Bezpečnost bankovních transakcí

Security of bank transaction

Bc. Lukáš Vojáček

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš VOJÁČEK**
Osobní číslo:	**A09414**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost bankovních transakcí.**

Zásady pro vypracování:

1. **Popište principy bankovních systémů.**
2. **Zhodnoťte možné způsoby úniku citlivých informací a jejich následné zneužití k páchání trestné činnosti prostřednictvím bankovních transakcí.**
3. **Analyzujte organizovaný zločin zaměřený na zneužití citlivých informací v bankovních systémech.**
4. **Odhadněte vývoj bankovních systémů.**
5. **V praktické části navrhněte opatření pro zkvalitnění bezpečnosti bankovních systémů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **MÁČE, Miroslav. Platební styk : klasický a elektronický. Praha : Grada, 2006. 220 s. ISBN 80-247-1725-5.**
2. **JUŘÍK, Pavel. Platební karty 1870-2006 : velká encyklopedie. Praha : Grada, 2006. 296 s. Dostupné z WWW: http://books.google.cz/books?id=uQ9Vd-fGEx8C&printsec=frontcover&v=onepage&q&f=false.**
3. **ZÁMEČNÍK, Petr. Internetové bankovnictví. Kde je bezpečné?. 2008, 5, s. 4. Dostupný také z WWW:http://earchiv.chip.cz/cs/earchiv/vydani/r-2008/internetove-bankovnictvi-kde-je-bezpecne.html.**
4. **MERVART, Dominik. Systém pro správu bankovních účtu. Praha, 2009. 79 s. Bakalářská práce. České vysoké učení technické v Praze.**
5. **SHARAD JOSHI, Mayur. Black Cards Forensics : Classification of ATM and credit card fraud schemes. India : Indiaforensic research foundtation, 2006. 94 s.**

Vedoucí diplomové práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tématem této diplomové práce je bezpečnost bankovních transakcí. V práci se seznámíte s tím, jak probíhají bankovní transakce, jak jsou zabezpečeny a jak je možné zabezpečení zvýšit. Neopomenutelnou částí je také popis trestné činnosti páchané zneužitím citlivých informací v bankovním sektoru. Závěrem jsou popsány návrhy na zvýšení bezpečnosti související s ochranou finančních prostředků klientů bank a obchodníků.

Klíčová slova: bankovní transakce, platební karta, finanční prostředky, PIN, číslo karty, organizovaný zločin

ABSTRACT

The topic of this Master Thesis is the security of banking transactions. The Thesis describes how banking transactions take place, how they are secured and how their security can be increased. The Thesis´s unomittable part is also the description of the criminal activity associated with the abuse of sensitive information in the banking sector. Finally, it describes the proposals for improving the safety related to the protection of the financial means of the banks´ clients and vendors.

Key words: banking transactions, credit card, financial means, PIN, card number, organized crime

Tímto chci poděkovat vedoucímu mé diplomové práce Ing. Rudolfu Drgovi za poskytnuté rady a informace. Především ale děkuji svým rodičům, přítelkyni a celé rodině za morální a finanční podporu při studiu.

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 práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Provádění bankovních transakcí se stalo součástí pracovního i osobního života lidí po celém světě. Některým nestačí jeden bankovní účet, a proto jich používají několik. Jen v České republice proběhlo za rok 2010 asi 240 milionů transakcí u obchodníků a bylo vydáno 9 milionů nových platebních karet. Jen v ČR funguje 48 bank. Množství dat, se kterými banky pracují je obrovské. Celý systém stále roste, ať už jde o síť bankomatů, platebních terminálů nebo internetového bankovnictví.

Banky se ubírají směrem zvyšování počtů transakcí a vlastních zisků, a pokud jim to zákon umožňuje, přesouvají maximální míru odpovědnosti za všechny transakce na zákazníka. Jedinou zemi kde to neplatí je USA, právě kvůli množství bankovních zločinů páchaných na jejím území. Nově zaváděné bezpečnostní prvky (např.: přechod na čipové karty a autentizaci PINem) pak většinou chrání zájmy bank a obchodníků, nikoliv však zákazníků. Dokazování zákazníkovy neviny v případě zneužití platební karty je někdy nelehké. Nutno podotknout, že banky jsou proti podvodu pojištěny, takže peníze dostanou vždy zpět. Pokud navíc zákazník nedokáže svou nevinu, musí chybějící finanční prostředky uhradit.

Existuje řada způsobů páchání trestné činnosti v bankovním odvětví. V této diplomové práci se však zaměříme na ty, které jsou prováděny nenásilně a nedestruktivně. Mnoho konkrétních metod páchání této trestné činnosti, které jsou dnes známé, jsou pro pachatele dostatečně bezpečné. Nejsilnějším impulzem v rozvoji této trestné činnosti se stal internet. Slouží ke komunikaci, kooperaci a k obchodům pachatelů. Organizovaný zločin, který vznikl v tomto odvětví stále roste. Existují organizované skupiny nebo jednotlivci obchodující s citlivými informacemi. Tito lidé využívají techniky anonymního prostředí internetu. Model podnikání této organizované trestné činnosti je založen na tom, že každý má svou funkci. Většina pachatelů mají funkce, na kterých pouze přeprodávají informace. Pachatele je pak těžké odhalit. Často se jedná o spolupráci pachatelů z různých částí světa. Systémem k provádění bankovních transakcí je propojen celý svět. V různých zemích se ale banky rozcházejí v bezpečnostních opatřeních. Nároky na jejich zabezpečení jsou jiné například v zemích Evropské Unie, Islandu anebo Thajsku. Dohody uzavřené pro Evropskou Unii povýšili její zabezpečení a zavedly se standardy, které se jinde ve světě nedaří zavádět v tak velké míře. Celosvětová modernizace bankovních systémů by však byla natolik nákladná, že ji není možné provést. Z toho plyne, že otevřenost systému po

celém světě umožňuje provádět v některých zemích nezákonnou činnost jednodušeji. Důležitá je informovanost klientů bank o bezpečnostní situaci, možnostech a právech, které mají.

I. TEORETICKÁ ČÁST

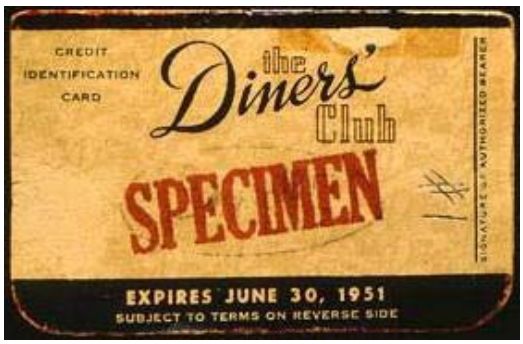
1 PLATEBNÍ KARTY

Platební karty nás v České republice provázejí od počátku devadesátých let a v současné době se najde jen minimum ekonomicky aktivních lidí, kteří nemají platební kartu. Mnoho klientů bank má dokonce platebních karet hned několik. Platební karty nám usnadňují život a umožňují nám pohodlně disponovat svými (debetní karty) nebo vypůjčenými penězi (kreditní karty). [1]

Lze jimi provádět bezhotovostní platby, výběr hotovosti a manipulaci na účtu. Jsou využívány spotřebitelským sektorem. Držiteli mohou být fyzické i právnické osoby. Jsou vydávány především bankami, ale i nebankovními vydavateli. Jedna platební karta může vázat uživatele k jednomu konkrétnímu účtu. Důležitá je informace o majiteli karty, kterým je po celou dobu její existence banka. Její uživatel a současně zákazník banky ji má od banky jen vypůjčenou a musí se řídit podmínkami stanovenými ve smlouvě.

1.1 Historie

Platební karty jsou nástrojem k manipulaci s finančními prostředky, které má k dispozici. K pochopení aktuálního stavu vývoje je vhodné popsat historii platebních karet. První platební kartu vydala společnost Diners Club. Měla již rozměry blížící se nynějším kartám, ale neobsahovala žádné technické prvky. Jmenovala se Diners Club Credit Identification Card a byla vynalezena v roce 1950. Tato nebankovní organizace předběhla i banky, které měly problémy s financováním výroby a reklamy. O pár let později však zavedla karty i společnost American express, která vznikla spojením několika velkých bank. Následovala Bank of America (dnešní společnost Visa), The Everything Card (dnešní karty Master Card) založena Citi Bank s dalšími bankami. První platební karta na území tehdejšího Československa byla vydána roku 1988 jako dispoziční karta k tuzexovému účtu.



Obr. 1 První platební karta ve světě a na území dnešní ČR [33]

Banky měly snahu o rozšíření co nejvíce karet. Kolem roku 1958 začaly posílat poštou statisíce karet zákazníkům. Dopadlo to tak, že mafie kupovala karty od poštovních doručovatelů za $50 a vybírali z nich $300. Některé banky měly ztráty až $70 milionů. Dnes by to znamenalo asi $70 miliard. Některé banky se ocitly na pokraji krachu. Banky neměly jak dostat své peníze zpět. Do této doby totiž neexistoval zákon, který by je chránil.

Bezpečnostní prvky, které bylo nutné v průběhu času zavádět se vyvíjely ve třech vrstvách:

- personální(fyzické)
- virtuální
- globální

V personální vrstvě se jednalo v první řadě o zavedení podpisu. Ten se ukázal jako výrazně nespolehlivý. Změna přišla s vynálezem telefonu. Obchodník, který si chtěl ověřit platbu, jednoduše zavolal do banky a vše potřebné zjistil. Pomalá, ale účinná metoda. Dalším prvkem, který ovlivnil vývoj karet, byl magnetický proužek (1966). Vymysleli jej v Anglii stejně jako požívání čipu a pinu. Následovali zanedlouho po magnetickém proužku. Karty byly v průběhu času také doplňovány o znaky pravosti, jako jsou obrázky měnící se při natočení karty. Technologie embosovaných karet zase přinesla zvýšení rychlosti i bezpečnosti v jednom. Novinkou posledních let je zavádění bezkontaktního přenosu informací z vaší karty do platebního terminálu nebo bankomatu (RFID). Co se týká vývoje virtuálního provádění transakcí prostřednictvím platební karty, šlo o číselný kód pro ověření pravosti (např.: Cvv kód). Master Card tuto technologii zavedl jako první (1997), následovala Visa a další. Dnes tuto technologii využívají všechny karty. Zvýšení ochrany mělo přinést zavedení metody ověřování 3D Secure (2004). V globální vrstvě jde o zavedení Payment card industries. Jedná se o globální pravidla pro zpracování, ochranu a ukládání dat v souvislosti s platebními kartami.

1.2 Rozdělení karet

Podle toho s jakými finančními prostředky lze s kartou nakládat

- *debetní - při platbě klient čerpá vlastní prostředky*
- *kreditní - při platbě klient automaticky čerpá úvěr, zpravidla však s jistým bezúročným obdobím (jedná se o manipulaci s penězi banky)*

- *charge - obdoba kreditní karty, bezúročný úvěr je klient povinen zaplatit v daném období po čerpání(jinak je penalizován sankčním úrokem), charge karty jsou určeny pro velmi bonitní klienty*
- *elektronická peněženka - kartou lze čerpat jen vyhrazený objem prostředků, kterým byl předem na kartu vložen (příkladem může být telefonní karta)*

Podle způsobu provedení

- *Elektronické platební karty - v ČR nejrozšířenější Tyto karty lze použít pouze pro online transakce – výběry z bankomatů či platby u obchodníků. Výhody těchto karet jsou: vedení zdarma, nízké poplatky za blokaci ztracené karty, nulová možnost zneužití zablokované karty*
- *Embosované platební karty - tyto karty mají plasticky vytištěny veškeré údaje o majiteli karty, platnosti, číslu karty. Bližší vysvětlení níže.*

[2]

Podle typu limitu (tyto limity neurčuje banka, ale vydavatel a zpracovatel karet)

- limit výběru
- limit transakce
- časový limit(denní, týdenní a další)

Konkrétní rozdělení banky, nebo vydavatele karet (např.: u společnosti Visa)

- Classic
- Prémiové karty - karty s vyšší úrovní služeb(Gold, Platinum, Infinite)
- Black card - nejexkluzivnější karty, nemají limit, údajně nejdražší věc koupena touto kartou byla Boeing 747, vlastní ji však pouze 10.000 lidí na světě

Obr. 2 Typy platebních karet VISA [34]

Podle technického vybavení karet (jedná se většinou o kombinace tohoto vybavení)

- magnetický proužek
- čip
- čip pro bezkontaktní platby

1.3 Popis platební karty

Mezinárodní norma ISO 3554 stanoví rozměr platební karty na 85,5 x 54 x 0,76 mm. Karta je vyrobena ze třívrstvého PVC, který musí být odolný, netoxický a elastický. Rozměr se nezměnil více než 40 let. Platební karty mají obě strany doplněny informacemi

pro jejich bezpečné a rychlé použití. Na přední straně naleznete logo banky, logo vydavatele, číslo karty, doba platnosti karty (expirační doba) a jméno majitele karty. Je-li karta služební, obsahuje navíc jméno společnosti, k jejímž účtu byla karta vydána Tyto všechny informace o kartě dost vypovídají. Pokud je text vystouplý karta je navíc embosovaná a skýtá další výhody. Posledním prvkem, který s určitostí najdete na přední straně platební karty je EMV čip pro autentizaci. Zadní strana obsahuje magnetický proužek, podpis vlastníka a verifikační kód pro bezkontaktní platby. Posledním prvkem objevujícím se na kartách je znak pro optické ověření, takzvaný hologram. Podobné jsou ochranné prvky viditelné jen pod UV světlem.

1.3.1 Číslo karty

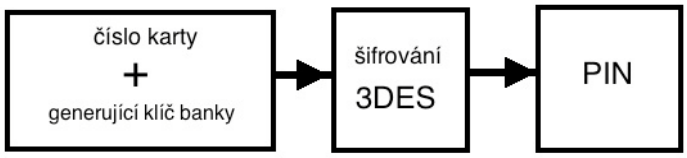
Základním prvkem karty je její číslo, které ji spojuje s konkrétním účtem. Všechny čísla platebních karet jsou generovány podle mezinárodní normy ISO 7812. Platební karty vydávané všemi společnostmi na světě jsou generované přes Luhnův algoritmus. Luhn byl inženýr ze společnosti IBM a algorytmus vymyslel v roce 1954. Používán je dodnes. Prvních 6 číslic čísla karty je nazýváno Issuer identification number, dříve Bank identification number (BIN). Takzvané identifikační číslo vydavatele. Z anglického názvu vyplývá, že karty nevydávají pouze banky, ale společnosti, které se zabývají technickou podporou bank (vydavatelé karet). Pomocí tohoto čísla je možné zjistit několik důležitých informací (vydavatele karty, zemi vydání, konkrétní typ karty, a telefonní číslo na zrušení karty). Dalších 9-12 čísel označuje číslo účtu u banky nebo vydavatele karty (identifikační číslo uživatele). Poslední číslo je kontrolní číslo pro ověření Luhnova algoritmu.

Obr. 3 Číslo karty

1.3.2 Bezpečnostní prvky platební karty

1.3.2.1 Pin

Označení pochází z anglického personal identification number (osobní identifikační číslo). Je to čtyřmístný bezpečnostní číselný kód, který je vyžadován při fyzickém použití platební karty. Pin není generován náhodně, ale na základě Primary account number(celé číslo karty) v kombinaci s generujícím klíčem(zná jej jen banka). Toto vygenerované číslo je na závěr zašifrováno metodou 3DES.



Obr. 4 Generování PIN kódu

Uživatelé mající na své kartě pouze magnetický proužek, nemohou pin měnit. Uživatelé, kteří mají kartu vybavenou i čipem mohou pin měnit. Změnit si svůj PIN bylo dříve možné pouze v bance. Nyní si je možné změnit PIN už i v bankomatech. Pokud si svůj pin změníte, není už zpětně vygenerovatelný. Pokud by generující klíč z banky unikl, byli by v bezpečí pouze uživatelé karet, co si změnili svůj pin. Tato situace je však nepravděpodobná.

1.3.2.2 Verifikační kód pro bezkontaktní platby

Jedná se o verifikační kontrolní kód, umístěný na platební kartě, jehož cílem je zabránit podvodům při platbách, u kterých nedochází k přímému kontaktu platební karty a terminálu. Jsou to takzvané „no present" platební transakce.

Tento kód existuje v několika verzích lišících se pouze minimálně (CVV,CVC, CID). Naleznete jej na většině karet na zadní straně reprezentováno třemi čísli. Pouze banka American Express má tento kód je složen z čtyř čísel a umístěn na přední straně karty. Ve všech variantách jde o generování z několika zdrojů. Tento kód je vytvořen kryptovací metodou, která používá číslo karty, servisní kód, expirační dobu a CVK (card

verification key), který zná jen banka. Při platbě například na internetu se pak ověřuje platnost kódu v závislosti na čísle karty a expirační době.

Obr. 5 Umístění CVV, CVC, CID [38]

1.3.2.3 Magnetický proužek

Proužek obsahuje množství magnetických částic kovového základu, schopných svou orientací uchovávat údaje. Takový magnetický proužek má poté dva až tři datové stopy pro záznam údajů. Bývá umístěn na zadní straně platební karty. Ve formě magnetického záznamu je na něm uložena řada informací, které jsou využívány k provedení bankovních operací. Nevýhodou magnetického proužku je fakt, že kapacita záznamu dat je omezená (1288 bitů). Záznam může být proveden s vyšší koercivitou (lepší ochrana proti poškození dat). Čtení magnetického proužku probíhá jeho protažením čtečkou se třemi čtecími hlavami. K provedení platby prostřednictvím magnetického proužku u obchodníka je k ověření nutný podpis vlastníka karty. Magnetickým proužkem je vybavena každá platební karta. I přes skutečnost, že se jedná o technologii zastaralou, musí být stále zaváděna kvůli zpětné kompatibilitě. Funguje na principu magnetického záznamu.

Při nahrávání dat na kartu se řídí vydavatelé karet pravidlem, které rozděluje země podle bezpečnosti. Každá zem je zařazena do rizikového stupně 1-10. Čím nižší stupeň, tím bezpečnější.

Podle posledního průzkumu je Česká republika označena číslem 6, stejně jako Slovensko. Proužek rozděluje norma ISO na tři datové stopy (tracky). První stopa slouží pro vnitrostátní off-line i on-line transakce. Její rozsah je 79 alfanumerických znaků a umožňuje pouze čtení dat. Druhá stopa slouží pro vnitrostátní a mezinárodní on-line transakce. Její rozsah je pouze 40 znaků a umožňuje také pouze čtení dat. Stopa třetí je pouze pro vnitrostátní off-line provoz, její rozsah je 107 znaků a je na vydavateli karty jak jej využije.

Složení první stopy je dáno normou ISO. Pokud se jedná o platební kartu, začíná vždy písmenem %B, následuje číslo karty, příjmení, jméno, expirační doba (4 čísla) a servisní kód. Tento kód je již zmiňovaný servisní kód na generování CVV, CVC a CID kódů. Jeho informační hodnota je ale ještě vyšší. Pokud má kód hodnotu 101, používá systém (např.: POS terminál) k ověření autentizace magnetický proužek. Pokud je hodnota kódu 201, používá k ověření čip. Záleží tedy na zařízení, přes které má být provedena transakce. Tuto službu totiž může nebo nemusí podporovat. Jestliže ji podporuje a na kartě není funkční ověřovací prvek, transakci nebude možné uskutečnit. To, co spojuje všechny banky je řada čísel, která následuje za servisním kódem. Je generován na základě issuer identification number. Tento kód je zásadní v tom, že je totožný u stejných typů karet (např.: stejný u všech Visa Classic). Banky tento kód čas od času mění. To je ale stále málo.

Příklad obsahu třístopého magnetického proužku:

1.stopa:

%B4406160384321844^NOVOTNY/ZDENEK.MR^021252116526000000000191

000000?;

2.stopa:

4406160384321844=02125211652619120?+

3.stopa:

014406160384321844=203000020000000030501200571310020000212 2=203162161814
71803==1=70000000000000000000? [7]

Obr. 6 VISA Electron ze které pochází data [7]

1.3.2.4 Podpis

Na zadní straně každé platební karty se nachází podpisový proužek, který slouží k ověření totožnosti majitele karty. Proužek lze vidět na obrázku 6. Na tomto proužku ze speciálního nenarušitelného materiálu se nachází podpisový vzor majitele platební karty. Nejčastěji je používán jako dodatečné ověření magnetického proužku ale je možné setkat se s podpisem jako jediným ověřením totožnosti. Kontrola porovnáním podpisů však už prakticky nefunguje. Obchodníci si podpis nechávají spíše kvůli doložení při problémech.

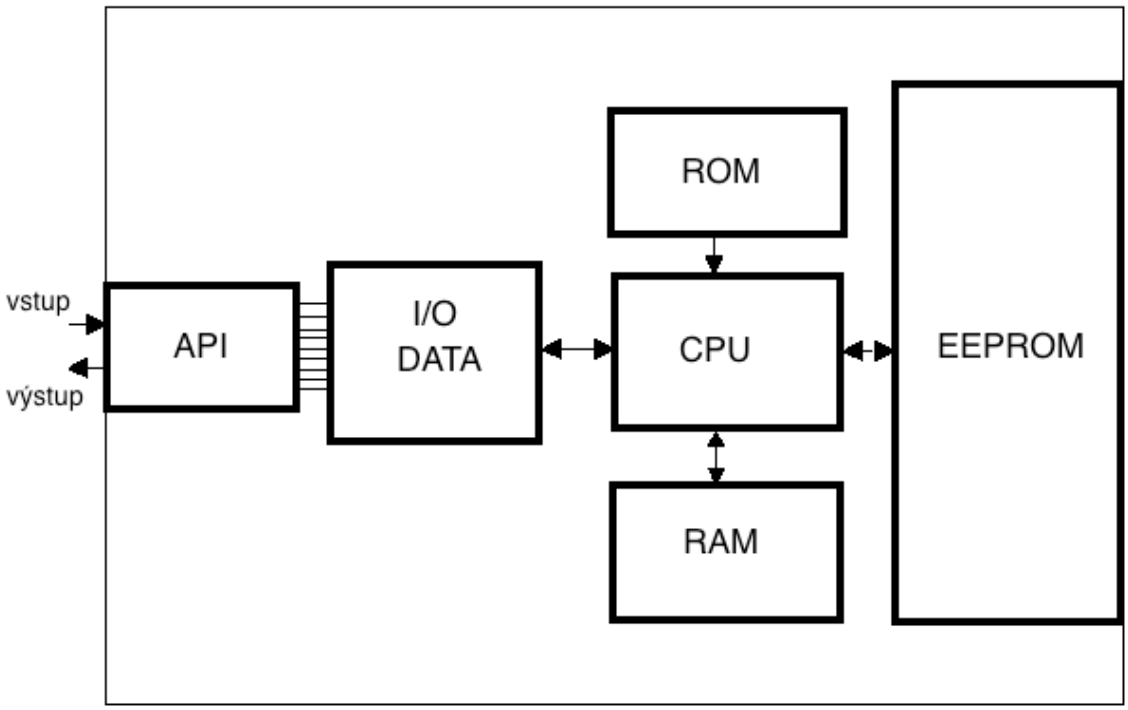
1.3.2.5 Čip

Čip je integrovaný obvod, který je schopen zpracovávat data. To znamená, že zařízení je schopno přijmout data, zpracovat je a vrátit požadované informace. Existuje řada důvodů, proč byly implementovány čipy na platební karty. Těmi nejdůležitějšími byli větší kapacita a bezpečnost. Konstrukce i programové vybavení mikroprocesoru umožňují do něj bezpečně vložit osobní PIN kód klienta nebo jiný verifikační prvek (např.: otisk prstu) a finanční parametry (limity apod.), které má klient k dispozici. Při použití čipu tak odpadá nutnost spojení bankomatu nebo platebního terminálu v reálném čase s autorizačními systémy (s čipem lze tedy provádět on-line i off-line ověřování PINu).

