škody spôsobené klientom hradia v plnej výške. [24]

2.5 Spying

Je to špehovanie pomocou škodlivého programu, ktorý nazývame spyware. Tento program si v 99% prípadov stiahneme pri surfovaní po internete. Spyware sleduje aktivitu užívateľov, kradne autorizačné údaje a čísla kreditných kariet. Potom všetko posiela útočníkovi. Tieto dáta sa veľa krát zneužívajú pre marketingové účely. Užívateľ nakazeného počítača si toho vôbec nemusí byť vedomý. Na odhalenie existujú antispywareové programy.

2.6 Tabnabbing

Je to sofistikovanejšia forma phishingu. Je založený na manipulácii so záložkami vo webovom prehliadači a nepozornosti užívateľa internetu. Jeho princípom je, že napríklad pri vyberaní nejakého tovaru na internete má užívateľ otvorených niekoľko záložiek. Preklikáva ich a porovnáva ceny výrobkov. Užívateľ má v úmysle si tovar kúpiť cez internetové bankovníctvo. Potom sa stane, že otvorí stránku, ktorá je napadnutá skriptovým trojským koňom tak, že spúšťa TabNabbingový skript. Na stránke nie je vidieť nič zvláštne, ale po určitom čase, keď sa prepne na inú stránku sa zmení ikona v záložke a stránka zrazu vyzerá ako stránka internetového bankovníctva. Užívateľ si pri väčšom množstve otvorených stránok bude myslieť, že stránku s internetovým bankovníctvom si otvoril sám a do podvrhnutej stránky napíše svoje prihlasovacie údaje. Keďže však väčšina internetových bankovníctiev potrebuje k prihláseniu viac ako prihlasovacie meno a heslo, tak táto taktika sa viac používa na získanie prístupu do sociálnych sietí. Najviac ohrozené sú stránky ako eBay alebo PayPal ktoré majú priamy prístup k účtom. [25]

2.7 Známi hackeri

Počiatky počítačových hackerov sa odhadujú už od 70. rokov. Jeden z prvých ľudí, ktorým sa vôbec podarilo oklamať techniku bol Američan John T. Draper. Zistil, že pokiaľ fúkne do píšťalky, ktorú výrobcovia pridávali do cereálii dosiahne frekvenciu 2600 Hz ktorá dokáže vyradiť hovor z autorizačného systému telefónnej spoločnosti AT&T. Postupne sa krádeže začítali stávať viac sofistikovanými. [26]

V roku 1981 sa spoločnosť AT&T stala znovu terčom útoku. Tentokrát sa hacker, ktorý si hovoril Captain Zap, nabúral cez modem na interné hodiny spoločnosti a posunul ich. Predtým boli hovory v špičke účtované drahšie ako v noci. Vďaka jeho posunu však ľudia v špičke platili málo a v noci veľa. [27]

2.7.1 Vladimír Leonidovič Levin

Je to jeden z najznámejších ruských hackerov. V roku 1994 niekoľko zákazníkov Citibank zistilo, že im zmizli z účtov peniaze. Následne banka prišla na to, že sa niekto nabúral do systému elektronického bankovníctva FICCM (Finanacial Institutions Citibank Cash Manager). Bol to predchodca dnešných elektronických bankovníctiev, ktorý nebežal na internete. Pomocou vyšetrovania sa zistilo, že nezmizlo len niekoľko sto tisíc dolárov, ale celková čiastka sa napokon vyšplhala až na 10 miliónov dolárov. Previedli ich celkom v 40 rôznych transakciách. Peniaze boli posielané väčšinou na zahraničné účty, ale niektoré skončili aj v San Franciscu. Účty sa podarilo v celkom rýchlom čase „zmraziť“. Keďže pre tieto zločiny ešte vtedy neexistovala špeciálna jednotka, tak krádež vyšetrovali ľudia na finančnú kriminalitu. To, že peniaze prišli na účty do San Francica bola prvá stopa pre FBI. Tieto účty patrili ruskému páru, ktorý žil v USA. Títo manželia vypovedali, že celú akciu riadil z Petrohradu majiteľ počítačovej firmy Vladimír Levin. Nakoniec sa však ukázalo, že Levin nebol geniálnym hackerom, ale skôr výborným obchodníkom. Krátko po jeho zatknutí sa objavili náznaky, že za nabúraním do systému stojí skupina ruských hackerov. Tí sa v systéme iba hrali. Levin od nich kúpil prístup k elektronickému bankovníctvu za 100 dolárov. Levin bol za svoj čin odsúdený iba na 3 roky väzenia. Z celkovej krádeže 10,7 miliona sa 10,3 miliona podarilo vrátiť naspäť. 400 tisíc, ktoré chýbali sa nikdy nepodarilo nájsť. Mená hackerov, ktorí v skutočnosti prenikli do systému nikdy neboli zverejnené.[28]

2.7.2 Kim Schmitz

Medzi známych hackerov patrí aj Kim Schmitz s prezývkou Kimble. Ako mladému sa mu podarilo nabúrať sa do systémov NASA, Pentagonu alebo rôznych bánk. Jeden z jeho najznámejších hackerských útokov bolo odpísanie malej čiastky z účtu približne štyroch miliónov zákazníkov Citibank. Celkovú sumu, ktorá nakoniec presiahla 20 miliónov dolárov Kim poslal na účet Greenpeace. V roku 1994 ho zatkli a bol obžalovaný z jedenástich počítačových podvodov a desiatich špionážnych útokov na citlivé dáta. Nakoniec kvôli nízkemu veku, mal vtedy dvadsať rokov, mu trest znížili a nemusel ísť do väzenia. [29]

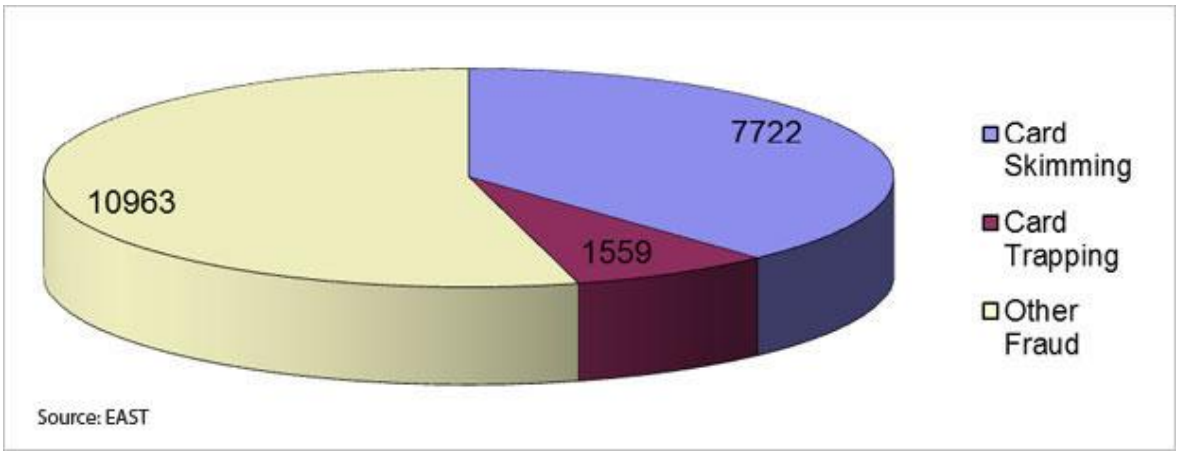
2.7.3 Albert Gonzales

Americký počítačový hacker, ktorému sa podarilo ukradnúť údaje zo 130 miliónov kreditných a debetných kariet . Jeho cieľom bolo 250 finančných inštitúcii napr. Heartland Payment System, Hannaford Brothers a podobne. Tieto karty použil k vlastnému obohateniu a spôsobil na nich škody až 200 miliónov dolárov. Gonzáles pracoval ako agent FBI v boji proti internetovej kriminalite. Za svoj čin mu bolo udelených 20 rokov väzenia, čo je doteraz najviac za internetový zločin. [30]

3 POROVNANIE ELEKTRONICKÝCH KRÁDEŽÍ NA SLOVENSKU A V EURÓPE

S elektronickými krádežami sa stretávame po celom svete. To isté sa týka aj Slovenskej republiky. Na Slovensku bol v posledných rokoch dosť rozšírený skimming. V roku 2012 bolo napadnutých 27 bankomatov. To predstavuje približne jedno percento všetkých bankomatov . Napadnutých kariet pri tom bolo len zanedbateľné množstvo a to približne 0,022% zo všetkých registrovaných kariet.[31]

V rámci Európy bolo napadnutých skimmingom v roku 2012 7722 bankomatov, čo je zobrazené na nasledovnom grafe.[32]



Obrázok 8 Graf napadnutia bankomatov: skimming, trapping, iné napadnutie [32]

Trapping je forma skimmingu, kedy páchatelia nekopírujú dáta z karty ale nechajú ju uväznenú v bankomate a chopia sa príležitosti po tom, ako obeť útoku ide hľadať pomoc. Pri tejto technike je tiež nutné zistiť PIN kód obete.