Čip se skládá z těchto částí:

- vstup a výstup - spojuje čip s vnějším světem, přes kontakty této jednotky prochází veškerá komunikace a zdroj napětí
- ROM - paměť pouze pro čtení, zde je uložen operační systém, umístěna v nejnižší vrstvě čipu, aby ji nebylo možné mapovat pomocí mikroskopu
- RAM - paměť k ukládání výsledků výpočtů ověřující vstupní kódy, data jsou ztracena po odpojení od napětí
- EEPROM - paměť k uložení programu a parametrů používaných pro jednotlivé aplikace, právě zde jsou uloženy všechny citlivé informace

- CPU - řídící jednotka mikroprocesoru, řídí a kontroluje veškerá data proudící v mikroprocesoru
- API - rozhraní pro komunikaci čipu s okolím



Obr. 7 Schéma čipu

V roce 1994 založily asociace Europay, MasterCard a VISA společnou pracovní skupinu pro vytvoření norem pro čipové platební karty (vychází z normy ISO 7816), zvanou Group EMV. Norma popisuje elektromechanické charakteristiky, interface a přenosový protokol, strukturu dat, strukturu dotazů a výběr aplikace v čipu. Pokud se některá banka nebo skupina bank rozhodne vyvinout například vlastní bankovní aplikaci, je detailně popsáno, jak si mohou banky počínat. Sestavení aplikace probíhá výběrem parametrů jako je řízení rizik, bezpečnost, personalizace karty a struktury dat.

Pokud budete platit čipovou kartou u obchodníka, který akceptuje čip, budete vyzváni k zadání PIN. Ve srovnání s ověřením prostřednictvím podpisu u karet s magnetickým proužkem, je ověření prostředním PIN bezpečnější. Hodnotu PIN má k dispozici pouze držitel karty na rozdíl od podpisu, který je viditelně zaznamenán na zadní straně karty. Data uložená v čipu jsou dostatečně chráněna a karty tak významně přispívají ke snížení rizika podvodných transakcí. Údaje, které jsou uloženy přímo v čipu jsou chráněny šifrováním(dříve 3-DES, dnes RSA). [3]

1.3.2.5.1 RSA

RSA (iniciály autorů Rivest, Shamir, Adleman) je šifra s veřejným klíčem, jedná se o první algoritmus, který je vhodný jak pro podepisování, tak šifrování. Používá se i dnes, přičemž při dostatečné délce klíče je považován za bezpečný. Bezpečnost RSA je postavena na předpokladu, že rozložit velké číslo na součin prvočísel (faktorizace) je velmi obtížná úloha. Z čísla n = pq je tedy v rozumném čase prakticky nemožné zjistit činitele p a q, neboť není znám žádný algoritmus faktorizace, který by pracoval v polynomiálním čase vůči velikosti binárního zápisu čísla n. Naproti tomu násobení dvou velkých čísel je elementární úloha. [4]

1.3.2.6 RRFID

Zkratka pochází z anglického Radio Frequency Identification (identifikace na principu rádiové frekvence). Jedná se o čip sloužící k bezkontaktní komunikaci na krátkou vzdálenost (podle ISO 14443 přibližně 10 cm). RFID čipy existují ve verzi pracující samostatně (aktivní) a s bezdrátovými dodávkami energie (pasivní). Implementace napájení do platební karty je zatím neproveditelná a tak jsou použity vždy pasivní RFID čipy.

Vysílač (terminál) periodicky vysílá do okolí elektromagnetické pulsy. Pokud se v blízkosti objeví pasivní RFID čip, využije přijímanou energii k nabití svého napájecího kondenzátoru a odešle odpověď. Jsou jimi vybavovány některé karty (u Master Card karty PayPass, u Visa PayWave). Tato technologie je většinou zaváděna do karet jako doplňková. Znamená to, že mimo magnetického proužku a běžného čipu je navíc vaše karta vybavena i čipem RFID. Existují však i karty vybaveny pouze RFID a tudž určeny pouze pro bezkontaktní platby. Tato metoda je využitelná u obchodníků a bank vybavených moderními technologiemi. Kartu už není nutné zasouvat ani ji protahovat čtečkou. Stačí ji jednoduše přiblížit ke speciálnímu terminálu. Banky nabízející tuto službu vidí zvýšení bezpečnosti v tom, že zákazník nedá kartu z rukou. Při použití této technologie není nutné zadání PIN kódu ani podepsání vlastníka karty. Mezi všemi metodami je placení využitím RFID nejrychlejší.

Tato technologie bezkontaktních plateb není implementována jen do platebních karet, ale i do klíčenek, mobilních telefonů a dalších zařízení. K rozeznání karet a míst, kde s mimi lze platit je použito jednoduché logo (Obr. 9)

Obr. 8 Platba kartou vybavenou RFID technologií [9]

Obr. 9 Označení RFID platební [35]

1.3.2.7 Emboss, reliéf

Vystouplé písmo, kterým jsou na platební kartě vyraženy karetní informace a informace o jejím držiteli (číslo platební karty a jméno majitele). Existence reliéfního písma na kartě výrazně rozšiřuje možnosti jejího použití - kromě obchodů vybavených elektronickým platebním terminálem lze embosovanou platební kartu použít také v obchodech, které jsou vybaveny pouze mechanickým snímačem (tzv. imprinterem). [5]

Obr. 10 Embossovaná platební karta

1.3.2.8 Vizuální bezpečnostní prvky

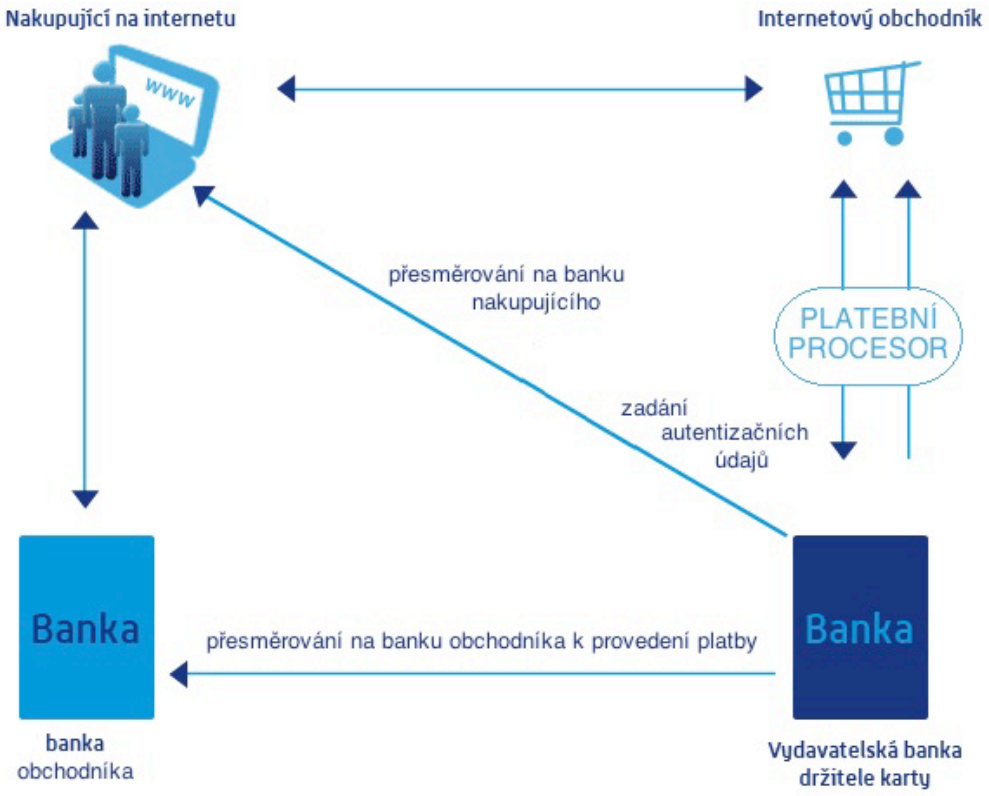
Nelze opomenout ani vizuální bezpečnostní prvky. Ty slouží k tomu, aby obchodník poznal na první pohled pravost platební karty. Už samotné logo banky vypovídá o důvěryhodnost. Dalším prvkem je kvalita provedení potisku karty. Nejvyšší důvěru v pravost karty však dodává hologram, umísťován na nové karty. Jedná se o lesklé obrázky, které mají svůj vzhled rozdílný pod různým úhlem. Člověku, který si bude chtít takto zkontrolovat kartu, stačí jen pohnout trochu kartou a hned pozná, jestli se jedná o pravou, nebo padělanou kartu.

Obr. 11 Hologram VISA

1.3.2.9 3D-SECURE

Velká část platebních bran dnes používá bezpečnostní systém 3D-secure, který zajišťuje bezpečnost tím, že údaje o své kartě nakupující neposkytuje obchodníkovi, ale prostřednictvím platebního procesoru je zjištěna banka nakupujícího, je přesměrován na její stránky a požádán o zadání autentizačních údajů. Po zadání správných autentizačních údajů je nakupující přesměrován na webové stránky banky obchodníka, kde provede

platbu. Přenos dat probíhá po SSL(secure socket layer), což je bezpečný protokol vložen mezi aplikační transparentní vrstvu. Přenos informací o kartě probíhá pomocí HTTPS protokolu (zabezpečená nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany), který údaje klienta zakóduje tak, že si nikdo kromě banky údaje nemůže přečíst. Zákazník mající kartu s aktivovaným 3D-secure navíc může rozšířit proces autentizace při placení o další údaje, které zná pouze on a nikdo jiný jeho kartou nezaplatí, i kdyby si zkopíroval obvyklé údaje kreditní karty (číslo, datum expirace, kontrolní číslo). Zákazník platící tímto typem karty, je pak vždy vyzván k zadání dodatečných údajů. Teprve po jejich zadání je transakce provedena. Tato metoda je používána pro virtuální transakce (např. internetové obchody).



Obr. 12 Schéma 3-D secure [8]

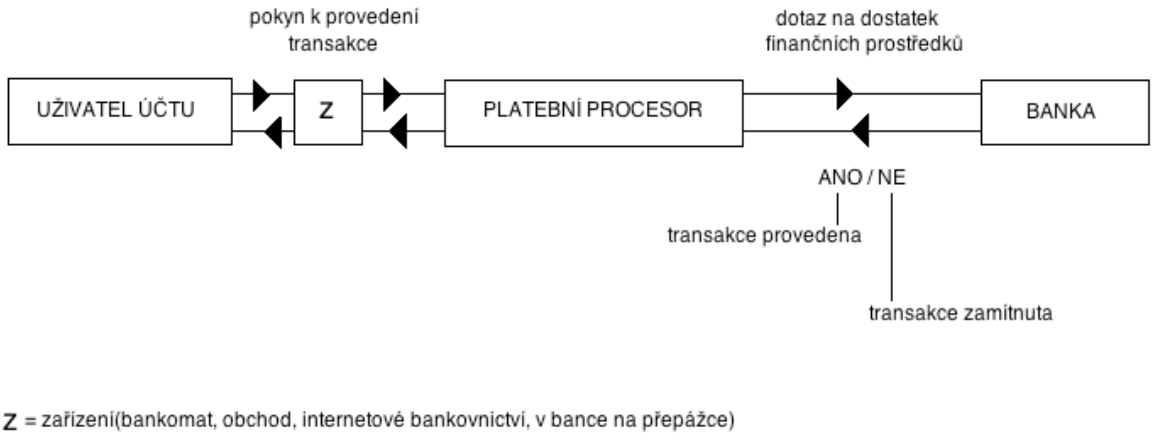
2 BANKOVNÍ TRANSAKCE

2.1 Popis

Bankovní transakce je jednou z mnoha bankovních operací. Bankovní operace se dělí na 2 hlavní skupiny. Pasivní bankovní operace jsou činností, které nemanipulují s finančními prostředky na rozdíl od aktivních bankovních operací, které s finančními prostředky manipulují.

Pasivní bankovní operace jsou v podstatě operace informačního charakteru. Slouží klientům k zjišťování zůstatků na účtu, přehledu transakční historie, nastavení bankovních služeb atd. Přes to, že při těchto operacích nedochází k žádné manipulaci s finančními prostředky, mohou být využívány pachateli trestných činů k zjišťování informací o účtech, které následně napadnou. Mezi aktivní bankovní operace patří například zřízení trvalého příkazu, příkaz k úhradě, zrušení trvalého příkazu a další. Tyto operace jsou zásadní. Dochází u nich k rozhodování o pohybu finančních prostředků. Může se jednat o okamžitý pohyb, pohyb za určitou dobu a pravidelně opakovaný pohyb. Konkrétní přesun finančních prostředků je bankovní transakce.

Samotnou bankovní transakci lze provést fyzicky, nebo virtuálně. Tyto dvě varianty jsou funkčně totožné. Zjednodušený model si popíšeme. Vše začíná u uživatele účtu, který dá pokyn k provedení bankovní transakce (např. v bankomatu nebo obchodě). Tento pokyn je odeslán na platební procesor. Tím je mimobankovní společnost, která spolupracuje s bankou na zprostředkování plateb. Nejedná se o součást banky ale o externího zřizovatele služeb spojených s bankovními transakcemi. Po té, co platební procesor přijme pokyn k transakci, zjistí banku příslušné karty a odešle do vydavatelské banky nebo externího autorizačního centra banky všechny informace (dotaz na dostatek finančních prostředků, PIN, odkud přichází požadavek na transakci). Banka ověří údaje, zjistí stav finančních prostředků a na základě něj odešle požadovanou informaci. Odpovědí banky je vždy buď ANO (na účtu je dostatek finančních prostředků k provedení transakce), nebo NE (na účtu není dostatek finančních prostředků k provedení transakce). Žádné další informace platebnímu procesoru neposílá. Pokud byla transakce provedena, vrátí se uživateli informace o provedení bankovní transakce. Následující postup se odvíjí od typu transakce. Závěrečná fáze celého modelu může být tedy převzetí hotovosti, zboží, nebo potvrzení platby jinou osobou. Celý tento proces trvá jen několik sekund.



Obr. 13 Základní model bankovní transakce

Důležitým faktorem je také to, jestli transakce proběhla on-line, nebo off-line. První jmenovaná metoda je spjata s třetí stranou, která je v systému pro ověření platby zákazníka. Třetí stranou je vydavatelská banka nebo externí autorizační centrum vydavatelské banky pro ověření. Jde o to ověřit zadaný PIN zákazníka za pomoci banky, která PIN vygeneruje z čísla karty a servisního kódu (následně zašifrováno kryptografickým klíčem banky). Totéž je provedeno na straně zákazníka. Ten zadá pin a ten je zašifrován kryptografickým klíčem Na základě shody je povolena platba. Je považována za bezpečnější než off-line platby. Ty využívají čipu platební karty, ze kterého je vygenerován PIN a ten pak porovnán s PINem, který zadá zákazník na klávesnici.

Pokud provádí tuzemský držitel karty platbu v zahraničí, autorizace je nejdříve nasměrována do příslušné karetní asociace (MasterCard, VISA, Diners Club, JCB a další) a odtamtud na autorizační host server vydavatelské banky, nebo externího autorizačního centra vydavatelské banky, kde se karta ověří. PIN není nikde uložen, uložen je u issuera pouze kryptografický klíč, pomocí kterého se PIN při verifikaci vygeneruje a kontrolu proti kryptografickému přepisu PIN, který přijde z terminálu.

2.2 Zprostředkování bankovních transakcí

2.2.1 Bankomat

Bankomat je samoobslužné technické zařízení, jehož cílem je ušetřit čas klientům kank. Bývá označován také zkratkou ATM (Automated teller machine). Umožňuje rychlý, snadný a v mnoha případech i neomezený přístup k penězům klientů. Obsluha bankomatu probíhá pomocí klávesnice. Po zasunutí platební karty do čtečky bankomatu a následném zadání PINu je bankomat zpřístupněn.

Čelní panel bankomatu je vyráběn z nerez oceli (zaručuje odolnost vůči korozi) a v provedení antivandal, což znamená, že bankomat není možné bez použití přístrojů zničit nebo poškodit. Díky tomu se také zvyšuje odolnost přístroje proti opotřebení uživateli.
Display neboli obrazovka – používají se TFT LCD obrazovky o velikosti 12,1" nebo 15"(1"(palec) = 2,634 cm). Používají se také dotykové obrazovky, které poskytují pohodlnější ovládání.

Čtečka platebních karet – instalují se hybridní čtečky, které umožňují číst karty s magnetickým proužkem i s čipovou technologií. V bankomatech se používají ty nejkvalitnější čtečky s certifikátem EMV 2000. Mechanismus pro pohyb platební karty dokáže kartu vydat v případě výpadku proudu, ale také kartu vtáhnout zpět do bankomatu a uchovat ji, pokud karta není po výběru odebrána uživatelem.
Kamera – bývá zabudována skrytě nebo je před ní krytka, která znemožňuje určit, kam je objektiv kamery nasměrován. Účelem kamery je především monitorování výběru pro případnou identifikaci vybírajícího a analýzu výběru.

Kazety pro bankovky – bývá jich čtyři až šest a každá dokáže pojmout až 2500 bankovek. Jednotlivé kazety bývají opatřeny zámkem, ale není to pravidlem.
Řídící jednotka (počítač) – v současnosti jsou nové přístroje vybavovány procesory Intel Pentium IV a Intel CoreDuo (obchodní označení pro dvoujádrový procesor). Jako operační systém je výhradně používán software od společnosti Microsoft s názvem Windows. Některé přístroje dosud běží na Windows 3. x z roku 1990 (prodávání licencí toho produktu skončilo v listopadu roku 2008), novější používají Windows 95 či NT. V drtivé většině nových přístrojů je instalován Windows XP upravený pro použití v bankomatech.
[11]
Datové připojení – pro přenos dat se používá protokol TCP/IP, který je hlavním protokolem celosvětové sítě internet. Data jsou přenášena po metalickém vedení nebo

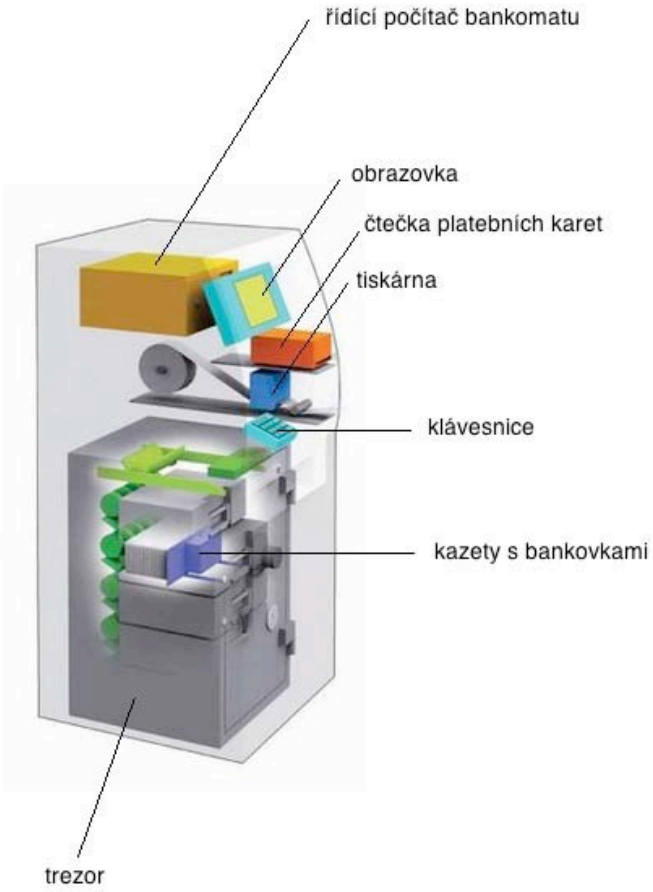
bezdrátově. Metalické vedení je realizováno pomocí telefonní linky. Pro bezdrátový přenos dat je bankomat vybaven GSM modulem a komunikace je zprostředkována datovou službou GPRS. [12]

Přenášená data jsou šifrována šifrou TripleDES.

Napájení – bankomat je připojen do „klasické zásuvky" (220 - 240 V, 50 - 60 Hz). [11]

Obr. 14 Přední strana bankomatu

Bankomat na obrázku 13. je bankomat ČSOB, který umožňuje výběr i vklad hotovosti (pouze bankovek). Tento bankomat je umístěn ve vnitřních prostorech. Jedná se o samostatnou místnost, do které je vchod přímo z ulice. Do místnosti je povolen vstup po použití magnetického pásku platební karty u čtecího zařízení dveří, které se následně otevřou. I když je bankomat vybaven vlastní kamerou, prostor okolo bankomatu střeží ještě jedna kamera.



Obr. 15 Bankomat uvnitř [20]

2.2.1.1 Rozdělení bankomatů

Podle umístění

- vnitřní - bankomat umístěn uvnitř budovy
- vnější - bankomat umístěn ve venkovních prostorech, většinou u stěny budovy

Podle režimu provozu

- neomezený provoz - 24 hodin denně
- omezený provoz - provozní doba omezena v důsledku konkrétních důvodů

Podle druhu služeb

- jednoúčelové - např. pouze pro výběr hotovosti
- víceúčelové - např. výběr, vklad, změna nastavení účtu, dobíjení kreditu na mobilní telefon

2.2.2 Imprinter

K otisku údajů vyražených reliéfním písmem na kartě na účtenku slouží již více než 50 let mechanický snímač zvaný také imprinter nebo validátor. Jeho princip je založen na přítlačných válečcích, které přitisknou reliéfní písmo karty a identifikačního štítku obchodníka na účtenku. Ta je nejčastěji vyrobena z chemického samokopírujícího papíru. Válečky jsou umístěny v rukojeti a mají obvykle seřiditelný přítlak. Některé imprintery mají ve své spodní části reliéfní číselník pro nastavení data transakce. Vyrobeny jsou z kovu a plastu.

Toto jednoduché mechanické zařízení zjednodušuje a zrychluje práci při vystavování prodejního dokladu. Odstranění ručního vypisování čísla karty a čísla obchodníka odstraňuje chyby při opisování čísel, i při jejich čtení a typování v bance. Otisk je rovněž dokladem o předložení karty (společně s podpisem klienta).

Identifikační štítek obsahuje název obchodníka, název města a zkratku státu. Pro každý platební systém (VISA, American Express a další). je na štítku uvedeno zvláštní identifikační číslo. Tento postup umožňuje používat jeden štítek a imprinter současně pro všechny druhy karet, na jejichž akceptaci má obchodník uzavřenou smlouvu. [6]

Obr. 16 Imprinter [13]

2.2.3 Platební terminál

Platební terminál nebo také POS terminál (z anglického Point of Sale) je elektronické zařízení sloužící k provádění bezhotovostních bankovních transakcí platební kartou. Důvodem k jejich zavedení bylo snížení administrativní činnosti obchodníků. Množství papírových dokladů o provedení transakce, které museli vypisovat, bylo se zvyšujícím se počtem platebních karet neúnosné. Platební terminál je vybaven tiskárnou, nebo komunikuje s externí tiskárnou, takže výrazně urychluje práci. Podle typu a technologie dokáží akceptovat elektronické, embosované a čipové karty. K ověření platnosti karty používají různou míru autentizace. Terminál je určen obchodníkům a podnikatelům, kteří chtějí přijímat bezhotovostní platby pomocí platebních karet. Terminály většinou zapůjčuje nebo prodává banka, která na základě informací získávaných z terminálu provádí přesun finančních prostředků z účtu držitele karty na účet obchodníka. Banka si obvykle účtuje poplatky za správu terminálu a za provedení transakce.

První platební terminály pracovaly off-line. Pracovaly na principu ověření informací z magnetického proužku (časová platnost karty, limit karty). Měly v sobě také uloženou databázi zakázaných a zablokovaných karet. Jednou týdně, později i každý den byly data o transakcích odesílány do banky nebo jiného zúčtovacího centra. PIN je v té době ověřován pomocí dekódovacího zařízení umístěného uvnitř terminálu (tzv. black box). Koncem 80 let se začaly požívat terminály pracující v on-line režimu. Ověření každé transakce probíhá v reálném čase. Všechny informace potřebné k ověření (číslo karty, číslo terminálu, nebo terminálu, PIN a další) jsou odeslány autorizační centrály, která je ověří a povolí nebo zamítne platbu.

Platební terminál může být samostatné zařízení, nebo zařízení o několika částech (např.: oddělená klávesnice pro zadání PINu zákazníkem). Může jít o mobilní nebo statické zařízení. Většinou je napojen na pokladní systém obchodníka, který předá požadovanou částku, která by byla vyžadována v hotovosti, platebnímu terminálu. Každý platební terminál se skládá z několika hlavních částí. Jsou jimi čtečky karet (magnetického proužku, čipu a v nejlepším případě obou), displej zobrazující požadované a zadané informace, klávesnice pro ovládání terminálu, tiskárnu a další zařízení. Komunikace probíhá většinou pomocí protokolu TCP/IP (UTP kabelem), nebo dial up připojením (telefonní kabel). Pokud se jedná o bezdrátový platební terminál, zařízení přibývá. Jde-li o GPRS komunikaci, musí terminál obsahovat SIM kartu a technické vybavení umožňující přenos

dat. Další možné komunikační metody jsou WI-FI a Bluetooth, pomocí nichž komunikují s dokovací stanicí a dále do sítě přes TCP/IP.

Obr. 17 Popis platebního terminálu

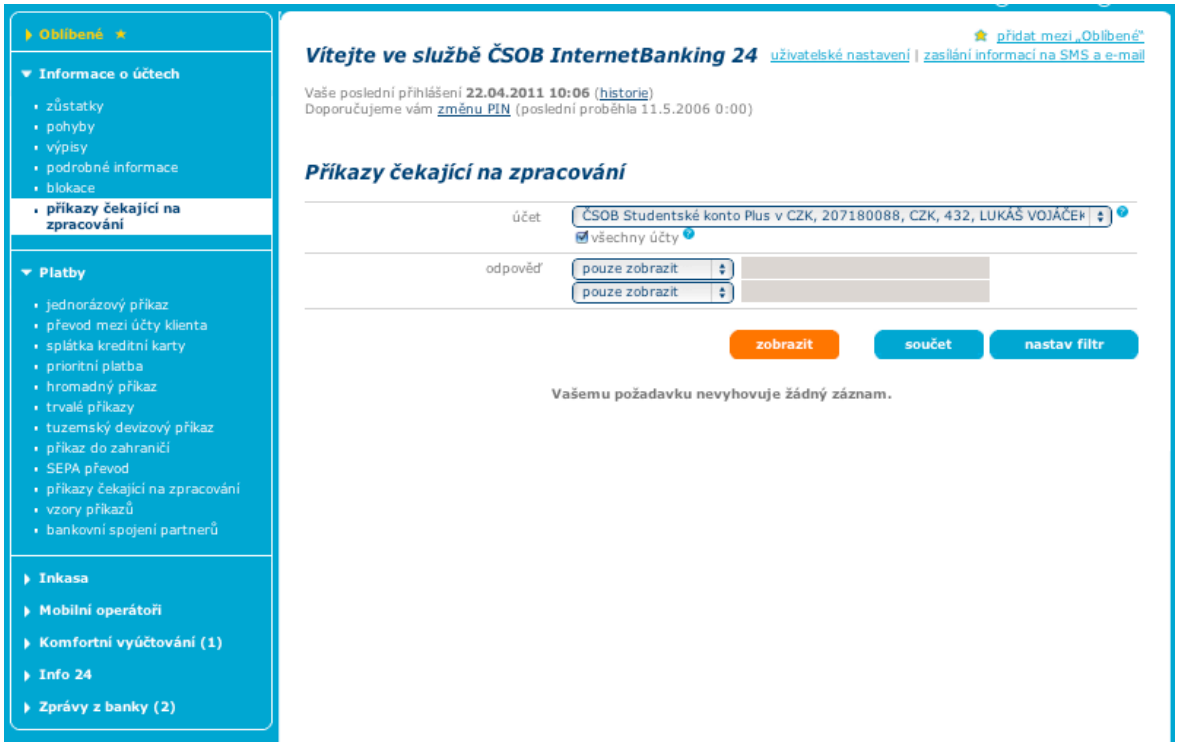
Velký význam pro platební terminály měl vývoj technologií bezkontaktních plateb. Do samotných platebních karet je implementována technologie RFID (popsána výše). Zavádění bezkontaktních platebních terminálů je prováděno hlavně díky rychlosti platby. V současné době k těmto platbám nejsou používány pouze platební karty. Jsou vyvíjeny klíčenky, a mnoho dalších přístrojů, které vykonávají tutéž funkci.

Obr. 18 Bezkontaktní řešení platebních transakcí VISA[14]

Obr. 19 Bezdrátový platební terminál GPRS [15]

2.2.4 Internetové bankovnictví

Zavedení služeb internetového bankovnictví do nabídky bank byla podobná událost jako zavedení prvního bankomatu. Umožňuje uživatelům spravovat své účty. Předfáze internetového bankovnictví bylo homebanking(domácí bankovnictví), které fungovalo prostřednictvím speciálního softwaru, dodávaného bankou. Práce v internetovém, virtuálním nebo také online bankovnictví funguje prostřednictvím webového rozhraní. Uživatel tedy potřebuje jakékoliv zařízení disponující internetovým připojením a schopností zobrazit uživatelské prostředí. Tím může být osobní počítač, nebo mnohá mobilní zařízení (notebook, netbook, mobilní telefon, tablet, PDA a další zařízení). Možnosti, které banky na jejich internetovém bankovnictví nabízí, se liší. U většiny bank lze provádět většinu pasivních i aktivních bankovních operací. Funkce je jednoduchá. Stačí se jen přihlásit na webové stránce banky a provádět operace. Prvky zabezpečení jsou zaměřeny na přihlašování do systému, potvrzování platebních transakcí a přenos dat.



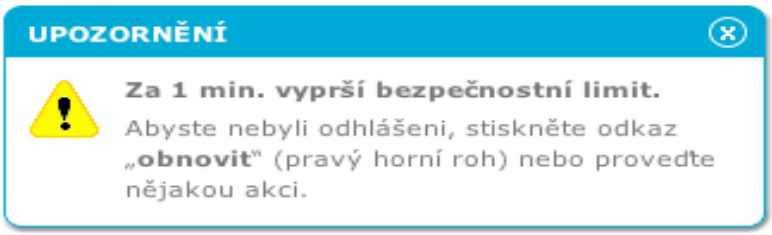
Obr. 20 Prostředí internetového bankovnictví ČSOB

2.2.4.1 Bezpečnostní prvky

Tolik flexibility, kolik přináší internetové bankovnictví uživatelům výrazně zvyšuje možnosti pachatelům trestných činů. Přístup jednotlivých bank k otázce zabezpečení je rozdílný. Za vyšší bezpečnost si musí většinou klient připlatit. Záleží tedy na bance a klientovi jakou možnost zvolí. Celé zabezpečení spočívá na autentizaci pomocí informací, které zná jen banka a klient. Díky rozvoji komunikačních nástrojů jako je mobilní telefon nebo osobní počítač probíhá autentizace často informacemi distribuovanými po těchto komunikačních kanálech. Důvěra je pak založena na pravosti údajů. Číslo mobilního telefonu, na který jsou klientovi banky posílány autentizační údaje lze změnit pouze osobně v bance po předložení občanského průkazu. Podobné principy jsou využity i v ostatních metodách (e-mail, adresa). Problémy nastávají s množstvím webových prohlížečů. Aplikace internetového bankovnictví totiž nemusí všechny prohlížeče podporovat a tak uživatelům doporučují vhodné prohlížeče. Tím se snaží předejít rizikům.

2.2.4.1.1 Přihlášení

Abyste se na webové stránce banky mohly přihlásit, musíte mít internetové bankovnictví aktivní. Ne každý si tuto službu aktivuje. Dále je nutné, aby uživatel uvedl autentizační údaje. Těmi můžou být kombinace informací, které uživatel vlastní, nebo je schopen je zjistit. Pokud je zadají několikrát nesprávně, internetové bankovnictví je zablokováno a klient banky je informován. Je pamatováno také na to, když nechá uživatel webovou stránku s přihlášeným internetovým bankovnictvím. Uživatel je systémem po několika minutách nečinnosti automaticky odhlášen (Obr. 20).



Obr. 21 Upozornění na automatické odhlášení (IB ČSOB)

Varianty autentizace při přihlášení

- identifikační číslo a pin - jsou přidělené bankou, většinou kombinace (nejedná se však o údaje, které naleznete na platební kartě, pin také není shodný s běžným PINem - lze jej měnit)
- přihlašovací SMS - mimo identifikačního čísla a PINu lze pro přihlášení vyžadovat i přihlašovací SMS
- podpisový certifikát - data o pravosti uživatele uloženy v zařízení (např.: PC)
- podpisový certifikát na čipu nebo na magnetickém proužku karty - je potřeba speciální karta a čtečka karet, data z karty slouží k autentizaci
- časově závislý token - každou minutu se mění kód na tokenu, který je vyžadován pro přihlášení

Obr. 22 Přihlášení (IB ČSOB)

2.2.4.1.2 Potvrzení transakce

K provedení bankovní transakce, která operuje s finančními prostředky je u většiny bank více zabezpečeno než jiné operace (např. sledování stavu účtu). Existuje několik pohledů na realizaci tohoto zabezpečení. Banky používají některé z těchto bezpečnostních prvků, a nebo jejich kombinace.

Podpisový certifikát

Autorizace transakce představuje dodatečné potvrzení dané transakce pomocí klientského certifikátu, který slouží k ověření identity klienta. Pro využívání pomocí klientského certifikátu je nutné mít uložen klientský certifikát v počítači, mobilním telefonu, flash disku nebo jiném zařízení. Certifikát je nejčastěji aplikace, prostřednictvím které se klient přihlásí ke službě a je oprávněn provádět transakce. Certifikát je jednoznačně spojen s klientem banky, umožňuje identifikaci klienta nebo banky ve vztahu k datové zprávě. Podpisový certifikát vytvořen a připojen k datové zprávě pomocí prostředků, které klient může udržet pod svou výhradní kontrolou. Nevýhodou je možnost zkopírování certifikátu a jeho následné zneužití. Za nejvíce nebezpečné se považuje umístění certifikátu na pevném disku v počítači, nebo na internetu. Tato metoda spojena obvykle s dalšími autentizačními údaji (např.: Autentizační SMS).

Podpisový certifikát na kartě

Bezpečným mobilním uložištěm podpisového certifikátu je karta. Rozměry odpovídají klasické platební kartě. Je však využívána pouze pro autentizaci. Podpisový certifikát uložený na čipové kartě je určen pro klienty, kteří požadují vyšší zabezpečení uložení certifikátu. Hlavní výhodou a vlastností čipové karty je, že certifikát z ní nelze zkopírovat. Pokud tedy nedojde k fyzické ztrátě čipové karty, je zneužití certifikátu prakticky vyloučeno. Bez hesel, které ji chrání na ni není možný přístup. Práce s certifikátem na čipové kartě je také mnohem snazší a rychlejší, neboť při využívání certifikátu na čipové kartě zadáváte pouze krátký PIN. Podobně je tomu i u magnetického proužku. Ten ale nenabízí tak silné šifrování. K použití karty je třeba vlastnit příslušnou

čtečku karet propojenou s osobním počítačem nebo notebookem. Většinou ji dodává přímo banka. Novinkou jsou i mobilní čtečky k mobilním telefonům nebo tabletům.

Obr. 23 Čtečka čipových karet [32]

Podpisový certifikát uložen na USB tokenu

Vzhledem k relativní jednoduchosti provedení a plošné dostupnosti rozhraní USB se začínají místo čteček čipových karet prosazovat USB tokeny (dongly, klíče). Mezi tokeny jsou poměrně velké rozdíly zejména ve funkci, možnostech a také zabezpečení. Nejjednodušší tokeny obsahují prostě paměťovou jednotku, v chytřejších zařízeních se dá najít procesor, který chrání přístup k datům a obsahuje vlastní OS a aplikační software, nejsložitější tokeny mají zvláštní procesor na kryptografické operace. Banky většinou nabízí vlastní tokeny, které nabízí při aktivování internetového bankovnictví.

Obr. 24 USB token

Autorizační SMS

Autorizace transakcí pomocí autorizačních SMS představuje jednoduchý a dostupný způsob zabezpečení transakce pomocí kódu zaslaného formou SMS zprávy do

mobilního telefonu klienta banky. Klient k tomu potřebuje pouze mobilní telefon schopný přijmout a zobrazit SMS zprávy. Kód v SMS je ale použitelný pouze po omezený čas (několik minut). Klient přepíše kód na webovou stránku internetového bankovnictví a dokončí transakci. Připomínám, že číslo mobilního telefonu je uloženo v databázi banky a je možné jej změnit jen osobně v bance po předložení dokladu totožnosti.

Autorizační šifrovaná SMS

Jde o stejnou metodu jako u nezašifrovaných SMS. Šifrovaná GSM komunikace, kterou je třeba vytvořit pro tento účel je založena na softwarovém šifrování. Banka a mobilní telefon klienta jsou vybaveni stejným softwarem. Banka pak může šifrovat SMS a klient je bez problému přečte.

Autentizační kalkulátor

Autentizační kalkulátor je generátor hesel pro vstup a ověření transakcí. Známý je také jako PIN kalkulátor, nebo generátor jednorázových hesel. Klient zadá své klientské číslo, PIN kód a atributy transakce. Kalkulátor vygeneruje autentizační kód, který je vždy a pro každého uživatele jiný a platí řádově jen několik minut. Autentizační kódy jsou generovány na základě interních parametrů kalkulátoru, takže každý kalkulátor generuje jinou posloupnost těchto kódů (kalkulátory jsou vzájemně nezaměnitelné). Kalkulátor nelze použít bez PINu, pomocí kterého se spouští. Autorizace na internet banking tedy probíhá zadáním kombinace údajů (např.: kalkulátor a SMS). Jedná se o jeden z nejbezpečnějších způsobů ověření.

Obr. 25 Autentizační kalkulátor [17]

Časově závislý token

Token každou minutu automaticky generuje nový jednorázový autorizační klíč, tzv. token kód, s omezenou časovou platností (každou minutu generován nový). Proto je použití tokenu zárukou vyšší bezpečnosti jak pro vlastní přístup do internetového bankovnictví, tak při zadávání jednotlivých platebních transakcí. Systém přihlašování a autorizace odchozích plateb prostřednictvím kombinace přístupového jména, vlastního PIN a token kódu. Protože je kód platný jen po jednu minutu, je na tokenu signalizován odpočet minuty. Na tokenu na obrázku 24 je signalizace realizována ubýváním čárek. Na obrázku je vidět, že klient má celou minutu k zadání kódu.

Obr. 26 Časově závislý token

TAN kód

TAN kódy jsou jednorázové kódy. Banka pošle poštou klientovi seznam tzv. TAN kódů (unikátních čísel), kterými se potvrdí bankovní operace. Počet TAN kódů v jednom balení se pohybuje od 50 do 100 kódů. Po potvrzení je TAN kód neplatný a je potřeba příště použít jiný. Tento systém je poměrně bezpečný, nebezpečím je ale případná ztráta kódů.

2.2.4.1.3 Přenos dat

Komunikace s bankou přes zaručený elektronický podpis zajišťuje vyšší zabezpečení. Elektronické výpisy z účtu, e-mailové konfirmace a zůstatkové e-maily jsou zabezpečeny elektronickým podpisem. Elektronický podpis Vám umožní zkontrolovat, že

e-mail nebo výpis byl vytvořen v bance a že nebyl změněn třetí stranou. Samozřejmostí je zabezpečit veškerých datových toků pomocí HTTPS (popsáno výše). Většina standardů vychází z PCI DSS.

2.2.5 Online platby mimo webové stránky internetového bankovnictví

Nakupování prostřednictvím internetu se stalo fenoménem. Mezi způsoby platby si většinou může nakupující vybrat. Nabízí se řada možností. Platba pomocí platební karty je jednou z nich. Po výběru zboží se sestaví objednávka a vybere se způsob platby - platební kartou. Jedná-li se o platbu s 3D-Secure, zákazník je přesměrován na stránku jeho banky. Pokud ne, vyplnění údajů probíhá u obchodníka, banky obchodníka, nebo platebního terminálu, kde je vyzván k vyplnění autentizačních údajů.

Obvykle požadované autentizační údaje:

- země ve které byla karta vydána
- křestní jméno
- příjmení
- způsob platby (kreditní, nebo debetní karta)
- typ karty (Visa, Mastercard, apod.)
- číslo karty
- doba platnosti karty
- CVC/CVV/CID číslo
- datum narození (den, měsíc, rok)

Tato metoda je považována za spolehlivou, ale najde se mnoho internetových obchodů přistupujících k platbám bez jakýchkoliv nároků na bezpečnost klienta. Ve světě se najdou obchody, u kterých je naprosto běžné zasílání údajů o kartě e-mailem přímo obchodníkovi. Plátci si často neuvědomují cenu poskytovaných informací. Nejčastěji však obchodníci vyžadují číslo karty, dobu platnosti karty, CVV/CVC/CID číslo. Tyto platby jsou považovány za nejslabší místo pro karty umožňující internetové transakce, protože při nich dochází nejčastěji a nejsnáze k úniku citlivých informací.

2.2.6 Na přepážce

Bankovní transakci lze provést také na přepážce. Tímto způsobem se, ale zabývat nebudeme. Jediné riziko je zde lidský faktor (zaměstnanec banky). Identifikace klienta probíhá pomocí občanského průkazu. Následně může provést operace na kterémkoli, ze svých účtů. Celý proces je navíc většinou monitorován bezpečnostní kamerou banky.

3 PRINCIPY, DOHODY A CERTIFIKACE

3.1 Infrastruktura

Vybudování infrastruktury pro platební karty je nákladný a dlouhodobý cíl. Po prvním desetiletí provozu uzavřených systémů platebních karet pochopily banky, že budoucnost mají jen otevřené systémy, do kterých se zapojí co nejvíce bank a obchodníků. Proto vznikly národní a mezinárodní bankovní asociace, které zajišťují vzájemné použití karet všech členských bank v bankomatech a obchodech, které obsluhují.

K hospodárnosti provozu platebních karet nepřispívají jen organizačně jednotné a spolehlivé pracující autorizační, bezpečnostní, clearingové a zúčtovací centrály asociací, ale také koncentrace zpracovatelských kapacit na straně bank. Na počátku měly banky snahu zabezpečit si potřebné služby vlastními prostředky. S tím, jak se prohlubovala specializace těchto služeb a rostl počet transakcí, karet a zdokonalovala se technika, ukázalo se, že je pro banky výhodnější konkurenčně neutrální činnost vyčlenit do společných bankovních center, nebo jejich zpracováním pověřit soukromé společnosti.

[6]

3.2 PCI DSS

Cílem PCI DSS (The Payment Card Industry Data Security Standard) je zamezit karetním podvodům a to zavedením vhodných bezpečnostních opatření u společností, které data držitele karty zpracovávají, přenášejí nebo uchovávají. Ač PCI Security Standards Council skromně uvádí, že se jedná jen o 12 požadavků, jde ve skutečnosti o soubor 197 naprosto konkrétních bezpečnostních opatření, u kterých je navíc i uvedeno, jakým způsobem ověřit, že byly splněny. Tato norma vyžaduje, aby všichni obchodníci (ale stejně tak i poskytovatelé služeb a banky obchodníků), kteří zpracovávají, přenášejí nebo uchovávají data o držitelích platebních karet a kartových transakcích, podstoupili akreditaci v rámci normy PCI DSS. Norma definuje 4 úrovně, to kterých jsou obchodníci zařazeni a kritéria k jednotlivým úrovním, které obchodník musí k získání certifikace splnit. Určení úrovně u obchodníka záleží na typu a počtu transakcí za rok. Kritéria pro akreditaci definovaná asociacemi pro obchodníky jsou specifikována následovně:

Požadavek č. 1: „Install and maintain a firewall configuration to protect cardholder data" požaduje, aby byly nainstalovány firewally, nastavena na nich odpovídající pravidla a byla

vytvořena a udržována dokumentace popisující datové toky, nastavení pravidel, uvedena odpovědnost jednotlivých osob za správu firewallů a popsán proces provádění změn. Dále standard požaduje, aby kontrola nastavení firewallu byla prováděna minimálně každých 6 měsíců. (18 opatření)

Požadavek č. 2: „Do not use vendor-supplied defaults for system passwords and other security parameters" požaduje, aby byla na všech systémech a zařízeních změněna defaultní hesla, zakázány nepoužívané služby a odinstalováno vše nepotřebné. V případě wireless zařízení by se měl místo defaultního WEP protokolu používat WPA nebo WPA2. Pokud ho zařízení nepodporuje, mělo by se upgradovat. Kromě toho by jednotlivé služby měly běžet na samostatných serverech. Ke konzoli serveru by se měl administrátor připojovat výhradně přes SSH nebo SSL. (9 opatření)

Požadavek č. 3: „Protect stored cardholder data" požaduje, aby do určeného a chráněného úložiště byly ukládány informace jen nezbytně nutné a uchovávány jen po nezbytně nutnou dobu. Měla by se používat pouze silná kryptografie, data by se měla šifrovat raději na úrovni disku než na úrovni souborového systému. Šifrovací klíče by měly být bezpečně distribuovány, ukládány, likvidovány, měly by se periodicky měnit a přístup k nim by měl být omezen. Dále je vyžadována segregace rolí a vícestupňová kontrola přístupu. Správa klíčů by měla být popsána. Pokud jde o zobrazování čísla karty, tak je povoleno zobrazovat maximálně jen prvních šest a poslední čtyři číslice. (18 opatření)

Požadavek č. 4: „Encrypt transmission of cardholder data across open, public network", požaduje, aby byla nasazena silná kryptografie, SSL/TLS nebo IPSEC protokol a neměl by se v žádném případě používat WEP. Číslo karty by nemělo být posíláno mailem apod. (3 opatření)

Požadavek č. 5: „Use and regularly update anti-virus software or programs" požaduje, aby byla nasazena ochrana proti malwaru a pokud možno na všech systémech a byl zajištěn automatický upgrade a vznikaly logy zaznamenávající činnost těchto antivirových prostředků. (3 opatření)

Požadavek č. 6: „Develop and maintain secure systems and applications" – požaduje, aby byly nasazovány patche a to nejpozději do jednoho měsíce od jejich uvolnění. Společnost by si měla zajistit, že bude informována o nově objevených zranitelnostech, např. tím, že bude odebírat nějaký bulletin. Měl by být stanoven bezpečný proces vývoje SW. Mělo by se vyvíjet v souladu s metodikou OWASP a důkladně by se mělo i testovat. Mělo by být

oddělené vývojové, testovací a produkční prostředí. Jedna osoba by neměla mít přístup do vývojového, testovacího a produkčního prostředí. K testování a vývoji by se neměla v žádném případě používat produkční data a před nasazením do produkce by měla být odstraněna testovací data a účty. (30 opatření)

Požadavek č. 7: „Restrict access to cardholder data by business need-to-know" požaduje, aby přístup k datům byl řízen na principu need-to-know a uživatel v systému disponoval jen právy nezbytně nutnými k výkonu dané práce. (7 opatření)

Požadavek č. 8: „Assign a unique ID to each person with computer access" požaduje, aby každé osobě bylo přiděleno jedinečné ID. Vzdálený přístup by se měl realizovat přes VPN a měla by být použita dvoufaktorová autentizace. Hesla by se měla měnit každých 90 dní, jejich minimální délka by měla být nastavena na 7 znaků a měla by obsahovat písmena a čísla. Historie hesel by měla být nastavena na hodnotu 4 a uživatel by měl mít k dispozici maximálně 6 pokusů o přihlášení, poté by mělo dojít k uzamčení účtu na 30 minut. (20 opatření)

Požadavek č. 9: „Restrict physical access to cardholder data" požaduje, aby fyzický přístup k serverům a síťovým prvkům byl umožněn pouze vybraným osobám. Každá osoba by měla nosit viditelně visačku. Pohyb osob by měl být monitorován. Logy o návštěvnících by měly být uchovávány minimálně po dobu třech měsíců. Média by měla být bezpečně uchovávána, přepravována a skartována. (19 opatření)

Požadavek č. 10: „Track and monitor all access to network resources and cardholder data" požaduje, aby bylo dokumentováno, co se má logovat a jaké údaje má auditní záznam obsahovat. Čas na všech serverech musí být synchronizovaný. Musí být zajištěno, že auditní záznam nemůže být modifikován, proto by se měl log zálohovat na centrální server. Auditní záznamy by měly být k dispozici minimálně rok dozadu. Logy by měly být vyhodnocovány nejméně 1x denně. (22 opatření)

Požadavek č. 11: „Regularly test security systems and processes" požaduje, aby se skenování zranitelností provádělo interně a externě a to minimálně každé 3 měsíce a po každé významné změně. Interní a externí penetrační testy by se měly provádět minimálně 1 ročně a též po každé významné změně. Funkce IDS/IPS by měla být též ověřována. (6 opatření)

Požadavek č. 12: „Maintain a policy that addresses information security" požaduje, aby byla vydána bezpečnostní politika, související bezpečností standardy a byli s nimi

prokazatelně seznámeni všichni zaměstnanci. Ti by se měli též školit a minimálně ročně by měli být přezkušováni. (42 opatření)

Kromě těchto 12 požadavků obsahuje standard ještě přílohu, ve které jsou uvedeny další 4 opatření. Vzhledem k tomu, že 201 opatření, které by měli obchodníci a další organizace implementovat, je opravdu dost a jejich zavedení může být pro mnohé z nich časově i finančně značně náročná záležitost, uvolnil PCI Security Standards Council spreadsheet, který umožňuje s jednotlivými opatřeními lépe pracovat. Nevím, co přesně vedlo PCI SSC k tomu, že všude uvádí jen 12 požadavků, když ve skutečnosti jich je mnohem více. Můžeme se jen domnívat, že nechtěl obchodníky a další organizace hned na začátku vystrašit. PCI DSS přináší soubor naprosto konkrétních a rozumných bezpečnostních opatření, která jsou navíc aplikovatelná i ve společnostech, pro které není tento standard primárně určen.