Čo sa týka phishingových útokov, tak jeden z najznámejších a najmedializovanejších bol útok na Slovenskú sporiteľňu z roku 2008. Klientom slovenskej sporiteľne bol rozoslaný podvodný mail najprv v anglickom jazyku a neskôr bol preložený do slovenčiny. Na mail vtedy zareagovalo približne 140 ľudí ale väčšina odpovedí bola prázdna alebo obsahovala nezmysly. Pravdivých bolo 9 údajov. Túto doménu mal založiť občan Českej republiky, konkrétne z Brna. [33]

Najviac napádanými krajinami v rámci Európy sú Rumunsko, Francúzko, Nemecko, Taliansko, Švédsko a Holandsko, čo môžeme vyčítať z Obrázok 9 Krajiny sveta, ktoré sú najviac napádané phishingovými útokmi.. Z týchto krajín má jediná, najviac napadnutí práve v online platobnom systéme a je ňou Nemecko.

Rank	Country	Percentage	Top Target Phished
1	United States	66%	Social networking site
2	China	14%	Social networking site
3	Romania	5%	Social networking site
4	Guam	5%	Social networking site
5	France	1%	Online auction site
6	Germany	1%	Online payment system
7	Italy	1%	Online auction site
8	Canada	1%	Online portal
9	Sweden	1%	Telecommunications provider
10	Netherlands	1%	Social networking site
graph powered by www.iresearch.ro			

Obrázok 9 Krajiny sveta, ktoré sú najviac napádané phishingovými útokmi.

Vo všeobecnosti sa dá zhrnúť, že Slovensko patrí medzi pomerne bezpečné krajiny, čo sa týka elektronických zločinov. Môže to byť spôsobené hlavne malým počtom ľudí využívajúcich služieb ako je internetbanking či smartbankig. V budúcnosti môžeme predpokladať nárast elektronických zločinov v súvislosti s postupným nárastom užívateľov internetbankingu a smartbankingu. Dá sa však predpokladať, že naša krajina sa nikdy nedostane do top rebríčkov krajín napádaných rôznymi druhmi elektronických krádeží.

4 NOVÉ TRENDY V OBLASTI ELEKTRONICKÉHO BANKOVNÍCTVA

Rýchly vývoj nových technológii nám poskytuje aj veľa noviniek v rámci elektronického bankovníctva. Nové trendy smerujú k fyzickej nezávislosti klienta, k vysokej bezpečnosti a jednoduchosti. Jednými z noviniek v tejto oblasti je už spomínaný smartbanking, zaujímame sa aj o QR platby či bezkontaktné technológie PayPass.

4.1 Smartbanking

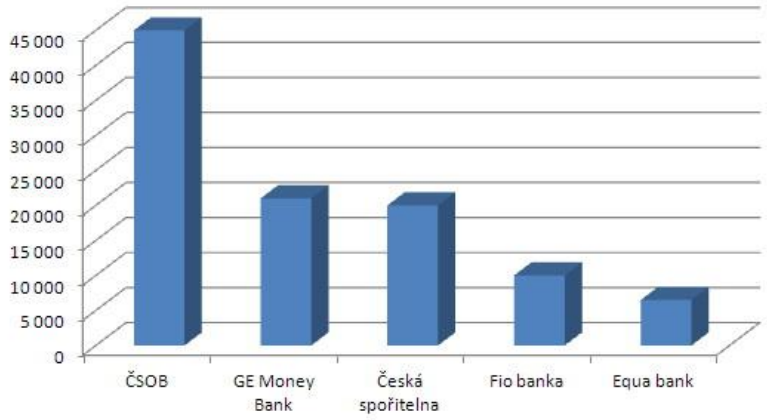
Smartbanking by sa dal definovať aj ako obsluhovanie bankového účtu pomocou smartfónu cez aplikáciu banky, ktorá v ňom musí byť nainštalovaná. Termín smartbanking je používaný iba na Slovensku a v Českej republike. V zahraničí sa využíva skôr pojem m-banking. Hlavnými predpokladmi pre používanie smartbankingu je vlastniť mobilný telefón alebo tablet s operačným systémom iOS, Android alebo Windows Phone. [34]

Banka	Android	iOS mobil	iOS tablet	Windows Phone
Air Bank		✓		
Citibank	✓	✓		
Česká spořitelna	✓	✓		
ČSOB	✓	✓	✓	✓
Era/Poštovní spořitelna	✓	✓	✓	✓
Equa bank	✓	✓		
Fio banka	✓	✓		✓
GE Money Bank	✓	✓		
ING Bank		✓	✓	
Komerční banka	✓	✓		
mBank	✓	✓	✓	
Raiffeisenbank	✓	✓	✓	
UniCredit Bank	✓	✓		✓
Volksbank Löbau-Zittau	✓	✓	✓	
Zuno Bank	✓	✓		

Obrázok 10 Zoznam podpory bank rôznych operačných systémov [35]

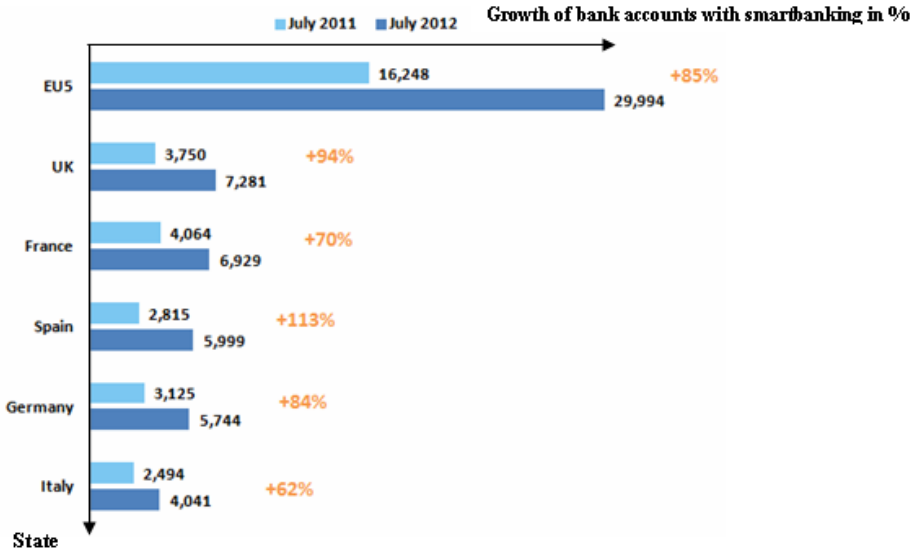
Výhodami smartbankingu oproti internetovému bankovníctvu je, že tu klient môže vyhľadávať bankomaty a pobočky s podrobným sprievodcom založeným na bázy GPS. Ďalej môže využívať kurzový lístok a zadávať platby načítaním QR kódu.

Na český trh sa smartbanking dostal po prvý krát v prvej polovici roku 2011 ako produkt spoločnosti Fio Banka a UniCredit Bank. Nasledovali ich Citibank a Equa bank, ktorí sa pripojili v lete v roku 2011. Na konci roku 2011 sa pridala aj GE Money Bank. V roku 2012 pribudli ďalšie banky – ČSOB, Poštová banka, Česká spořitelna a mBank. [36]



Obrázok 11 Počet užívateľov smartbankingu v jednotlivých bankách v rámci ČR [36]

Čo sa týka užívateľov smartbankingu v rámci EU5 nastal v roku 2012 oproti predchádzajúcemu roku obrovský boom v užívaní smartbankingu.



Obrázok 12 Porovnanie množstva používateľov smartbankingu v rokoch 2011 a 2012 [34]

4.2 Bezkontaktné platby PayPass

S touto technológiou prišla po prvý krát spoločnosť MasterCard. Je to platenie bezkontaktne a pri nižších čiastkach aj bez zadávania PIN kódu. Dochádza k zrýchleniu transakcie a zvýšenej bezpečnosti pri platení. Zvýšená rýchlosť sa prejavuje hlavne pri platbách do 500 Kč, kedy odpadá zadávanie PIN kódu a odborníci odhadujú skrátenie platby o cca 5 sekúnd. Vyššia bezpečnosť je vďaka tomu, že klient sám prikladá kartu k terminálu a teda nedochádza k manipulácii ďalšími osobami. Za pokrok môžeme považovať aj fakt, že daná technológia sa dá aplikovať napríklad do mobilného telefónu, prívesku na kľúče, samolepky, hodiniek atď. Klient teda nemusí nutne zo sebou nosiť kartu ale stačí ak si zoberie len kľúče alebo hodinky, ktoré vždy nosí pri sebe. [37] V Českej republike momentálne ponúka možnosť bezkontaktnej karty 12 bánk – Air Bank, Equa Bank, Citibank, Česká spořitelna, ČSOB, Fio banka, GE Money Bank, Komerční banka, mBank, Poštovní spořitelna – Era, Raiffeisenbank, Zuno Bank. Prvou bankou ktorá začala ponúkať bezkontaktné karty bola v júni roku 2011 Citibank. Nasledovala ju Česká spořitelna, ktorá prišla s prvou debetnou bezkontaktnou kartou. [38]

V rámci bezpečnosti, by sme mohli polemizovať nad faktom, že pokiaľ nám niekto kartu odcudzí alebo ju stratíme, tak páchateľ môže robiť neobmedzený počet nákupov do 500 Kč až pokiaľ neminie všetky peniaze alebo karta nie je zablokovaná. Preto vydavatelia karty ručia 100% vrátením peňazí pri jej zneužití.