[18]

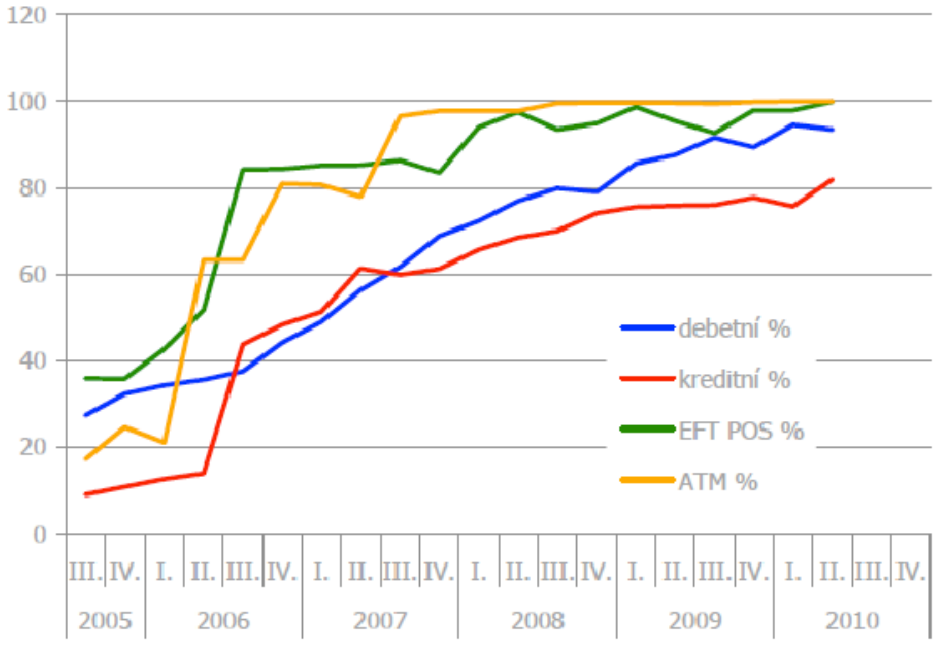
3.3 EMV Liability shift

Jedná se o dohodu platnou od ledna 2005 na území Evropské unie související se zaváděním EMV čipových karet. Tento systém byl zaveden, aby zvýhodnil místa k provádění bankovních transakcí, která jsou vybavena čtecím zařízením pro čip. Pokud dojde k reklamaci bankovní transakce a zjistí se, že jedna strana ze zúčastněných neakceptuje čipovou technologii, bude za problém zodpovědná právě tato strana (např. banka, která terminál provozuje). Pravidlo platí ovšem pouze pro fyzické bankovní transakce. Virtuální bankovní transakce do této dohody pochopitelně nespadají.

Z údajů v tabulce 1 můžete vidět zavádění čipové technologie v České republice. Dnešní stav je vyvážený v důsledku nerozšířenosti starších technologií na našem území. Největší zájem o zavedení čipové technologie mají očividně banky se svými bankomaty.

Tab 1. Zavádění čipové technologie v ČR [10]

		debetní %	kreditní %	EFT POS %	ATM %
2005	III.	27,34	8,99	35,90	17,22
	IV.	32,37	10,85	35,78	24,62
2006	I.	34,26	12,66	42,68	21,07
	II.	35,57	13,95	51,73	63,3
	III.	37,58	43,72	84,16	63,22
	IV.	44,19	48,33	84,34	80,97
2007	I.	48,97	51,28	85,11	80,67
	II.	56,31	61,29	85,17	77,92
	III.	61,63	59,87	86,30	96,56
	IV.	68,79	61,22	83,49	97,76
2008	I.	72,30	65,60	93,90	97,76
	II.	76,86	68,43	97,46	97,76
	III.	79,82	70,00	93,44	99,59
	IV.	79,01	74,10	94,89	99,69
2009	I.	85,60	75,50	98,69	99,69
	II.	87,56	75,82	95,41	99,61
	III.	91,57	75,97	92,62	99,47
	IV.	89,31	77,70	97,94	99,86
2010	I.	94,49	75,68	97,88	100,00
	II.	**93,44**	**81,85**	**99,94**	**100,00**
	III.				
	IV.				



Obr. 27 Zavádění čipové technologie v ČR [10]

II. PRAKTICKÁ ČÁST

4 ORGANIZOVANÝ ZLOČIN ZAMĚŘEN NA ZÍSKÁVÁNÍ A ZNEUŽÍVÁNÍ CITLIVÝCH INFORMACÍ V BANKOVNÍM SEKTORU

I přes dlouhou dobu vývoje bankovních systémů se nepodařilo docílit stoprocentních úspěchů při jejich zabezpečení. Většinou se jedná o neopatrnost a špatnou informovanost klientů banky. Mnohdy ale chybují i samotné banky či jiní držitelé citlivých informací.

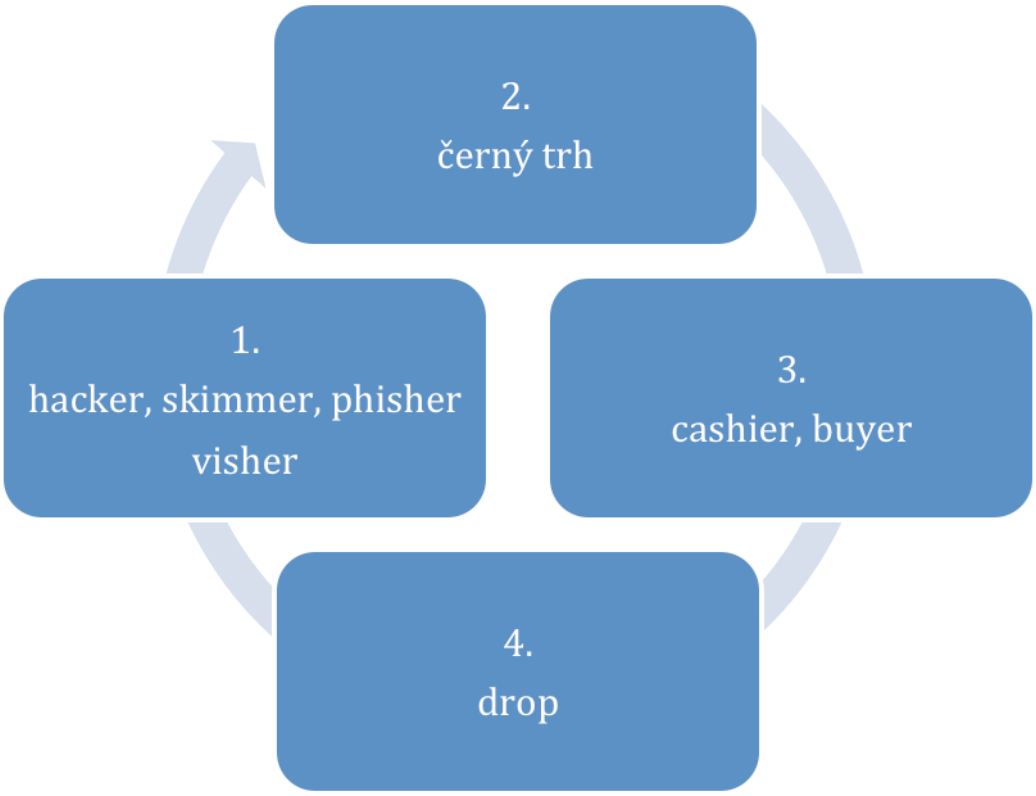
Pravdou je, že se organizovaný zločin zaměřen na zneužití citlivých informací z bankovního sektoru za 10 posledních let výrazně rozrostl. Banky informují o ztrátách, které tvoří pouhé promile ze všech platebních bankovních transakcí. Málokdo si však uvědomí skutečný objem všech bankovních transakcí na světě. Za rok 2010 objem světových bankovních transakcí činil 3 triliony Eur. Promile z tohoto čísla už opravdu není zanedbatelná suma. Podle IC3 (Internet Crime Complaint Center) konzorcia byly v roce 2008 podvody spojené s únikem citlivých informací z bankovního sektoru až na třetím místě v trestné činnosti páchané prostřednictvím internetu. Za předem zaplaceným a následně nedoručeným zbožím a fiktivními aukcemi. V roce 2010 jsou už na prvním místě v zločinech páchaných prostřednictvím sítě internet.

4.1 Obchodní model

Tato trestná činnost dokáže být za určitých podmínek výnosná bez ohrožení pachatelů. Určitou míru bezpečnosti pachatelům přináší obchodní model. Pokud se jednotlivec bude snažit vykonávat všechny fáze této trestné činnosti sám, většinou je brzy odhalen a dopaden. Pokud však jednotlivec vykonává pouze jednu z fází a doposud zjištěné informace předá dalšímu člověku, který vykoná další, stává se tato trestná činnost méně nebezpečná. Jsou dvě varianty jak model využít:

- práce jednotlivců - využití černého trhu, každý však dělá pouze část práce a její výstup prodá
- práce v týmu - přímá komunikace mezi jednotlivci v týmu, každý má svou pozici

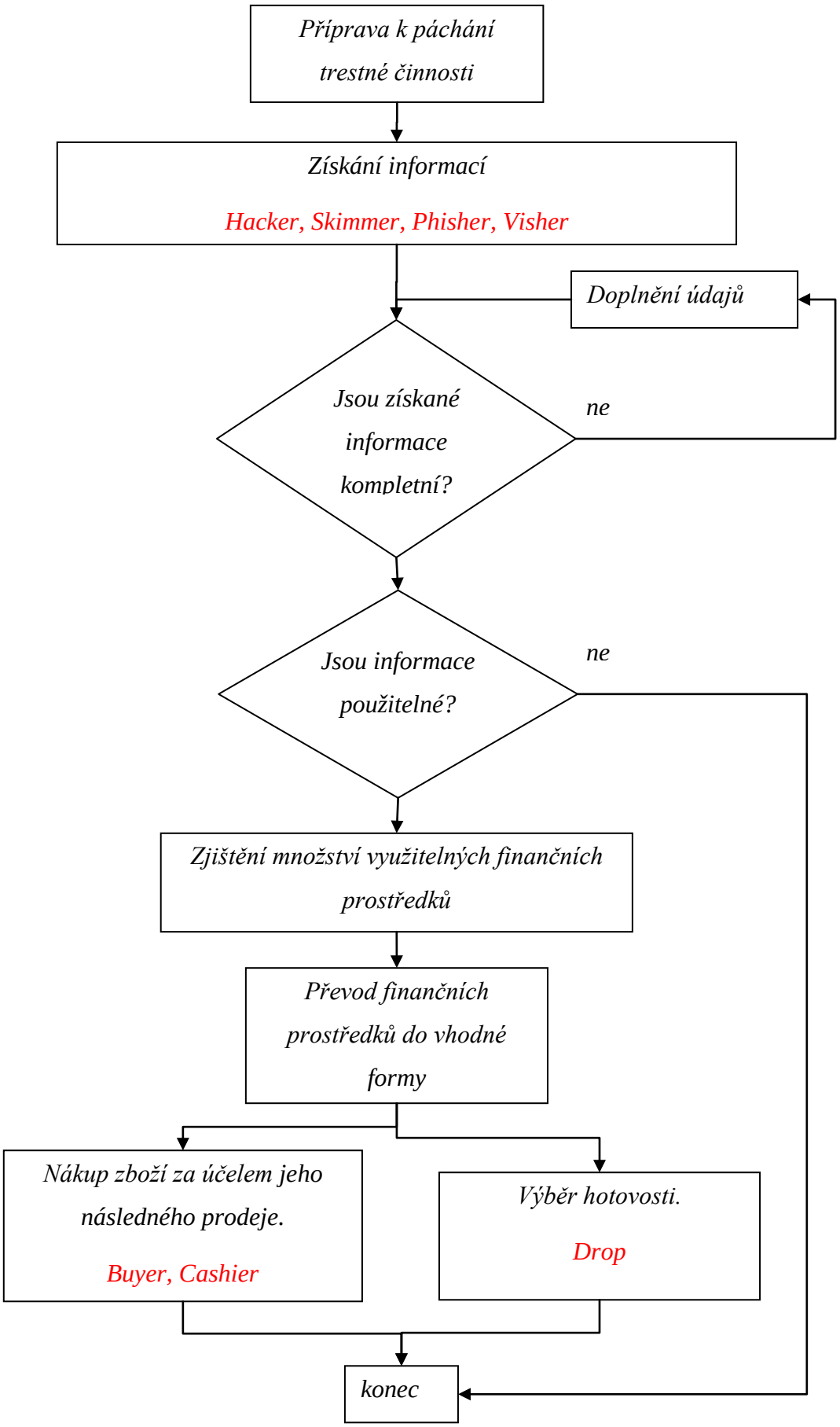
Model je tedy tvořen třemi, nebo čtyřmi fázemi. Podle toho jestli je při něm užita přímá komunikace, nebo zprostředkovávaná komunikace černým trhem. Překlad některých označení by byl nevhodný a tak budeme používat anglické názvy těchto činností.



Obr. 28 Obchodní model

Ať se jedná o práci jednotlivců, nebo týmu, spolupracující pachatelé se snaží být od sebe co nejvíce vzdáleni. To jim dodává vysokou míru anonymity. Na vykonávání jednotlivých fází jsou na různých místech světa různé nároky. Zásadním problémem je nutnost zpětné kompatibility systému (např. v USA a Kanadě je stále mnoho bankomatů vybavených pouze čtečkou magnetického proužku). Někde tak pachatelé využívají nedokonalého systému. Výhodou České republiky je nezastaralost technologií. Ve srovnání s vyspělými státy probíhá v ČR stále značná část plateb v hotovosti. Například v USA je podezřelé platit v hotovosti, protože kartu vlastní opravdu skoro každý. A pokud ne, tak za něj zaplatí kartou někdo jiný. Na druhou stranu je v USA pácháno tolik trestné činnosti spojené se zneužitím citlivých informací z bankovního sektoru, že je dnes nejsledovanější zemí na světě. Americké karty jsou podle statistik nejvíce zneužívané i v jiných zemích světa(např. Thajsko, Itálie, Anglie). Jedná se hlavně o země, kam jezdí Američané trávit dovolenou. Dalším příkladem výjimečné země je Island, kde je možné zaplatit kartou v 90% všech obchodů.

Pro přehlednost jsem vypracoval vývojový diagram (pod textem), popisující obecný postup při nelegálním zneužití citlivých informací z bankovního sektoru. Jednotlivé pozice z obchodního modelu jsou červeně zvýrazněny.


Příprava k páchání trestné činnosti
Získání informací
Hacker, Skimmer, Phisher, Visher
Doplnění údajů
Jsou získané informace kompletní?
ne
Jsou informace použitelné?
ne
Zjištění množství využitelných finančních prostředků
Převod finančních prostředků do vhodné formy
Nákup zboží za účelem jeho následného prodeje.
Buyer, Cashier
Výběr hotovosti.
Drop
konec

4.1.1 Hacker, skimmer, phisher, visher

V první fázi je nutné zjištění potřebných citlivých údajů ať už z karet nebo třeba z prostředí internetu. V žádném případě ve výčtu forem vykonávání této trestné činnosti nenaleznete zloděje.

4.1.1.1 Hacker

Hackeři jsou počítačoví specialisté či programátoři s detailními znalostmi fungování systémů, dokážou je výborně používat, ale především si ho i upravit podle svých potřeb. Jejich úkolem je získávat údaje o platebních kartách. Čím více údajů tím lip. Nejedná se pouze o základní informativní prvky na kartě (číslo karty, CVV, expirační dobu apod.), ale i datum narození držitele karty, rodné příjmení matky atd. Tyto údaje jsou používány např. v USA při dodatečném ověřování plateb.

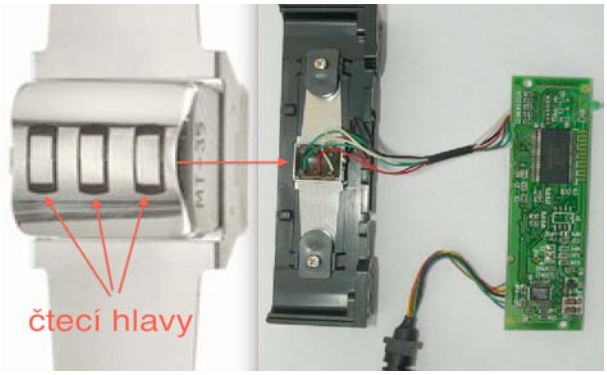
Hacker má nejmenší výdělek za jednotlivé informace z celého modelu. Za jednu kartu získává průměrně 1$. Nejlukrativnějšími a tedy nejlépe placenými kartami jsou kreditní karty z EU a Hongkongu (vysoké limity, velké množství finančních prostředků, málo omezení). Nejnižší cenu mají naopak debetní karty vydány v USA (cena pár centů). Cena roste s počtem zjištěných informací. Výjimkou není ani zjištění PIN kódu.

4.1.1.2 Skimmer

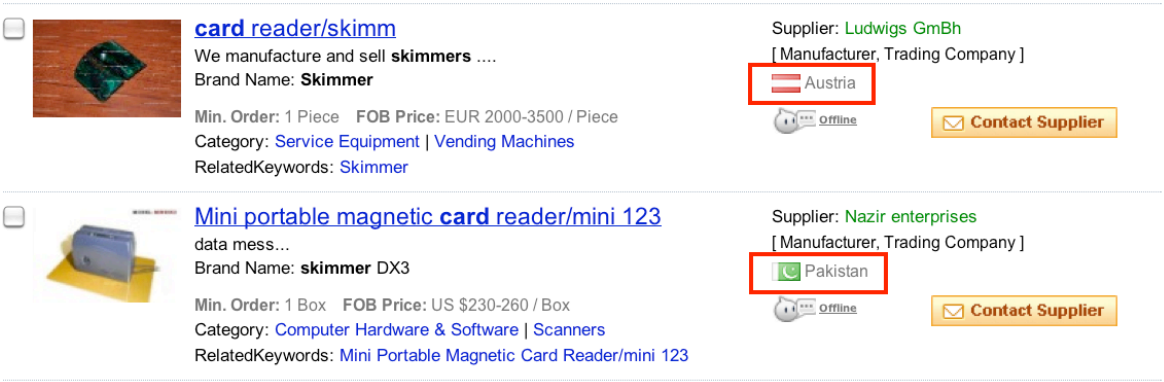
Název pozice skimmer vychází z anglického označení činnosti, pří které dochází k získávání údajů z platebních karet, pomocí speciálních zařízení. Jedná se o zařízení, které dokáže přečíst data z magnetických platebních karet (o získávání dat z čipu jde pouze v minimu případů) a buďto je zaznamenat do paměti nebo je následně posílá pachateli. Toto zařízení se nachází v několika verzích. Využívá se vždy zařízení s totožnou primární funkcí jen různě technicky vybaveného. Většina těchto zařízení je možné koupit prostřednictvím internetu z nejrůznějších míst světa. Na obrázku 29 si můžete všimnou zařízení z Rakouska a Pákistánu.

Skimovací zařízení je v podstatě čtečka dat, uložených na magnetickém proužku platební karty, která je schopna záznamu do vlastní paměti. Lépe vybavená zařízení jsou schopna posílat bezdrátově přečtená data. Je možné zařízení naprogramovat na různé funkce. K odesílání dat okamžitě po jejich přečtení, odeslání dat až po zaplnění paměti apod. Zařízení je složeno z několika částí, které jsou v plastovém krytu. K řízení slouží mikroprocesor, k ukládání dat flash paměť. Čtení dat probíhá pomocí čtecí hlavy (se třemi

pruhy). Toto základní vybavení v lepších modelech doplňuje modul pro bezdrátovou komunikaci.



Obr. 29 Demontované skimovací zařízení



Obr. 30 Ukázka zboží z internetového serveru Alibaba.com [19]

4.1.1.2.1 Formy skimmingu

4.1.1.2.1.1 Skimovací zařízení v bankomatu

Jednou z častých forem užití skimovacího zařízení je jeho aplikace do Bankomatu. Konkrétně do prostoru pro vložení karty (Obr. 31). Aby mohlo zařízení fungovat, musí být instalováno přímo před otvor pro kartu. Skimovací zařízení je vloženo do plastového krytu, který je v barvě bankomatu, nebo se jí alespoň přibližuje. Aplikace trvá jen pár sekund. Jakmile je do otvoru vložena karta, projde nejprve skimovacím zařízením a přes něj do bankomatu. Zařízení je těžko rozpoznatelné, běžní uživatelé bankomatu si pravděpodobně ničeho zvláštního nevšimnou. O tom, že si někdo nahrál data z jejich karty nemají ani tušení. Díky bezdrátovému přenosu stačí pachateli zařízení pouze aplikovat, sedět v dosahu

a přijímat data z karet. Většinou se zdržuje v dosahu, pokud nemá dostatek dat, nebo se nevybije baterie. Skimovací zařízení poté většinou zanechá na místě.

Obr. 31 Vlevo bankomat se skimovacím zařízením a vpravo bez něj [21]

Při skimování v bankomatech je využíváno i několik prostředků ke zjištění většího množství informací. Jedním z těchto prostředku je fiktivní klávesnice, která je využita k odposlechu zadaného PINu. Jedná se buď o imitaci originální klávesnice aplikované na původní (klient zadávající PIN jej zadává pin přes imitaci, která zaznamenává stlačení a přitom funguje i originální klávesnice pod ní), nebo o přesnou kopii klávesnice, kterou vymění za původní (méně nápadná, obtížněji aplikovatelná). Pokud je v prostoru bankomatu instalována bezpečnostní kamera, je aplikace klávesnice ztížená, nebo přímo nemožná. Dalším prostředkem ke zjištění PIN kódu je použití vlastní kamery ke snímání prostoru klávesnice. Jedná se o kameru velmi malých rozměrů, která je aplikována přimo na bankomat. Konkrétní použití je závislé na dispozicích bankomatu (typ, velikost, prostředí). Typickým příkladem je aplikace do prostoru nad obrazovkou bankomatu. Případem vůbec prvního odhalení zařízení tohoto typu v ČR bylo v roce 2007. Policie ČR zadržela Rumunské občany, kteří měli u sebe právě toto zařízení. Jednalo se o lištu nad obrazovku bankomatu, uvnitř s mobilním telefonem s integrovaným fotoaparátem (kamerou). Telefon byl naprogramován k odesílání dat a ovládání na dálku, takže pachatelům stačilo sedět opodál a pouze přijímat data.

Obr. 32 Lišta s kamerou [22]

Obr. 33 Fiktivní klávesnice na originální [23]

Banky se snaží skimmingu co nejvíce bránit. Instalují kamery, které sledují prostory kolem bankomatů a také antiskimovací zařízení. Antiskimovací zařízení je plastový nástavec, který instalaci skimovacího zařízení fyzicky znemožňuje. Bývá v barvě bankomatu nebo ve výrazné zelené barvě. Většinou je přizpůsoben i fimware bankomatu, který klienta informuje o antiskimovacího zařízení. Informativní grafické zobrazení navede klienta ke kontrole antiskimovacího zařízení. Pokud se realita neshoduje s grafickým zobrazením, bankomat je podezřelý ze skimingu. Sama policie ČR však potvrzuje, že tyto zařízení nemají 100% účinnost. V roce 2007 byly tyto antiskimmovací zařízení nainstalovány plošně v ČR. Z informací ze serveru Bankovníkarty.cz, je jasně viditelné, že bezúspěšně(Tab.2). Po roce 2007 je vidět jistý pokles, ale další roky opět roste.

Tab 2. Počet skimmingů na bankomatech v ČR

Rok	počet skimmingů
2006	20
2007	94
2008	53
2009	70
2010	85

Obr. 34 Antiskimmovací zařízení

4.1.1.2.1.2 Fyzicky provedený skimming

Jedná-li se o platební transakce prostřednictvím platebního terminálu, které mohou proběhnout v podstatě za cokoliv, nabízí se otázka, jak nebezpečný je samotný obchodník. Žádný z bezpečnostních prvků mu nemůže zabránit využít nepozornosti zákazníka a kartu naskimovat. Zákazník považuje místo, kde platí za důvěryhodné a často vůbec nesleduje kartu, což je velká chyba. Vzhledem k tomu, že je karta použita za delší dobu, zákazník provádějící desítky transakcí měsíčně nedokáže odhadnout, kde došlo ke skimmingu. Nutno podotknout, že většina fyzicky provedeného skimmingu se odehrává nejčastěji ve velkoměstech a turistických centrech s velkým množstvím pohybujících se osob.

Prvním příkladem této trestné činnosti je běžný nákup v obchodě. Obchodník má umístěn terminál na takovém místě, aby ho zákazník neviděl. Je vybaven externí klávesnicí pro zadávání PINu. Zákazník se většinou soustředí na to aby nikdo neviděl jeho PIN. Netuší však, že má obchodník vedle terminálu skimmovací zařízení, kterým protáhl kartu ještě před vložením do terminálu. Po provedení platby si obchodník ještě může zapamatovat bezpečnostní kód pro bezkontaktní platby a následně si jej zapsat. Zákazník odchází nic netušíc se zaplaceným zbožím a obchodníkovi zůstávají údaje z jeho magnetického proužku a bezpečnostní kód. Někteří obchodníci využívají také metodu akustické klávesnice. Jedná se o upravenou klávesnici pro zadávání PINu, která vydává tóny, specifické pro každou klávesu. Zkušený obchodník tak dokáže odposlechnout PIN a zapamatovat si jej. Nemožný není ani datový odposlech komunikace mezi externí klávesnicí a terminálem.

Dalším příkladem je platba v restauraci. Zákazník sedí u stolu a přeje si platit kartou. Obsluhující servírka nabídne zákazníkovi, že může provést platbu u baru, kde mají pevný terminál (zákazník jí předá kartu a podepíše poté stvrzenku a tím potvrdí transakci), nebo může přinést bezdrátový terminál a mohou provést platbu přímo u stolu. Opatrný

zákazník si nechá přinést terminál ke stolu. Předá servírce kartu a ta ji ještě před protažením terminálem protáhne nepozorovaně skimovacím zařízením. Získaná data jsou okamžitě odeslána prostřednictvím technologie pro bezdrátový přenos (např. Bluetooth) do počítače servírky, který má opodál.

4.1.1.2.1.3 Skimming RFID platebních karet

Zavedení RFID platebních karet má mnoho výhod, nejen pro jejich uživatele, ale i pro útočníky. Díky rádiovému přenosu, který umožňují se s kartou na okamžik spojit a dostat z ní data podobně jako z magnetického proužku, nebo čipu. Celé zařízení pro získávání těchto dat lze složit z originální, nebo jiné, čtečky RFID a komunikačního modulu, který přeposílá nebo ukládá data. Průzkumy z roku 2010 informují o více než 300 miliónech RFID platebních karet v oběhu. V místech kde je tato technologie rozšířena není problém získávat velké množství dat. Nejlépe lze bezdrátově odcizit data z karet v místech s výskytem velkého množství osob.

Nejčastěji se jedná o:

- hromadnou dopravu
- kulturní akce
- sportovní akce
- meetingy
- nákupní centra a další

Obr. 35 Ukázka zařízeni pro skimování RFID [24]

4.1.1.3 Phisher, visher

Phishing (rybaření) je podvodná technika, při které útočník využívá internetu k získávání citlivých údajů od svých obětí. Principem je rozesílání fiktivních e-mailových zpráv, tvářících se jako oficiální žádosti banky či jiné podobné instituce a vyzývají adresáta

k zadání jeho údajů na odkazovanou stránku. Stránka je ale také fiktivní a jediné, co na ní opravdu funguje, je vkládání informací od obětí. Nejprve provedou tzv. monitoring. Rozesílají podvodné e-maily v desetitisících. Slouží k informaci kolik a které oběti zareagovaly. Až další řada e-mailů, zaslaných pouze reagujícím obětem odkazuje na stránky se sběrem citlivých údajů. Řada těchto pokusů je důvěryhodnou kopií designu banky s náležitými detaily. Najdou se však i e-maily zasílané se špatnou gramatikou nebo v cizím jazyce. Útoky mají úspěšnost v rozmezí 15-27%.

První přímý pokus napadnout platební systém je z června roku 2001, kdy se cílem stal E-Gold (elektronický platební systém krytý zlatem). Tento pokus byl následován krátce po útocích 11. září 2001 na Světové obchodní centrum. Oba útoky byly zachyceny ještě dřív, než stačily napáchat škody. Do roku 2004 byl phishing brán jako plně průmyslová část organizovaného zločinu spojeného se získáváním a následným zneužíváním citlivých údajů v bankovním sektoru.

V dnešní době se nenajde déle působící banka bez pokusu o phishing. Nejvíce phishingu je soustředěno na Ameriku a službu Paypal (internetový platební systém používaný globálně). S phishingem zaměřeným na bankovní sektor souvisí i pojem FULLZ. Tak jsou označovány shromážděné doplňující informace o určité osobě (např.: datum narození, social security number-identifikační číslo vydáno občanům a dočasným obyvatelům žijícím v USA, jméno matky za svobodna). Na základě těchto údajů existují v USA on-line úvěry, které nabízí většina bank. Funguje, ikdyž není karta platná. Průměrný poskytnutý úvěr je $500 - $25000. Cena informací získaných phishingem se pohybuje od $20 do $700. Phisheří se snaží vytěžit maximum z každé získané informace. Soustřeďují se mimo informací z bankovního sektoru i na Paypal účty, Herní konta, Facebook, Rapidshere a další.

Vishing je obdobou phishingu a k útoku využívá telefon nebo VoIP. V případě takového vishingového útoku obdrží člověk e-mail nebo SMS zprávu s žádostí aby zavolal na bezplatné telefonní číslo a potvrdil své údaje, nebo obdrží nahranou telefonickou zprávu s žádostí o zadání údajů k jeho bankovnímu účtu. Obvykle je vyhrožováno, že na účtu nejsou žádné finanční prostředky atd. Vishingu se taky mnohdy přezdívá SMiShing. Hrozbou budoucnosti je vishing, který k odcizení informací využívá VoIP.

Banky ve většině případech odmítají vyplácet tyto útoky, které mají za cíl finanční ztráty, protože se jedná o chybu klienta banky.

4.1.2 Černý trh

Černý trh je označení pro neoficiální ekonomiku. Stejně jako u běžného trhu zde existují dodavatelé a odběratelé zboží, nebo služeb, smluvní ceny, obchodní zvyky atd. Zboží směněné na černém trhu není daněno, nachází se mimo kontrolu státu jako formální autority. Na černém trhu je obchodováno nejčastěji s nelegálními komoditami. Slouží mimo jiné také k prodeji citlivých informací z bankovního sektoru.

Virtuální černý trh sloužící k obchodu s citlivými informacemi z bankovního sektoru funguje v různých formách. Od dobře zabezpečených až po otevřená fóra.

4.1.2.1 Formy černého trhu

Mailing list

Jde o speciální použití elektronické pošty. Umožňuje šíření informací po internetu mnoha uživatelům, kteří jsou v seznamu (mailing listu). Důležitou adresou je adresa mailing listu, která slouží k distribuci nabídek, nebo poptávek. Přijde-li na ni e-mail od zaregistrovaného uživatele, je tento e-mail automaticky rozeslán všem ze seznamu. Jedná se o tzv. e-mailovou konferenci, která je uzavřená (mají do ní přístup pouze registrovaní uživatelé). Všechny mailing listy mají zabezpečení proti spamu. Komunikace může být taky moderovaná. To znamená, že e-maily prochází kontrolou a až poté jsou distribuovány. Přihlášení do mailing listu zabývajícím se obchodem s citlivými informacemi je nelehká záležitost. Obvykle je vyžadován registrační poplatek $1000 - $15000, nový uživatel musí být doporučen určitým počtem stávajících uživatelů mailing listu (např.3,5,10).

IRC

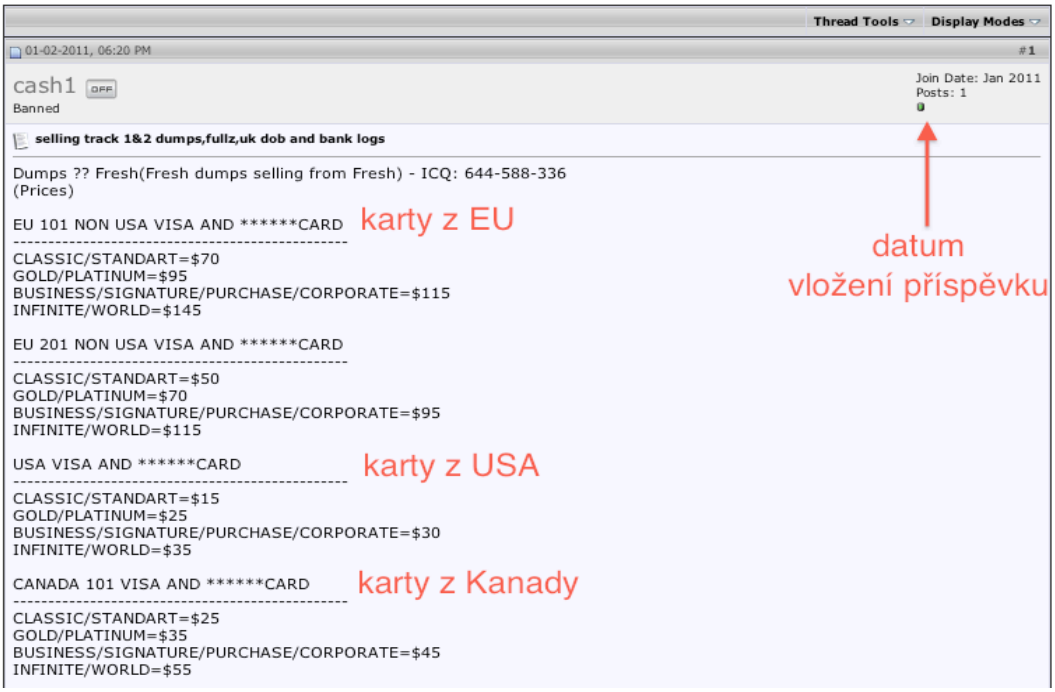
Internet relay chat byla jednou z prvních forem komunikace prostřednictvím internetu, která se odehrávala v reálném čase. IRC je otevřený protokol, který používá TCP (jeden ze základních protokolů internetu zaměřen na transportní vrstvu) a volitelně SSL (zabezpečení komunikace, autentizace, šifrování). Uživatelé komunikují v tzv. kanálech, které jsou podobné chatovým místnostem. Uživatel potřebuje k použití speciální software - tzv. IRC klient. IRC klient spolupracuje s webovým prohlížečem a všechna práce probíhá přes něj. Podmínky přihlášení do systému jsou shodné jako u mailing listu.

SILC

Secure internet live conferencing nabízí téměř totožné služby jako IRC, soustřeďuje se však více na zabezpečení. SILC zabezpečuje pomocí šifrování jak spojení mezi klientem a serverem či dvěma servery, tak i vlastní zprávy odesílané uživatelem jinému uživateli nebo na kanál. Během používání SILC není možné cokoliv poslat nezašifrované, vše je automaticky šifrováno. Nejedná se ale pouze o lépe zabezpečenou verzi IRC, ale díky jejímu modernímu zpracování lze přenášet prakticky cokoliv (např. streamované video). Podmínky přihlášení do SILC, stejně jako u předchozích typů, velmi vysoké.

Internetová diskuse

Internetová diskuse, nebo také internetové fórum je webová stránka, kam jsou vkládány příspěvky uživatelů. Černý trh využívá weby, které jsou zaměřeny pouze na nabídky a poptávky členů fóra. Zabezpečení diskusí je různé. Najdou se fóra vyžadující podobně vysoké podmínky jako předchozí případy a taky fóra s téměř nulovým zabezpečením, které je možné si přečíst bez přihlášení. Ukázka takového fóra je na obrázku níže. Uživatel se snaží prodat naskimované magnetické proužky z karet. Upozorňuji, že jde asi jen o třetinu celé nabídky. Na závěr nabídky prodejce upozorňuje na slevy za odebrání většího množství dat. Jedná se o fórum Account Market fungující od roku 1999.



Obr. 36 Ukázka internetového fóra Accountmarket.com [36]

4.1.2.2 Platby

Platby za nelegální zboží samozřejmě nemohou probíhat prostými převody z účtu na účet. Byly by snadno dohledatelné. Existuje několik služeb, které nabízí jistou míru anonymity. Jde o služby fungující elektronicky prostřednictvím internetu.

4.1.2.2.1 eGold

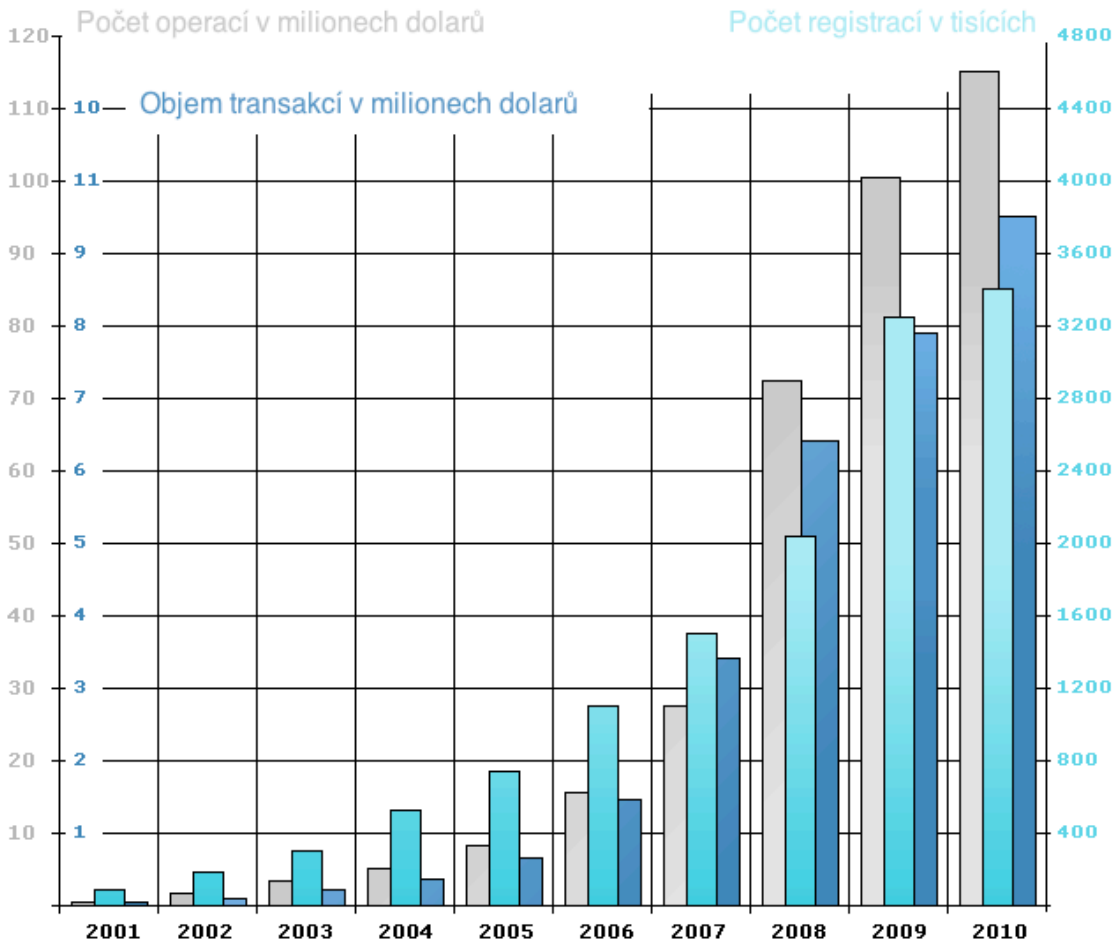
Jedná se o elektronický platební systém krytý zlatem. Systém založen na nákupu zlata, ve kterém jsou následně uloženy peníze. Pokud chce klient prostřednictvím eGoldu peníze vybrat, cena se odvíjí od aktuální ceny zlata. Založení společnosti Gold and silver reverse Inc., která provozovala eGold bylo v roce 1996 dvěma doktory. Do roku 2007 byla zaznamenána řada podezřelých účtů, na kterých se nacházela téměř miliarda dolarů. Počátkem roku 2008 bylo zjištěno 5 milionů eGold účtů. Použití eGoldu pro nelegální platby je ale minulostí. Oba zakladatelé si odpykávají tresty ve vězení a eGold, se sídlem na Karibském ostrově Nevis, je dnes již pod Americkou federální správou. Každý dolar vložený do eGoldu nyní musí být legální.

Obr. 37 Logo G&SR

4.1.2.2.2 WebMoney

WebMoney je platební systém pro online platby, který umožňuje provádět převody mezi účty uživatelů WebMoney nebo obchodníky v celé řadě měn. WebMoney je Moskevská společnost, za kterou stojí ruská banka, do které je z hlediska vyšetřování nemožné se dostat. Většina technického zázemí je právě v Moskvě, majitelé a vedení mají oficiální sídlo ve státě Belize, ležícího ve střední Americe. Stát je Konstituční monarchií vedenou Velkou Británií. Počet účtů u WebMoney přesahuje 11 milionů a nabízí jednu z nebezpečnějších metod zpracování online plateb. Řadí se také mezi nejstarší a nejzavedenějších firem na trhu, které se věnují online platebním systémům.

Obr. 38 Logo WebMoney [25]



Obr. 39 Statistiky společnosti WebMoney 2001-2010 [25]

Funkce Webmoney je označována jako elektronická peněženka. To je platební procesor, který nabízí řadu funkcí k manipulaci s finančními prostředky. Jedná se např. o zprostředkování plateb z běžného bankovního účtu, jako u 3D SECURE, vkládání jen určitého množství finančních prostředků atd. Nejznámějšími elektronickými peněženkami jsou e-Bay, PaySec a další.

K registraci ve WebMoney je třeba jen správně vyplnit údaje o bankovním účtu, s kterým bude komunikovat. Uživatel má na výběr z několika uživatelských prostředí:

- software WebMoney - nutný nainstalovat do počítače
- webový prohlížeč s HTTPS přenosem
- software WebMoney pro mobilní zařízení

WebMoney uživatelé získávají body, které slouží k hodnocení uživatelů a indikátor důvěryhodnosti. Přijímat, nebo odesílat platby je možné v několika nabízených měnách. Na každou z nich je třeba mít založenu elektronickou peněženku. Za každou transakci je účtován minimální poplatek 0,8%. Ten u některých měn a velikostí částek narůstá. Využití

finančních prostředků je možné platbou za služby nebo zboží, převod na účet a nabitím předplacené WebMoney elektronické karty.

Měny WebMoney:

- RUR - Ruské rubly
- USD - Americké dolary
- EUR - Euro
- UAH - Ukrajinská hřivna
- BYR - Běloruský rubl
- UZS - Uzbekitánský sum

Největší odhalený podvod spojen s WebMoney je známý z roku 2008, kdy se 28 letý ruský emigrant snažil vybrat v bankomatech velké množství hotovosti. Upozornil na sebe tak, že vybíral veškerou hotovost z bankomatů Citi Bank na Manhattanu. Zaměstnanci banky dostávali hlášení o tom, že stále více bankomatů v jedné z poboček nemá hotovost. Když se vydali tuto informaci prověřit, zahlédli pachatele, který se pohybuje od jednoho bankomatu k dalšímu. Našli u něj řadu karet, které obsahovali kradená data a byly na ně převedeny finanční prostředky právě prostřednictvím WebMoney. Celkově se jednalo o $2 miliony a bylo odsouzeno 5 pachatelů. WebMoney ale dál bez problému funguje.

4.1.2.2.3 Liberty Reserve

Jedná se o další typ elektronické peněženky. Na oficiálních stránkách Liberty Reserve je společnost popisována jako největší platební procesor a transakční nástroj na světě. Jestli tomu tak opravdu je je těžké odhadovat. Žádné oficiální informace k počtu uživatelů Liberty Reserve nebyla vydána. Při několika časově vzdálených návštěvách byl ale web Liberty Reserve očividně přetížený. To může mít za důvod extrémní nápor nově registrovaných uživatelů.

Nabízí podobné služby jako eGold a WebMoney. Je připojen ke konkrétnímu bankovnímu účtu. Je používán ke zprostředkování plateb a dalším úkonům. Sídlo Liberty reserve je na Kostarice (pobřežní stát Střední Ameriky) a podle informací z internetových fór je služba naprosto bezpečná vzhledem k zveřejňování informacím o transakcích vyšetřovatelům.

Obr. 40 Logo LR [26]

Následující prostor je věnován závěru nabídky dat z karet použita jako příklad internetového fóra. Všimněte si mimo jiných důležitých informací jako jsou slevy a osobní informace nabízejícího také způsobů platby, které vyžaduje. Naleznete dvě platební metody, které jsme si popsali. Zkratka WU(Western Union) bude vysvětlena později.

Obr. 41 Dokončení nabídky [36]

4.1.2.3 Exchange service

Aby bylo možno dostat se k finančním prostředkům v takové formě, jaké pachatelům vyhovuje, zabezpečují tzv. Exchange servisy. Ty dokážou převádět téměř jakékoliv částky např. z Liberty Reserve na PayPal. Za tuto činnost si však Exchange servisy účtují poplatky ve výši 5-25% podle typu služby a místa odkud kam je požadováno prostředky převést. Některé zdroje mluví až o pěti stech existujících Exchange servisů (sídlí např. v Rusku, Číně, na Kostarice). Většina provozovatelů těchto servisů je téměř nedostižitelná. Jednu z databázi Exchange servisů provozuje již zmíněná Liberty Reserve. Doporučuje jich 28.