V budúcnosti sa uvažuje aj o možnosti pridať k bankomatom snímacie zariadenia obdobné tým, čo sa využívajú k bezkontaktným platbám, aby výber z bankomatu mohol tak isto prebiehať bezkontaktne a dokonca s absenciou platobnej karty. Stále však existuje problém zneužitia, ktorý by sa v budúcnosti mohol riešiť napríklad pomocou biometrickej autentizácie.

4.3 QR kódy a platby

QR kódy vznikli v roku 1994 a vytvorila ich pobočka automobilky Toyota pre lepšiu evidenciu vozidiel vo výrobe. Skratka QR znamená Quick Response, teda rýchla reakcia, pretože kód je navrhnutý na rýchle dekódovanie. Čiernobiely obrazec dokáže pojať viac než 4000 alfanumerických znakov, čo je oproti čiarovému kódu s 20 alfanumerickými znakmi neporovnateľný rozdiel. Masovo sa však začali používať až s prvými mobilnými telefónmi so vstavaným fotoaparátom. [39]

Každý QR kód sa skladá z viacero častí:

- Terčík pre správne zameranie pri čítaní
- Informáciu o formáte kódu
- Informáciu o verzii kódu
- Samotné data [40]

Existuje niekoľko verzií kódu, ktoré sa líšia schopnosťou odolávať poškodeniu a kapacitou. Podľa typu informácie môžeme uložiť 7089 číslic, 4296 alfanumerických znakov, 2953 bajtov ľubovoľných dát, 1817 japonských znakov. Výhodou QR kódu je aj to, že veľmi dobre odoláva poškodeniu. Existujú štyri stupne ochrany obsahu:

- úroveň L – môže mať až 7 % poškodenej plochy
- úroveň M – môže mať až 15 % poškodenej plochy
- úroveň Q – môže mať až 25 % poškodenej plochy
- úroveň H – môže mať až 30 % poškodenej plochy [40]

By Square – platby pomocou QR kódov

By Square sa u nás prvý krát objavilo v roku 2012. Slúži na zjednodušenie vyplnenia platobného príkazu v mobilnej bankovej aplikácii. Podstatou By Square je vyfotenie QR kódu z faktúry a platobný príkaz sa sám automaticky vyplní a nemusíme zložito prepisovať číslo účtu, variabilný symbol a ďalšie údaje. Celé to funguje veľmi jednoducho. Odosielateľ vystaví faktúru, zakóduje platobný príkaz a ďalšie potrebné údaje do vygenerovaného By Square QR kódu. Tento dokument je obsahuje aj špeciálny QR kód a je poslaný prijímateľovi v tlačenej faktúre alebo elektronicky vo formáte PDF. Prijímateľ faktúry, ktorá obsahuje By Square QR kód nemusí manuálne zadávať údaje ale iba mobilným telefónom zosníma kód a v mobilnej aplikácii internetbankingu potvrdí platbu. Veľké uľahčenie práce touto technológiou prichádza hlavne pre podnikateľov a účtovníkov, ktorý denne spracúvajú obrovské množstvá faktúr. [41]

4.4 Mobito

Mobito je elektronická peňaženka, ktorú možno nabiť pomocou bankového účtu alebo platobnou kartou. Ku svojmu Mobito účtu je možné pripojiť až 3 rôzne bankové účty. U niektorých bánk je možné dokonca prepojenie s internetovým bankovníctvom. Ostatné je možné si dobíjať platobnou kartou alebo prevodom z účtu. Pri prevode z účtu na účet mobita je spoplatnenie podľa cenníku banky, a pri dobíjaní bankomatovou kartou je to 1,5% z nabíjanej čiastky plus 3 Kč. Je možný aj prevod z mobita na bankový účet. Toto využívajú hlavne obchodníci. Užívatelia Mobita si môžu navzájom posielať peniaze na svoje elektronické peňaženky. Stačí poznať telefónne číslo a zadať čiastku, ktorú chcete inému užívateľovi Mobita previesť. Majiteľovi druhého účtu príde SMS správa s tým, že mu užívateľ s konkrétnym číslom zaslal peniaze. Mobito je spojené s konkrétnym mobilným telefónnym číslom, ktoré zadáva užívateľ pri registrácii. Zároveň toto číslo slúži ako jeden z možných identifikačných prostriedkov užívateľa. Mobito funguje na väčšine telefónov okrem Windows Phone a Symbian Belle a dokonca nie je nutné mať smartphone. Účet je možné založiť priamo na stránkach Mobita, v internetovom bankovníctve alebo pomocou mobilnej aplikácie. Funkčnosť služby je garantovaná len na území ČR. [42]

4.5 3D secure

Je to systém platby na internete, ktorý ma za úlohu zvýšiť bezpečnosť internetových transakcií. Dnes ho už podporuje väčšina internetových obchodníkov. Tento spôsob platby overuje okrem platobného inštrumentu aj identitu držiteľa. Týmto sa zvyšuje úroveň zabezpečenia transakcie a naopak znižuje riziko zneužitia. Tieto technológie sú známe pod názvom „Verified by Visa“ a „MasterCard Security code“. Funguje to nasledovne: Pri platbe a internete ste presmerovaní na stránku banky obchodníka. Vyplníte platobné údaje vrátane čísla karty a odošlete ich. Následne banka obchodníka zašle žiadosť o overenie karty vašej banke. Tá vás prostredníctvom prehliadača požiada o zadanie kódu, hesla apod. Pokiaľ je autentizácia úspešná tak platba prebehne.

Dodanie hesla či kódu majiteľovi karty môže nastať troma spôsobmi:

- Autentizačný kalkulátor – dostáva sa k platobnej karte a na ňom sa generuje kód, ktorý sa zadáva do formulára. Používajú sa napríklad v Rakúsku.

- Zaslanie SMS – SMS sa posiela na číslo, ktoré ste popredu banke poskytli pre túto službu.
- Vygenerovanie autentizačného kódu priamo na platobnej karte, ktorá má zabudovaný display. [43]

Obrázok 13 Logo označujúce internetové obchody, ktoré podporujú 3D security [43]

Názov 3D Secure skrýva základnú myšlienku sily zabezpečenia, ktorá sa ukrýva v tom, že behom transakcie medzi sebou komunikujú tri strany:

- Klient
- Banka klienta
- Banka obchodníka [44]

Obrázok 14 Stránka 3D secure pre ČSOB

4.6 Biometrické systémy

Biometria je vedná disciplína, ktorá meria a následne analyzuje biologické dáta jednotlivca. Môžu to byť odtlačky prstov, obrázky sietnice, črty tváre a pod. Biometriou nazývame charakteristickú črtu, ktorá je merateľná. Je to fyzická alebo zvyková črta jedinca, ktorá sa používa na overovanie totožnosti daného jedinca. Je to najsilnejšia jednozložková metóda overenia totožnosti. Biometrické črty ako odtlačok prsta alebo štruktúra rohovky je jednoznačne zviazaná s jedincom, a teda nemôže byť ukradnutá, stratená alebo zabudnutá. [45]

4.6.1 Rozdelenie biometrie

Biometriu delíme na:

- Statická biometria (fyzické črty)
- Dynamická biometria (zvykové črty)

Do statickej biometrie patrí odtlačok prsta, štruktúra rohovky, črty tváre, geometria ruky a štruktúra ciev sietnice. Do dynamickej zaraďujeme charakteristiky, ktoré sú založené na meraní akcií vykonávaných jedincom v čase, kde meraná akcia ma začiatok, stred a koniec. Sem radíme napríklad podpis, zadávanie z klávesnice, chôdzu a pod. [45]

4.6.2 Porovnanie rôznych typov biometrických technológii

Existuje veľa druhov biometrie ale jediná univerzálna a vhodná na všetky druhy aplikácii neexistuje. Biometria s najvyššou bezpečnosťou nemusí byť aj najvhodnejšou. Treba vždy brať do úvahy viacero faktorov ako je finančná náročnosť, rýchlosť, presnosť jednoduchosť a v neposlednom rade nemôže obťažovať jedinca. [45]

Biometrický systém	Univerzálnosť	Jedinečnosť	Stálosť	Možnosti získania	Prijatie verejnosťou	Pravdepodobnosť oklamania
Tvár	Vysoká	Nízka	Stredná	Vysoká	Vysoká	Nízka
Odtlačok prstu	Stredná	Vysoká	Vysoká	Stredná	Vysoká	Vysoká
Tvar ruky	Stredná	Stredná	Stredná	Vysoká	Stredná	Stredná
Dynamika písania na klávesnici	Nízka	Nízka	Nízka	Stredná	Stredná	Stredná
Duhovka	Vysoká	Vysoká	Vysoká	Stredná	Nízka	Vysoká
Sietnica	Vysoká	Vysoká	Stredná	Nízka	Nízka	Vysoká
Podpis	Nízka	Nízka	Nízka	Vysoká	Vysoká	Nízka
Hlas	Stredná	Vysoká	Vysoká	Stredná	Vysoká	Nízka
DNA	Vysoká	Vysoká	Vysoká	Nízka	Nízka	Nízka

Tabuľka 1 Porovananie rôznych biometrických technológii [46]

V predchádzajúcej tabuľke si môžeme všimnúť porovnanie rôznych biometrických technológii na základe ich univerzálnosti, jedinečnosti, stálosti, možnosti získania, prijatia verejnosťou a pravdepodobnosti oklamania.