Obr. 42 Web LR Exchange service [27]

4.1.3 Buyer, cashier

Jedná se o nejdůležitější pozice celého systému. Jejich úkolem je získávání prostředků z karet (fyzicky nebo virtuálně). Ve výsledku se jedná o reálné věci (finanční prostředky nebo zboží). Pozice vyžaduje důkladnou znalost systému a prostředky jak znalostí využít. Práce těchto dvou pozic je z počátku stejná. Nakupují, nebo jsou jim poskytovány citlivé informace a zjišťují jejich využití.

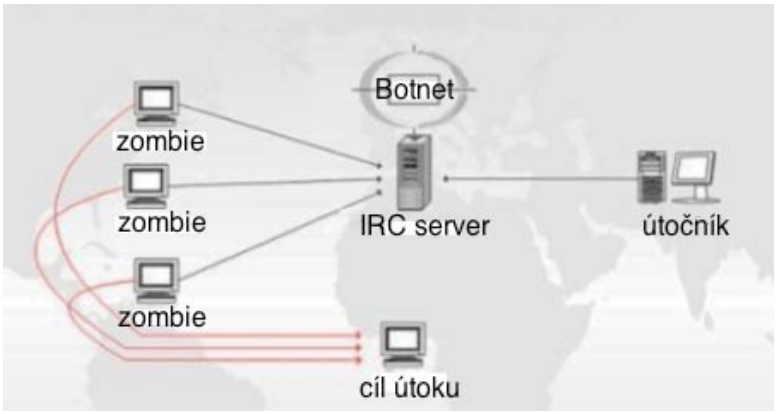
Buyer a cashier jsou pozice, které se zaměřuje na nákup zboží, a to většinou na objednávku. Finanční prostředky jsou získány z nezákonně nabytých informací předchozími pozicemi v obchodním modelu. Buyer a cashier mají za úkol celý proces provést co nejopatrněji bez jakéhokoliv ohrožení jich samotných či celé skupiny. Jedná se o nákup zboží za nelegálně získané finanční prostředky. Zboží je většinou nakupováno na objednávku. Celý proces funguje tak, že nabízí na nějakém specifikovaném internetovém fóru, IRC, nebo SILC své služby (např.: Koupím cokoliv z internetového obchodu za 20% ceny, platba předem).

Stanovené procenta z ceny se liší:

- nezávislí - 15-20% z ceny
- ve skupině - 30-50% z ceny

K zabezpečení využívají anonymní proxy servery, což jsou zařízení (HW nebo SW), která fungují jako prostředník pro komunikaci mezi počítačem Buyera a serverem, kde nakupuje. Důvodem je to, že v obchodě se nedozví jeho skutečnou IP adresu (číslo, které jednoznačně identifikuje zařízení připojené do sítě internet), ale zprostředkovanou anonymním proxy serverem. V podstatě se tedy jedná o IP adresu anonymního proxy serveru. Tyto proxy servery se nacházejí po celém světě.

Dalším nástrojem, který využívají je takzvaný botnet. Je to automatický nebo autonomní program nainstalován do počítače schopný jej vzdáleně ovládat. Počítače infikované tímto programem jsou využívány k nákupu, platbám a dalších úkonům, podle toho jak jsou upraveny. Program obsahuje komunikační a řídící modul. Od virů se liší tím, že vir nelze po jeho vypuštění upravovat. Botnety ano. Ovládání botnetů probíhá prostřednictvím několika komunikačních kanálů. Mezi nejpoužívanější patří již zmíněný IRC (využívají komunikační porty 6666 a 6667). Počítače infikované botnetem se nazývají „zombie“, počítače ovládané bez vědomí uživatele. Více takových počítačů se nazývá armáda zombie, které vykonávají to, co po nich útočník požaduje.



Obr. 43 Botnet schéma

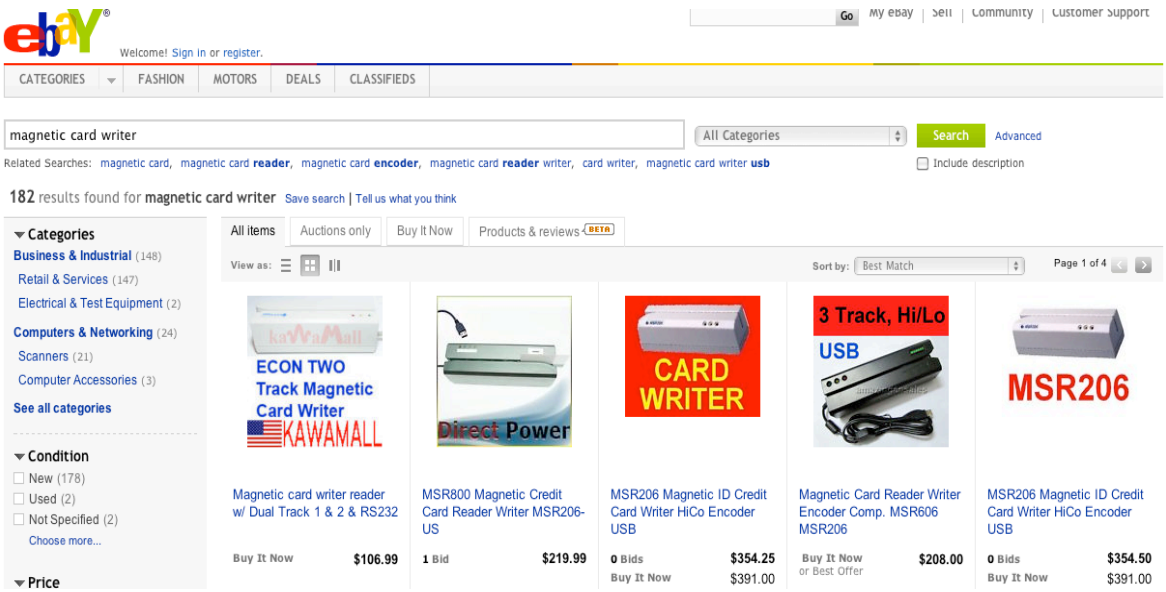
4.1.4 Drop

Nejnebezpečnější pozice. Tito lidé přichází do reálného kontaktu s padělanými platebními kartami. Většinou jsou to právě tito lidé, kteří jsou dopadeni a obviněni za trestné činy spojeny se zneužitím citlivých informací z bankovního sektoru ke krádeži. Existují ale také organizované skupiny působící více než 10 let. Možností jak se dostat k finančním prostředkům je celá řada. Často se jedná o zaměstnance banky, nebo jiných institucí zastírající tuto trestnou činnost. Nejbezpečnější známou používanou technikou je využití Western Union (vysvětleno později).

Jejich nejčastější práce je výběr hotovosti z bankomatu pomocí vlastních vytvořených karet ze získaných dat (např.: skimming). Díky komunikaci a načasování může celý proces vypadat takto: 15:50 středoevropského času naskimována karta v ČR, 16:00 vybrána hotovost v Thajsku. Dostupnost zařízení k nahrávání dat na platební karty (magnetické proužky) je velká. Uvádím nabídku internetového serveru eBay. Jeho použití není složité. Stačí mít jen data a vhodný software, pomocí kterého probíhá zápis. Ceny těchto zařízení se pohybují od $100 do $500. Konkrétní popis metod bude popsán v další kapitole.

Pozice má následující finanční ohodnocení:

- nezávislí - 20-50%
- ve skupině - 20-40%



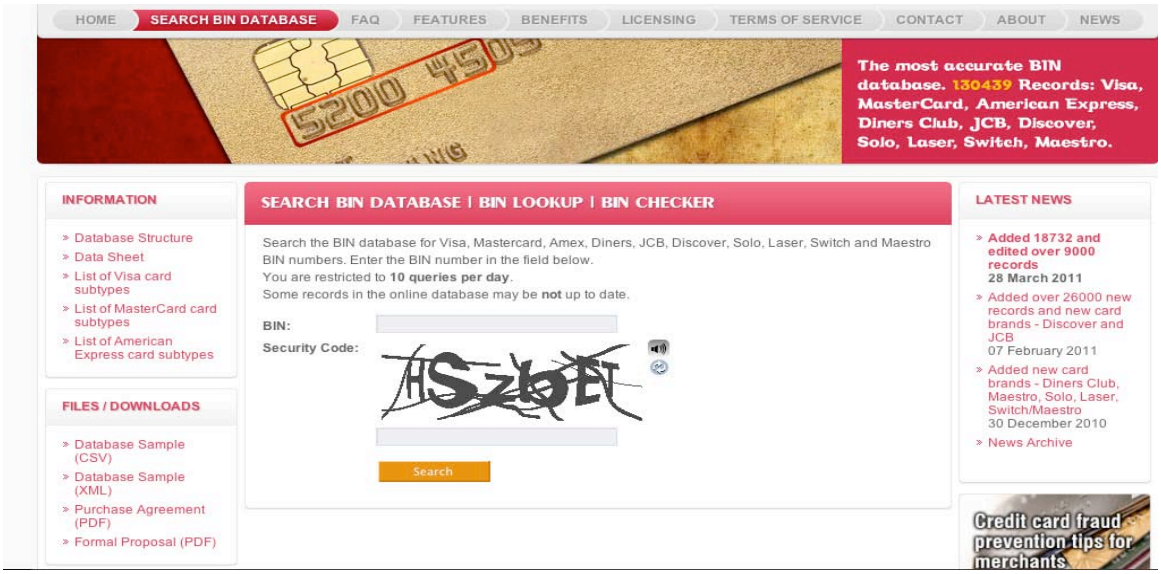
Obr. 44 Nabídka zařízení pro zápis magnetické proužky ze serveru eBay.com

5 METODY VYUŽÍVANÉ PŘI NELEGÁLNÍ PRÁCI S CITLIVÝMI INFORMACEMI Z BANKOVNÍHO SEKTORU

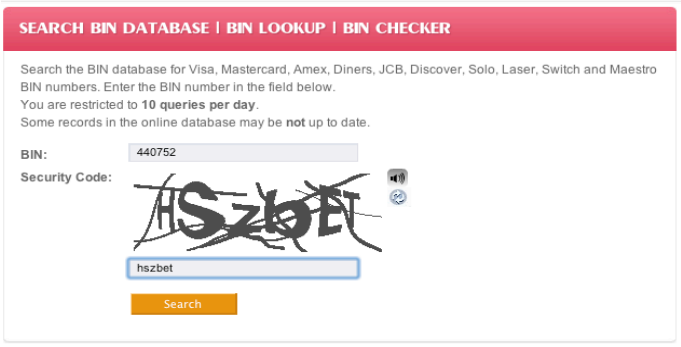
5.1 Využití Issuer identification number

Jak bylo psáno v popisu čísla karty, toto šestimístné číslo poskytuje mnoho údajů. Nemusíte mít však přístup do databází údajů bank, abyste zjistili všechny informace, které Issuer identification number ukrývá. Existují webové služby, nabízející zjišťování těchto informací. Tato služba je nazývána také Bin checker, vycházející z minulého označení tohoto šestičíslí. Webových stránek nabízející tuto službu jsou desítky. Na jedné z nich si ukážeme jejich funkci.

Po otevření stránky vás služba informuje, které platební karty dokáže prověřit a kolik prověření je možné provést denně. Po vypsání Issue identification number a opsání bezpečnostního kódu webu jsou zobrazeny zjištěné informace.

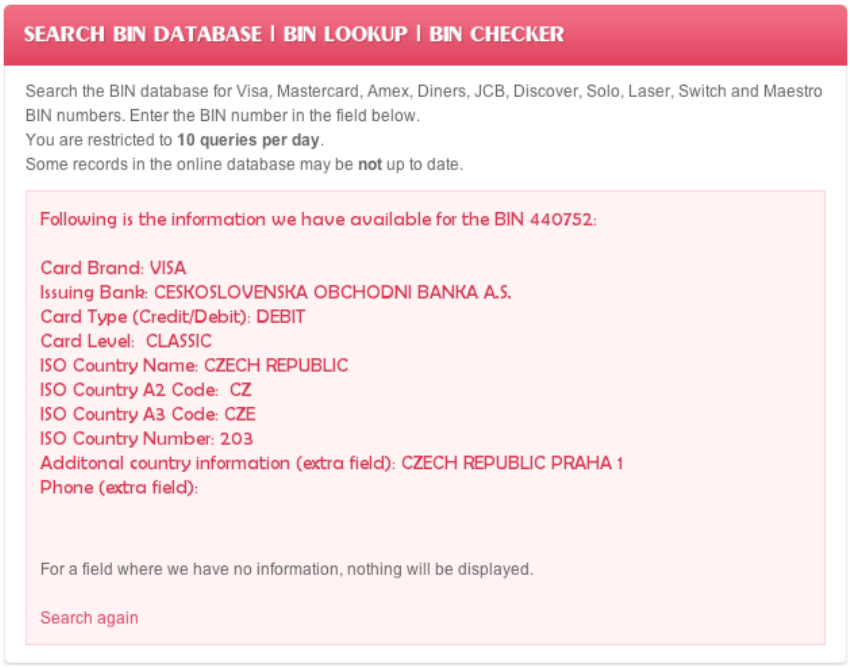


Obr. 45 Úvodní stránka použité služby Binbase.com



Obr. 46 Vypsání IIN a bezpečnostního kódu

Pro kontrolu údajů byla použita moje osobní karta (Obr. 3). Jak můžete sami vidět, všechny údaje souhlasí. Z toho plyne, že člověk, který má naskimovanou kartu zjistí během pár sekund tyto údaje. S využitím anonymního proxy serveru může provádět neomezené množství zjišťování těchto údajů. Z nabídky bank, nebo např. z průzkumů (Tab. 1) lze jednoduše zjistit limit karty. Pokud bych si na své kartě Visa Classic nezměnil limit, byl by jednoduše dohledatelný.



Obr. 47 Zjištěné informace

Tab 3 Přehled limitů českých bank z druhé poloviny roku 2010 [31]

Banka	Debetní karta	Základní limit výběru z bankomatu	Základní limit platby	Období limitu	Poplatek za změnu
Citibank	Maestro	40 000	20 000	týdenní limit	90 korun
Česká spořitelna	Visa Electron	15 000	30 000	týdenní limit	30 korun
ČSOB	Visa Electron	dohromady 15 000		týdenní limit	20 korun
GE Money Bank	Maestro	15 000	20 000	denní limit	zdarma
Komerční banka	Perfect karta	10 000	10 000	týdenní limit	zdarma
LBBW	Maestro	dohromady 10 000		týdenní limit	zdarma
mBank	Visa Classic	50 000	40 000	denní limit	zdarma
Poštovní spořitelna	Maxkarta	dohromady 15 000		týdenní limit	1.zdarma, pak 26 korun
UniCredit	Visa Electron	10 000	20 000	denní limit	100 korun

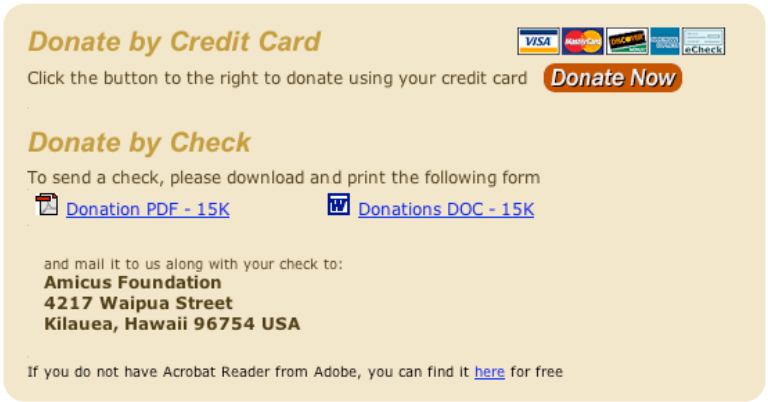
5.2 Ověření funkčnosti karet

Aby pachatelé zjistili funkčnost karty, a nemuseli přitom navštívit fyzicky banku, bankomat nebo platební terminál, využívají několik technik. Ty je ochrání od nebezpečí odhalení.

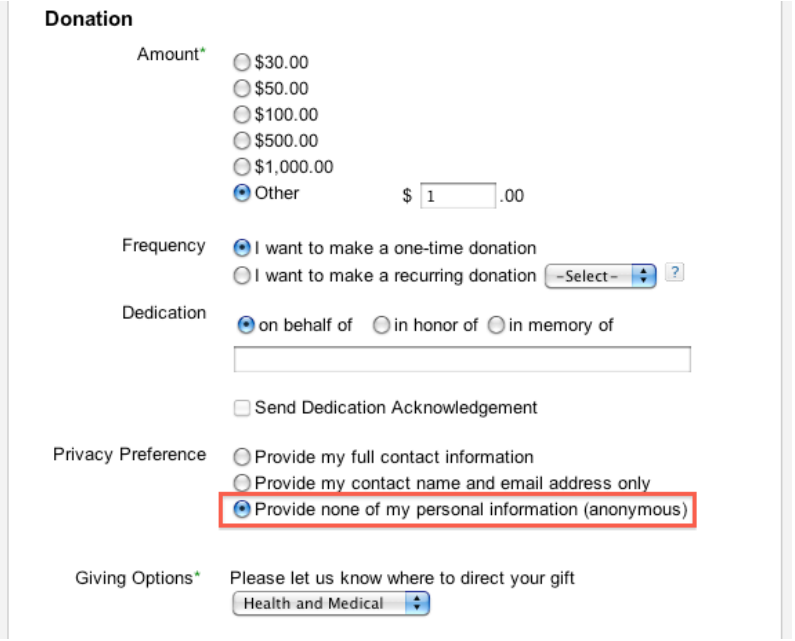
5.2.1 Využití služeb Donate for me

Služby, které jsou zřizovány hlavně pro přispívání na podporu charity, nemocných, zasažených katastrofou a mnoha dalších. Doslovný překlad zní: Daruj mi. Tyto služby jsou umístěny na webových stránkách. Stačí jen vyplnit formulář a odeslat jej. Provede-li se platba, karta je funkční. Tuto metodu používá většina pachatelů těchto trestných činů. Donate for me služeb jsou na internetu stovky. Nejkurióznější případ pochází z kampaně Amerického prezidenta Obamy, který umožnil lidem podpořit jeho kampaň. Až po jeho zvolení bylo federálními složkami zjištěno, že $45 milionů bylo právě z ověřování karet.

Na ukázku této služby jsem našel stránky nadace AMICUS (amicusfoundation.org), která se mimo jiné zabývá pomocí v postižených oblastech Thajska po tsunami. Hned na úvodní stránce najdete tlačítko Donate Now. Po kliknutí na něj se otevře stránka s formulářem, ve kterém jsou vyžadovány osobní údaje, údaje z karty (vydavatele karty, typ karty, číslo karty, expirační dobu, bezpečnostní kód pro bezkontaktní platby). Důležité je že kromě údajů o kartě neprobíhá žádná kontrola zadaných informací o darujícím. Lze vybrat i možnost anonymního dárce (Obr. 49).



Obr. 48 Výzva k darování



Obr. 49 Část Donate for me formuláře

Po odeslání formuláře nadace poděkuje a ujistí dárce, že platba proběhla v pořádku.

5.2.2 Využití platebního procesoru

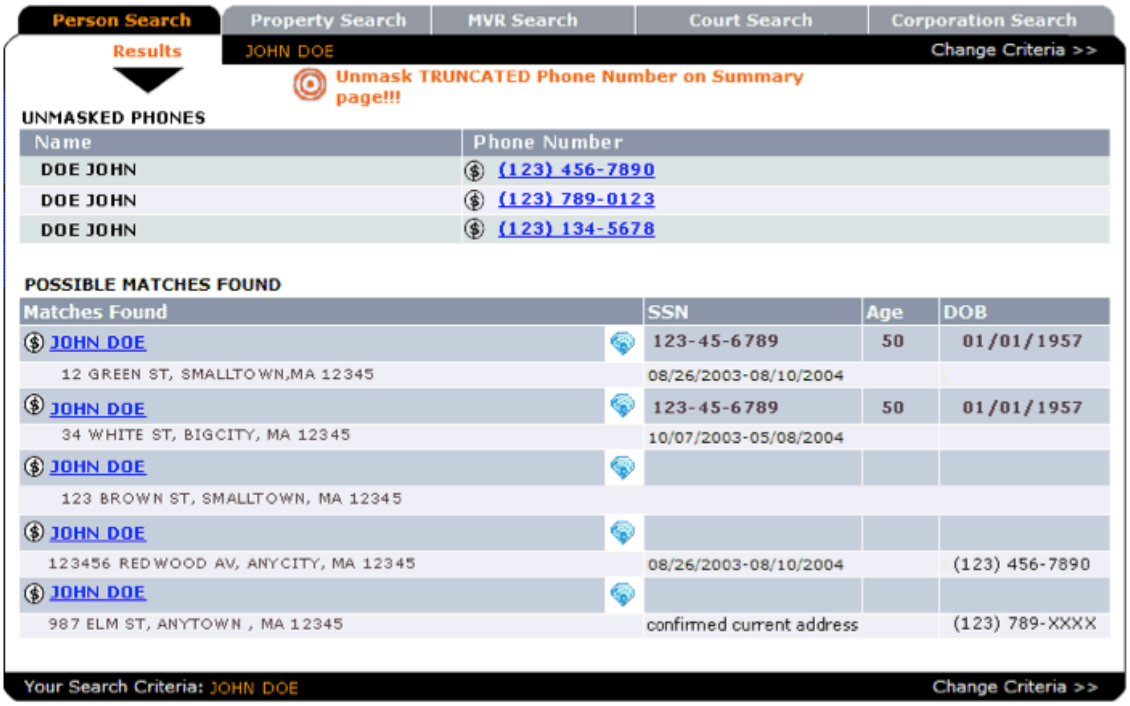
Jak je známo, platební procesor slouží ke komunikaci při platbách. Používají ho bankomaty, platební terminály ale internetové obchody a různé platební společnosti. Systémy platebních procesorů jsou několikastupňové. K ověření funkčnosti karet je možné využít dvoustupňové, nebo třístupňové systémy. Tyto systémy lze použitím různých technik zastavit po jednotlivých stupních. Dvoustupňový systém je jednodušší. V prvním stupni se dotazuje na dostatek finančních prostředků (v závislosti na platbě), pokud ano, druhý stupeň proběhne jejich převod. Logicky ověřovatelé zastavují systém po prvním stupni. Vrátí se jim informace o velikosti finančních prostředků. Třístupňové systémy pracují podobně. Ve druhém stupni je navíc požadováno zadání PSČ, neboli ZIP CODE vydavatelské banky.

Samotné využití probíhá tak, že je napadnut nějaký internetový obchod. Na něm si spustí útočníci vlastní HTML script, který dokáže přerušovat činnost při ověřování stavu účtu. Tato metoda je pro ověřovatele funkčnosti karet nejbezpečnější, protože při ní nedochází k přesunu finančních prostředků. To není schopen detekovat žádný bezpečnostní systém. Všechny jsou založeny na platebních transakcích. Některé platební procesory se proti těmto útokům snaží bránit. Nedaří se jim to kvůli vysokému počtu transakcí.

5.3 Zjišťení dodatečných údajů vyžadovaných pro ověření

Využití dodatečných informací o majiteli karty používají některé společnosti (bankovní i nebankovní) k dodatečnému ověřování osob. Těmito informacemi může být cokoliv od data narození až po social security number (využívané jen v USA). Tento systém funguje v Anglii, USA, Německu a dalších zemích světa. V ČR ani na Slovensku tento systém nefunguje. Je však předpokládán jejich příchod.