- Univerzálnosť popisuje ako je bežne nájdená biometrika v jedincovi
- Jedinečnosť nám udáva ako dobre dokáže systém rozoznať rôzne biometrické dáta
- Stálosť hovorí o odolnosti systému voči starnutiu
- Možnosti získania udávajú ako ľahko je možné biometrické dáta získať.
- Prijatie verejnosťou popisuje súhlas verejnosti s používanou technológiou v každodennom živote
- Pravdepodobnosť oklamania ako ľahko je možné oklamať systém

Systém, ktorý použijeme treba posudzovať zo všetkých hľadísk, ktoré sú tu popísané. Nemôžem napríklad vybrať systém posudzovania DNA len preto lebo ma vysokú univerzálnosť, jedinečnosť, stálosť a nízku pravdepodobnosť, keď má na druhú stranu ťažké získavanie údajov a nízke prijatie verejnosťou.

PRAKTICKÁ ČÁST

5 NÁVRH MODELU DOPORUČENIA ZABEZPEČENIA ELEKTRONICKÉHO BANKOVNÍCTVA PROTI ZNEUŽITIU

Cieľom je navrhnúť bezpečnejší model autentizácie a autorizácie a náhrada doterajších hesiel, prihlasovacích mien, certifikátov, PIN kódov či platobnej karty. Návrh bude využívať hlavne biometrické systémy, o ktorých bolo písané v kapitole 4.6. Aby sme mohli navrhnúť bezpečnejší systém elektronického bankovníctva je potrebné si najskôr vymedziť pojmy autentizácia a autorizácia. Následne rozdelíme elektronické bankovníctvo na 3 časti :

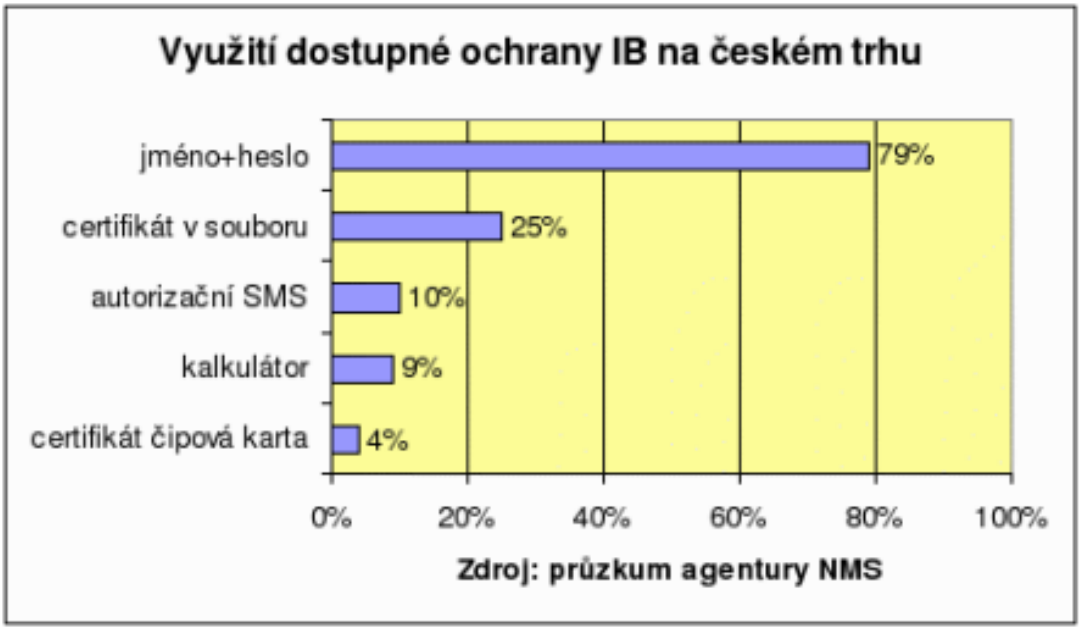
- bankomaty a platobné karty
- smartbanking
- internetové bankovníctvo

V každej z týchto častí rozanalyzujeme dnešné riešenie bezpečnosti a môj návrh riešenia do budúcnosti. Tieto návrhy budú posúdené z hľadiska výhod a nevýhod pre banky a výhod a nevýhod pre klienta. V návrhu budem opisovať súčasné riešenie elektronického bankovnícva ČSOB a.s. a Komerčnej banky a.s. a v návrhu bude opis bezpečnejšej autorizácie a autentizácie.

5.1 Autentizácia a autorizácia

Autentizácia je overenie identity prihlasovacím menom, heslom, certifikátom alebo biometrickou metódou. Pri autorizácii sa jedná o oprávnenie osôb pracovať s dátami. Pri zabezpečovaní elektronického bankovníctva môžeme použiť viacero metód, ktoré najviac môžeme navzájom kombinovať. Tieto metódy sú:

- Meno a heslo
- Certifikát: súbor a čipová karta
- Autorizačná SMS
- Kalkulátor
- Biometrické systémy



Obrázok 15 Využitie ochrany internetového bankovníctva na českom trhu [47]

5.1.1 Užívateľské meno, klientské číslo a heslo

Užívateľské mená a klientské čísla slúžia hlavne na identifikáciu osôb a najčastejšie sa kombinujú s heslami. Tento spôsob autentizácie je veľmi obľúbený. Pri prihlasovaní do internetbankingu sa môže využívať číslo platobnej karty, číslo účtu ale aj náhodne vygenerované klientské číslo. To je v tomto prípade najbezpečnejšou variantou.

Autentizácia heslom a menom je najjednoduchšia, nie je však veľmi bezpečná. Bezpečnosť sa v tomto prípade dá zvýšiť hlavne použitým heslom, ktoré by malo mať minimálne 8-12 znakov a malo by byť odolné proti slovníkovým útokom, čiže musí obsahovať čísla, znaky a malé a veľké písmená. Na druhú stranu by však heslo nemalo byť prehnane zložité lebo si ho klient nezapamätá.

Banky pri procese autentizácie menom a heslom po troch neúspešných pokusoch riešia situáciu zablokovaním prihlasovacej aplikácie pre konkrétneho užívateľa.

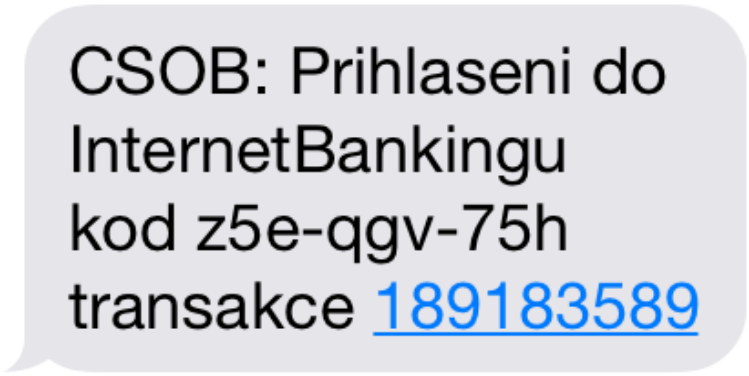
5.1.2 PIN

S touto skratkou sa stretli už všetci užívatelia mobilných telefónov a platobných kariet. V tejto spojitosti si používanie PIN kódu najčastejšie vybavíme. PIN je skratka personal identification number a znamená osobné identifikačné číslo. Slúži k autentizácii užívateľa pri prístupe do určitého tokenu. Token je fyzické hardvérové zariadenie určené na

autorizáciu. Termín token môže znamenať aj softvérový token. Výhodou tokenu je automatické zablokovanie po niekoľkých neúspešných pokusoch. Po takomto zablokovaní je potrebné poznať PUK (personal unlock key) kód. Túto metódu overenia sa dá veľmi ľahko zneužiť, pokiaľ by chcel niekto zablokovať cudzí účet. Stačilo by mu zadať niekoľko krát nesprávne PIN aplikácia by bola neprístupná aj pre oprávnenú osobu. Preto sa PIN kódy väčšinou spájajú s nejakým osobným hardvérovým zariadením (mobilný telefón, kreditná karta). [48]

5.1.3 Autorizačná SMS

Táto forma autorizácie sa stala veľmi obľúbenou hlavne v oblasti zabezpečenia internetového bankovníctva. Základným predpokladom na využívanie tejto služby je vlastniť mobilný telefón. Pri vytváraní internetového bankovníctva sa zadáva telefónne číslo pre potreby autentizácie a autorizácie. Pri prihlasovaní do internetbankingu alebo pri požiadavkách na transakciu je klientovi zaslaná autorizačná SMS ktorá informuje klienta o tom prečo bola odoslaná. Môže to byť len informácia o prihlásení do internetového bankovníctva a identifikačný kód, alebo v prípade transakcie by mala obsahovať detailné informácie týkajúce sa konkrétnej transakcie. Hlavnou nevýhodou môže byť neúplné pokrytie mobilných sietí. [48]