V USA existují webové služby na vyhledávání osob. Cena za vyhledávání se liší počtem informací, které jsou požadovány. Databáze webu obsahuje SSN, data narození a další informace mnoha osob. Tyto služby jsou v některých případech zastírány jako detektivní činnost zaměřena na vyhledávání osob. Lidi, kteří tyto údaje zjišťují to velmi láká, protože se tím dá vydělat několik tisíc dolarů měsíčně. Většinou se jedná o osoby z takových pozic, které mají přístup k databázím (policisté, státní úřady apod.).



Obr. 50 Ukázka z webu, určeného pro zjišťování dodatečných údajů [37]

Obr. 51 Web soukromé detektivní společnosti

5.4 Zjištění množství použitelných finančních prostředků na účtu

Zjistit kolik použitelných finančních prostředků se nachází na účtu je pro pachatele důležité. Nezajímá je tedy celkový stav konta, ale alokovanou sumu, kterou lze použít na jednu transakci. Víc transakcí z bezpečnostních důvodů neprovádí. Toto množství finančních prostředků je označována jako Ballance. Jakmile se k této sumě dostane zloděj, vybere bez problému o dolar nižší sumu. Odpadá tedy testování různých částek v bankomatu.

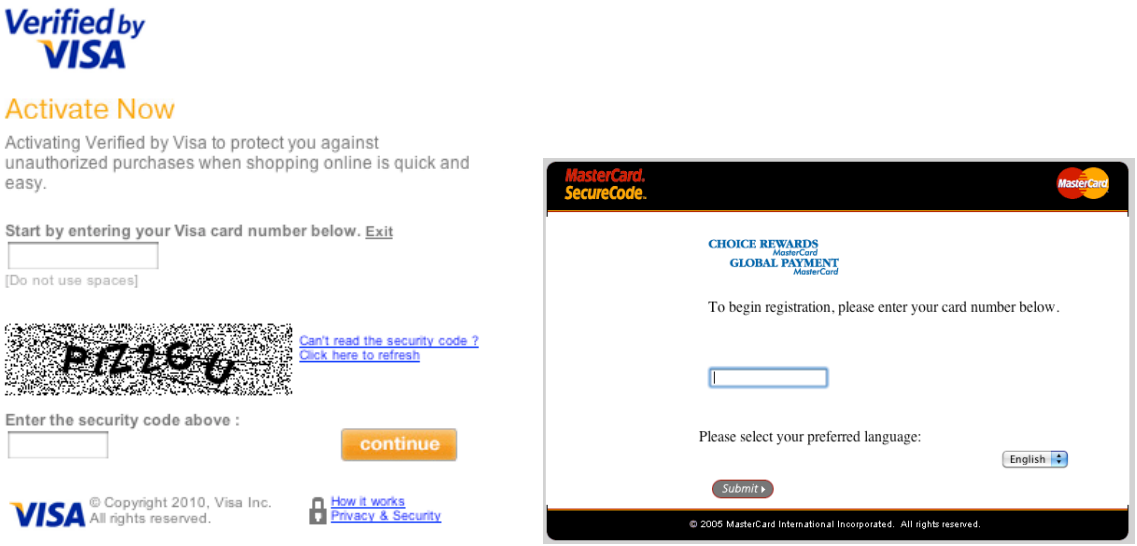
Existuje několik způsobů, jak to provést. Prvním je využití Bank of America, americké banky, která nabízí automatický systém ke zjištění ballance a dalších informací. Služba funguje automaticky prostřednicvím speciálního SW. Princip je jednoduchý. Pošlete SMS na číslo služky s textem co chcete zjistit a poslední čtyři čísla platební karty(bal chk9445). Obratem je na číslo, ze kterého byla SMS odeslána SMS s výší alokovaných finančních prostředků. Služba je označována jako text banking .Uživatelé z USA, kteří tuto službu chtějí využít musí zadat navíc SSN. Po testování této služby v ČR bylo zjištěno, že nefunguje. Slovenská republika tuto službu podporuje. Celý systém přístupu k informacím o všech kartách vychází z toho, že Bank of America je majitelem VISA. Má tedy přístup ke všem informacím o VISA kartách. Zároveň existuje smlouva mezi bankami o vzájemné výměně dat s Master card, Amex a další. Z této služby lze zjistit kolik je možné z účtu vybrat, ale také jestli karta a účet vůbec fungují.

Další možnou metodou k zjištění ballance je využití platebního procesoru jako v minulém případě. Je to proces testování různého množství finanančních prostředků. Jakmile částka projde, znamená to, že tato částka je alokovaná.

5.5 Prolomení 3DSecure

Bezpečnostní prvek 3D secure poskytne obchodníkovi očekávajícímu informaci od třetí strany pouze rozhodnutí, jestli transakce proběhla, nebo ne. Nedostává žádnou informaci o tom jestli platba proběhla pomocí 3D secure nebo nikoliv. Obchodník nemůže ověřit kartu na základě Issuer identification number. Právě díky vložení třetí strany do provedení transakce se obchodník nedozví žádné citlivé informace o zákazníkovi. Obchodníkům garantuje banka návratnost podvodů při používání 3D secure (do určité výše).

Technologie 3D secure , které obchodníci v e-shopech používají, jsou v 95% případech předávány velkým společnostem. Společnost Achex, koupena společností First Data je jednou z nich. Achex je platební procesor, který se zabývá 3D secure už od jeho založení. Na jejich stránkách si je možné ověřit, jestli banka podporuje 3D secure. Zjištění probíhá pomocí čísla karty. Jestliže je klient přesměrován na stránky své banky, přihlásí se do systému a tam zjistí, jestli má službu aktivní. Pokud ji aktivní nemá, většinou to znamená, že je mu služba nabídnuta. Samozřejmě, že pokud službu nechcete, neaktivujete ji.



Obr. 52 Přihlášení do systému 3D Secure u společností Visa a Master Card

Jeden z bezpečnostních prvků, který je často používán je technologie Geo IP. Je zaváděna do mnoha e-shopů a funguje i na serveru Achex. GeoIP detekuje, z které části světa uživatel přistupuje (na základě IP adresy). Internetové obchody tyto data ukládají a přiřazují k platbám. Mají tak pocit vyššího zabezpečení transakcí. Jedním ze způsobů jak oklamat Geo IP je využití botnetů. Existuje řada botnetů fungujících několik let. Obsahuje stovky tisíc živých proxy, které si lze na botnetu koupit a využívat je. Velmi těžké detekovat botnety, protože nepoškozují, ale pouze využívají. Botnety se do využívaných počítačů dostávají např. společně s nelegálně staženými daty z internetu (SW, počítačové hry, hudba apod.) a pak využívají uživatelovu IP adresu. Infikované počítače pak fungují několik let bez povšimnutí majitelů. Každá bot v PC využívá minimální část připojení, aby byl odhalen co nejpozději. Ceny infikovaných IP vhodných k využití se pohybují od $20 do $40 za 5 proxy.

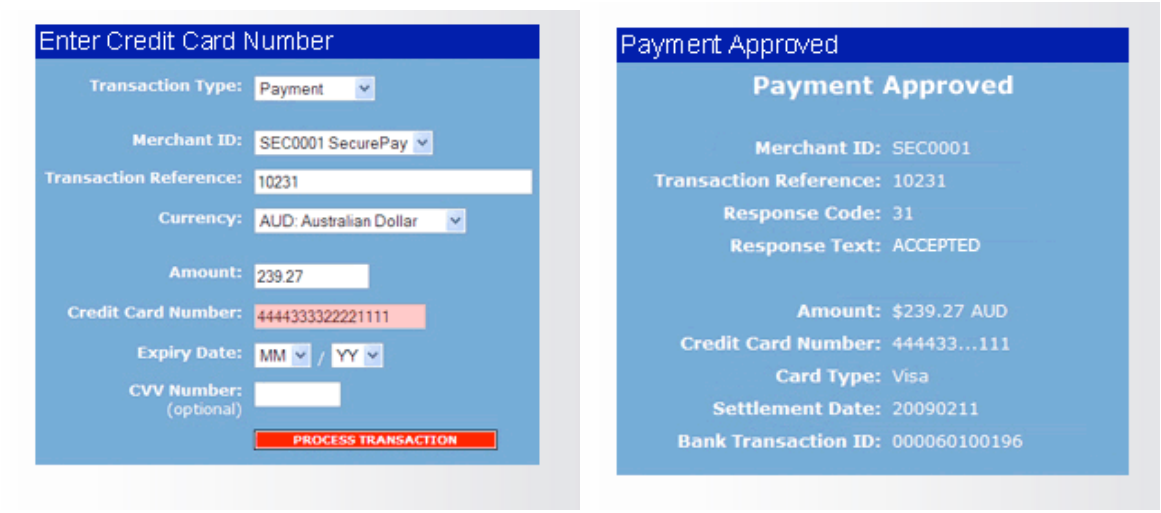
Podle posledních průzkumů se za rok 2010 dostalo mezi deset největších botnetů dostalo šest, které ještě v roce 2009 neexistovaly. Těchto 10 největších botnetů znamená podle předpokladů 47% z celkového počtu botnetů. Za rok 2010 je odhadováno deset milionů infikovaných IP adres.

5.6 Získávání finančních prostředků z karty

5.6.1 Virtuální platební terminál

Tuto službu nabízí některé banky. Funguje stejně jako reálný platební terminál, ale všechny informace požadované k provedení transakce jsou umístěny na platební kartě. Jedná se o totožné informace jako při online platbách.

Důvodů, proč jsou platební terminály používány je rychlost přesunu finančních prostředků od plátce k příjemci. Při platbě přes virtuální terminál banky jsou finanční prostředky přesunuty z jedné banky do druhé do 24 hodin (platba online v internetovém obchodě bývá přesunuta v několika dnech, i týden). Jakmile jsou peníze v jiné bance, je velmi složité se k nim dostat. Tuto věc je třeba řešit soudní cestou. To zabere určitý čas, což znamená více času pro zloděje.



Obr. 53 Virtuální platební terminál [28]

5.6.2 Služba Western Union

Název Western Union je 200 let starý. Tehdy se zabývala převozem hotovosti a cenin dostavníky. Dnes jsou nabízeny různé formy transakcí. Patří společnosti Citi Group (vlastní i Citi Bank), mající přístup ke všem Master Card datům. Pro potvrzení platby přes Western Union je nutné zavolat z čísla vlastníka karty do Western Union. Operátor hovoru se klienta zeptá na nějaké kontrolní údaje pro ověření platby (jméno manželky, jméno matky za svobodna apod.). Odpoví-li klient špatně, transakce je zamítnuta. K získání dodatečných údajů vyžadovaných k ověření je využito databází popsaných výše. Jediným zabezpečením, pokud pachatelé zjistí dodatečné informace o držiteli karty je jeho telefonní číslo. Přepsat v databázi banky jej není nemožné. Nabízí se tak možnost spoofingu. Spoofing je nelegální služba provozována např. zaměstnanci telefonního operátora, který nabízí změnu vašeho čísla na jakékoliv jiné. Jakmile pak probíhá volání, tak se číslo tváří jako číslo majitele karty. Po ukončení hovoru je číslo pachatele změněno zpět. Western Union je již vybavena kontrolním SW a tak je využití spoofingu stále těžší.

5.6.3 Fyzický výběr hotovosti z bankomatu

Pachatelé, kteří získávají data z magnetických proužků a čipů platebních karet je většinou distribuují v textovém formátu. K výběru hotovosti je nutné převést zpět do formy magnetického záznamu. Je nutné zapisovací zařízení připojit k počítači a pomocí vhodného SW zapsat data zpět na kartu.

Jsou odhadovány stovky skupin po celém světě, vybírající hotovost z bankomatů. Hotovost je rozdělena mezi všechny členy skupiny. Cashier, jak je tento člověk pojmenováván si vybírá co nejbezpečnější bankomaty (bez kamer a zaměstnanců banky). Průměrný výdělek středně velké pracovní skupiny je $150 000 denně.

Pokud pachatelům chybí jedna ze stop na magnetickém proužku, existují služby, které jej dokážou zpětně vygenerovat. Na jednu z těchto služeb jsem narazil na webových stránkách binchecker.com., které slouží také k získávání informací o kartě pomocí BINu. Nabízí bezplatně a bez registrace generování stopy 1. ze stopy 2., jména a příjmení vlastníka karty. Vzhledem k tomu, že stopa 1. nabízí větší množství údajů, je sama o sobě důležitější. Nezbytná je také pro správnou funkčnost magnetického proužku karty. K ověření správnosti jsem použil data ze stopy 2., která je uvedena při vysvětlení magnetického proužku. Při kontrole shody originálu a vygenerované stopy jsem narazil na mírné chyby, které však lze jednoduše odstranit. Výběru z karty už pak nic nebrání.

Obr. 54 Generování 1. stopy magnetického proužku

6 NÁVRHY NA ZVÝŠENÍ BEZPEČNOSTI BANKOVNÍCH SYSTÉMŮ

6.1 Pro klienty bank

6.1.1 Základní bezpečnostní pravidla pro bezpečné použití bankovních systémů

Důležité je uvědomit si, že platební karta je klíčem k většímu množství finančních prostředků. Kartu doporučuji nosit odděleně od osobních dokladů. V případě získání údajů může pachatel operovat s dodatečnými osobními údaji. Nezapisujte si PIN a už vůbec ne do blízkosti karty nebo dokonce na kartu samotnou. Při platbě zkontrolujte, že vám byla vrácena opravdu vaše karta. Zbavujte se také všech dokumentů obsahujících číslo karty (účtenek, výpisů, potvrzení o průběhu platební transakce apod.). Pokud kartu ztratíte, okamžitě hlaste ztrátu bance buď na pobočce, nebo na bezplatnou linku vydavatele karty. Při krádeži banky informujte policii a podejte trestní oznámení na neznámého činitele.

6.1.2 Zvýšení bezpečnosti

Více platebních karet

Při rozložení všech finančních prostředků na několik bankovních účtů je předcházeno napadení všech. Nosit pohromadě karty ze všech těchto účtů se nedoporučuje. Hlavní výhodou používání více účtů a tím pádem i více karet je možnost účelového využití jednotlivých karet.

Návrh na použití jednotlivých karet:

- karta č. 1. - pro platby v okolí bydliště (menší nákupy,běžné a známé obchody)
- karta č. 2. - pro platby dražšího zboží nebo služeb
- karta č. 3. - Pro platby v zahraničí (pro vyšší bezpečnost do každého státu jedu)

Kartu noste na bezpečné místě sledujte ji

Kartu noste na bezpečném místě, nenechávejte v automobilu ani jiném nebezpečném místě. Krádež není sice považována za klasický příklad zneužití karty. Zloděje většinou zajímá hotovost v peněžence, které se následně zbaví i s kartou, ale mohou se najít i zloději znalí systému. Jak již bylo psáno, doporučuji okamžitě informovat banku a policii. Pokud dáváte kartu z ruky, vždy kartu sledujte. Platíte-li kartou v obchodě,

nenechejte obchodníka zmizet z vašeho dohledu. Případně ho následujte na místo, kde provede platbu. Předejdete tak skimingu. Kartu v žádném případě nedávejte do zástavy.

Před použitím bankomatu si jej pečlivě prohlédněte. Zvýšenou pozornost věnujte místu pro vkládání karty. Zkuste, jestli na ní není nic nalepeno tak, že zkusíte vnější část odlepit. Zaměřte se i na klávesnici, kterou ohmatejte a ohledejte. Sledujte také prostor kolem bankomatu, z důvodu odposlechu PINu jak kamerou, tak fyzicky. Je-li vše v pořádku, přikryjte si ruku zadávající pin. Nikdy neodcházejte od bankomatu před ukončením odhlášení, vyjmutí karty a hotovosti. Jestliže karta nevyjela z bankomatu, bankomat neopouštějte a zavolejte policii.

Real time kontrola účtu

Jestliže se přes všechnu vaši opatrnost stane to, že jsou vaše peníze v ohrožení nebo jsou již ukradeny, je důležité jednat rychle. Aby se okradený klient banky o krádeži nedozvěděl až na výpisu z účtu, nabízejí banky realtimové služby pro kontrolu účtu. Jejich využití je vhodné právě z důvodu toho, že jste informováni o všech pohybech na vašem účtu. Máte tak možnost okamžitě reagovat na nesrovnalosti. Jednou z možností kontroly účtu je internetové bankovnictví. Jak již víme, poskytuje mimo jiné i informace aktuálních pohybech na účtu. Stačí jednou za den navštívit internetové bankovnictví a ujistit se, že je vše v pořádku. Další možností je využití informačních SMS, které informují o všech pohybech na účtu. SMS je odeslána okamžitě po přijetí nebo odeslání finančních prostředků. Lze si také nastavit automatickou opakovanou informativní SMS odesílanou v určitou dobu (např. každé pondělí v 9:00) .

Výběr na přepážce

Pokud chcete vybrat větší finanční obnos a vaše banka není natolik vzdálena proti bankomatu, využijte radši přepážku ve vaší bance. Na přepážce neprokazujete žádné z údajů vyžadovaných při jiných transakcích (stačí většinou občanský průkaz). Prostor banky je monitorovaný a většinou i střežený ostrahou. Zaměstnanci banky jsou důvěryhodní, a pokud by se pokusili o nějaký podvod, byli by okamžitě odhaleni.

Změna PIN kódu

Jak je známo, PIN lze změnit mnoha způsoby. Jakmile je změněn, není jej zpětně možné vygenerovat pomocí čísla karty a generujícího klíče banky. Je nepravděpodobné, že

by mohl uniknout, ale pokud by se to stalo, banka by jistě nestihla včas zareagovat na problém a přišla by o hodně peněz.

Využívání pouze čipu

Kvůli častému zneužívání magnetického proužku se nabízí otázka, proč nevydávat karty pouze s čipem. Bylo by s ní možné platit pouze v obchodech podporujících čip (tedy těch důvěryhodných), ale nebylo by možné ji naskimovat. V budoucnu se bohužel zavádění takových karet nechystá. Jedinou možností je tedy mechanicky poškodit magnetický proužek. Splnilo by to všechny požadavky. Toto konání by však bylo nezákonné. Klient banky a tedy i držitel karty má kartu v jejím funkčním období od banky zapůjčenou a proto ji ani nemůže poškodit. Nabízí se také otázka, jestli by toto nákladné rozhodnutí bank nemělo za důsledek pouze přeorientování skimmerů na čipy.

Platební transakce na internetu

Pro platby v internetových obchodech nebo práci v internetovém bankovnictví platí podobná pravidla. Základem je mít kvalitně zabezpečeny technické parametry. Mít silné heslo do operačního systému, požívat šifrované spojení, využít některou z dalších možností k zabezpečení autorizace (např.: časově závislý token). Od počítače, na kterém jste zadávali bezpečnostní údaje a jste tedy oprávněni provádět bankovní transakce, nikdy neodcházejte. Při nákupu v internetových obchodech si všímejte kvality webového prostředí (grafika) a použitých identifikačních prvků. Při práci ve společenských prostorech, kde se nachází velké množství osob, se snažte co nejvíce skrýt proces autorizace a samotné práce v internetovém bankovnictví nebo internetovém obchodě. Nabízí se i možnost použití TAN kódů či jiných nadstandardních prvků internetového bankovnictví.

Bezkontaktní platební karty

Problém těchto karet je jasný: bezkontaktní přenos dat, který lze využít k získání dat z karty. Ochranou proti tomuto způsobu útoku je použití speciálních obalů. Jsou to plastové obaly, ve kterých se nachází stínící vrstva, která znemožní jakoukoli bezdrátovou komunikaci. Klient ji po každém použití jednoduše zasune zpět do obalu a data jsou v bezpečí. Je mnoho produktů, které nabízí tyto vlastnosti (obaly, peněženky, brašny).

Pokud na vás byl spáchán zločin

Stanete-li se objetí zločinu spojeného s odcizením finančních prostředků z vašeho účtu, nečekejte na interní vyšetřování banky a okamžitě nechejte kartu zablokovat a celou událost oznamte na policii. Podáním trestního oznámení na neznámého pachatele předejdete jakýmkoliv dalším problémům a nenecháte vše jen na bance. Některé banky jsou nespolehlivé. Interní vyšetřování banky se může bez zásahu policie protáhnout. V procesu vyšetřování může být zapojeno hned několik subjektů: klient, obchodník, vydavatel karty, banka klienta a banka obchodníka. Bankám jde o jejich jméno a tak se snaží případné podvody tajit před médii a Soudy. Často tak dochází k mimosoudnímu vyrovnání, nebo dokonce k navrácení zcizené částky. Banky také vychází vstříc aktivním klientům, kteří reagují na podezřelé pohyby na účtu. Banky přejímají plnou zodpovědnost za všechny transakce uskutečněné 48 hodin před zablokováním karty (tento časový interval se u různých bank liší).

6.2 Pro obchodníky

Obchodník, který by chtěl předejít problémům se snaží skloubit bezpečnost s rychlostí provedení transakce. Je důležité mít odborně proškolený personál, který transakce provádí (jak z funkčního tak bezpečnostního hlediska). Seznámení s pravidly akceptace platebních karet zvýší a pravidelné školení udrží ve společnosti vysokou míru bezpečnosti. Problémy by mohly mít v některých případech vliv na vývoj obchodní společnost, která platbu provádí. Při prvním kontaktu s kartou ji důkladně prohlédněte. První informací je celkový vizuální dojem z karty. Platnost karty poskytne obsluze informaci jestli má vůbec pokračovat v transakci. Emboss a hologram jsou nejdůvěryhodnější vizuální prvky karty. Komunikujte se zákazníkem a sledujte jakékoliv podezřelé chování. Tím může být nákup velkého množství zboží, nebo nezájem o doplňkové informace k produktu. Každou takovou platbu okamžitě ohlaste a ověřte, jestli se nejedná o podvod. V nejnutnějším případě požádejte zákazníka o průkaz totožnosti k porovnání s údaji na kartě.

Nebraňte se investovat do kvalitních technologií. Nutná je bezpečná komunikace a kvalitní terminál. Využití čipu a dohody EMV Liability Shift dává Českému platebnímu systému, tak jako mnoha evropským, kvalitní základy. Využívání POS terminálu k zjištění rozdílů čísla karty je efektivní a často opomíjená metoda. Zaměstnanec obchodní společnosti provádějící platbu jednoduše vytiskne na tiskárně číslo karty z magnetického proužku.

7 ODHAD VÝVOJE BANKOVNÍCH SYSTÉMŮ

7.1 Globální vývoj

Odhad vývoje bankovních systémů je závislý na okolnostech několika rovin (politické, ekonomické a personální). Jsou vyvíjeny nové technologie, standardy a legislativní opatření, které jsou postupně testovány a zaváděny do bankovních systémů. Prioritou je bankovní systémy činit rozsáhlejší, bezpečnější a mobilnější než jsou doposud.

Nejvíce pozornosti je v poslední době věnováno technologiím, zabývajících se bezkontaktní platbou. Většina velkých karetních vydavatelů a bank spatřují v této formě platby budoucnost. Na světě je vydáno více než 320 milionů bezkontaktních bankovních karet. V roce 2011 je očekáván vyšší než 20% nárůst. Na konci roku by tak podíl bezkontaktních karet měl činit 10% ze všech platebních karet v oběhu. Bezkontaktní platby jsou podporovány nejen typickými bankovními kartami, ale i jinými prostředky. Dlouho se například mluví o bezkontaktní platbě pomocí mobilního telefonu. Vyvinutá technologie se nazývá NFC (Near Field Comunication) a je schopna platit podobně jako RFID karty. Jsou schopny komunikace na 20 centimetrů. To je o 10 centimetrů více než RFID platební karty. Rozvoj této technologie závisí hlavně na výrobcích telefonů, telefonních operátorech a bankách. V této technologii spatřuji bezpečnější variantu bezkontaktních plateb. Majitel telefonu, vybaveného NFC technologií může jednoduše ovládat bezkontaktní komunikaci. Pokud telefonem není prováděna platba, NFC funkci nechává majitel vypnutou a tudíž není napadnutelný. Mělo by být taky možné nastavit limit, po jehož překročení bude nutné zadat bezpečnostní kód prostřednictvím telefonu.