Obrázok 16 Príklad autorizačnej SMS od ČSOB pri prihlásení do internetbankingu

5.1.4 Certifikáty

Zabezpečenie elektronickými certifikátmi je jeden z bezpečnejších spôsobov. Využíva sa tu asymetrická kryptografia (šifrovanie verejným kľúčom a dešifrovanie súkromným). Banky ich používajú hlavne k bezpečnému overeniu identity užívateľa a k autorizácii. Užívateľ vlastní verejný a súkromný kľúč, kde verejný kľúč je certifikovaný príslušnou autoritou napr. bankou. Súkromný kľúč je bezpečne uložený na čipovej karte, ktorú neopustí a prístup na ňu je chránený PIN kódom. Certifikáty nemusia byť uložené len na čipovej karte, ale môžu byť aj súčasťou PC v podobe softvéru, môžu byť súčasťou digitálneho podpisu alebo môžu byť nahrané na USB token. [48]

Obrázok 17 Čítačka kariet a čipová karta [49]

Certifikáty sa delia na softvérové a hardvérové. Hlavným rozdielom je, či sú uložené na nejaký token alebo do počítača. Ak certifikát uložíme do PC je to menej bezpečné lebo sa sem môže nabúrať hacker naopak certifikáty na čipovej karte sú považované za najbezpečnejšie. V čipovej karte je tajný osobný kľúč, ktorý je bezpečne uložený a každá správa je týmto kľúčom podpísaná. V praxi to znamená, že je doplnená o unikátny kód, ktorý je odvodený z obsahu správy a tajného kľúča. Z karty sa tento kód nedá žiadnym spôsobom získať a ani uhádnuť. Banka prijme správu od klienta až potom, čo overí elektronický podpis podľa certifikátu, ktorý klientovi vydala. Najľahšie a najjednoduchšie je používanie USB tokenu. Pri používaní čipových kariet je potreba vlastniť čítačku kariet. USB token vyzerá ako obyčajný USB kľúč. Prístup k certifikátu na tokene je chránený PIN kódom tiež. [48]

Obrázok 18 USB token [50]

5.1.5 Autentizačné kalkulátory

Sú považované za jednu z najbezpečnejších metód zabezpečenia internetového bankovníctva. Prístup k nim je chránený PIN kódom. Po jeho zadaní kalkulátor vygeneruje heslo, ktoré je časovo obmedzené a slúži k autentizácii či autorizácii. Tieto zariadenia sú zosynchronizované so systémom v banke tak, aby obidve strany generovali rovnaký kľúč, ktorý užívateľ opisuje do aplikácie. Tým sa dá jednoducho dokázať, že je majiteľom príslušného kalkulátoru. [48]

Okrem PIN kalkulátorov patria do tejto skupiny aj generátory jednorázových hesiel. Tieto vygenerujú heslo buď na požiadanie alebo heslo generujú automaticky stále a po zadaní požiadavku ho zobrazia. Podobajú sa na USB kľúče. [48]

Obrázok 19 Obrázok generátoru jednorázového hesla [51]

5.1.6 Biometria

Základné princípy fungovania biometrie sme si opísali už v bode 4.6.

Banky už pomaly začínajú využívať metódy biometrie pri autentizácii užívateľov. V ČR sa väčšina užívateľov elektronického bankovníctva ešte s týmito metódami nestretla. Zavádzanie týchto noviniek do praxe je náročné hlavne po finančnej stránke to znamená nákup skenerov a náklady na ich údržbu.

Pre klienta českých bánk je momentálne autentizácia do elektronického bankovníctva pomocou biometrických metód zatiaľ nepredstaviteľná. Na trhu sa však pomaly začínajú objavovať snímače odtlačkov prstov, ktoré vyzerajú ako USB kľúče a ich nákup nepredstavuje veľkú investíciu.

Obrázok 20 USB kľúč s funkciou snímania odtlačkov prstu [52]

5.2 Riešenie pre bankomaty a platobné karty

5.2.1 Dnešný systém bankomatov a platobných kariet

Bankomaty a platobné karty sa stali bežnou súčasťou našich životov a preto je potrebné aby aj ich ochrana bola čo najvyššia. V dnešnej dobre je autorizácia a autentizácia riešená dvojmo: bankomatovou kartou a PIN kódom. Klient príde k bankomatu kde vloží bankomatovú kartu, zadá PIN kód a môže pracovať so svojim účtom. Systém funguje dobre. ale tento spôsob ochrany by sa dal hodnotiť ako priemerný. Hlavné nebezpečenstvo predstavuje jednoduché odcudzenie karty a ľahké odpozorovanie PIN kódu. Krádeže z cudzích účtov sú aj popri zvyšovaní bezpečnosti kamerami stále bežné. To, že sú pri bankomatoch nainštalované kamery je určite výhodou, ale v konečnom dôsledku to má

skôr psychologický efekt. Hlavnou nevýhodu kamier je fakt, že aj pokiaľ viem ako vyzeral človek, ktorý kradol z bankomatového účtu tak stále si neviem priradiť k tejto tvári meno a teda je veľmi ťažké takéhoto človeka vystopovať. Veľkou nástrahou pri vyberaní z bankomatu je určite skimming, o ktorom som písala v kapitole 2.4. Čím ďalej tým viac sa rozširujú bezkontaktné platobné karty a teda aj možnosť, že po bezkontaktných termináloch prídu aj bezkontaktné bankomaty. Tu vzniká ďalšie možné riziko, ktoré treba riešiť.

Výhody dnešného systému pre banku

Výhodou pre banky je určite to, že systém je dobre zabehnutý a funguje. Banky museli investovať veľa finančných prostriedkov do vybudovania sietí bankomatov, ale aj do vytvárania platobných kariet. Systém je pomerne bezpečný, jednoduchý a rýchly. Ovládanie bankomatu zvládajú bez problémov aj starší ľudia.

Nevýhody dnešného systému pre banku

V prvom rade sú to určite krádeže, ďalej kazovosť a potreba obsluhy bankomatov. Pri krádeži nemusí byť nevýhodou len vracanie financií, ktoré boli odcudzené ale aj možná ďalšia nedôvera klienta k banke.

Výhody dnešného systému pre klienta

Pre klienta je výhodou hlavne jednoduchá obsluha bankomatov a fakt, že v mestách sa bankomaty nachádzajú takmer „na každom rohu“.

Nevýhody dnešného systému pre klienta

Hlavnou nevýhodou je určite nutnosť mať bankomatovú kartu, bez ktorej sa človek pri vyberaní z bankomatu nepohne. Ľudia môžu byť frustrovaní zo strachu straty bankomatovej karty, a to hlavne v prípade ak vlastnia bezkontaktné karty. Ďalšou nevýhodou je, že pokiaľ vlastníme viacero kariet môže tu byť aj nutnosť pamätať si viacero PIN kódov. Nepríjemnosťou je aj fakt, že na dedinách je pomerne málo bankomatov a ľudia za nimi doslovne musia cestovať do miest.

5.2.2 Nový systém pre bankomaty a platobné karty

V tejto časti bude navrhnuté nové riešenie problematiky bankomatov a platobných kariet. Tento systém by mal byť riešený určite dvojitou autentizáciou, tak ako je to riešené aj dnes. Systém platobných kariet je tu už veľmi dlho a stále nie je dokonalý, hlavne čo sa týka bezpečnosti. Do budúcnosti budeme navrhovať autentizáciu kartami zameniť za autentizáciu čipom. Tento čip môže byť zabudovaný v telefóne, hodinkách, prívesku a podobne. Po autentizácii čipom by nasledovala autentizácia odtlačkom prstu. Odtlačok prstu volíme hlavne kvôli vysokej spoľahlivosti a rýchlosti. Systém by fungoval nasledovne:

a) Klient by prišiel k bankomatu a nechal si zosnímať čip
b) Systém by z databázy vyhodnotil o koho ide a požiadal by ho o priloženie prstu na biometrický systém
c) Po úspešnom porovnaní by klient mohol pristupovať ku svojmu kontu v prípade neúspešného pokusu by bolo snímanie prevedené ešte maximálne dva krát a následne by došlo k zablokovaniu.

Autorizáciu čipom by sme ponechali hlavne preto, aby sa odtlačky prstov v databáze už len porovnávali. Pokiaľ by systém autentizoval rovno odtlačkom prstu mohol by nastať veľký problém s rýchlosťou, pretože systém by hľadal odtlačok prstu medzi každým jedným klientom každej banky na svete, ktorá by používala biometrické systémy. Ďalší problém pri zosnímaní len odtlačku prstov bez autorizácie čipom je, že veľa ľudí má viacero bankových kont a preto by nemuselo byť jasné z ktorého konkrétneho chce vyberať.

Obrázok 21 Návrh bankomatu so zabudovaným biometrickým systémom odtlačku prstu [53]

Výhody nového systému pre banku

Hlavnou výhodou je určite obrovské zvýšenie bezpečnosti. Systém by hneď na začiatku autentizoval klienta a povolil mu prístup ku svojmu kontu. Faktom je aj to, že zmena by nebola radikálna, a teda by si ľudia na to nemuseli dlho zvykať. Bankám by odpadla starosť s platobnými kartami, ktoré by nahradili autorizačné čipy. Dalo by sa predpokladať, že v prípade autorizačných čipov bude počet krádeží oveľa nižší ako v prípade platobných kariet, nakoľko biometrický systém nie je také ľahké oklamať.

Nevýhody nového systému pre banku

Najväčšia nevýhoda sú financie, ktoré by sa do tohto návrhu museli dať. Namontovať na každý bankomat nový snímač odtlačkov prstov a čipový snímač by určite bolo finančne dosť náročné hlavne vzhľadom k množstvu bankomatov. Nepríjemnosťou pre banky by bola aj nutnosť zosnímať každému jednému klientovi banky odtlačok prstu. Táto akcia by však bola iba jednorazová.

Výhody nového systému pre klienta

Nový systém by klientovi odľahčil starosti s pamätaním PIN kódov. Tento problém nastáva hlavne pokiaľ má človek viacero platobných kariet a na každej iný PIN kód. Každého klienta banky tiež určite poteší aj zvýšenie bezpečnosti ich bankového konta.

Nevýhody nového systému pre klienta

Nevýhodou je, že autorizácia stále prebieha pomocou čipov a teda stála nutnosť mať pri sebe autorizačný čip. Niektorým ľuďom by mohlo vadiť zosnímávanie prstov z hygienických dôvodov.

5.3 Riešenie pre Smartbanking

5.3.1 Dnešný systém smartbankingu

Smartbanking nie je zatiaľ ani zďaleka taký rozšírený ako napríklad bankomaty a platobné karty. Napriek tomu, aj tak treba dbať o jeho bezpečnosť, ale aj jednoduchšiu autorizáciu a autentizáciu. V dnešnej dobe je riešenie mobilného bankovníctva pomerne zložité a zbytočne zdĺhavé. Pri bežnom prihlasovaní treba zadať prihlasovacie meno a PIN kód. Následne príde na telefón (väčšinou na ten istý odkiaľ sa prihlasujeme) SMS s autorizačným kódom, ktorý treba zadať do prihlasovacej aplikácie a znova treba zadať prihlasovací kód. Toto riešenie mi príde z pohľadu klienta veľmi nepraktické. V novom návrhu opäť využijem biometrické systémy ako súčasť autorizácie a autentizácie. Pri mobilných telefónoch zavádzanie biometrických systémov nie je ťažké. Dnes už máme na trhu telefón, ktorý podľa odtlačku prstu autorizuje majiteľa a povoľuje mu prístup bez zadávania hesla. Takisto býva bežne v lepších smartfónoch zabudovaná aplikácia, ktorá povoľuje prístup do telefónu zosnímaním tváre. V našom návrhu sa budeme viac zameriavať opäť na biometrické systémy a konkrétne odtlačky prstov. Vzhľadom na vývoj mobilných telefónov sa dá predpokladať, že mobilných telefónov so zabudovaným biometrickým systémom, ktorý skúma odtlačky prstov bude pribúdať.

Výhody dnešného systému z pohľadu banky

Aplikácia pre smartbanking funguje spoľahlivo a rýchlo. Je veľmi prehľadná a má jednoduché ovládanie. Výhodou je, že aj pri krádeži telefónu sa páchateľ bez platného prihlasovacieho mena a hesla nedostane do bankovej aplikácie.

Nevýhody dnešného systému z pohľadu banky

Medzi veci, ktoré považujeme za nevýhody smartbankingu je nutnosť vlastniť smartfón. Bez smartfónu si človek totiž nestiahne aplikáciu pre elektronické bankovníctvo. Toto môže byť problém hlavne u starších ľudí, ktorí majú problém so samotným ovládaním

mobilného telefónu a teda prichádzajú o možnosť používania elektronického bankovníctva. Nevýhodu je aj fakt, že momentálne sa začínajú objavovať nové vírusy, ktoré napádajú mobilné telefóny a sú priamo určené pre sledovanie prihlasovacích mien a hesiel do systému.

Výhody dnešného systému z pohľadu klienta

Výhodami pre klienta je určite, že aplikácia je prístupná zadarmo a že ju takisto ako Android poskytuje aj Apple a Windows Phone. Výhodou je jednoduchá manipulácia a hlavne, že svoje bankovníctvo môžeme ovládať odkiaľkoľvek pokiaľ tam máme prístup na internet.

Nevýhody dnešného systému z pohľadu klienta

Hlavný problém klienta pri používaní internetového bankovníctva vidím v zadávaní dlhých prihlasovacích mien a hesiel. Problémom je hlavne uskladnenie týchto hesiel, keďže ich uloženie do telefónu predstavuje obrovské riziko.

5.3.2 Nový systém pre smartbanking

Ako bolo písané vyššie, dnes sa už pomaly začínajú objavovať telefóny s biometrickým systémom odtlačku prstov. Ten zatiaľ slúži len na odblokovanie telefónu. V budúcnosti by sa však táto forma autorizácie dala použiť aj na iné účely prihlasovania a v neposlednom rade by to mohlo byť pre smartbanking. Pri smartbankingu by som nechala prihlasovanie do systému len na základe biometrického prihlásenia, teda zosnímania odtlačku prstu. To by slúžilo na prihlásenie do systému a teda by človek videl, aký má zostatok na účte. Pokiaľ by chcel s peniazmi aj manipulovať, bolo by treba zadať PIN kód, ktorý by bezpečnosť systému viac podporil. V tomto prípade by sme určite vynechali autentizáciu SMS kódom, keďže v 99% prípadov by SMS prišla na telefón z ktorého je užívateľ prihlásený do smartbankingu.

Fungovanie systému sa teda dá zhrnúť v nasledujúcich krokoch:

a) Spustenie aplikácie pre smartbanking
b) Zosnímanie odtlačku prstu pomocou zariadenia zabudovaného v mobilnom telefóne.

Obrázok 22 Jedna z možností ako by mohlo vyzerať prihlasovanie do smartbankingu

c) Priradenie konkrétneho odtlačku prstu ku klientskému kontu

Obrázok 23 Jedna z možností ako by mohla vyzerať prebiehajúca autorizácia pri prihlasovaní do smartbankingu

d) Prihlásenie do internetbankingu

Výhody nového systému pre banky

Vyššia bezpečnosť internetového bankovníctva a tým vyššia dôvera klienta voči banke.

Nevýhody nového systému pre banky

Nutnosť spraviť novú aplikáciu pre smartbanking a potreba zosnímania odtlačkov prstov všetkých klientov, ktorý by sa chceli prihlasovať do smartbankingu pomocou odtlačkov prstov.

Výhody nového systému pre klienta

Vyššia bezpečnosť a jednoduché prihlásenie. Ak klient iba kontroluje zostatok na účte tak nie je nutnosťou si pamätať PIN kód.

Nevýhody nového systému pre klienta

Nutnosť vlastniť mobilný telefón so zabudovaným biometrickým systémom na snímanie odtlačkov prstov.

5.4 Riešenie pre Internetbanking

5.4.1 Dnešný systém internetbankingu

Internetbanking ČSOB má autorizáciu a autentizáciu svojich klientov dnes vyriešenú pomocou prihlasovacieho mena a PIN kódu. Po zadaní týchto dvoch požiadavkov môže byť klient rovno presmerovaný na elektronické bankovníctvo, alebo môže nasledovať ešte autorizácia pomocou autorizačnej SMS správy. Tento systém je zdĺhavý a nepohodlný pre klienta. Takisto nie je veľmi bezpečný, hlavne čo sa týka napadnutia počítača spywareom alebo podvodnými technikami akými sú phishing, pharming a vishing o ktorých som písala v kapitole 2. Pre porovnanie, v Komerčnej banke je prihlasovanie do internetového bankovníctva riešené pomocou certifikátu, ktorý vydá klientovi banka a ten si ho uloží do počítača, na USB kľúč alebo na iné zariadenie. Okrem certifikátu klient zadáva aj heslo a podľa nastavenia môže aj nemusí zadávať autorizačný kód z SMS správy.

Výhody dnešného systému pre banky

Systém sa stáva čím ďalej populárnejším a začína ho používať veľké množstvo ľudí čo môže pre banky znamenať hlavne zníženie počtu ľudí na pobočkách. Čo sa týka bezpečnosti, pokiaľ je klient dobre informovaný o phishingu a pharmingu, má dobrú ochranu počítača a má nastavenú autentizáciu tromi krokmi, tak môžeme povedať, že je jeho internetbanking veľmi dobre zabezpečený.

Nevýhody dnešného systému pre banky

Nevýhodou pre banky je hlavne fakt, že sa stále vyskytuje veľké množstvo phishingu a pharmingu. Preto sa stále stáva, že klientom bánk sú kvôli týmto podvodným technikám odcudzené finančné prostriedky. Tým vzniká prípadná nedôvera voči bankám.

Výhody dnešného systému pre klienta

Jednoduché ovládanie, rýchla manipulácia a v neposlednom rade nie je nutnosťou pri prihlasovaní do internetového bankovníctva vlastniť počítač alebo iný komponent pripojený k počítaču, ktorý by slúžil na biometrické overenie identity a následné prihlásenie.

Nevýhody dnešného systému pre klienta

Jednou z veľkých nevýhod je stále veľké množstvo napádania počítačov hlavne phishingom a pharmingom. Ďalej prihlasovanie je zdĺhavé. V rámci ČSOB si treba pamätať dlhé prihlasovacie meno a PIN kód.

5.4.2 Nový systém pre internetbanking

Bankový klienti by namiesto zadávania prihlasovacieho mena a PIN kódu previedli len autentizáciu pomocou odtlačku prstov. Zariadenia na snímanie odtlačkov prstov sa už dnes bežne vyskytujú zabudované v notebookoch. Pokiaľ klient nemá v notebooku zabudovaný snímač odtlačkov prstu, môže si zakúpiť snímač, ktorý je zabudovaný v USB kľúči. Fungovanie systému:

a) Po spustení stránky s internetovým bankovníctvom by si užívateľ najskôr nechal zosnímať odtlačok prstu

b) Ako druhý krok by prebehlo porovnávanie snímku s databázou klientov konkrétnej banky.
c) Ďalej by si systém vypýtal zadanie PIN kódu
d) Po úspešnom overení bude klient, bez ďalších zadávaní autorizačných SMS, automaticky pripustený k obsluhovaniu svojho internetového bankovníctva.

Aby tento systém fungoval, je samozrejmosťou potreba zosnímania odtlačkov prstov klientov. Na rozdiel od bankomatov kde sme zvolili najskôr autentizáciu čipom a až potom biometrickým systémom sme tu zvolili rovno biometrický systém. Je to hlavne preto, že pri výbere z bankomatu nie je dopredu jasné k akej banke klient patrí, zato pri prihlasovaní do internetového bankovníctva je vopred jasné do ktorej banky klient patrí a tým sa rapídne znižuje počet možných prihlasovaných ľudí . Prihlasovanie by sa dalo riešiť aj trojitou ochranou a to napríklad zadávaním mena potom PIN kódu a až potom by nasledovalo zosnímanie odtlačku prstu. Tento systém by mohol byť ešte bezpečnejší, ale je, pri zachovaní čo najvyššieho komfortu klienta, nevhodný. Čo sa týka prevodov z účtu na účet, bude systém autorizovať klienta navyše pomocou autorizačnej SMS správy.

Výhody nového systému pre banku

Vyššia bezpečnosť a zabránenie páchateľom využívať podvodné techniky ako sú phishing a pharming.

Nevýhody nového systému pre banku

Hlavnou nevýhodou je nutnosť vytvorenia novej aplikácie. Medzi nevýhodami je aj potreba zosnímať odtlačky prstov všetkých klientov

Výhody nového systému pre klienta

Jednoduchosť prihlasovania - z troch prihlasovacích krokov sa stanú iba dva, vyššia bezpečnosť a vyšší komfort.

Nevýhody nového systému pre klienta

Nutnosť vlastniť zariadenie, ktoré z počítača, notebooku alebo z iného zariadenia pripojeného k počítaču alebo notebooku zosníma odtlačky prstov.

5.5 Zhnutie

Vo všetkých troch častiach (bankomaty a platobné karty, smartbanking, internetbanking) je návrh zameraný na biometrické systémy odtlačku prstu. Tento systém bol volený hlavne pre jeho jednoduchosť získania, jedinečnosť a pre to, že sa vekom nemení. Pri výbere biometrického systému sa rozhodovalo medzi odtlačkom prstu a hlasom. Hlas má veľmi podobné vlastnosti ako odtlačok prstu a mikrofóny na snímanie hlasu sú súčasťou takmer každého telefónu, tabletu a notebooku ale biometrický systém snímania hlasu má jednu zásadnú nevýhodu a to zmena hlasu pri chorobe, zachrípnutí alebo prípadná strata hlasu. Vtedy by užívateľ nemal šancu sa prihlásiť. Zvyšné biometrické systémy mali iné nevýhody ako zlé priatie verejnosťou či problém so zabudovaním do mobilných telefónov, tabletov, notebookov a stolných počítačov.

ZÁVĚR

Elektronické bankovníctvo je forma komunikácie banky a klienta, kedy nie je potrebné sa osobne stretávať ale komunikácia prebieha iba vo virtuálnej forme. Takúto formu komunikácie je teda treba dostatočne zabezpečiť.

V teoretickej časti práce bola postupne spracovaná charakteristika jednotlivých foriem elektronického bankovníctva – platobné karty, mobilné bankovníctvo a internetové bankovníctvo. Ku každej forme bolo napísané ako funguje a v krátkosti rozobraná ich bezpečnosť. Ďalej sa práca zaoberala jednotlivými druhmi elektronických krádeží zameraných na bankový sektor. Hlavnými podvodnými technikami, ktoré boli vypísané sú phishing, pharming, vishing, skimming, spying a tabnabbing. Každý človek, ktorý využíva najmenej jednu z foriem elektronického bankovníctva by mal mať o týchto technikách aspoň minimálne znalosti. Tiež boli v tejto kapitole vymenovaný najznámejší hackeri, ktorým sa podarilo odcudziť bankám nemalé finančné prostriedky. V tretej časti práce bolo písané o porovnaní bankových krádeží na Slovensku a v Európe. Tu sme dospeli k názoru, že na Slovensku je elektronické bankovníctvo pomerne bezpečné oproti iným krajinám Európy. Posledná kapitola teoretickej časti sa zaoberala novými technológiami v oblasti elektronického bankovníctva. Boli tu opísané nové technológie ako smartbanking, paypass, QR kódy, mobito, 3D secure ale hlavne biometrické systémy ktoré sme aplikovali do praktickej časti.

Praktická časť opisovala spôsoby autorizácie a autentizácie a následne bola rozdelená na tri časti a to bankomaty a platobné karty, smartbanking a internetbanking. V každej z týchto troch častí bolo opísané zdokonalenie bezpečnosti autorizácie a autentizácie pomocou biometrických systémov. Všetky návrhy obsahovali jeden konkrétny biometrický systém a to biometrický systém odtlačku prstu. K jednotlivým častiam je navrhnutý nový spôsob prihlasovania do systému, ktorý zahrňuje zosnímanie odtlačku prstu. Na konci praktickej časti bolo opísané, prečo sme sa rozhodli práve pre tento systém.

Prínos práce vidím v komplexnom zhrnutí problematiky elektronického bankovníctva zrozumiteľným a niekedy nevedeckým štýlom písania. Dúfam, že čitateľ si z tejto práce odnesie aspoň minimálne znalosti o problematike bezpečnosti elektronického bankovníctva.

SEZNAM POUŽITÉ LITERATURY

[1] KLIMKOVÁ, M. *Platobný stik*. Bratislava: Maradal Capital Services, 2008. ISBN 978-80-968458-9-7.

[2] PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy*. 1. vyd. Praha: Computer Press, 2000. 44 s. ISBN 80-722-6328-5.

[3] MÁČE, Miroslav a Jan KALA. *Platební styk: klasický a elektronický*. 1. vyd. Praha: Grada, 2006, 220 s. Praxe manažera. ISBN 80-247-1725-5.

[4] JUŘÍK, Pavel. *Svět platebních a identifikačních karet*. 2.přepr.vyd. Praha: Grada Publishing, 2001. ISBN 80-247-0195-2.

[5] Skimming. [online]. 2010 [cit. 2014-05-23]. Dostupné z: http://turek.co/post/44057699176/skimming

[6] Internetbanking neohrozuje kamenné pobočky. Znižuje len množstvo v nich spotrebovaného papiera. [online]. 2013 [cit. 2014-05-23]. Dostupné z: http://www.investujeme.sk/internetbanking-neohrozuje-kamenne-pobocky-znizuje-len-mnozstvo-v-nich-spotrebovaneho-papiera/

[7] Internet Banking: Boon or Bane ?. [online]. [cit. 2014-04-20]. Dostupné z: http://www.arraydev.com/commerce/jibc/2004-12/perumal.htm

[8] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management : BTSM 2007 : sborník mezinárodní konference, 12. a 13. září 2007, Zlín. Zlín: Univerzita Tomáše Bati, 2007. ISBN 9788073186050.

[9] Homebanking. [online]. č. 2012 [cit. 2014-05-23]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/home-banking/pruvodce/

[10] Nastavení stahování výpisů a odesílání příkazů. [online]. 2012 [cit. 2014-05-23]. Dostupné z: http://www.ucetnictvi-vyhodne.cz/nastaveni-stahovani-vypisu-a-odesilani-prikazu-homebanking/

[11] Mobilní bankovnictví. [online]. 2010 [cit. 2014-05-23]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/mobilni-bankovnictvi/pruvodce/

[12] Přímé bankovnictví. [online]. 2009 [cit. 2014-05-23]. Dostupné z: http://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/

[13] PROTIVINSKÝ, Miroslav. *Bankovní loupeže*. Vyd. 1. Praha: Armex, 2001, 279 s. ISBN 80-862-4421-0.

[14] Warning: Phishing Mail Targeted at PayPal Users. *Search engine optimization* [online]. 2007, [cit. 2014-03-17]. Dostupné z: http://seo.mhvt.net/blog/?p=163

[15] A Brief History of Phishing. *Symantec* [online]. 2007 [cit. 2014-03-12]. Dostupné z: http://www.symantec.com/connect/blogs/brief-history-phishing-part-i

[16] Brief hitory of Phishing. *Bright hub* [online]. 2011 [cit. 2014-03-12]. Dostupné z: http://www.brighthub.com/internet/security - privacy/articles/82116.aspx

[17] První phishing v Česku, terčem byla CitiBank. *Finance* [online]. 2006 [cit. 2014-03-17]. Dostupné z: http://www.finance.cz/zpravy/finance/63677-prvni-phishing-v-cesku-tercem-byla-citibank/

[18] První phishing v Česku, terčem byla CitiBank. *Finance* [online]. 2006 [cit. 2014-03-17]. Dostupné z: http://www.finance.cz/zpravy/finance/63677-prvni-phishing-v-cesku-tercem-byla-citibank/

[19] Jak se dělá phishing. [online]. 2008 [cit. 2014-03-17]. Dostupné z: http://www.lupa.cz/clanky/jak-se-dela-phishing/

[20] Inside a phishing attack: 35 credit cards in 5 hours. *We live security* [online]. 2011 [cit. 2014-03-17]. Dostupné z: http://www.welivesecurity.com/2011/01/26/inside-a-phishing-attack-35-credit-cards-in-5-hours/

[21] Original fishing scheme against Poste Italiane. *Security Affairs* [online]. 2013[cit. 2014-03-17]. Dostupné z: http://securityaffairs.co/wordpress/18883/cyber-crime/complex-fishing-poste-italiane.html

[22] Pharming. [online]. 2009 [cit. 2014-03-17]. Dostupné z:
http://www.sociotechnika.ic.cz/web/web/pharming/pharming.html

[23] Nový typ podvodu v internetbankingu - „vishing“. [online]. 2010 [cit. 2014-03-17].
Dostupné z: http://www.sbaonline.sk/sk/presscentrum/tlacove-spravy-sba/novy-typ
podvodu-v-internetbankingu-vishing.html

[24] Dajte si pozor na skimming! Viete rozpoznať sfalšovaný bankomat?. [online]. 2013 [cit. 2014-03-17]. Dostupné z: http://www.itnews.sk/spravy/bezpecnost/2013-03-04/c154590-dajte-si-pozor-na-skimming-viete-rozpoznat-sfalsovany-bankomat

[25] DOBDA, Luboš. *Ochrana dat v informačních systémech*. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.

[26] Najväčšie hackerské útoky všetkých čias. *TS PCR/wired* [online]. 2001 [cit. 2014-05-23]. Dostupné z: http://www.itnews.sk/spravy/internet/2001-02-08/c115008-najvacsie-hackerske-utoky-vsetkych-cias

[27] Hacking, cesta za poznáním. [online]. 2009 [cit. 2014-05-23]. Dostupné z: http://nadsencuv.blog.zive.cz/2009/06/hacking-cesta-za-poznanim/

[28] Příchod Hackerů: Vladimír Leonidovič Levin. [online]. 2014 [cit. 2014-05-23]. Dostupné z: http://nadsencuv.blog.zive.cz/2009/06/hacking-cesta-za-poznanim/

[29] Nejznámější hackeři světa začali útočit již v dětském věku. [online]. 2008 [cit. 2014-05-23]. Dostupné z: http://vtm.e15.cz/nejznamejsi-hackeri-sveta-zacali-utocit-jiz-v-detskem-veku

[30] Hacker z FBI půjde na 20 let do vězení za krádež dat z platebních karet. [online]. 2010 [cit. 2014-05-23]. Dostupné z: http://pcworld.cz/novinky/hacker-z-fbi-pujde-na-20-let-do-vezeni-za-kradez-dat-z-platebnich-karet-9496

[31] Skimming na Slovensku. [online]. 2013 [cit. 2014-05-23]. Dostupné z: http://www.sbaonline.sk/sk/presscentrum/tlacove-spravy-sba/skimming-slovensku.html

[32] ATM Cash Trapping on the Rise. [online]. 2013 [cit. 2014-05-23]. Dostupné z: http://www.bankinfosecurity.com/atm-cash-trapping-on-rise-a-4675/op-1

[33] Phishingový útok na Slovenskú sporiteľňu sa šíri už aj v slovenčine. [online]. 2008 [cit. 2014-05-23]. Dostupné z: http://www.itnews.sk/spravy/bezpecnost/2008-03-26/c86735-phishingovy-utok-na-slovensku-sporitelnu-sa-siri-uz-aj-v-slovencine

[34] Mobile banking. [online]. 2012 [cit. 2014-05-23]. Dostupné z: http://books.google.cz/books?id=pB_6qEL5ppkC&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[35] Bankovní účty Přímé bankovnictví Mobilní bankovnictví Mobilní aplikace bank a pojišťoven pro iOS, Android a Windows Phone. [online]. 2013 [cit. 2014-05-23]. Dostupné z: http://www.mesec.cz/clanky/mobilni-aplikace-bank-a-pojistoven-pro-ios-android-windows-phone/

[36] European Mobile Banking Users Get Smarter. *Banking/Finance, Europe, Mobile* [online]. 2012 [cit. 2014-05-23]. Dostupné z: http://www.comscoredatamine.com/2012/09/european-mobile-banking-users-get-smarter/

[37] Co je to MasterCard® PayPass™?. [online]. 2010 [cit. 2014-05-23]. Dostupné z: http://www.paypass.cz/stranka/1/co-je-paypass/

[38] Bezkontaktní platební karty. Jsou bezpečné?. [online]. 2011 [cit. 2014-05-23]. Dostupné z: http://www.penize.cz/platebni-karty/259327-bezkontaktni-platebni-karty-jsou-bezpecne

[39] Využívate QR kódy?. [online]. 2012 [cit. 2014-05-23]. Dostupné z: http://vat.pravda.sk/technologie/clanok/26773-tip-vyuzivate-qr-kody/

[40] QR kódy: kilobajty v malém obrázku. [online]. 2010 [cit. 2014-05-23]. Dostupné z: http://www.root.cz/clanky/qr-kody-kilobajty-v-malem-obrazku/

[41] By Square: Platba faktúr pomocou QR kódov. [online]. 2012 [cit. 2014-05-23]. Dostupné z: http://www.zive.sk/clanok/56556/by-square-platba-faktur-pomocou-qr-kodov

[42] Startuje Mobito, mobilní elektronické peníze po česku nejen pro smartphony. [online]. 2012 [cit. 2014-05-23]. Dostupné z: http://www.lupa.cz/clanky/startuje-mobito-mobilni-elektronicke-penize-po-cesku-nejen-pro-smartphony/

[43] Citibank spustila u svých karet podporu 3D Secure. Jak to funguje?. [online]. 2011 [cit. 2014-05-23]. Dostupné z: http://www.mesec.cz/clanky/citibank-spustila-u-svych-karet-podporu-3d-secure/

[44] Who Needs 3D Secure? Verified By Visa and MasterCard SecureCode Examined. [online]. 2011 [cit. 2014-05-23]. Dostupné z: http://www.getelastic.com/who-needs-3d-secure-verified-by-visa-and-mastercard-securecode-examined/

[45] Biometrické technológie. [online]. 2010 [cit. 2014-05-23]. Dostupné z: http://www.ktl.elf.stuba.sk/~orgon/lednicky/?page=54

[46] Authentication. *Security Engineering*. [online]. 2007 [cit. 2014-05-23]. Dostupné z: http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/biometric.html

[47] Jak je to s bezpečností internetového bankovnictví?. [online]. 2006 [cit. 2014-05-23]. Dostupné z: http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/

[48] MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008, 125 s. ISBN 978-802-1045-569.

[49] VPN siete s OpenVPN. . [online]. 2009 [cit. 2014-05-23]. Dostupné z: http://linuxos.sk/clanok/vpn-siete-s-openvpn-5/

[50] EToken. . [online]. 2009 [cit. 2014-05-23]. Dostupné z: http://safesolution.co.in/aladdin-usb-token/

[51] Generátor hesel ZyXEL. . [online]. 2011 [cit. 2014-05-23]. Dostupné z: http://www.losancomputers.cz/75411-ZyXEL-ZyWall--OTP-One-Time-Password--5U-Starter-Pack---Autentification-token-Safenet-NETZ0115.html

[52] Fingerprint usb disk. . [online]. 2011 [cit. 2014-05-23]. Dostupné z: http://www.diytrade.com/china/pd/6407561/Fingerprint_usb_disk.html

[53] Biometric ATMs, the future?. [online]. 2005 [cit. 2014-05-28]. Dostupné z: http://www.rediff.com/money/2005/oct/11atm.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PIN	Osobné identifikačné číslo
GSM	Globálny systém mobilných komunikácií
WAP	Protokol pre bezdrôtové zariadenia
SMS	Krátka textová správa
SSL	Vrstva bezpečných socketov
TCP/IP	Primárny prenosový protokol
HTTP	Hypertextový prenosový protokol
HTTPS	Zabezpečený hypertextový prenosový protokol
DNS	Systém názvov domén
PC	Osobný počítač
FBI	Federálny úrad pre vyšetrovanie
GPS	Globálny lokalizačný systém
DNA	Deoxyribonukleová kyselina
ČR	Česká republika
ČSOB	Československá Obchodná Banka a.s.
PDF	Prenosný formát dokumentov

SEZNAM OBRÁZKŮ

SEZNAM TABULEK