Obr. 55 Platba mobilním telefonem [29]

Zajímavý postoj k bezkontaktním platbám zaujala společnost Master Card. Ve své nabídce má totiž dvojici karet, které dostanete k jednomu účtu. Jedna je běžná bankovní karta, druhá obsahuje pouze vyjmutelný čip (stejný jako SIM karta do mobilního telefonu), který je určen pro speciální hodinky. Čip se do hodinek jednoduše zasune a hodinky je možné použít pro bezkontaktní platby. Hodinky je tak možné používat např. pro menší platby a kartu použít jakmile jde o vyšší částku. Produkt byl představen na Pařížské výstavě Cartes and IDentification v prosinci 2010.

Obr. 56 Hodinky pro bezkontaktní platby [30]

Největší novinkou pro rok 2011 se však staly platební karty vybaveny technologiemi, které doposud nebylo možné implementovat. Těmito technologiemi jsou klávesnice a displej. Jejich zavádění do systému právě probíhá. Zajímavé jsou řešení společností Visa, Master Card a dalších. Karty s těmito technologiemi jsou označovány jako lépe zabezpečené. Zaměříme se zase na řešení společnosti Master Card. Nabízí dvě verzí tohoto produktu. V případě, že je karta embosovaná, není na ní klávesnice. Je-li elektronická, je na ní umístěna i klávesnice. Karta bez klávesnice má jedno tlačítko, po jehož stisknutí je vygenerován jednorázový autentizační kód (pro fyzické platby, pro

potvrzení transakcí na internetovém bankovnictví a nákupy v internetových obchodech). Pokud bude karta ztracena, nebo odcizena, Nebude nic bránit tomu, aby ji kdokoliv použil stejně jako její oprávněný uživatel (vygeneruje kód a platí). Karta s Klávesnicí je na tom o hodně lépe. Nejprve je na její klávesnici zadat PIN. Až poté je vygenerován jednorázový bezpečnostní kód. Prostřednictvím klávesnice lze i kontrolovat stav účtu (ten se aktualizuje vždy při použití karty v bankomatu, nebo v platebním terminálu).

Obr. 57 Karty s displejem [30]

Kombinací všech nejnovějších technologií(RFID, klávesnice a displeje) vzniká naprosto jedinečná karta, která se stává největší události od zavedení čipu. I přes množství bezpečnostních prvků je bezdrátový (bezkontaktní) přenos stále největším rizikem. Jak bylo již popsáno v kapitole skimmer, není složité získat data z takové karty. S tím spojen je i obchod s ochranou těchto karet. Zabývá se kryty, obaly, peněženkami apod. Toto příslušenství bude v budoucnu jistě bankou dodáváno s platební RFID kartou.

Strategií bank je pokrývat stále více míst svými platebními terminály. Místa, kde lze platit prostřednictvím bankovní karty jsou někdy až kuriózní. K ještě většímu pokrytí světa platebními terminály přispívají výrobci opravdu mobilních platebních terminálů (velikost mobilního telefonu).

Otázkou zůstává, kam aplikace nových technologií v budoucnosti dospěje. S příchodem nových technických řešení stále rostou možnosti jejich uplatnění. Nejednou bylo polemizováno nad myšlenkou čipů, globálně implementovaných pod kůži. Tato myšlenka je dokonce implementována na některých místech světa. Lokální implementace této technologie je prozatím jediné, co se podařilo uskutečnit. Lidé s bezdrátovými čipy

komunikující bezdrátově se vším, kde lze prokázat identitu. Výsledkem této myšlenky je využití autentizace pomocí podkožního čipu pro bankovní a jiné platební systémy, přístupové systémy a další místa, kde je nutné prokázat svou totožnost. Nevýhodou zavedení této technologie je však otevřenost systému, která bude nutná k jejímu rozvoji. Dostupnost informací díky otevřenosti by měla za následek zvýšení kriminality v souvislosti se zneužitím citlivých informací.

7.2 Vývoj v ČR

Banky České republiky zastávají opatrnou strategii. Zbytečně se do ničeho netlačit a vyčkat reakce globálního trhu. Tato strategie se vyplatila v minulosti, kdy bylo vyčkáváno na čipovou technologii, ale přitom nedocházelo k přílišné zahlcenosti technologií magnetického proužku. Dnešní evropská dohoda EMV Liability Shift staví ČR mezi lépe zabezpečené země světa, stejně jako ostatní země EU.

Co se týká technologií zaváděných ve světě a v ČR, průměrně se jedná o zpoždění jednoho a více let. Kupříkladu karty Master Card s displejem, představeny na výstavě v Paříži v roce 2010, se u nás tento a možná i příští rok určitě neobjeví. Problémem je výrobní cena a cena zařízení, které dokáží s touto technologií pracovat. Bariérou je také skutečnost, že pro výrobu těchto karet s displejem jsou pro výrobu certifikovány pouze dvě společnosti. Ani jedna z nich sídlí v zemích EU.

Tento rok by se však měla do ČR dostat technologie bezkontaktních plateb. Např. Komerční banka ohlásila začátek používání bezkontaktních plateb na začátek druhé poloviny roku 2010. Očekáváno je i zavedení nových a bezpečnějších virtuálních karet pro platby prostřednictvím internetu. Na území ČR jsou registrovány první bezobslužné obchody s možností platby kartou. Karty Master Card a Maestro by měly konečně podporovat zjišťování zůstatků na účtu prostřednictvím bankomatu. Karty Visa tuto službu již několik let podporují. Očekáváno je i započetí prodeje jednoúčelových dárkových karet a předplacených karet. Nabízí se také otázka, proč stále některé banky nezavedly možnost změny PIN kódu. Tato změna je již dlouho očekávána jejich klienty. Strategií bank je nabízet více bezpečnějších služeb a to na co nejvíce místech republiky. Proto se snaží o zvýšení počtu míst, kde bude možné zaplatit kartou. Důraz je kladen na zvýšení počtu mobilních terminálů (taxi, pouliční prodej, těžko dostupná místa apod.). Jednotlivé České banky snad v budoucnu začnou nabízet klientům více nástrojů pro vyšší zabezpečení účtů a nebude nutné kvůli nim banku měnit.

ZÁVĚR

Závěrem mé práce bych rád zrekapituloval prezentované informace. Na úvod byl představen hlavní nástroj pro spravování bankovních účtů. Platební karta, jak je nejčastěji označována, je a bude nejdůležitějším prvkem personálního bankovnictví. Její vývoj bude mít nemalý vliv na vývoj bankovních systémů. Celý bankovní systém je však složen z mnoha dalších prvků. Tyto prvky jsou rozšířeny po celém světě a navzájem komunikují. Vybudování infrastruktury a otevřenost systému přináší flexibilitu, ale také rizika. Úctyhodné je množství způsobů provádění transakcí. Platby kartou, výběr na přepážce, internetové bankovnictví, nebo platby v obchodě jsou běžné činnosti lidí v civilizovaném světě.

Banky se často snaží co nejlépe zabezpečit přístup k finančním prostředkům u nich uloženým. Jsou však tlačeny požadavky zákazníků k co největší flexibilitě. Najít rovnováhu mezi flexibilitou a zabezpečením bankovních služeb je opravdu nelehký úkol. Pachatelé trestných činů, zabývající se bankovní kriminalitou jsou velmi vynalézaví a dokážou využívat důmyslné techniky. Realita je většinou taková, že techniky, které jsou odhaleny se přestanou používat a jsou nahrazeny jinými. Takovými, které nabídne trh. V podstatě se jedná o to, že s novými službami nebo produkty přichází i nové příležitosti páchání trestné činnosti. Typickým příkladem je zavedení RFID technologie a její následné zneužívání. Domnívám se, že při zavádění této technologie si byli vývojáři vědomi, že existuje velké riziko. Vycházeli jistě i ze zkušenosti se skimingem magnetických proužků karet. Produkt však nakonec zavedli do sytému a asi je jasné proč. Zavádění nové technologie do celého světa přinese miliardy dolarů zisku, spojené s požadavky na tento produkt. Strategie bank je soustředěna na vytěžení maxima i při vyšetřování podvodů. V případech, kdy je klient banky okraden, snaží se banka přenést zodpovědnost na něj. Dobré jméno si banky snaží hájit až v případě, kdy jim hrozí mediální zviditelnění ve věci bankovního podvodu. Banky vyjde jako daleko levnější řešení minimalizovat povědomí veřejnosti o bankovních zločinech a způsobech jejich páchání. Činí takto ze dvou hlavních důvodů. Prvním důvodem je udržení si důvěry klientů a druhým možné využití technik k páchání trestné činnosti.

Práce popisuje stav zabezpečení bankovních systémů, který je podle mého názoru většině lidí, kteří jej využívají neznámý. Metody, techniky a služby popsány v praktické části byly prověřeny do takové míry, do jaké to bylo z právního hlediska možné. Jistě však

existuje mnoho nezveřejněných způsobů, jak zneužít bankovní systémy k nelegálnímu získání finančních prostředků. Jsou však používány lokálně a je tedy nemožné cokoliv o nich zjistit. Tato práce může být použita jako základ pro jiné práce zabývající se tímto tématem.

ZÁVĚR V ANGLIČTINĚ

At the end of my Thesis, I would like to recapitulate the information presented. At the beginning, the main instrument for managing bank accounts was introduced. The credit card, as it is usually called, is and will be the most important personal banking tool. Its development will have a significant influence on the evolution of banking systems. However, the entire banking system is composed of many other elements. These elements are spread throughout the world and communicate with each other. Raised infrastructure and openness the system provide flexibility, but also risks. The number of ways to perform transactions is impressive. Payments by the card, withdrawals at the counter, Internet banking or payments in shops are common activities of people in the civilized world.

Banks often try their best to secure access to funds deposited with them. However, they are pushed to utmost flexibility by the requirements of their clients. Finding a balance between flexibility and security of banking services is really a difficult task. Criminals engaged in bank-related crime are very resourceful and able to use the technology that makes one astound. The reality is often so that the techniques that are revealed are abandoned and replaced by others, those that are offered by the market. In essence, the issue is that new services or products bring along new opportunities for committing criminal activity as well. A typical example is the introduction of the RFID technology and its subsequent abuse. I believe that with the introduction of this technology, developers were aware that there is a big risk. Certainly, they drew from the experience with the skimming of magnetic card stripes. However, the product was introduced into the system after all and it is probably obvious why. Introducing new technology worldwide will bring billions of dollars related to the requirements of the product. The banks´ strategy is to make the most of the situation even in fraud investigations. In cases where the bank´s client is robbed, the bank tries to pass the responsibility on them. The banks try to defend their reputation only when they are faced with the risk of hyping regarding the bank fraud. For banks, it is much cheaper to minimize public awareness of banking crimes and the ways of their committing. They do so for two main reasons. The first reason is to maintain the client´s trust and the other is the possible use of the techniques for committing criminal activity.

The Thesis describes the security of the banking systems, which is, in my opinion, unknown to most users. Methods, techniques and services described in the practical part were tested as much as permitted by law. There are certainly many unpublished ways how to abuse the banking systems to obtain money illegally. However, they are used locally and by small numbers of perpetrators. It is therefore impossible to find anything about them. This Thesis may be used as a basis for other papers on this topic.

SEZNAM POUŽITÉ LITERATURY

[1] Z. CHVÁTAL, Dalibor. Čipová karta s domácí úpravou pro lepší bezpečnost. Měšec.cz [online]. 20. 2. 2008, -, [cit. 2011-04-15]. Dostupný z WWW: <http://www.mesec.cz/clanky/cipova-karta-s-domaci-upravou-pro-lepsi-bezpecnost/>.

[2] Platební karta. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 28. 3. 2011 [cit. 2011-04-15]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta>.

[3] Prevencepodvodu.cz [online]. 2009 [cit. 2011-04-19]. Dostupné z WWW: <http://www.prevencepodvodu.cz/obrana-a-prevence/platby-kartou.php>.

[4] RSA. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 2011 [cit. 2011-04-19]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/RSA>.

[5] MasterCard [online]. 2009, 2011 [cit. 2011-04-19]. Dostupné z WWW: <http://www.mastercard.com/cz/personal/cz/viceokartach/typy_karet_pouzita_technologie.html>.

[6] JUŘÍK, Pavel. Svět platebních a identifikačních karet. Praha 7 : Grada publishing, 1999. 248 s.

[7] Pandatron.cz [online]. 2008 [cit. 2011-04-27]. Pandatron. Dostupné z WWW: <http://pandatron.cz/?535&karty_s_magnetickym_pruhem>.

[8] Fast Centrik [online]. 2010 [cit. 2011-04-28]. Fast Centrik. Dostupné z WWW: <http://www.fastcentrik.cz/aktuality/nova-platebni-brana-payu-pro-e-shop-prijimejte-platby-na-internetu-snaz.aspx>.

[9] RFID Global [online]. 2008 [cit. 2011-04-28]. Rfid GLOBAL.org. Dostupné z WWW: <http://www.rfidglobal.org/Product/>.

[10] Sbk webside [online]. 2010 [cit. 2011-04-28]. Bankovnikarty.cz. Dostupné z WWW: <http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html>.

[11] WINCOR - NIXDORF [online]. 2007 [cit. 2009-04-14]. Dostupný z WWW:<http://www.wincornixdorf.com/internet/cae/servlet/contentblob/371430/publicationFile/51675/BrochureProCash2150xeEN.pdf>.

[12] Global Payments Europe : Nákup, úpravy a instalace ATM [online]. 2005 [cit.2009-04-16]. Dostupný z WWW: <http://www.globalpaymentsinc.com/europe/czech/products/atms/setup.html>.

[13] POSregister [online]. 2010 [cit. 2011-04-28]. POSregister. Dostupné z WWW: <http://www.posregister.com/credit-card-imprinters.html>.

[14] Visa.cz [online]. 2011 [cit. 2011-04-29]. VISA. Dostupné z WWW: <http://www.visa.cz/cz/osobni_karty/visa_paywave.aspx>.

[15] Sonet.cz [online]. 2011 [cit. 2011-04-29]. Sonet. Dostupné z WWW: <http://www.sonet.cz/sonet-pos-terminal-t4230.php>.

[16] Nxp [online]. 2011 [cit. 2011-05-02]. NXP. Dostupné z WWW: <http://www.nxp.com/#/pip/pip=[pfp=71599]|pp=[t=pfp,i=71599]>.

[17] Alsoft [online]. 2010 [cit. 2011-05-03]. Alsoft. Dostupné z WWW: <http://www.alsoft.cz/products/Security/Vasco/Digipass-Products-Family>.

[18] Clever and smart [online]. 2010 [cit. 2011-05-03]. Clever and smart. Dostupné z WWW: <http://www.cleverandsmart.cz/pci-dss-konkretni-bezpecnostni-opatreni/>.

[19] Alibaba [online]. 2011 [cit. 2011-05-06]. Dostupné z WWW: <http://www.alibaba.com/showroom/card-card-skimmer.html>.

[20] České trezory [online]. 2010 [cit. 2011-05-06]. Dostupné z WWW: <http://www.jinova.cz/jak-funguje-bankomat>.

[21] Red Team [online]. 2008 [cit. 2011-05-08]. Dostupné z WWW: <http://blogs.23.nu/RedTeam/2008/08/antville-18652/>.

[22] PC Authority [online]. 2009 [cit. 2011-05-09]. Dostupné z WWW: <http://www.pcauthority.com.au/News/145706,credit-card-fraud-costs-australia-120m-but-there-are-ways-to-protect-yourself.aspx>.

[23] Lidové Noviny [online]. 2007 [cit. 2011-05-09]. Dostupné z WWW: <http://www.lidovky.cz/policie-zabavila-rumunum-mobilni-ctecku-platebnich-karet-poprve-v-historii-171-/ln_domov.asp?c=A091021_130739_ln_domov_ter>.

[24] Youtube [online]. 2010 [cit. 2011-05-09]. Dostupné z WWW: <http://www.youtube.com/watch?v=GjOduug-SC8&feature=player_embedded#at=142>.

[25] WebMoney [online]. http://www.wmtransfer.com [cit. 2011-05-10]. Dostupné z WWW: <http://www.wmtransfer.com>.

[26] Liberty Reserve [online]. 2011 [cit. 2011-05-10]. Dostupné z WWW: <http://www.libertyreserve.com/>.

[27] Liberty reserve exchange service [online]. 2011 [cit. 2011-05-11]. Dostupné z WWW: <http://www.lrexchange.com/exchangers/auexchanges>.

[28] Secure Pay [online]. 2011 [cit. 2011-05-15]. Dostupné z WWW: <http://citace.com/generator.php?druh=7&ukol=1>.

[29] TG Daily [online]. 2011 [cit. 2011-05-18]. Dostupné z WWW: <http://www.tgdaily.com/mobility-brief/55517-angry-birds-try-to-make-nfc-cool>.

[30] Mesec.cz [online]. 2011 [cit. 2011-05-17]. Dostupné z WWW: <http://www.mesec.cz/clanky/novinky-v-platebnich-kartach-v-roce-2011/>.

[31] HRUŠKOVÁ, Monika. IDnes [online]. 2010 [cit. 2011-05-21]. Dostupné z WWW: <http://finance.idnes.cz/limity-pro-vyber-na-platebnich-kartach-obtezuji-za-zmenu-vetsinou-zaplatite-1wc-/bank.asp?c=A100518_152930_bank_hru>.

[32] Google [online]. 2010 [cit. 2011-05-22]. Dostupné z WWW: <http://images.google.com/search?tbm=isch&client=safari&rls=cs-cz&hl=cs&source=hp&biw=1228&bih=574&q=chip+card+reader&gbv=2&aq=f&aqi=&aql=&oq=>.

[33] Penize [online]. 2007 [cit. 2011-05-24]. Dostupné z WWW: <http://www.penize.cz/platebni-karty/18777-jak-dosly-platebni-karty-do-ceskych-zemi-aneb-historie-karet-plna-zajimavosti>.

[34] Google [online]. 2011 [cit. 2011-05-24]. Dostupné z WWW: <http://images.google.com/search?tbm=isch&client=safari&rls=cs-cz&hl=cs&source=hp&biw=1228&bih=574&q=visa+card&gbv=2&aq=

f&aqi=g2&aql=&oq=>.

[35] Rfid-shield [online]. 2009 [cit. 2011-05-24]. Dostupné z WWW: <http://www.rfid-shield.com/info_isrfid.php>.

[36] Account Market [online]. 2011 [cit. 2011-05-24]. Dostupné z WWW: <http://www.accountmarket.com/forums/showthread.php?p=15027>.

[37] TUREK, Rastislav. Vimeo [online]. 2010 [cit. 2011-05-24]. Dostupné z WWW: <http://vimeo.com/8869477>.

[38] Libreria Ancora [online]. 2010 [cit. 2011-05-24]. Dostupné z WWW: <http://www.ancoraitalia.it/annuario_pontificio_2010.html>.

[39] MÁČ, Miroslav. Platební styk : klasický a elektronický. Praha : Grada, 2006. 220 s. ISBN 80-247-1725-5.

[40] JUŘÍK, Pavel. Platební karty 1870-2006 : velká encyklopedie. Praha : Grada, 2006. 296 s. Dostupné z WWW: http://books.google.cz/books?id=uQ9Vd-fGEx8C&printsec=frontcover#v=onepage&q&f=false.

[41] ZÁMEČNÍK, Petr. Internetové bankovnictví. Kde je bezpečné?. 2008, 5, s. 4. Dostupný také z WWW:http://earchiv.chip.cz/cs/earchiv/vydani/r-2008/internetove-bankovnictvi-kde-je-bezpecne.html

[42] MERVART, Dominik. Systém pro správu bankovních účtu. Praha, 2009. 79 s. Bakalářská práce. České vysoké učení technické v Praze

[43] SHARAD JOSHI, Mayur. Black Cards Forensics : Classification of ATM and credit card fraud schemes. India : Indiaforensic research foundtation, 2006. 94 s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Rozhraní pro programování (Application Programming Interface)
ATM	Bankomat (Automated Teller Machine)
BIN	Identifikační číslo banky (Bank Identification number)
BYR	Měna - běloruský rubl
CID	Mezidoménové směrování bez tříd
CPU	Procesor (Central Processing Unit)
CVC	Kód pro bezkontaktní platby (Card Verification Code)
CVK	Bezpečnostní kód banky (Card verification Key)
CVV	Kód pro bezkontaktní platby (Card Verification Value)
CID	Kód pro bezkontaktní platby (Card Identification Digit)
DOB	Datum narození (Date of Birth)
EEPROM	Elektronicky vymazatelná PROM paměť(Electrically Erasable PROM)
EMV	Standard čipové technologie (Europay, MasterCard, Visa)
EU	Evropská Unie
EUR	Měna některých států Evropské unie (EURO)
G&SR	Název solečnosti (Gold and Silver Reverse)
GPRS	Mobilní internet (General Packet Radio System)
GSM	Globální systém pro mobilní komunikace (Global System for Mobile communications)
HTTP	Hypertextový přenosový protokol (HyperText Transfer Protocol)
HTTPS	Zabezpečený hypertextový přenosový protokol (HTTP - Secure)
IB	Internetové bankovnictví (Internet banking)
IC3	Společnosi zabývající se internetovou kriminalitou (Internet Crime Complain Center)
ICQ	Volně dostipný komunikační program (I Seek You)

ID	Identifikační číslo (Identification Digit)
IDS/IPS	Systém detekce útoku (Intrusion Detection System, Intelligent Power Switch)
IIN	Identifikační číslo klienta banky (Issue Identification number)
IP	Standardní síťový(internetový) protokol(Internet Protocol)
IRC	Komunikační metoda prostřednictvím internetu (Internet Relay Chat)
LCD	Zobrazovací zařízení (Liquid Crystal Display)
LR	Finanční společnost (Liberty Reverse)
NFC	Technologie bezdrátové komunikace (Near Field Comunication)
OS	Operařní systém
PC	Osobní Počitač (Personal Computer)
PCI	Společnost zabývající se standardizací (The Payment Card Industry)
PCIDSS	Společnost zabývající se standardizací (The Payment Card Industry data security standard)
PDA	Kapesní počítač (Personal Digital Assistent)
PIN	Čtyřmístný bezpečnostní kód (Personal Identification Number)
POS	Platební terminál (Point Of Sale)
PVC	Chemická sloučenina (Poly Vinyl Chlorid)
RAM	Operační paměť (Random Acces Memory)
RFID	Technologie bezdrátové komunikace (Radio Frequency Identification)
ROM	Paměť pouze pro řtení (Read Only Memory)
RSA	Kryptografická metoda (Rivest, Shamir, Adleman)
RUR	Ruská měna (Ruský Rubl)
SILC	Metoda internetové komunikace (Secure Internet Live Conferencing)
SIM	Čip používaný v mobilních telefonech (Subscriber information Module)

SMS	Krátké textové zprávy (Short Message Service)
SSN	Osobní identifikační číslo občanů USA(Social Security Number)
SSH	Zabezpečený protokol v počítačových sítích (Security Shell)
SSL	Bezpečnostní vrstva v počítačových sítích (Secure Socket Layer)
SW	Programové vybavení (Soft Ware)
TCP/IP	Řídíci přenosový/internetový protokol (Transmission Control Protocol / Internet Protocol)
TFT	Označení dotekového displeje (Thin Film Tranzistor)
TLS	Bezpečnostní transportní vrstvy (Transport Layer Security)
UAH	Měna - ukrajinská hřivna
USA	Spojené Státy Americké (United States of America)
USB	Sběrnicová norma (Universal Serial Bus)
USD	Měna - americký dolar
UTP	Typ kabeláže pro počítačové sítě (Unshielded Twisted Pair)
UV	Ultrafialové záření (Ultra Violet)
UZS	Měna - uzbecký sum
VPN	Virtuální soukromá síť (Virtual private network)
WEP	Zastaralé zabezpečení počítačové sítě (Wired Equivalent Privacy)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK