Bezpečnosť platobných kariet

Bc. Tomáš Belianský

Diplomová práca
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš Belianský**
Osobní číslo:	**A14561**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnost platebních karet**
Téma anglicky:	**Credit Card Security**

Zásady pro vypracování:

1. **Proveďte literární rešerši tématu bezpečnostních prvků a zabezpečení platebních karet.**
2. **Analyzujte způsoby použití platebních karet v obchodním styku a definujte rizika.**
3. **Definujte možnosti a způsoby zneužití platebních karet včetně identifikace uživatele.**
4. **Identifikujte slabá místa v systému bezpečnosti.**
5. **Vyhodnoťte návrhy řešení bezpečnosti platebních karet a další možnosti vývoje.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PŘÁDKA, Michal; KALA, Jan. Elektronické bankovnictví : rady a tipy. 1.vyd. Praha : Computer Press, a.s., 2000. 166 s. ISBN 80-722-6328-5.**
2. **MÁČE, Miroslav. Platební styk: klasický a elektronický. 1. vyd. Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.**
3. **JUŘÍK, Pavel. Platební karty: 1870-2006 : velká encyklopedie. 1. vyd. Praha: Grada, 2006, 296 s. ISBN 80-247-1381-0.**
4. **NEHYBOVÁ, Marta. Bankovní služby nejen pro podnikatele: 1870-2006 : velká encyklopedie. . Brno: Miroslav Nehyba, 1999, 140 s. ISBN 80-902-6454-9.**
5. **PŘÁDKA, Michal a Jan KALA. Elektronické bankovnictví: rady a tipy. Vyd. 1. Praha: Computer Press, 2000, xii, 166 s. Praxe manažera. ISBN 80-722-6328-5.**
6. **JUŘÍK, Pavel a Jan KALA. Platební karty: ilustrovaná historie placení. 1. vyd. Praha: Libri, 2000, xii, 166 s. Praxe manažera. ISBN 9788072774982.**
7. **JAMES, Lance. Phishing bez záhad. 1. vyd. Praha: Grada, 2007. 281 s. ISBN 978-80-247-1766-1.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne 13.05.2016

.....
podpis diplomanta

ABSTRAKT

Práca sa zaoberá bezpečnosťou platobných kariet a rizikami spojenými s ich používaním. Cieľom tejto práce je zameranie na analýzu možností zneužitia platobných kariet a spôsoby ich ochrany. Najprv sú analyzované použité technológie, ktoré sú do dnes spájané s platobnými kartami a ich používaním a bezpečnosťou. Sú rozobrané ich slabiny a spôsoby útokov, ktorých cieľom je získať údaje o karte a následne krádež finančných prostriedkov. Následne je detailne spracované porovnanie vybraných útokov s cieľom krádeže finančných prostriedkov vo vybraných svetových oblastiach. Na túto analýzu potom nadväzujú návrhy odporúčaní a opatrení s cieľom minimalizovať dopad alebo pravdepodobnosť zneužitia platobných kariet.

Kľúčové slova: platobné karty, útoky, zneužitie, ochrana proti zneužitiu, analýza, štatistiky

ABSTRACT

The work deals with the security of payment cards and the risks associated with their use. The aim of this work is focused on analyzing the possibilities of misuse of payment cards and methods for their protection. First analyzed the technology used in today that are associated with payment cards and their use and safety. There are analyzed their weaknesses and methods of attack, designed to obtain data on the card and then the theft of funds. It is then processed in detail comparison of selected attacks in order theft of funds in selected regions of the world. For this analysis, then follow the recommendations and proposals of measures to minimize the impact or the likelihood of misuse of payment cards.

Keywords: payment cards, attacks, abuse, protection against abuse, analysis, statistics

Ďakujem vedúcemu práce doc. Mgr. Romanovi Jaškovi, Ph.D. za odborné vedenie, cenné rady a pripomienky počas spracovania práce.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Používanie platobných kariet je súčasťou bežného života v 21. storočí aj v rozvojových krajinách. Tento prostriedok umožňuje ľuďom nakupovať tovar alebo služby a využívať tieto výhody bez nutnosti disponovania hotovostnými finančnými prostriedkami. Veľa ľudí si už bez platobných kariet nedokáže predstaviť svoj každodenný režim, čo je už v modernej ľudskej spoločnosti prirodzené. S neustálym rozvojom internetu si ľudia rozšírili možnosti nákupov a objednávok z pohodlia domova alebo aj z práce, pričom využívajú k platbe cez Internet bezhotovostné platobné prostriedky.

Táto práca popisuje základné teoretické znalosti v oblasti bezhotovostných platieb, transakcií rôznymi typmi platobných kariet, či už s kontaktom alebo bez kontaktu s platobným prostriedkom. Niektorí ľudia nepoznajú základné druhy platobných kariet, rozdiely medzi nimi, ich bezpečnostné prvky a neuvedomujú si potencionálne riziká, ktoré používaním platobných kariet vzniká. Pri rozdelení druhov a spôsobov platieb sú popisované jednotlivé procesy a miery bezpečnosti pri daných procesoch platieb.

Práca má viacero vylepšení pre bezpečnosť. Ku zníženiu miery rizika bezpečnosti používania platobných kariet boli navrhnuté opatrenia ku zvýšeniu bezpečnosti používania platobných kariet. Ak bankové subjekty alebo finančné spoločnosti vydávajúce platobné karty z akceptovateľných dôvodov neposkytli požadovanú súčinnosť, táto práca môže prispieť k tomu, aby podľa miery zisteného rizika prijali opatrenia k ochrane držiteľa alebo vlastníkov kariet. Práca má význam pre samotných držiteľov platobných kariet, aby si uvedomili reálnosť nebezpečenstva pri ich použití. Dodržiavaním odporučených zásad vydavateľov kariet totiž môžu výrazne prispieť k zvýšeniu bezpečnosti používania platobných kariet. Taktiež držiteľ karty môže znížiť riziko zneužitia svojej karty na základe vyhodnotení a odporúčaní v tejto práci.

Použité technológie platobných kariet do istej miery eliminujú riziko zneužití. Karty sú stále zraniteľné pre rôzne typy útokov individuálne. Avšak je možné sa proti útokom brániť, poprípade znížiť dopad už vykonaného zneužitia. Vzhľadom k tomu, že sú platobné karty napojené na bežné účty klienta je hrozba straty finančných prostriedkov vysoká s veľkým dopadom. Z toho dôvodu netreba podceňovať bezpečnosť a riziká minimalizovať.

Táto práca je rozdelená na teoretickú a praktickú časť. Teoretická časť objasňuje vznik, vývoj a históriu platobných kariet. Taktiež aj vznik asociácií, ktoré do dnes držia popredné

priečky pri návrhoch bezpečnostných technológií v tomto smere. Ďalej teoretická časť popisuje druhy kariet podľa použitia, technológie a účelom.

Záverom teoretickej časti je definovanie najčastejších spôsobov útokov na platobné karty. Tieto útoky sú detailne analyzované z pohľadu pravdepodobnosti zneužitia, zraniteľnosti a úrovni možného prevedenia konkrétneho útoku.

Druhá praktická časť tejto práce je porovnanie štatistík vybraných oblastí sveta na vybrané typy útokov a ich individuálne vyhodnotenie pre každú oblasť a následné porovnanie a dopad na tieto oblasti ako celok.

Porovnanie štatistík útokov na platobné karty vo vybraných svetových oblastiach odpovedá, ktorý útok je najčastejší, ako sa líšia útoky vzhľadom na oblasť. Aká technológia je použitá a to spôsobuje zvýšenie alebo zníženie miery útokov. Vyhodnotenie týchto štatistík v praktickej časti sa zaoberá touto problematikou.

Cieľom doporučení v závere praktickej časti nie je nahradenie bežných pravidiel odporúčaných bankovými sektormi a finančnými inštitúciami. Priamym zámerom týchto odporúčaní je navrhnúť doplňujúce možnosti ochrany a konkrétne riešenia. Cieľom tejto práce nie je zameriavať sa na útoky a možnosti ich obchádzania ani kriminalitou a zločinnosťou spájanou s platobnými kartami. Ale naopak cieľom je analyzovať a detailne rozobrať spôsoby útokov proti platobnej karte bez súhlasu držiteľa karty. Navrhnúť odporúčania pre maximálne eliminovanie rizík zneužitia a ako sa proti týmto útokom najlepšie brániť.

I. TEORETICKÁ ČÁST

1 PLATOBNÉ KARTY

Platobné karty umožňujú takzvanú bezhotovostnú platbu alebo jednoduchý a rýchlejší prístup k požadovanej hotovosti pomocou bankomatov. Ďalšie možnosti ich použitia môžu byť rôzne funkcie jednotlivých služieb, ktoré sa líšia vždy od závislosti na banke, ktorá kartu vystavila. Platobné karty boli v minulosti vyrábané z papiera, avšak z dôvodu jednoduchého falšovania sa v dnešnej dobe vyrábajú len v plastovej podobe, ktorá zabezpečuje ako dlhšiu životnosť, tak aj umiestnenie bezpečnostných prvkov. Veľkosť a rozmery karty sú dané medzinárodnou normou ISO 3554, rozmery sú 85,6 x 54 mm. Držiteľom karty môže byť ako fyzická, tak aj právnická osoba, ktorá na žiadosť dala súhlas k vystaveniu a používaniu platobnej karty. Každý držiteľ má pridelené identifikačné číslo karty, ktoré je zhodné s číslom účtu karty, ktoré je vytvorené taktiež bankou, ktorá kartu vydala. Každá z vydaných kariet je vybavená identifikačnými údajmi držiteľa, pričom ochrana daných údajov pred prípadným zneužitím zaisťujú bezpečnostné prvky platobnej karty. V terajšej dobe je platobná karta akceptovaná u väčšiny predajcov, kamenných či internetových obchodov. Platobné procesy sú tak rýchlejšie, presné a bezpečné. Takáto karta je hlavne symbolom dostupnosti, keďže je možné ju mať vždy u seba a k dispozícii. Jedna z nevýhod môže byť nastavený kreditný limit, ktorý určuje najvyšší možný limit (za deň), tento limit si určuje držiteľ platobnej karty sám cez internet banking alebo po dohodnutí s vydávajúcou bankou buď na vlastnom uvážení alebo na základe napríklad platobnej histórie. Niektoré platobné karty ponúkajú aj rôzne benefity na základe používania práve bezhotovostných platieb použitím karty. [1]

Princíp bezhotovostného platobného styku

Bezhotovostný platobný styk je platba medzi dvoma subjektami, pri ktorých sa nepoužíva hotovosť. Jedná sa o platbu priamo z bankového účtu na iný bankový účet. V dnešnej dobe sú bankami umožňované aj platby v inej mene, ktorá je automaticky prevádzaná v aktuálnej hodnote podľa ich vlastného kurzovného lístku. [2]

1.1 História platobných kariet

- 1914 – Americká telefónna a telegrafná spoločnosť Western Union Telegraph Company vyrobila prvú platobnú kartu na svete, vďaka ktorej sa dala uhradiť platba alebo využiť bankový úver. Materiálom bol plech.

- 1924 – General Petroleum Corporation of California (dnes Mobil Oil) vyšli na trh s kreditnou kartou umožňujúcou bezhotovostnej platby za čerpanie pohonných hmôt a potom ďalších služieb tejto spoločnosti v USA.
- 1929 – začala výroba veľkého množstva platobných kariet na základe vysokého konkurenčného boja na trhu. Avšak kvôli hospodárskej kríze bolo toto vydávanie najmä vernostných platobných kariet pozastavené.
- 1938 – Americká spoločnosť AT&T zaviedla pre svojich zákazníkov karty s názvom Bell Systém Credit Card .
- 1950 – Diners Club International prichádza s prvými univerzálnymi platobnými kartami.
- 1951 – Diners Club platobné karty sa ako prvé na svete stávajú medzinárodnými. Banka The Franklin National ako prvá prichádza s kreditnými kartami.
- 1958 – American Express ako ďalšia americká finančná spoločnosť a cestovná kancelária vydáva platobné karty. Ďalej taktiež americká spoločnosť Bank of America vydáva platobné karty Bank Americard, ktoré slúžia ako rodinné kreditné karty.
- 1965 – Ďalšie štyri americké banky v Chicagu vydávajú vlastné platobné karty a zakladajú Midwest Bank Card Association.
- 1966 – Sedemnásť ďalších amerických bank zakladá California Bank Card Association a prichádzajú s vlastnou licenciou k vydaniu platobnej karty držiteľovi.
- 1968 – V Kalifornii zakladajú ďalšie štyri banky Western States Bancard Association (WSBA) a vlastný názov pre platobné karty a to Master Charge. Historicky

  prvá možnosť urobiť platbu vďaka platobnej karty v Československu. Akceptuje ich Diners Club v spolupráci s cestovnou kanceláriou Čedok. Následne spoločnosť Čedok dalej spolupracuje aj s kartami Bank Americard, JCB, American Express a Master Charge.
- 1980 – Je predstavený jeden zo sponzorov olympijských hier v Moskve, pri tejto príležitosti vydáva práve VISA prvé platobné karty v krajinách Sovietskeho zväzu.

- 1988 – KHB maďarská banka zaoberajúca sa zahraničným obchodom vydáva platobné karty s názvom VISA Classic.
- Československo, presne Živnostenská banka vydáva prvé platobné karty pre československých občanov. Karta bola ako dispozičná pre účty spoločnosti Tuzex, bolo možné vyberať poukazy v bankách ako SBČS alebo ČSOB.
- 1990 – American Express oficiálne otvára prvú českú pobočku v Prahe.

  Česká Živnostenská banka v tomto roku začína vydávať karty VISA Classic.
- 1991 – V Českej republike vzniklo Medzinárodné združenie pre platobné karty MSPK. Členovia združenia sú, Poštová banka, Investičná banka, Komerčná banka, Agrobanka Praha, Tatra banka, Všeobecná úverová banka a I.S.C. MUZO. Tieto karty sú známe aj v dnešnej dobe.

  Vybudovali v tomto období jednotný bankový kartový systém pre platenie, prvotne pre Cirus, Eurocard a MasterCard, neskôr aj pre karty VISA.

  Česká Živnostenská banka v tomto roku zároveň vydáva karty VISA Business.
- 1992 - Česká Živnostenská banka začala preberať príjem kariet Diners Club a JCB od spoločnosti Čedok, ktorá v tomto období zároveň ukončila svoju činnosť.
- 1998 – Diners Club začalo po prvý raz v Českej republike ponúkať charge karty. Zároveň zahájila Česká a Slovenská sporiteľňa ponuky kreditných kariet svojim verným klientom.
- 2000 – Bank Austria Creditanstalt (HBV Bank) začína vydávať kreditní kartu Maxim.
- 2001 – Väčšie zastúpenie kreditných a charge kariet v České a Slovenskej republike.
- 2005 – Všetky elektronické karty od tohto roku začínajú používať výhradne čipovú technológiu. [1, 2]

1.2 Vývoj platobných kariet

V Českej a Slovenskej republike príde k najväčšiemu rozšíreniu a vývoji platobných kariet aj samozrejme celého používaného systému po roku 1991, bolo dňa 4. februára založené Medzinárodné združenie pre platobné karty a na ich základoch a princípoch vytvorený

jednotný kartový systém pre banky v našej krajine. Tento projekt následne dostala pod správu spoločnosť I. S. C. MUZO, ktorá mala ako primárnu úlohu vybudovať modernejší a prepracovanejší systém bánk, ktorý sa mal sústrediť na spracovanie databázy platobných kariet, autorizácie pri výberoch z bankomatu a transakciách v obchodoch. Bol kladený dôraz na vytváranie a rozdeľovanie PIN kódov. Úlohou tejto spoločnosti bolo taktiež aj vybrať vhodných dodávateľov, ktorí by okrem samotného dodania zároveň aj spravovali platobné terminály a bankomaty. [3]

Princíp používania kariet mal byť v prvom rade, čo najjednoduchší, pričom sa tento spôsob zachoval až do súčasnosti. Pôvodne stačilo len kartu predložiť poverenej osobe, ktorá následne overila totožnosť držiteľa karty a jeho podpis podľa podpisového vzoru uvedeného na karte. Prvé platobné karty boli vyrábané z kovu a mali určitú podobnosť s vojenskými identifikačnými štítkami. Kov bol neskôr nahradený papierom. Avšak oba materiály sa osvedčili ako nevyhovujúce a ľahko falšovateľné, keďže neumožňovali umiestnenie dostatočne účinných bezpečnostných prvkov. V súčasnosti sú karty vyrábané len v plastovom prevedení. [3]

1.3 Rozdelenie platobných kariet

Banky nám v súčasnosti ponúkajú veľký výber platobných kariet a s nimi taktiež rôzne možnosti ich využitia. Medzi najpoužívanejšie platobné karty patria napríklad kreditné debetné a charge. Novinkou na trhu sú v rámci platobných kariet aj elektronické peňaženky. [4]

Každá karta musí obsahovať nasledujúce prvky:

- označenie vydavateľa,
- meno držiteľa, poprípade identifikácia držiteľa (napr. rodné číslo, podpis),
- číslo karty
- platnosť
- záznam dát (magnetický pásik, mikročip, optický alebo iný špeciálny záznam alebo identifikátor). [4]

Platobné karty je možné rozdeliť podľa niekoľkých kritérií.

Platobné karty				
Podľa spôsobu zaúčtovania	Podľa spôsobu prevedenia	Podľa vydavateľskej asociácie	Podľa použiteľnosti	Podľa použitej technológie
Debetné	Elektronické	MasterCard	Domáce (tuzemské)	Magnetický prúžok
Kreditné	Embossované	VISA	Medzinárodné	Čip
Charge	-	JCB	-	Embossing
Vopred nabité	-	AMEX	-	Bezkontaktné
Nákupné, úverové	-	Diners Club	-	Hybridné

Tab. 1. Rozdelenia platobných kariet [4]

1.3.1 Kreditné karty

Kreditné karty umožňujú svojmu majiteľovi čerpať tzv. revolvingový úver. Ide o princíp kupovania na úver, ktorý držiteľ následne spláca, z tohto dôvodu je vopred posudzovaná bonita a schopnosť klienta úver splácať.

Kreditná karta umožňuje čerpať úver do výšky čiastky, ktorá je vopred stanovená pri vydaní karty. Pre daný úver je taktiež stanovená doba splácania, do ktorej musí byť splatená celá čiastka alebo jej stanovená časť. Ak je v tejto lehote celý úver alebo požadovaná časť splatená, je po majiteľovi karty požadovaný nulový úrok z úveru. Tento princíp je známy aj u dohodnutého prečerpania pri bežnom bankovom účte do mínusových položiek. V prípade, ak nastane situácia, že klient danú lehotu prekročí, bude po ňom požadovaný vopred dohodnutý úrok, ktorý bežne presahuje štandardné úrokové miery.

V Slovenskej i Českej republike je bezúročné obdobie štandardne pre väčšinu kreditných kariet 55 kalendárnych dní. Po prekročení tohto obdobia sa úroková sadzba pohybuje v rozmedzí od 18,99% do 23,99% p.a. [4]

Charge karty

Charge karty (charge cards) na rozdiel od kreditných kariet vyžadujú splatiť celý úver do určitého časového obdobia, nie je povolené splatenie len určitej časti. Zároveň nie je obmedzený limit, ktorého môže držiteľ s kartou dosiahnuť. Tento druh karty je určený predovšetkým pre veľmi bonitných klientov, než sú užívatelia kreditných kariet. Cieľovou kategóriou týchto kariet sú majetní ľudia s ochotou utrácať na dlh, avšak zároveň natoľko zodpovední aby svoje záväzky včas splatili v plnej výške. Na základe používania charge kariet a objemu použitých platobných prostriedkov sú pre klientov dostupné zľavy a vernostné programy. [4]

1.3.2 Debetné karty

Debetne karty (debit cards) sú karty, ktoré priamo súvisia s finančnými prostriedkami uloženými na bežnom bankovom účte. Po transakcii urobenej kartou (platba v obchode, vyber z bankomatu) dôjde k odčítaniu danej čiastky z účtu. U elektronických kariet sa transakcie bežne zaúčtujú maximálne do týždňa. Čo sa týka embosovaných kariet je možné zaúčtova-nie aj neskôr. Ak je u bežného účtu zriadený tzv. kontokorent alebo dohodnuté prečerpanie, môže prísť k povolenému prečerpaniu účtu k zápornému zostatku. Debetné karty tvoria najväčší používaných kariet na Slovensku. [4]

1.3.3 Prednabité karty

Prednabité karty sú v používaní vo veľkom množstve rôznych variant, avšak princíp vždy ostáva rovnaký. Ide o kartu, ktorá nie je napojená na klientov účet ale je v nej nabitá konkrétna čiastka, ktorú môže držiteľ uplatňovať v závislosti na type karty. Takéto karty sú väčšinou vydávané konkrétnymi spoločnosťami, ako môžu byť napr. obchodné reťazce alebo benzínové pumpy a následne je možné ich použiť len v konkrétnom reťazci. Avšak môže sa jednať aj o nezávislé karty, ktoré môžu byť vydané napr. s spolupráci s VISA, tieto karty je potom možné použiť ako klasickú debetnú kartu len do výšky vopred dobitej sumy.

Prednabité karty na jedno použitie

Vopred nabité karty na jedno použitie sú zväčša obmedzené na platbu v konkrétnom obchode a sú častokrát označované ako voucher alebo poukaz na nákup v určitej hodnote.

Po vyčerpaní nabitej sumy v karte, už konkrétnu kartu nie je možné ďalej použiť. [4]

Prednabité karty na viac použití

Prednabité karty na viacero použití sú väčšinou vydané v spolupráci s kartovou asociáciou ako môže byť napr. VISA, tieto karty taktiež nesú aj logo tejto spoločnosti. Škála využitia týchto kariet je v rovnakej miere, ako pri debetných kartách. Je možné ich použiť kdekoľvek, kde je možnosť platiť debetnou kartou, taktiež ako aj pri výbere hotovosti a iných službách bankomatu. Jediný rozdiel je ten, že karta nie je napojená na bežný bankový účet ale je možné disponovať len s peňažnými prostriedkami, ktoré na kartu boli uložené. V prípade vyčerpania prostriedkov na karte je nutné individuálne znovu dobitie karty. Pre dobitie jestvuje viacero spôsobov nabitia. Môžu to byť prevody z účtov, presun peňažných prostriedkov pomocou debetnej karty alebo je možnosť aj cez spoplatnenú SMS v určitej sume. Všetky transakcie spájané s týmto typom karty sú spoplatnené vyššími poplatkami ako u bežných transakciách.

Výhodou predplatenej karty je predovšetkým ochrana bežného účtu klienta pri možnom zneužití a dostupnosť aj pre klientov, ktorý nemajú bežný účet v banke. [4]

1.4 Technológie platobných kariet

Pri historicky dlhom vývoji platobných kariet sa dostalo k používaniu veľa technológii. Keďže sa v súčasnej dobe jedná o celosvetové používanie platobných kariet, preto karty podliehajú viacero štandardizáciám, ktoré zabezpečujú ich transparentnosť, prenositeľnosť a použiteľnosť kdekoľvek na svete. Použité technológie väčšinou kombinujú viacero rôzne určených zameraní. Jedná sa o kombináciu zjednodušovania transakcií a zabezpečenia karty. Platobné karty podliehajú štandardu ISO/IEC 7810 ID-1, ktorý určuje ich fyzické vlastnosti. Štandard ID-1 stanovuje rozmery karty 85,6 x 53,98 mm s hrúbkou 0,76mm a zaoblenie rohov. Tento štandard taktiež stanovuje ďalšie požiadavky na horľavosť, odolnosť voči chemikáliám ohybnosť a ďalším podobným vlastnostiam. Norma ISO/IEC 7812 určuje spôsob popisu kariet. Definuje číslovanie a font písma, ktoré sa používajú. ISO/IEC 7811 a 7813 definuje požiadavky pre magnetický prúžok a embossing. ISO/IEC 8583 a 4909 určuje spôsoby ukladania informácií a komunikácie s magnetickým prúžkom pre účely finančných transakcií. ISO/IEC 7816 určuje konkrétne požiadavky pre kontaktné čipové karty. ISO/IEC 14443 určuje naopak požiadavky na bezkontaktné čipové karty. Vďaka týmto štandardizáciám môže byť viacero kariet od rôznych vydavateľov použitých v jedom termináli a je to veľkou výhodou ako pre obchodníka (nemusí zabezpečiť

viac terminálov), tak aj pre držiteľa karty, keďže ma väčšie množstvo miest, kde môže kartu použiť.

Väčšina platobných kariet na svete, no najmä v Európe podlieha a zodpovedá štandardu EMV. Jedná sa o platobné karty s čipovou technológiou.

Nasledujúci obrázok a vysvetlenie dolu popisuje jednotlivé body od 1 do 11, každý bod označuje miesto a použitú technológiu platobnej karty a význam jednotlivých technologických prvkov je dolu pod obrázkom.

Obr. 1. Platobná karty s označením jednotlivých prvkov

1. Logo banky
2. EMV čip
3. Číslo karty (prvé číslo je zároveň identifikátor sektoru karty, prvých 6 čísel identifikuje vydavateľa karty, ďalšie čísla sú identifikátorom držiteľa.
4. Dátum platnosti vydanej karty, dátum určuje kedy sa končí platnosť karty.
5. Meno držiteľa karty
6. Logo vydávajúcej kartovej asociácie
7. Symbol, ktorý označuje kartu s bezkontaktnou technológiou.
8. Bezpečnostný hologram slúžiaci k ochrane karty proti falšovaniu a manuálnej prehliadke a overeniu pravosti.
9. Podpis držiteľa karty, slúži k overeniu pravosti podľa podpisového vzoru.
10. CVV2 kód, ktorý slúži ako potvrdenie pri transakciách, pri ktorých nie je potreba fyzickej prítomnosti karty. Používa sa pri internetových platbách.
11. Magnetický prúžok

1.4.1 Magnetický prúžok

Táto technológia ukladania dát na špeciálny kovový prúžok pomocou magnetizmu je známa už od dôb druhej svetovej vojny. Práve do spojenia s platobnými kartami sa magnetický prúžok dostal vďaka spoločnosti IBM, ktorej vývojári ako prví prišli s plastovou platobnou kartou opatrenou magnetickým prúžkom, ktorý mal mať uložené dáta o karte. [5]

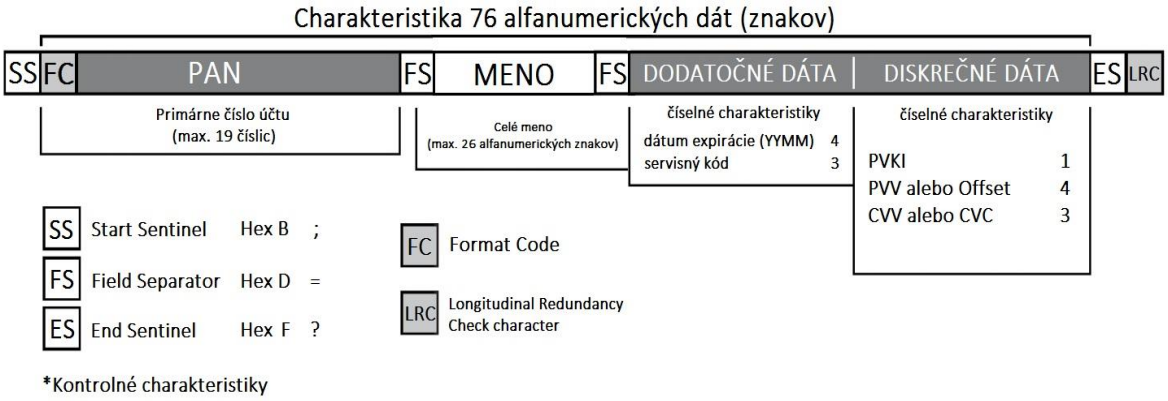
Magnetický prúžok ako taký umožňuje rýchlu komunikáciu s platobným terminálom alebo bankomatom, ktorý je vybavený čítačkou magnetického prúžku. Prechodom platobnej karty správnym smerom sa tak získajú všetky potrebné informácie pre prijatie alebo naopak zamietnutie transakcie. [5]

Vďaka vzájomnej dohode medzi kartovými asociáciami je možné pri platení pomocou terminálu alebo pri použití bankomatu použiť karty rôznych vydavateľov, keďže majú zhodný formát rozmery a sú navrhnuté podľa jedného štandardu ISO/IEC 7813, ktorý určuje fyzické charakteristiky platobnej karty, ako sú veľkosť, tvar, zaoblenie rohov, umiestnenie magnetického prúžku a ďalej aj štruktúru, v ktorej sú dáta na tomto prúžku uložené. [5]

Magnetický prúžok je navrhnutý tak, že sa skladá s troch stôp, pričom každá z nich nesie určité informácie. Prvá stopa ako jediná ukladá informáciu o mene držiteľa karty, zároveň celkovo obsahuje až 79 alfanumerických znakov. Druhá stopa na magnetickom prúžku nesie 40 numerických znakov. Tieto dve stopy spolu zaznamenávajú všetky potrebné dáta pre samotný prevod platby. Zaznamenávajú číslo účtu, meno držiteľa, dobu splatnosti karty, servisný kód, ktorý nesie konkrétne pokyny pre používanie karty napr. používanie za určitých okolností alebo či je alebo nie je vyžadované potvrdenie pomocou PIN kódu. Tretia stopa na magnetickom prúžku je jediná prepisovateľná stopa. Môžu na nej byť zapísané napr. informácie o poslednej transakcii, ktoré potom možno využiť pri urobení offline transakcie. Vo väčšine prípadov nie je táto tretia stopa využitá a u niektorých kartách ani nie je použitá. Potom sa jedná o takzvané platobné karty s tenkým prúžkom. [5]

Karty vybavené magnetickým prúžkom významne uľahčujú platenie pomocou karty, avšak v dnešnej dobe je táto technológia oveľa viac zraniteľná. Magnetický prúžok je možné ľahko prečítať a následné získať údaje, ktoré potom môžu byť zneužité pri platbách na internete alebo k samotnému vytvoreniu kópie karty, s ktorou potom podvodník môže platiť. Ako náhrada magnetického prúžku nastúpila technológia čipových kariet

so štandardom EMV. Tieto karty sú oveľa viac bezpečnejšie. Avšak aj skrz to sú karty naďalej vybavené magnetickým prúžkom, aby sa zachovalo dosiahnutie kompatibility aj v oblastiach, kde sa ešte úplne neprešlo na technológiu čipových kariet. [5]



Obr. 2. Charakteristika a formát dát na druhej stope magnetického prúžku [5]

- PAN - číslo účtu, ktoré identifikuje vydavateľa karty a taktiež samotnú kartu.
- Dátum expirácie (Expiration code) – určuje dátum platnosti karty, do kedy je karta platná a môže byť využívaná. Určuje len mesiac a rok, každý z týchto údajov priamo v dvojcifernom formáte.
- Servisný kód (Service code) – určuje príkazy ako sa s kartou bude zaobchádzať. Prvá číslica určuje, kde sa môže karta používať, či už národné alebo medzinárodné platby, ďalej komunikáciu s kartou, či je nutné použiť aj čip alebo nie.
  Druhý číslicový znak určuje požiadavku na online overenie u vydavateľa.
  Tretia číslica slúži na možnosti použitia karty, napr. k tovaru, službám, výberu hotovosti, použitie len pre bankomat a pod. alebo určí bez obmedzenia. Ďalej kladie požiadavky pri ktorých platbách treba zadať PIN kód a pri ktorých netreba.
- PVV a PVKI sú špeciálne kódy slúžiace pre overovanie PIN kódu.
- CVC alebo CVV sú špeciálne kódy veľmi podobné s CVV2/CVC2 kódmi. Ich úlohou je overiť, či je pri konkrétnej platbe skutočne použitá existujúca platobná karta. [5]

1.4.2 Čipové karty

Použitá čipová technológia v platobných kartách, taktiež známa ako smart cards je používaná v drvivej väčšine pri platbách pomocou terminálu alebo výberu v bankomate. Tieto karty sa nespoliehajú na magnetický prúžok ale komunikácia je smerovaná priamo

na integrovaný čip. Rovnako ako u všetkých technológií použitých pri platobných kartách, taktiež aj čip podlieha medzinárodnému štandardu, ktorý združuje akceptovanie kariet od rôznych vydavateľov. Čipové karty podliehajú štandardu EMV (Europay, MasterCard, Visa), ktorý je rovnako štandardizovaný normou ISO/IEC 7816 pre kontaktné karty, pre bezkontaktné karty je norma ISO/IEC 14443. [6]

Pre použitie čipovej karty je potreba terminál štandardu EMV, samotná komunikácia s terminálom je šifrovaná, tým zabraňuje jednoduchému načítaniu a záznamu informácií, ako je to možne u magnetického prúžku. Samotná šifrovaná komunikácia s terminálom pomocou integrovaného čipu používa šifrovacie algoritmy ako sú napr. SHA, 3-DES alebo RSA. [6]

Pre lepšie zabezpečenie čipových kariet je napr. nutnosť potvrdenia platby PIN kódom, ako overenie držiteľa karty. PIN kód v tomto prípade nahrádza staršie overovacie metódy ako podpis pokladničného bloku, manuálne overenie totožnosti držiteľa karty a pod. V niektorých krajinách, často z historických dôvodov je stále používaný variant Chip & Signature, kedy sa držiteľ karty verifikuje pomocou vlastnoručného podpisu. Avšak daný spôsob nie je natoľko bezpečný ako modernejšie použitie PIN kódu (tento spôsob je nazývaný Chip & PIN). Spôsob verifikácie pomocou PIN kódu je najrozšírenejší v Európe. Naopak spôsob verifikácie pomocou podpisu je rozšírený v Austrálii a USA. Naviac môže byť použitá aj kombinácia týchto spôsobov, čo zodpovedá overeniu čipovou technológiou, zadaním PIN kódu a vlastnoručným podpisom. [6]

EMV čipové karty sú v dnešnej dobe najbezpečnejším modelom platobnej karty. Ako veľká slabina týchto kariet je stále používaný magnetický prúžok, ktorý naďalej uchováva informácie potrebné k úspešnému prevodu transakcie a zároveň umožňuje spätnú kompatibilitu pri platobných systémoch, kde ešte nie je použitý EMV štandard. I keď nie je možné túto kartu zneužiť v EMV termináli bez poznania PIN kódu (na zadanie PIN kódu sú spravidla 3 pokusy), je možné túto kartu zneužiť veľmi jednoducho u predajcov, ktorý ešte EMV terminál nemajú alebo pri internetových platbách pomocou platobnej karty, ktoré vyžadujú okrem všetkých požadovaných údajov z karty ako hlavný bezpečnostný prvok zadanie kódu CVV2/CVC2. [6]

Toto je hlavný dôvod, prečo sa kartové asociácie snažia, čo najrýchlejšie rozšíriť používanie EMV terminály. K dočasnému riešeniu prišlo od roku 2005 v Európe, kedy sa všetka zodpovednosť za zneužitie karty prenáša na predajcu, ktorý ešte nedisponuje

EMV terminálom, aby prípadným zneužitiam zabránil. Vďaka týmto opatreniam sa rozšírenie EMV terminálov v Európe poznateľne urýchlilo. Kartové asociácie plánujú podobným spôsobom urýchliť túto bezpečnejšiu variantu aj do iných oblastí Sveta. Myšlienka a plánovanie využitia čipových kariet nie je zďaleka len na účel funkcií v oblasti platenia, transakcií, či výberov hotovosti. Pôvodne zamýšľaná funkcionalita je uchovávanie užívateľských dát, ako napr. biometrické údaje držiteľa a pod. Ďalej by táto myšlienka mala smerovať k jednej osobe a jednej používanej karte, daná karta by mala spájať všetky rôzne funkcionality kreditnej a debetnej karty, ako i elektronickú peňaženku aj rôzne kupóny pre zľavy atď. Na jednom fyzickom nosiči. V dnešnej dobe zatiaľ nie je využitý celkový potenciál čipových kariet ale je naplnená len jedna konkrétna funkcia. [6]

Čip

Čipom je označovaný integrovaný obvod vo veľmi malom prevedení, ktoré je určené pre spracovanie informácií alebo slúži ako pamäť. Skladá sa z nasledovných častí:

- Elektrické kontakty – definované normou ISO/IEC 7816-2.
- CPU (mikroprocesor) – 8 alebo 16 bitový procesor, využívajúci spravidla sadu Motorola 6805 alebo Intel 8051,
- Kryptografický koprocesor určený na zložité výpočty s kryptografickými operáciami.
- Pamäte typov RAM, ROM a EEPROM. [6]

Obr. 3. Uloženie a priradenie kontaktov na čipovej platobnej karte

Priradenie kontaktov:

C1-VCC (power supply) – napájací

C2-RST (reset signal) – reset

C3-CLK (clock signal) - hodiny

C5-GND (ground) – uzemnenie

C6-VPP (programy voltage input) [6]

Vznik EMV

V 90. rokoch začali vznikať prvé prototypy čipových kariet. Predpoklad zvýšenia úrovne bezpečnosti vďaka čipu a kombináciou s PIN kódom. Na skúšku sa zaviedlo 120 tisíc kusov čipových kariet podľa štandardu EMV. Vzhľadom na obrovský záujem a úspešnosť tejto série bola ako prvá krajina Veľká Británia, ktorá začala s výmenou všetkých platobných kariet na EMV čipové karty. Toto však vyžaduje taktiež, aby aj predávajúci, obchodník mal terminál s EMV technológiou. Vďaka tejto technológii sa len v Európe zabránilo veľkému množstvu podvodných transakcií. Pri tejto technológii je už práve priamo prenesená zodpovednosť na obchodníka. To znamená, že samotné odhalenie podvodnej činnosti s platobnou kartou je schopný odhaliť aj sám obchodník a zvážiť možné riziká. [7]

1.4.3 Bezkontaktné karty

Bezkontaktné platobné karty sú v dnešnej dobe veľmi obľúbené a moderné. Sú z väčšiny postavené na systéme PayPass od spoločnosti MasterCard, ktorá systém po prvýkrát otestovala a vyskúšala v roku 2003. Kompatibilita tejto technológie použitej v platobných kartách vychádza z normy OSP/IEC 14443. Tomuto štandardu odpovedá ako PayPass od MasterCard, tak aj PayWave od spoločnosti VISA. [8]

Platobné karty s bezkontaktnou technológiou sú z väčšiny prípadov postavené na štandarde EMV čipových kariet a taktiež sú aj kompatibilné s EMV platobnými terminálmi. Platba vykonaná bezkontaktne vyžaduje prítomnosť terminálu kompatibilného podľa normy ISO/IEC 14443, ktorý s kartou dokáže komunikovať. [8]

Bezkontaktná platobná karta okrem EMV čipu obsahuje taktiež integrovaný čip pre rádiovú komunikáciu a anténu. Čip zaisťuje zhodné funkcie ako bolo napísané v predchádzajúcej kapitole o čipových kartách. Pomocou dát uložených na čipe následne

komunikuje cez anténu s EMV terminálom. Bezkontaktné karty nie sú vybavené napájaním ani zdrojom energie, to znamená, že nekomunikujú aktívne a neobsahujú zdroj energie. Karty začnú komunikovať až na základe priblíženia do elektromagnetického alebo magnetického poľa, ktoré je natoľko silné aby tvorilo napájanie integrovaného čipu, preto je nutné priložiť kartu veľmi blízko platobnému terminálu. Maximálna možná vzdialenosť je štandardne uvádzaná ako 4 palce alebo približne 10 cm, zo skúsenosti je ale známe, že je vo väčšine nutnosťou kartu priložiť priamo na terminál. [8]

Samotné priblíženie karty, na čo najkratšiu vzdialenosť je navrhnuté hlavne preto, aby sa zabránilo nechcenému prečítaniu karty a taktiež zabezpečenie karty proti nevedomému prevodu a platbe, kedy by prišlo k jednoduchému priblíženiu mobilného terminálu a prečítaniu karty treťou osobou. [8]

Akceptovaná vzdialenosť medzi terminálom a platobnou kartou podlieha rôznym faktorom, ako napr. veľkosť antény alebo sila vysielania platobného terminálu. Daná bezkontaktná technológia kariet nie je úplne totožná s technológiou RFID tagov, avšak zdieľa zhodné základné princípy. Vďaka tomu je možné použiť bezkontaktnú kartu napríklad pomocou použitej antény, ak je daná karta aktivovaná na určitú funkciu, môže napr. otvoriť dvere vybavené bezpečnostným rámom. K tomu je možné využitie použitej technológie. [8]

Bezkontaktná technológia v platobných kartách pripomína skorej EMV čipové karty, avšak je používaný len iný komunikačný prvok.

Ako aj EMV karty, tak aj bezkontaktné karty majú spojenie s terminálom šifrované pomocou rôznych metód šifrovania, jedná sa napr. o šifru 3-DES. Taktiež ako EMV karty, tak aj bezkontaktné karty vyžadujú overenie totožnosti držiteľa pomocou PIN kódu, v dnešnej dobe je nutné toto overenie len pri platbách presahujúcich stanovený limit, spravidla to býva platba, ktorá je vyššia ako 20 eur. Platby v limite do tejto sumy nevyžadujú overenie PIN kódom. Toto opatrenie je v rámci bezpečnosti zneužitia a zároveň núti držiteľa mať kartu stále pri sebe a uchrániť ju pred zneužitím, taktiež aj proti prečítaniu magnetického prúžku. Aj skrz tieto opatrenia stále existujú dohady o zraniteľnosti karty, hlavne pre jednoduchú komunikáciu a nadviazanie komunikácie bez vedomia držiteľa. [8]

Obr. 4. Symbol bezkontaktnej technológie

1.4.4 E-Commerce

Platby na diaľku a ďalšie internetové platby sú oproti iným štandardným platbám špecifické a odlišné najmä tým, že pri realizáciách platby nie je potrebná samotná karta ale len informácie o nej. Z tohto dôvodu sa transakcie daného typu označujú ako CNP (Card Not Present). Toto označenie sa používa aj pri platbách cez telefón, ktoré majú s platbami cez internet veľa spoločného.

Rôzne platobné aplikácie a platobné brány vyžadujú rozdielne údaje o kartách. Niektorým stačia len základné informácie o karte. Zatiaľ, čo iné vyžadujú z bezpečnostných dôvodov viacero údajov pre dôkladnejšie overenie držiteľa karty. CNP platby na rozdiel od platieb, kde je potrebná fyzická prítomnosť karty neprešli rozsiahlou štandardizáciou a existuje tak viac spôsobov, ktorými sa obchody snažia overiť držiteľa. Platobnej karty. S príchodom, čoraz väčšieho objemu internetových platieb sa asociácie snažia prísť na jednoduchú a zároveň bezpečnejšiu formu overenia totožnosti držiteľa karty.

Väčšina platobných brán a aplikácií vyžaduje zadanie údajov z platobnej karty, vďaka ktorým následne schváli transakciu. [9]

Číslo karty

Pri platbe je vždy požadované číslo karty, keďže je to základný identifikačný údaj. V začiatkoch používania platieb na internete bolo postačujúce zadať len číslo karty, čo však nieslo silnú bezpečnostnú hrozbu hlavne pre obchodníka prijímajúceho platbu. Čísla platobných kariet nie sú generované a vyberané náhodne ale vznikajú na základe určitého algoritmu. Následne pri pokusoch o falšovanie kariet je možné postupovať podľa tohto algoritmu a tým generovať čísla kariet. Bolo by potom len otázkou času, kedy by sa niektoré z týchto čísel zhodovalo s skutočným používaným číslom platobnej karty. Obchod by transakciu bez pochybností autorizoval. Ďalšou nevýhodou platieb na základe

len čísla platobnej karty bola dlhá autorizácia. Vzhľadom k tejto zraniteľnosti boli požadované údaje rozšírené a v dnešnej dobe sa táto metóda nepoužíva.

Číslo a meno karty

Číslo karty nahradila kombinácia číselného údaju o karte (číslo karty) a meno držiteľa karty, v takom tvare ako je uvedené na karte. Číslo karty naďalej slúži ako identifikácia a meno karty slúži ako overenie pravosti platobnej karty. Pri pokuse o realizáciu platby overí platobná brána alebo aplikácia u vydavateľa karty zhodnosť čísla karty s menom držiteľa karty (meno uvedené na karte). Keďže toto sú dva od seba nezávislé údaje, rieši to zraniteľnosť, ktorá bola spomenutá vyššie. Ak sa zhoduje číslo karty s menom uvedeným na karte, tak daná karta existuje a týmto je zraniteľnosť prvej platobnej metódy cez internet odstránená. Avšak, ako aj číslo karty, tak aj meno držiteľa je ľahko získateľné. Oba tieto údaje sú na karte napísane alebo vyrazené lisovaním. Zároveň sú aj zaznamenané na magnetickom prúžku karty. V prípade krádeže karty alebo prečítaniu dát z magnetického prúžku, tak môže prísť k veľmi jednoduchému zneužitiu, čo sa týka internetových platieb.

Číslo karty a CVV2/CVC2 kód

CVV2 alebo CVC2 je trojciferný bezpečnostný kód, ktorý je účelovo zapísaný na zadnej strane karty napravo od podpisového prúžku. Tento kód vylučuje zneužitie na základe prečítania údajov z magnetického prúžku, keďže sa na ňom ako záznam nenachádza. Tento kód je každému držiteľovi generovaný podľa tajného algoritmu, ktorý pozná výhradne len vydavateľ karty. To znamená že bez tohto poznatku nie je možné priradiť k číslu karty aj odpovedajúci bezpečnostný kód. Ak dôjde k odcudzeniu karty, nie je možné zabrániť prípadnému zneužitiu, aj keď je karta vybavená CVV2/CVC2 kódom, páchateľ môže manuálne použiť všetky údaje z karty, taktiež aj tento bezpečnostný kód.

3D-Secure

Systémy 3D-Secure majú cieľ zvyšovať bezpečnosť realizovaných platieb v internetovom prostredí. VISA ako prvá navrhla systém Verified by Visa. MasterCard prišiel so systémom MasterCard SecureCode. American Express a JCB J/Secure po novom prichádzajú s American Express SafeKey.

Princípy všetkých týchto systémov sú zhodné. Pri internetovej platbe je do procesu vložený ďalší krok, ktorý presmeruje kupujúceho na stránku vydavateľa karty. Tu zákazník

naviac zadá ešte bezpečnostný kód, ktorý následne overí jeho totožnosť. Jedná sa o overenie vo forme kódu, ktorý sa na platobnej karte nenachádza vytlačený a taktiež nie je ani zaznamenaný na magnetickom prúžku. Tento kód zabezpečuje zneužitie karty pri jej odcudzení. Ako možnosť sa ponúka overenie držiteľa platobnej karty pomocou odoslaného bezpečnostného kódu pomocou správy SMS. Túto možnosť zatiaľ využívajú len niektoré platobné brány. [9]

Overenie pomocou skúšobnej platby

Tento bezpečnostný spôsob je považovaný ako veľmi bezpečný. Jedná sa o overenie držiteľa kreditnej karty, ktorý používa napr. platobný portál PayPal. Zákazník si zaregistruje svoju platobnú kartu u obchodníka, ten následne zrealizuje platbu s nízkou sumou (PayPal používa 2 eurá). V transakčnom výpise od svojej banky potom klient nájde danú transakciu a v detailoch tejto platby nájde kód, ktorý pre neho obchodník náhodne vygeneroval. Tento kód potom klient zadá na stránkach obchodníka a týmto potvrdí, že je skutočným držiteľom overovanej platobnej karty.

Tento spôsob overenia držiteľa karty je jeden z najsilnejších ochrán vôbec, keďže overuje a potvrdzuje klientov samotný prístup k bankovému účtu. Avšak toto overenie nie je využiteľné pri bežných obchodných podmienkach, keďže na každú transakciu je stanovená lehota od banky.

1.4.5 Embossing

Embossing je fyzické vyrazenie kľúčových údajov do karty. Jedná sa o číslo karty, dátum platnosti a meno držiteľa karty. Embossing je jednou z prvých technológií, ktoré mali zjednodušiť prevod transakcie. Pri platení embossovanou kartou je možné použiť imprinter. Imprinter je prístroj, do ktorého sa vloží karta a prejdením valčeka cez kartu sa vyvýšené kľúčové symboly na karte otlačia na potvrdenku k transakcii. [10]

Spracovanie formou imprintera bola oveľa rýchlejšia ako pôvodné ručné prepisovanie údajov. Zabránilo sa tak zároveň aj prípadným chybám pri opisovaní. V dnešnej dobe je tento spôsob platenia veľmi zriedkavý. Niekedy je využitý len v prípade poruchy platobného terminálu. Výhodou tejto technológie je najmä možnosť platby tam, kde sú zatiaľ stále využívané len imprintery. Nevýhodou je slabšia bezpečnosť karty. Zablokovanie takejto karty spravidla trvá približne 24 hodín. [10]

Embossing je v dnešnej dobe takmer na pokraji používania. Avšak stále sú krajiny, kde sa veľmi často používa a karta bez embossingu by bola nepoužiteľná. Preto je stále používaný vzhľadom na spätnú kompatibilitu. Tieto karty naviac preukazujú väčšiu dôveryhodnosť. [10]

1.5 Útoky na platobné karty

Typy útokov na platobné karty je možno rozdeliť podľa typu transakcií a sú CNP a CP útoky. CP útoky sú vedené priamo voči fyzicky prítomnej platobnej karte. CNP útoky sú prevádzané tak, že nie je fyzicky prítomná karta a je napadnutá len sprostredkovane informácií, ktoré o nej poskytne užívateľ.

V týchto prípadoch väčšinou nejde o fyzické zmocnenie sa a odcudzenie karty, keďže toto by bolo čoskoro nahlásené ako krádež či strata a tým by sa stala karta pre možnosť zneužitia bezcenná. Samotným cieľom je práve získanie dát o karte bez vedomia držiteľa karty a tak potom vytvoriť falšovanú kartu alebo len CNP spôsobom získané dáta len zneužiť na nákup, kde obchod alebo platobná aplikácia vyžaduje len informácie z karty.

Vydavatelia kariet a taktiež banky sa nezameriavajú len na prevenciu útokov ale zároveň sa aj aktívne podieľajú na samotnom urýchlenom odhalení. Pre tieto účely slúžia napr. automatizované systémy, ktoré pomocou rôznych algoritmov a údajov v databázach hľadajú podozrivé dáta a údaje, ktoré môžu predbežne vyhodnotiť ako zneužitie karty. Zo skúsenosti to potom vyzerá napríklad po realizovaní pochybnej platby banka urýchlene kontaktuje držiteľa karty s overením, či naozaj danú platbu zrealizoval. Môže sa jednať o platby, ktoré sú pre daného klienta neobvyklé (platby do ďalekého zahraničia a pod.). V prípade viacero takto vyhodnotených úkonov v krátkom čase alebo potvrdenia zneužitia karty je následne karta uvedená na stoplist. Výhodou týchto systémov je vysoká efektivita a väčšinou odhalia zneužitie skôr ako ho zaznamená sám klient. Tým skrátia dobu, počas ktorej by mohol páchateľ kartu zneužívať vo svoj prospech.

1.5.1 Ciele útokov

Útoky je možné taktiež rozdeliť podľa cieľov. Sú dva typy cieľov, ktoré sa môžu z určitých pohľadov prekrývať. Ako prvý typ útokov majú za cieľ získať informácie a dáta z karty. Priamym cieľom nie je získanie finančných prostriedkov. Cieľom je len získať dostatočné množstvo údajov z karty, aby mohli byť finančné prostriedky ukradnuté v budúcnosti. V tomto prípade je ide o snahu získať tieto údaje tak, aby držiteľ karty nepostrehol. Že mu

boli údaje z karty odcudzené. Preto v niektorých prípadoch prejde medzi odcudzením a zneužitím údajov dlhšia doba. Väčšinou v dobe až niekoľkých mesiacov, v tomto čase páchateľ zahladzuje stopy, aby spätne nebolo jednoduché k jeho vypátraniu. Príklady týchto útokov sú popísane a rozobrané v kategóriách nižšie. Patrí k nim phishing, skimming, krádež karty a krádež identity.

Druhým typom je útok, ktorého cieľom sú samotné pokusy o odcudzenie finančných prostriedkov vďaka nelegálnemu získaniu informácií o karte alebo držiteľovi. Avšak týchto typov útokov je podstatne menej, väčšinou sa jedná o sfalšované karty, teda novovytvorené karty, ktoré obsahujú vopred získané údaje. Takto ukradnutú kartu alebo aj v prípade nájdenia stratenej karty páchateľ môže využiť získané informácie tak, že objedná od internetového predajcu rýchlo speňažiteľný tovar (napr. elektronika). Pri tomto type útoku je takmer vždy isté, že bude páchateľ odhalený, či už samotnou bankou alebo políciou. Objednaný tovar je na presné meno a adresu, uvádza sa aj telefónne číslo. Ďalej tovar prechádza prepravnou spoločnosťou s komunikáciou pred a podpisom pri doručovaní tovaru. Týmto je cesta k páchateľovi odhalená, poprípade sa prechádza k následnému vyšetrovaniu. Užívateľ môže prísť na zneužitie pri zistení nezrovnalostí na svojom výpise z účtu alebo na základe pohybu na účte, ktorý môže mať od banky notifikovaný formou SMS správ.

Štatistické údaje o kriminalite spojenej s platobnými kartami zväčša sledujú práve informácie o druhom type útokov. Avšak získanie priamych informácií o tom, kde a ako boli zneužité údaje získané je v mnoho prípadoch veľmi ťažké alebo priam nemožné. Ak sa nejedná o významné množstvo týchto útokov, častokrát potom tieto údaje ani nie sú uvádzané.

1.5.2 Krádež karty

Ak príde ku krádeži alebo k strate platobnej karty je vždy nutné nahlásiť to bezodkladne banke a kartu tzv. stoplistovať, tým sa zníži nebezpečenstvo zneužitia danej karty. Aj cez prepracované a v dnešnej dobe najbezpečnejšie opatrenia a technológie čipových kariet a ochranu PIN kódom je stále možné kartu zneužiť. Je to možné pri platbe cez internet, keďže je veľmi jednoduché z karty vyčítať všetky dostačujúce informácie, ktoré stačia na jej zneužitie.

Krádeže a následné zneužívanie novo vydaných kariet bolo veľmi rozsiahle v dobe, kedy boli platobné karty v začiatkoch zavádzania a boli zákazníkom posielame vo veľkom

množstve. Často sa karty zneužívali a klient o týchto zneužívaniach nemal ani tušenie. Princíp tohto typu zneužitia karty spočíva v tom, že sa páchateľ zmocní zásielky s novou kartou, ktorá je na ceste ku klientovi. Či už sa jedná o odcudzenie počas transportu alebo vybraním poštovej schránky držiteľa karty. Cieľom páchateľa je získanie originálnej platobnej karty s prázdnym políčkom pre podpisový vzor, do ktorého môže podľa mena napísať svoj vlastnoručný podpis, ktorý následne môže používať ako pravý a podpisovať sa ním pri neoprávnených platbách touto kartou, keďže sa overuje podpis na pokladničnom bloku s podpisom na karte. Preto je nemožné zistiť, že podpis na karte je v skutočnosti podvrh.

Na základe rozšírenia týchto útokov prišlo opatrenie zo strany bánk, ktoré sú špecifické tým, kto môže komunikovať s klientom ohľadom novej karty. Je niekoľko spôsobov ako týmto zneužitiam zabrániť a väčšinou sa použije aspoň jeden.

Dátum platnosti

Novo vydaná platobná karta je priamo bankou expedovaná k držiteľovi s určitým časovým odstupom. Klient je o tomto odoslaní vopred informovaný. Dostáva inštrukcie a v prípade, ak mu karta nepríde do určitého časového obdobia, má kontaktovať banku. Týmto sa zlepšuje bezpečnosť, aby do tejto doby nebola karta zneužitá inou osobou. Platnosť karty je buď od určitého dátumu, od ktorého bude karta plno funkčná alebo môže zákazník svoju platobnú kartu aktivovať cez IB (Internet Banking).

Prevzatie karty na pobočke banky

Ďalším bezpečnostným opatrením môže byť prevzatie platobnej karty na pobočke banky, kde má klient otvorený účet. Pri tomto type opatrení je zvykom poslať zvlášť poštou v obálke PIN kód s prípadným vyjadrením, že je alebo kedy bude nová karta pripravená na vyzdvihnutie. Pri preberaní karty osobne na pobočke je klientova totožnosť overovaná buď jedným alebo až dvomi dokladmi totožnosti (napr. občiansky preukaz a vodičský preukaz). V tomto prípade je PIN kód pre prípadného páchateľa bez platobnej karty zbytočný.

Aktivácia karty

Klient po prevzatí platobnej karty musí následne realizovať jej aktiváciu. Banka aktivuje kartu po zodpovedaní otázok, ktoré by mal vedieť len skutočný držiteľ karty. V prípade ak sú tieto otázky overené je karta aktivovaná a klient môže platobnú kartu ďalej aktívne

používať. V dnešnej dobe je bežná aktivácia karty cez Internet Banking, kde je klient prejde k aktivácii karty a dokončí ju opísaním bezpečnostného kódu, ktorý mu príde na vyžiadanie formou SMS správy.

1.5.3 Krádež identity

Odcudzenie identity je špecifický útok, ktorého docielením nie je získanie klientovej platobnej karty alebo údajov o nej. Cieľom krádeže identity je pomocou získaných informácií o skutočnom držiteľovi presvedčiť banku, že podvodník je práve oprávneným skutočným držiteľom platobnej karty. Ak sa páchateľovi podarí cielený podvod, môže následne prevziať kontrolu nad bankovým účtom bez vedomia skutočného majiteľa. V prípade zmeny doručovacej adresy potom zabezpečí aby sa majiteľ nedostal k výpisom a následne nahlási skutočnú kartu ako ukradnutú alebo stratenú. Ďalej si páchateľ nechá vystaviť novú kartu, s ktorom potom môžu na základe podvodného dohodnutia s bankou disponovať v najvyšších limitoch výberov a transakcií. Samotná krádež identity nemusí byť len na platobnú kartu, rovnako týmto spôsobom môže podvodník získať úver alebo dohodnúť prečerpanie účtu do určitých mínusových limitov. Skutočný majiteľ účtu a zároveň poškodený sa pravdepodobne o tomto zneužití dozvie až vtedy, keď po ňom začnú byť splátky vymáhané.

Dumpster diving

Tento spôsob je skladaný z viacero činností. Najčastejšie je vyberanie a prehľadávanie odpadov budúceho cieľa, ktorý chce páchateľ poškodiť. Daný spôsob získavania informácií vychádza z predpokladu, že každý dostáva korešpondenciu a oznámenia z úradov, bánk, obchodov alebo od zamestnávateľa. Zo získaných dokumentov sa potom vyberajú potrebné informácie. Taktiež sa vychádza z predpokladu, že nie každý pred vyhodením tieto dokumenty buď zničí alebo iným spôsobom znehodnotí. Ďalším spôsobom môže byť priame vyberanie korešpondenčnej schránky. Tento spôsob môže byť pre páchateľa neúspešný vzhľadom k tomu, že by poškodený mohol byť viac všímavý a postrehol by chýbajúce dopisy, ktoré mu pravidelne prichádzajú. [11]

Ako vhodné opatrenie voči týmto útokom je dôkladne dbať na to, aby žiaden dokument nebol vyhodený do koša v takom stave, aby bolo možne z neho niečo kľúčové vyčítať a získať. Odporúča sa dané dokumenty skartovať alebo dôkladne roztrhať, tak aby údaje z nich boli nečitateľné. Kľúčové dokumenty môžu byť všetky, na ktorých sú uvedené identifikačné čísla, rodné čísla, výpisy z účtov a podobne. [11]

Social Networking

S veľkým rozšírením používania internetu a sociálnych sietí sa odkrýva aj značná príležitosť k získaniu osobných údajov alebo kľúčových údajov pre zneužitie platobných kariet. Sociálne siete sú cieľom páchateľov hlavne pre dobrovoľné zdieľanie veľkého množstvá informácií, ktoré užívateľ zverejňuje sám o sebe. Preto je skutočne vhodné aby si užívateľ sám uvedomil, čo môže a čo naopak nemôže byť zneužité. [12]

Páchateľ môže získať údaje jednoducho cez rôzne súťaže, hry a kvízy, ktoré užívateľovi dávajú otázky, ktorých cieľom je lepšie poznanie majiteľa účtu. Získavanie informácií od užívateľa je cielenými otázkami, pri ktorých podvodník získa napríklad navštevovanú základnú školu, meno matky za slobodna, prezývka, meno prvej učiteľky alebo obľúbený herec či film. Toto sú odpovede na často kladené otázky pri verifikácii užívateľa v krokoch nasledujúcich pri zabudnutí hesla od rôznych účtov. Tieto údaje potom páchateľ môže použiť a dostať sa tak postupne k dôležitejším informáciám. K informáciám, ktoré majú väčšiu váhu môže následne páchateľ prísť napríklad, ak sa dostane do e-mailovej schránky alebo priamo môže prísť na heslo do bankovníctva. [12]

Pre internetové bankovníctvo by sa malo používať bezpečné a originálne heslo, ktoré užívateľ nepoužíva nikde inde a pravidelne prístupové heslo mení. Keďže tomu vždy tak nie je, práve preto je väčšinou najslabším článkom v tejto problematike sám klient. Väčšina užívateľov používa rovnaké heslo ako k bankovníctvu, tak aj k iným svojim účtom. Preto je veľká pravdepodobnosť, že ak páchateľ získa heslo napríklad do e-mailovej schránky alebo do sociálnej siete môže toto heslo taktiež fungovať aj do internetového bankovníctva alebo internetovej peňaženky, kde už môže byť priamo aktivovaná a plne sprístupnená aj platobná karta. [12]

1.5.4 Skimming

Skimming je azda asi najznámejším útokom na platobné karty. Tento útok je často prevádzaný páchateľmi. Tieto útoky sú častokrát medializované a sú robené časté prevencie. Avšak existujú formy skimmingu, ktoré sú pri správnom a dokonalom prevedení takmer neodhaliteľné. Jedná sa o spôsob útoku, pri ktorom sa kradnú údaje o držiteľovi priamo pri realizácii transakcie, samozrejme bez vedomia samotného držiteľa. Deje sa tak pomocou čítačiek magnetického prúžku. Tieto čítačky sú účelovo umiestnené na bankomat alebo platobný terminál, ta aby pôsobili nenápadne a nebudili podozrenie. Nebýva pravidlom ale často je na takto zavedené zariadenie nainštalovaná aj miniatúrna

kamera, ktorá má za úlohu snímať priestor klávesnice, čím zaznamenáva zadávaný PIN kód, ktorý držiteľ karty zadáva. Podvodník týmto spôsobom tak získa naraz všetky údaje z magnetického prúžku a zároveň aj PIN kód k danej platobnej karte. [13]

Skimming spôsob ma zároveň širšie využitie. Nejedná sa len o úpravu bankomatu alebo platobného terminálu. Formou skrimmingu sa dajú získať neoprávnene aj údaje za pomoci obsluhy terminálu, či už z čítačky karty alebo fyzickým prepísaním údajov z karty. V Slovenskej a Českej republike dochádza čoraz častejšie k týmto podvodom za pomoci obsluhy. Tieto podvodné činy sa najčastejšie uskutočňujú v reštauráciách, hoteloch, baroch, čerpacích staniciach a podobne. Preto je dôležité si kartu pri platbe kontrolovať a nedovoliť aby obsluha s kartou odišla napríklad do inej miestnosti, taktiež nedovoliť obsluhe ani manipuláciu s kartou, ktorá by bola mimo dohľad majiteľa karty. [13]

Skimmovacie zariadenie

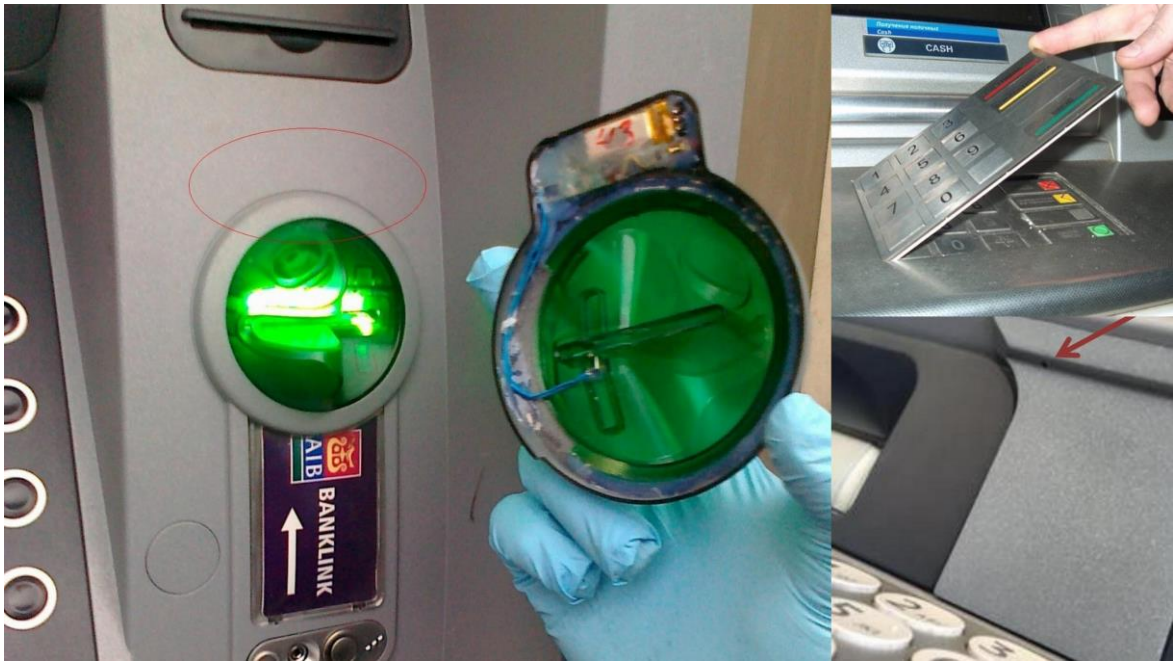
Zariadenie na prevádzku skimmingu je technický prístroj, ktorý spokíruje elektronické údaje z platobnej karty. Tieto zariadenia sú najčastejšie namontovávané na bankomaty v mieste kde sa karta vkladá. Skladá sa z dvoch častí z hľadiska funkčnosti. Prvá časť prečíta a získa dáta z karty. Druhá časť má za úlohu získať číselný identifikátor, teda PIN kód. Aby páchateľ mohol vyrobiť kópiu platobnej karty, potrebuje mať získané údaje z oboch častí skimmovacieho zariadenia. Následne potom môže vyrobiť falšovanú kópiu platobnej karty a robiť nelegálne výbery v domovskej krajine ale aj v cudzine. [13]

Tieto zariadenia sú zväčša montované v otvore pre vkladanie karty. Samotné montovanie je prevádzané formou rôznych nástavcov napodobňujúcich originál alebo inštaláciou panelu, ktorý je namontovaný už na originálnu časť bankomatu. Prístrojom pre odpozorovanie PIN kódu je väčšinou umiestňované v hodnej časti panelu bankomatu. Je to väčšinou kamera, mini kamera alebo mobilný telefón, kamera je väčšinou umiestnená v hornej lište nad obrazovkou. Môže to taktiež byť aj falošná klávesnica buď vo forme celého panelu alebo samostatne. Takto je situovaná na originálnu klávesnicu a dokáže odpozorovať zadávaný PIN kód. [13]

Tieto zariadenia sú vždy, čo najpodobnejšie použitým materiálom, kovom a farbám, z ktorých je vyrobený bankomat. Tým sú tieto zariadenia pri bežnom pohľade takmer nerozpoznateľné a nebudia žiadne podozrenie. Tento podvodný spôsob sa začal rozširovať a preto banky zaviedli tzv. antiskimmingový prvok, ktorý je navrhnutý ako nástavec

a je namontovaný na otvor pre vloženie karty. Tento nástavec má úlohu zabrániť podvodnému namontovaniu skimmovacieho čítacieho zariadenia. [13]

Avšak nové poznatky v zlepšovaní bezpečnosti preukázali, že nové skimmovacie zariadenie je práve v tvare nástavca, ktorý má opačnú úlohu a tou je práve zabrániť skimmingu.



Obr. 5. Zariadenie skimmingu (prečítanie karty, odčítanie PIN kódu, kamera) [14]

1.5.5 Phishing

Phishing je čoraz viac používanejší druh útoku na platobné karty, ktorý sa rozširuje spolu s rastom internetového bankovníctva, platbami cez internet a emailovými . Zo strany útokov na platobné karty je cieľom získať dostatočné množstvo údajov o karte pre realizáciu transakcie. Jedná sa takmer vždy o získanie mena držiteľa, čísla a platnosti karty. Pre overenie je treba naviac získať CVV2/CVC a PIN overovacie kódy. Páchateľ skúša a posiela podvodné emaily, ktoré vyzerajú ako oficiálne správy od banky, štátnych inštitúcií alebo iného dôverného odosielateľa. Kvalita týchto správ sa môže líšiť podľa toho ako prepracovane tieto dôverné správy páchateľ falšuje. Tieto správy pôsobia akoby skutočne boli od banky, keďže sa všetky použité obrázky texty môžu použiť identické aj zo strany páchateľa. Takáto podvodná správa vyzýva klienta, aby sa prihlásil na konkrétnu stránku a tam overil svoje údaje o platobnej karte, prípadne ich odoslal na zadanú adresu. Takto sa môže páchateľ pokúsiť podvodne kontaktovať viac ľudí naraz a tým získať viac údajov

pre prípadné zneužitie. Taktiež v týchto správach je klient tlačený k overeniu týchto údajov podľa uvedeného časového limitu, zároveň je aj v správe upozornený na to, ak tak neučiní bude jeho účet zrušený, na základe možného ohrozenia alebo bude podliehať sankciám a pod. Podvodná stránka alebo adresa potom pôsobí ako oficiálna stránka danej banky alebo inštitúcie. V skutočnosti ale slúži len na zber potrebných dát, údajov a informácií. Pri sofistikovanejších phishingových emailových správ môže byť uvedené aj telefónne číslo, ktoré má páchateľ nastavené tak, aby sa klient dostal napr. na automatizované vyberanie menu ako robota v podobe hlasového záznamníku, ktorý klientovi potvrdí autenticitu odoslaného „podvodného“ emailu. Phishing ako podvodný spôsob je známym útokom nie len, čo sa týka platobných kariet. Phishing je známym útokom nielen pre platobné karty ale dajú sa ním získať napr. osobné údaje, prihlasovacie údaje do internetového bankovníctva alebo do iných účtov. Banky apelujú na svojich klientov, aby nedávali žiadne z týchto kľúčových údajov nikomu a neposkytovali ich ďalej, keďže samotná banka po klientovi tieto údaje nikdy požadovať nebude. Vzhľadom k rozširujúcemu sa povedomiu o phishingu sú klienti dostatočne ostražitý a preto sa aj rozširuje množstvo a vznik nových útokov, ktoré pôsobia viac dôveryhodne. Sú používané na prvý pohľad bezpečnejších komunikačných kanáloch. Tieto útoky sú napr. smishing, ktorý má podobu SMS správy alebo vishing, ktorý používa priamy telefónny hovor. [15]

1.5.6 Pharming

Pharming ako útok je nebezpečnejší ako phishing, keďže aj skúsený užívateľ nemusí postrehnúť rozdiel medzi originálnou stranou a falšovanou kópiou. Páchateľ väčšinou pracuje s DNS záznamami. V praxi to potom znamená že zákazník je pri zadaní adresy presmerovaný na podvodnú stránku páchateľa, ktorá môže byť úplne rovnaká ako stránka banky. Klient potom vyplní do prihlasovacích polí svoje identifikačné údaje s pocitom, že sa jedná o skutočnú stránku banky. Následne tak páchateľ získa prihlasovacie údaje od zákazníka. Bez jeho vedomia. Ďalším spôsobom môže byť prostrední medzi internetovým bankovníctvom a užívateľom. Prostredník následne môže preposlať len autorizačné údaje banke ale s údajmi o transakciách môže manipulovať páchateľ. Môžu to byť len kľúčové ako číslo účtu a prevádzaná čiastka. [15]

1.5.7 Spyware

Spyware je v podstate škodlivý program, ktorý napadá počítače. Jeho cieľom je zberanie informácií o činnostiach na počítači. Ten môže počítač napadnúť napr. v podobe trojského koňa alebo môže byť nenápadne stiahnutý ako súčasť iného veľmi bežného a používaného programu. Tento program využíva chýb operačného systému alebo prehliadača k tomu, aby prenikol do počítača. Pomocou spyware sa následne páchateľ prepracuje až k citlivým údajom poškodeného Tieto údaje a informácie môžu byť napr. prístupy k internetovému bankovníctvu alebo k iným účtom, ktoré môžu viesť k odcudzeniu finančných prostriedkov. [15]

1.5.8 Libanonský uzol

Pri tomto spôsobe útoku ide o veľmi rafinovaný trik. Páchateľ do otvoru pre platobné karty v bankomate o trik, pri ktorom páchateľ do tohto otvoru vloží kúsok pásky napr. z videokazety. Keď potom klient vloží kartu do bankomatu, páska ju zadrží tak, že bankomat nemôže kartu zasunúť ani vysunúť. Páchateľ je pripravený v blízkosti bankomatu a následne za zámienkou poškodenému pomôcť mu poradí, aby skúsil zadať znovu PIN kód. Páchateľ tento kód odpozoruje a potom, keď ide klient reklamovať danú situáciu do banky, páchateľ využije situácie, vytiahne kartu a znovu ju použije už s použitím odpozorovaného PIN kódu. Páchateľ následne vyberie hotovosť skôr než klient stihne zablokovať svoju platobnú kartu. [15]

1.5.9 E-Commerce

So stále narastajúcim počtom internetových platieb taktiež rastie aj kriminalita v tejto oblasti. V internetovom rozhraní existujú rôzne útoky od páchateľov. Na niektorých sa môže pričiniť sám predajca, iné môžu byť urobené práve za pomoci prelomenia bezpečnostného predajcovho systému. Môže sa jednať o nabúranie do databázy, ktorá obsahuje informácie o platobných kartách. Transakcie robené cez internet majú veľa spoločného s transakciami robenými cez poštu alebo telefón. Sú na nich rovnaké útoky a tak isto aj tie isté spôsoby prevencie a ochrany. [16]

Podvodní predajcovia

Cieľom podvodných e-shopov nemusí byť len získanie peňazí a zákazníkovi neposlať žiadny tovar ale najmä získanie informácií o platobných kartách svojich zákazníkov. Tieto získané informácie môže páchateľ zneužiť buďto sám alebo tieto údaje ďalej predať.

Najbezpečnejším spôsobom je nakupovanie z overených e-shopov. Na základe dôveryhodného zdroja alebo aj certifikátu. [16]

Odcudzenie informácií z databázy

E-shopy a internetové stránky, ktoré majú možnosti platieb pomocou platobných kariet si archivujú a udržiavajú užívateľské účty, ku ktorým bývajú priradené údaje o kreditných kartách. Hlavným cieľom je pohodlnosť pre klienta, aby nemusel pri každej transakcii dookola zadávať všetky potrebné údaje. V prípade krádeže týchto údajov, hlavne u veľkých spoločností môže prísť k ohrozeniu bezpečnosti tisícok platobných kariet. Príklad takejto krádeže sa stal v roku 2011 spoločnosti SONY Corporation. V tomto prípade unikli informácie z viacej ako 100 miliónov účtov vrátane údajov platobných kariet.

Preto takto citlivé dáta sú už v databáze následne šifrované. Samotná krádež týchto údajov potom nemusí znamenať zneužitie týchto údajov. Aj skrz tieto opatrenia je v rámci bezpečnosti zvýšiť pozornosť a sledovať aktivity platobnej karty alebo ju priamo radšej vymeniť. [16]

1.5.10 Bezkontaktné karty

Bezkontaktné karty patria zároveň medzi najnovšie technológie medzi platobnými kartami. Práve preto sú po ich zavedení stále stredobodom pre odborníkov v oblasti bezpečnosti, ktorí našli určité slabiny, ktoré boli následne odstránené alebo označené za bezpečnostne nízku hrozbu, preto sa môže takouto kartou platiť bez zadania PIN kódu len v menších sumách. Vďaka tomuto opatreniu už vydavatelia významne znížili predpoklad záujmu zo strany podvodníkov. [17]

Šifrovanie bezkontaktných kariet

Ako hneď prvé série PayWave a PayPass mali významne trhliny v bezpečnosti. Umožňovali páchateľovi jednoduché získanie údajov z karty. Karty komunikujú s terminálmi pomocou šifrovaného spojenia, avšak prvé série bezkontaktných kariet nemali šifrované niektoré údaje ako napr. číslo karty, vďaka ktorému bolo možné sa k údajom dostať. V dnešnej dobe už sú aj tieto chyby doladené a samotné šifrovanie je použité na všetky údaje z karty. [17]

Relay útoky

Útoky typu relay nie sú považované len ako teoretická možnosť zneužitia ale najmä boli aj overené a vyskúšané priamo v praxi. Samotná podstata relay útoku spočíva v sprostredkovaní komunikácie medzi bezkontaktnou kartou a terminálom. Využíva najmä toho, že nie je nutnosťou s kartou nijako manipulovať, je nutné kartu len jednoducho priložiť blízko alebo úplne priblížiť k platobnému terminálu. Pomocou napr. mobilného telefónu, ktorý môže ideálne simulovať kartu sa podvodník priblíži k terminálu. Terminál začne komunikovať s mobilným telefónom ako keby sa jednalo priamo o bezkontaktnú kartu, keďže telefón obsahuje taktiež čip pre bezkontaktné karty. Telefón v tomto prípade tvorí len sprostredkovateľskú funkciu a preposiela údaje z terminálu do iného zariadenia, ktoré potom páchateľ priblíži k niekoho inej platobnej karte. Ta týmto spôsobom v praxi odpovie inému falošnému terminálu, v prípade ak nie je samozrejme vyžadované zadanie PIN kódu, keďže údaje sa nemenia ale jedná sa len o takýto sprostredkovaný podvodný prenos, ktorý nebudí pozornosť. [17]

1.6 Ochranné prvky

Typ a zobrazenie ochranných prvkov jednotlivých druhov kariet znázorňuje tabuľka nižšie (*Tab. 2.)* Tabuľka zobrazuje prehľad základných ochranných prvkov kariet. Niektoré bezpečnostné prvky nie je možné zverejniť, pretože podliehajú utajeniu. Nie je cieľom popisovať detailne aj z dôvodu, že podvodníci, ktorí falšujú platobné karty ich podrobne nenapodobujú. Pre účely neoprávnených výberov finančných prostriedkov z ATM používajú polotovary z plastu s magnetickým prúžkom, ktorý je na zadnej strane, poprípade s nápisom na prednej strane. Tento nápis je striebornej alebo zlatej farby. [18]

Typ karty	VISA	MasterCard	American Express	Diners Club	JCB
Počet číslic udávajúcich číslo karty	13 alebo 16	16	15	14	16
Hologram	Strieborný trojrozmerný obraz holubice, pri pohybe máva krídlami	Trojrozmerný obraz zemskej pologule	Bežne nemá, ak má jedná sa o šachovnicu alebo preliv farieb	Trojrozmerný obraz mapy sveta s nápisom Diner Club International	Strieborný alebo zlatý trojrozmerný obraz vychádzajúceho slnka alebo obraz Zeme
Logo karty	Emblém Visa v modro-bielo-zlatom prevedení	2 prepojené kruhy v farbách červenej a žltej s nápisom MasterCard	Centurion s ostrými rysmi	Nápis DC v ľavom hornom rohu v tmavomodrej farbe s textom Diners Club International	Zvislé pruhy červenej, čiernej a modrej farby s nápisom JCB
Zvláštne znamenia (viditeľné)	Letiace "V" na prednej strane	Do seba zapadajúce písmená MC na prednej strane karty	Mikrotext opakujúceho sa názvu American Express	Štylizovaný symbol DC	Čínske ornamenty
Skryté znamenia (viditeľné pod UV svetlom)	Letiaca holubica	Písmená MC	Nápis AMEX Fosforeskujúci nápis Centurion	Logo Diners Club International	Písmená JCB

Tab. 2. Prehľad ochranných prvkov a znakov platobných kariet [18]

2 SPRACOVANIE TRANSAKCIÍ

Procesy bezhotovostných platieb prostredníctvom platobnej karty za tovar či služby alebo výber hotovosti kartou ide členiť na procesy overenia, autorizácie, clearing a zúčtovanie.

2.1 Overenie

Procesom overenia je myslené overenie platobnej karty pri transakcii u obchodníka, ktorý je povinný skontrolovať pravosť karty a jej platnosť, či ju predkladá oprávnená osoba, na ktoré meno je karta vystavená a pod. V prípade pochybností má obchodník oprávnenie si vyžiadať od osoby disponujúcej kartou doklad totožnosti, môže to byť občiansky preukaz alebo cestovný pas. Táto povinnosť platí všeobecne pri všetkých platobných transakcií nad 100 tisíc Kč alebo približne 3600 €. Pri čipových kartách je totožnosť overovaná POS terminálom a zadaním bezpečnostného kódu PIN.

2.2 Autorizácia

Autorizácia nasleduje po overení. Jedná sa o proces komunikácie ATM alebo POS terminálov u obchodníkov s vydavateľskou bankou držiteľa alebo majiteľa karty cestou danej kartovej asociácie. Autorizácia je overenie, kedy sa zisťujú údaje ako finančné prostriedky na účte, či je karta uvedená na stopliste a pod. U kariet bez čipu sa najskôr overuje samotná karta a až potom dochádza k samotnej autorizácii. [19]

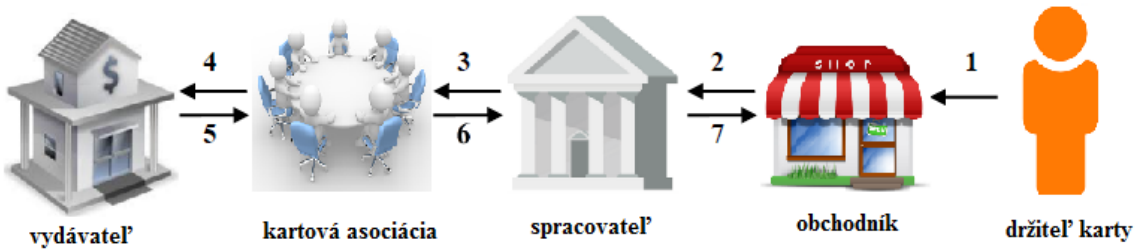
2.3 Hlasová autorizácia

U platby pri starších mechanických imprinterov je obchodník povinný urobiť telefonickú (hlasovú) autorizáciu na autorizačné centrum v prípadoch prekročenie autorizačného limitu. Autorizačné limity sú dôverné a pre dané obchodné miesto ich v zmluve stanovuje spracovateľská banka. Daný limit sa vzťahuje na súčet všetkých transakcií v jednom dni na jednom mieste, tak aby sa platba nedala obísť rozložením na viacero transakcií. Hlasová autorizácia je následný proces, ktorý je nutné urobiť taktiež v prípade pochybností o pravosti karty alebo podozrení, či danú kartu predkladá neoprávnená osoba. Pri hlasovej autorizácii operátor centra následne požaduje číslo platobnej karty, platnosť, číslo obchodného miesta, typ transakcie (platba alebo výber), daná čiastka alebo ďalšie informácie. V prípade pozitívnej autorizácie je operátorom predaný autorizačný kód obchodníkovi, tento kód sa zapisuje na predajný doklad lebo je transakcia zamietnutá. Ak nasleduje

pokyn k zadržaniu karty, obchodník následne zváži situáciu, či predmetnú kartu zadrží sám alebo privolá Políciu. [19]

2.4 Automatická autorizácia

Automatická autorizácia prebehne vtedy, ak transakcia prebieha cez ATM alebo POS terminál. Proces elektronickej autorizácie vo väčšine prípadov činí 5 až 12 sekúnd. Proces autorizácie znázorňuje obrázok.



Obr. 6. Proces autorizácie [19]

1. Vloženie karty do POS terminálu, ktorý indikuje dáta uložené na magnetickom prúžku alebo čipu.

2. POS terminál odošle údaje o karte s danou čiastkou transakcie spracovateľovi (banke obchodníka).

3. Spracovateľ údaje prepošle do kartového systému asociácie, kde sú overované niektoré údaje napr. bezpečnostné prvky kariet.

4. Autorizačné centrum kartovej asociácie pošle autorizačnú požiadavku vydavateľovi, ktorá overí oprávnenosť požadovanej transakcie z pohľadu krytia dostatočnou výškou finančných prostriedkov na účte, poprípade ďalej overuje PIN.

5. Vydavateľ pošle kartovej asociácii autorizačnú odpoveď (kladná alebo záporná).

6. Asociácia prepošle autorizačnú odpoveď spracovateľovi.

7. Spracovateľská banka ďalej prepošle odpoveď do POS terminálu, a z jeho podnetov začali požiadavky k autorizácii. [19]

Outsourcing

Outsourcing znamená využitie pre spracovanie autorizácie ďalšieho subjektu, ktorým prideľuje certifikáciu kartová asociácia. V SR je dozor Národná banka Slovenska (NBS).

Využívajú ich niektoré banky z dôvodu úspor za investovanie do nových systémov a technológií. V SR sa jedná o spoločnosť napr. Global Payments Europe.

2.5 Clearing

Proces výmeny údajov o finančnej transakcii medzi spracovateľom a vydavateľom k umožneniu zaúčtovania transakcie na účet držiteľa karty a rekonciliácie pozície člena asociácie k vysporiadaniu. Poplatky za tento proces nebude hradiť držiteľ karty, pretože sa medzi sebou vysporiadajú účastníci transakcie (vydavateľ, spracovateľ, obchodník, kartové asociácie).

2.6 Zaúčtovanie

V tejto poslednej fáze platobnej transakcie dochádza k prevodom finančných prostriedkov medzi účastníkmi uvedenými v procese autorizácie. Clearingové organizácie posielajú vydavateľom informácie o transakciách (mená klientov, čísla platobných kariet, dáta, časy, čiastky, meny a miesta transakcií).

II. PRAKTICKÁ ČÁST

3 ANALÝZA ÚTOKOV

Do analýzy rizík môžeme zaradiť dve časti. V prvej časti je porovnanie štatistík o útokoch v rôznych regiónoch, tie analyzujú a následne vyhodnocujú dáta od príslušných inštitúcií a orgánov v rôznych krajinách sveta. V druhej časti je následná kvantitatívna analýza rizík spájaných s používaním platobných kariet v Českej republike. Na základe vyhodnotení sú následne navrhnuté riešenia pre zníženia rizík.

3.1 Analýza štatistík útokov pre rôzne oblasti

Cieľom je porovnať štatistiky útokov podľa vybraných jednotlivých krajín. Získajú sa najčastejšie použité typy útokov, samozrejme v závislosti na každú vybranú oblasť,)prípadná celková štatistika a vyhodnotenie, kde sú jednotlivé najčastejšie páchané.

Ako objekt týchto analýz sú útoky, ktorých cieľom je priama krádež finančných prostriedkov, nie útoky, ktoré sa zameriavajú len na získanie dát a údajov o klientovi a karte. Tieto analyzované útoky nemusia byť priamo v danej krajine alebo oblasti či regióne a na rozdiel od útokov, kedy sú ukradnuté priamo finančné prostriedky, je veľmi zložité ich odhalenie.

3.1.1 Porovnávacia metóda

Začiatkom analýzy je výber a identifikácia kľúčových krajín alebo oblastí. Pretože pre jednotlivé regióny zväčša nie sú dostupné celkové údaje, prehľady a dáta. Ako vhodná oblasť môže byť SEPA oblasť. Môže sa stať, že nie sú dostupné údaje ani pre jednotlivé krajiny. Preto pre konkrétne vybrané oblasti sú stanovené kľúčové krajiny, ktoré sú v tomto prípade považované ako reprezentovanie danej oblasti.

Ďalším krokom v analýze je výber pre porovnanie tak, aby boli celkovo všetky dáta z daného obdobia a rozlišovali útoky na platobné karty pre rovnaké typy. Údaje sú následne prevedené do rovnakých formátov, napr. dopočtami zmien v útokoch oproti predchádzajúcemu roku na základe štatistík z rokov napr. 2014 a 2015, ďalej je prepočet mien daných štátov do meny jedného štátu pre porovnanie celkového dopadu. Ako spoločná mena daných štátov je vybrané Euro s kurzom k 31.12.2014 podľa kurzového lístku ECB33. Následne podľa výberu typov útokov na platobné karty bude urobené porovnanie.

3.1.2 Identifikovanie dát

Pre túto analýzu boli vybrané krajiny z celého sveta. Sú nimi Kanada a USA (zastupujú Severnú Ameriku), SEPA oblasť (zastupujúca Európu), Juhoafrická republika (zastupuje oblasť Afriky) a Austrália. Pre oblasti ako Ázia a Južná Amerika sa nepodarilo získať dostatočné množstvo dát, preto do tejto analýzy nebudú zapojené.

Kompletne všetky analyzované dáta a údaje sú analyzované z roku 2015. Zdrojom týchto dát sú inštitúcie, štátne orgány, úrady alebo samotné bankové asociácie vybraných krajín alebo oblastí.

Vybrané typy útokov

Ako najčastejšie a vhodné typy útokov na platobné karty boli vybrané nasledujúce útoky:

- Krádež alebo strata karty. Tu sú zarátané karty, či už stratené alebo odcudzené, behom ich používania alebo aj platobné karty, ktoré sa vďaka páchateľovi nikdy k právoplatnému majiteľovi nedostali.
- Sfalšované platobné karty. Pri tejto analýze ide o uvedené štatistiky pre urobené kópie kariet ako celok. Zo všetkých pohľadov.
- CNP spôsoby transakcií. Táto analýza zahrňuje všetky podvodom urobené transakcie v rámci e-commerce. Jedná sa o všetky platby typom napr. cez telefón, za použitia platobnej karty a údajov cez internet a pod.

Informácie pre jednotlivé oblasti

Údaje pre jednotlivé analyzované oblasti sú rozdelené podľa konkrétneho typu tabuľky. Tieto typy sú navrhnuté podľa typov útokov. Sú to krádež kariet, sfalšované karty, ID krádeže, CNP podvodné transakcie. Tieto tabuľky sú boli prispôsobené podľa toho v akej oblasti a krajine sa dané údaje sledujú. Prvý stĺpec v každej tabuľke vždy ukazuje údaje o celkovej strate za rok 2015. Pre konkrétny typ útoku, vždy strata v domácej mene. Stĺpec s percentom informuje o podiele vybraného útoku proti platobným kartám v určenej oblasti. Stĺpec zmeny informuje o poklese alebo náraste daného typu útoku voči predchádzajúcemu roku 2014. Menový kurz informuje o kurze, ktorý je v danom období použitý pre prevod medzi domácou menou a eurom koncom roku 2015. Stĺpec na konci informuje o celkovej strate pre konkrétny útok v danom prepočte určenom pre spoločnú menu, ktorou je euro. Táto spoločná mena bola určená z hlavného dôvodu a to, aby sa dalo všetko následne presne porovnať.

SEPA oblasť

SEPA oblast spája v celkovom počte dvadsaťosem krajín EÚ (Európska únia) a šesť krajín mimo EÚ. SEPA oblasť združuje krajiny, v ktorých platia rovnaké podmienky pri platbách, ako kedy sa jednalo o jeden štát. Platba je označovaná ako SEPA Europrevod a je bez poplatku v celej SEPA zóne. Ak sa presadzuje určité opatrenie proti útokom na platobné karty, zakročí sa v rámci celej tejto oblasti. Preto sa rozvoj alebo opatrenia riešia iniciatívne zo strany SEPA.

Pre krajiny SEPA udržuje a tvorí štatistiky a závery ECB (Európska centrálna banka). Každoročne zverejňuje údaje s využívaním a kriminalitou v rámci platobných kariet. Tieto štatistické údaje obsahujú detaily ohľadom jednotlivých krajín a kompletne pre celú SEPA oblasť.

SEPA (oblasť)	Percento (%)	Zmena (%)	Celkom (EUR)
Krádež / Strata	15,96%	-4,8%	198 215 816
Sfalšované karty	20,66%	-1,4%	258 498 522
CNP	58,33%	+9,8%	766 299 587

Tab. 3. Štatistika zneužití platobných kariet v SEPA oblasti [20]

Austrália

Austrália má taktiež všetky štatistiky týkajúce sa platobných kariet a kriminality spájanej s kartami. Tieto štatistiky robí Australian Payments Clearing Association, Táto organizácia zaisťuje dohľad, prehľad, a reguláciu nad systémami pre platobné karty v rámci celej Austrálie. Toto združenie zároveň udržuje a pravidelne vydáva štatistiky jednotlivo pre platobné kanály.

K typom útokov sú identifikované straty a krádeže platobných kariet a ich zneužitie v CNP prostredí. Ostatné údaje uvedené nie sú.

Austrália (oblasť)	Celkom (AUD)	Percento (%)	Zmena (%)	Kurz	Celkom (EUR)
Krádež / Strata	3 576 289	2,38%	+21,54%	1 EUR = 1,467 AUD	2 437 825
Sfalšované karty	22 052 046	14,7%	-1,4%	1 EUR = 1,467 AUD	15 032 070
CNP	68 758 269	45,83%	-1,36%	1 EUR = 1,467 AUD	46 869 986

Tab. 4. Štatistika zneužití platobných kariet v Austrálii [23]

Kanada

Oblasť Kanada má štatistiky, ktoré sa týkajú platobných kariet a s nimi spojenou kriminalitou. Tieto štatistiky sú publikované cez Canadian Bankers Association. Táto organizácia tvorí funkciu zástupcov kanadských bankových domov a uchováva sumárne celkové štatistiky.

K získaným typom útokov sú krádeže a straty platobných kariet, falšované karty, celkové zneužitie v CNP prostredí. Ďalej sú uvedené aj údaje o krádeži identity.

Kanada (oblasť)	Celkom (CAD)	Percento (%)	Zmena (%)	Kurz	Celkom (EUR)
Krádež / Strata	26 177 086	5,87%	-16,17%	1 EUR = 1,505 CAD	17 393 413
Sfalšované karty	114 566 251	27,21%	+9,63%	1 EUR = 1,505 CAD	76 123 754
CNP	260 516 268	62,43%	+2,73%	1 EUR = 1,505 CAD	173 100 510
Krádež ID	13 136 899	2,73%	+0,24%	1 EUR = 1,505 CAD	8 728 837

Tab. 5. Štatistika zneužití platobných kariet v Kanade [21]

Spojené štáty americké (USA)

USA ukladá dáta o platbách a platobných kartách spojených s kriminálnou činnosťou. Organizácia Federal Reserve System spravuje tieto údaje. Avšak táto inštitúcia neposkytuje úplne všetky potrebné údaje. Ďalšie doplňujúce údaje poskytuje organizácia Federal Trade Commission , ktorá zaznamenáva do štatistík hlavne sťažnosti od klientov. Avšak ani kombinácia týchto štatistík netvorí úplný celok. Stále chýbajú viaceré údaje.

Táto štatistika informuje o zneužití odcudzených alebo stratených kariet. Následne zneužitia v CNP rozhraní.

USA (oblasť)	Celkom (AUD)	Percento (%)	Kurz	Celkom (EUR)
Krádež / Strata	919 miliónov	22%	1 EUR = 1,084 USD	847 785 978
Sfalšované karty	1,467 miliardy	34%	1 EUR = 1,084 USD	1 353 321 033
CNP	1,58 miliardy	42%	1 EUR = 1,084 USD	1 457 564 576

Tab. 6. Štatistika zneužití platobných kariet v USA [22]

Juhoafrická republika (JAR)

Štatistické údaje pre Juhoafrickú republiku sú k platobným kartám a k nim spojenou kriminalitou. Tieto údaje uchováva a pracuje s nimi South African Banking Risk Association (SABRIC), ktorá naviac ešte informuje o nebezpečných spojeniach s bankovými službami celosvetovo.

Uvedené typy útokov sú krádež a strata platobných kariet, falšované karty, zneužitia v prostredí CNP, taktiež ak krádeže identity vedúce k zneužitiu platobnej karty.

JAR (oblasť)	Celkom (ZAR)	Percento (%)	Zmena (%)	Kurz	Celkom (EUR)
Krádež / Strata	16,2 milióna	5,33%	-19%	1 EUR = 16,3 ZAR	993 865
Sfalšované karty	108,6 milióna	37%	-49%	1 EUR = 16,3 ZAR	6 662 577
CNP	159,4 milióna	54,93%	+12%	1 EUR = 16,3 ZAR	9 779 141
Krádež ID	1,2 milióna	0,004%	+34%	1 EUR = 16,3 ZAR	73 620

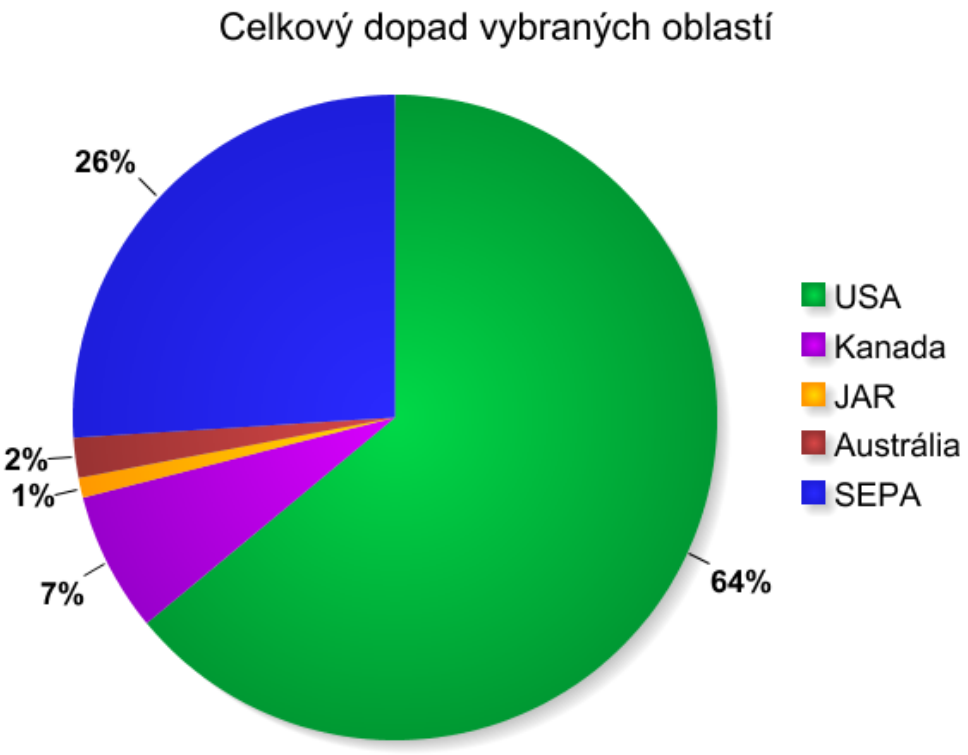
Tab. 7. Štatistika zneužití platobných kariet v Juhoafrickej republike [24]

3.1.3 Celkový dopad zneužitia platobných kariet

Celkové zhrnutie a dopad zneužitia platobných kariet pre vybrané sledované oblasti a krajiny znázorňuje, že najväčší podiel zo všetkých vybraných sledovaných oblastí majú Spojené štáty americké. Tieto štatistiky a zistenia odpovedajú aj s údajmi niektorých spravodajských staníc a médií, kde aj podľa nich USA korešponduje s takmer polovičným

celosvetovým dopadom zneužití platobných kariet. Samotný tento stav môže byť spôsobený taktiež aj veľkou obľúbenosťou platobných kariet na celom území USA. Alebo môže mať naopak USA najmenší záujem o bezpečnosť oproti iným krajinám alebo celkovým oblastiam, v ktorých môže byť používanie platobných kariet na rovnakej úrovni. Všetka používaná technológia EMV, ako je tomu v SEPA oblasti, už je zapojená v plnom rozsahu aj pre USA, avšak do dnešnej doby nie je táto technológia propagovaná a používaná, tak ako je tomu v Európe.

Celkový dopad a odhad však neposkytuje detailnejšie údaje, keďže sa jedná o viacero oblastí a trhy, ktoré sú rôznych veľkostí, kedy Austrália, Kanada či Juhoafrická republika sa nemôžu porovnávať s trhom o oblastiach ako je USA alebo SEPA zóna. Možným riešením by bol prepočet dopadu na jednu kartu. Údaje a informácie o počte kariet pre konkrétny trh môžu byť ešte nedostupnejšie, ako všetky získané informácie o kriminálnych činnostiach spájaných s platobnými kartami.

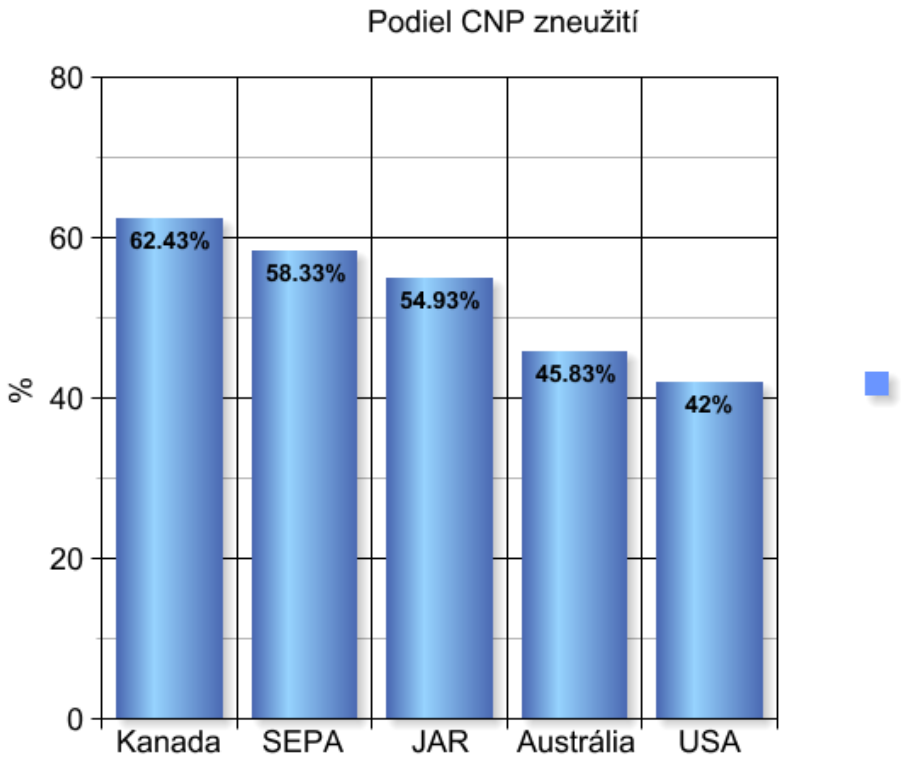


Obr. 7. Graf celkového dopadu vybraných oblastí

3.1.4 Porovnanie najčastejších typov útokov

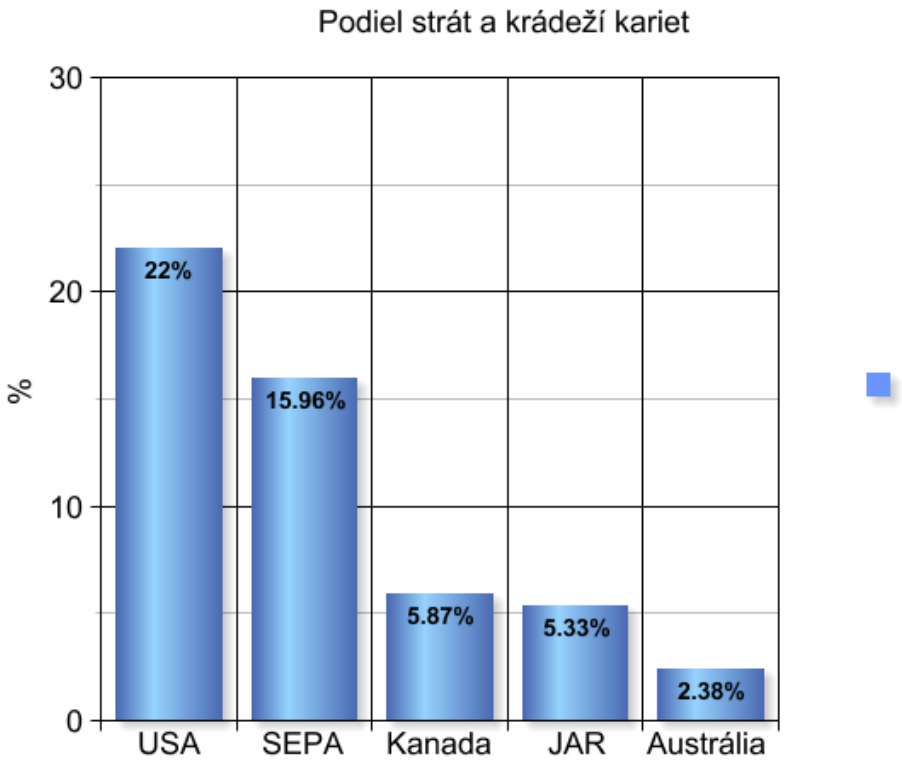
Najväčší podiel zneužitia pomocou sfalšovanej karty je v oblasti, kde ešte neprebehla úplná migrácia EMV technológie. Je možnosťou zapojenia tejto technológie naplno, avšak v krajine USA to prebieha zatiaľ pomaly. Celková oblasť Afriky a USA ako svetové trhy prechádzajú na EMV technológiu. Oblasti ako Kanada a SEPA propagujú a rýchlejšie prechádzajú na túto technológiu a sú v rámci EMV technológie na tom najlepšie. V dnešnej dobe je SEPA zóna v rámci terminálov a kariet s EMV technológiou takmer v absolútnej obsadenosti. Pri prechode na používanie EMV technológie sa takmer vždy tento prechod odrazí na znížení podielu falšovaných platobných kariet, keďže zneužitie je zložitejšie a zároveň samotné falšovanie kariet je hlavne v krajinách, kde zatiaľ nie sú použité dostatočné bezpečnostné technológie. Časť podvodníkov sa preto často presúva do krajín s nižšou bezpečnosťou pre platobné karty, tieto krajiny a oblasti sú najmä Afrika a USA.

Následné trendy pri prechodoch na bezpečnejšie technológie pri platobných kartách sú najme častejšie zneužitia v CNP prostredí, čo je vidno na prehľadoch a štatistikách zneužití daných oblastí. Preto oblasť, ktorá má malý podiel falšovaných kariet, spravidla má zvýšený podiel zneužití v CNP prostredí. Taktiež oblasti, ktoré majú zvýšený počet falšovaných kariet, majú zároveň nižšie zneužitia v prostredí CNP. Celosvetovo je zaznamenávaný skorej stúpajúci nárast zneužití v prostredí CNP, čo je hlavne pripisované zvýšenej obľúbenosti týchto platieb, čo je viditeľné na silnom náraste platieb v tomto prostredí.



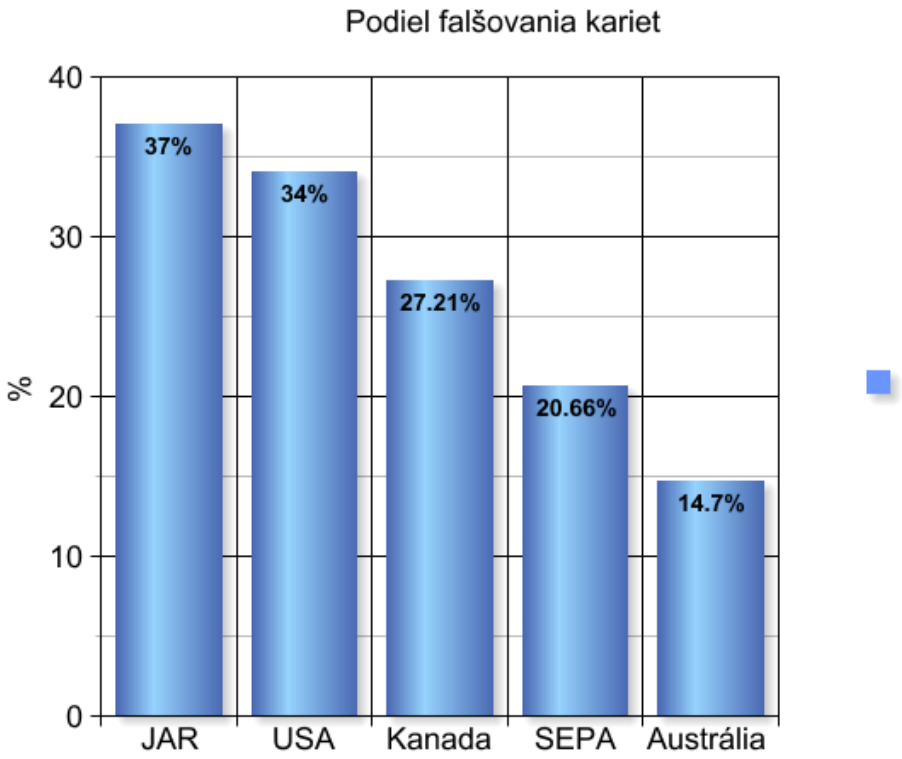
Obr. 8. Graf porovnania podielu zneužití v CNP prostredí pre vybrané oblasti

V rámci ukradnutých a stratených platobných kariet postupom času klesá ich zneužívanie, keďže sú karty takmer vždy chránené PIN kódom, čo výrazne obmedzuje možnosť zneužitia. Ďalším faktorom je veľké riziko odhalenia, keďže len jednoduché získanie údajov o karte môže prebehnúť bez povšimnutia až pokiaľ nedôjde k zneužitiu útoku. Ďalej aj krádež karty alebo strata je zaznamenaná v kratšej dobe a tým je ďalej po nahlásení bankou zablokovaná. Austrália je v tomto prípade výnimkou, keďže podiely strát a krádeží kariet vzrástol v posledných rokoch o takmer 70%.



Obr. 9. Graf porovnania podielu krádeží a strát pre vybrané oblasti

Ako nový spôsob zneužitia sa považuje krádež identity klienta. Nie všetky inštitúcie tento spôsob zatiaľ rozlišujú. Tento spôsob je v poslednom období v náraste. Daný typ zneužitia je jednoduchší a je zložitejšie jeho odhalenie. Zároveň sa týmto páchateľ môže dostať efektívne k vysokým výnosom.



Obr. 10. Graf porovnania podielu falšovania kariet pre vybrané oblasti

3.1.5 Vyhodnotenie analýzy

Záver tohto vyhodnotenia taktiež odpovedá aj záverom ECB, ktorá považuje ako stúpajúcu hrozbu najmä rýchlo vzrastajúce platby v CNP prostredí. Tieto platby majú rozdielne stupne zabezpečenia. Oproti bežným platbám typu výber z bankomatu alebo platba v komunikácii s terminálom sú platby v CNP prostredí na veľmi nízkej bezpečnostnej úrovni. Tento stav má opačný efekt, keďže je rastúci počet CNP platieb, tak z pohľadu falšovania platobných kariet, ich počet klesá a do budúcna sa predpokladá taktiež pokles. Pokles falšovania platobných kariet je taktiež spôsobený aj nárastom EMV terminálov a bankomatov najmä v SEPA oblasti, do ktorej patrí celá Európa a niektoré ďalšie krajiny. EMV technológie sa rozširujú pomaly do celého sveta a tým sa maximalizuje bezpečnosť platobných kariet.

Predpoklad do budúcna je stále zvyšujúci sa záujem o zneužitie platobných kariet na internetové platby. Potvrdzujú to štatistiky, podľa ktorých tento záujem neustále stúpa. K tomuto rastu sa pripája viacero faktorov. Jedná sa o stále väčší záujem a používanie online platieb, taktiež aj stále viac ponúk, ktoré poskytujú a umožňujú tieto platby z pohľadu obchodníka. Toto spôsobuje čoraz väčšie riziká v tejto oblasti. Tento spôsob

platieb s udrží svoje prvenstvo v štatistikách zrejme až do času, kedy aj CNP prostredie prejde celkovou štandardizáciou. Pri tejto štandardizácii sa môže postupovať ako pri štandardoch pre bežné platobné karty. Tým sa môže prejsť zo zodpovednosti z bánk na predajcov, ako je tomu u terminálov alebo bankomatov.

Keďže záujem zo strany podvodníkov o falšovanie kariet výrazne klesá, stále zostávajú pomerne veľa zastúpene pri niektorých typoch útokov. Preto je nutné s týmito útokmi rátať a reagovať na nich primeranou ochranou. Stále pretrvávajúci význam týmto hrozbám je možné pritakávať na jednoduchosť, s ktorou môže páchateľ získať informácie o karte a tie napr. ďalej predávať.

4 NÁVRH ODPORÚČANÍ A OPATRENÍ

Opatrenia a odporúčania v tomto prípade predstavujú dodatočné možnosti a spôsoby, ktoré môžu pomôcť a hlavne znížiť pravdepodobnosť a riziko zneužitia platobnej karty. Taktiež sa tieto odporúčania sústredia aj na to, ako zakročiť pre zníženie dopadu v prípadoch, kedy skutočne už k zneužitiu príde. Tieto navrhnuté riešenia a odporúčania nie sú náhradou bežných bankových opatrení a bodov podľa, ktorých je taktiež nutné postupovať a rešpektovať tieto odporúčania, ktoré sú dôležité pre ochranu a bezpečnosť platobnej karty.

4.1 Cielenie odporúčania

Cielenie odporúčaní je hlavne spravidla pre najväčšiu skupinu ľudí, ktorým sa najčastejšie stávajú zneužitia platobných kariet. Cieľová skupina ľudí pre navrhované opatrenia a odporúčania sú vybraní ľudia vo veku približne 15 až 26 rokov, hlavne študenti a osoby, ktoré študujú. Podľa aktuálnych prieskumov je práve táto skupina najviac aktívna v širokom využívaní platobnej karty, či už výbery z bankomatu, platby u obchodníka, internetové platby a podobne. Aktuálne prieskumy Raiffeisen banky hovoria, že 52% ich klientov medzi študentami aspoň jedenkrát mesačne absolvujú výber z bankomatu a 47% absolvuje aspoň jedenkrát mesačne platbu u obchodníka buď na internete alebo priamo v kamennom obchode. Ďalšie zameranie je na internetové platby, keďže u študentov najmä vysokých škôl prevláda v drvivej väčšine platenie cez internet, pri ktorých sú vytýčené špecifické riziká, na ktoré budú reagovať navrhované odporúčania a opatrenia.

4.2 Odporúčanie pre zníženia dopadu zneužitia

Odporúčanie pre zníženie dopadu zneužití ráta s tým, že informácie o platobnej karte už boli nejakým zo spôsobom odcudzené alebo už zneužité. Ak sa budú dodržiavať nasledujúce odporúčania a opatrenia je šanca na výrazné zníženie dopadu na finančné prostriedky držiteľa platobnej karty tým, že sa obmedzia prípadné prevedenia podvodných transakcií alebo včasné informovanie držiteľa karty o neautorizovanej akejkoľvek aktivite spájanej s jeho platobnou kartou.

4.2.1 Virtuálne platobné karty

Virtuálne platobné karty (e-cards) sú odlišné od bežných typov platobných kariet tým, že nie sú všetky údaje zoskupené na fyzickom plastovom nosiči ale namiesto toho sú tieto údaje len zhrnuté a je možné ich použiť pri väčšine platieb v CNP prostredí (niektoré platobné brány vyžadujú autorizáciu kódom poslaným v SMS držiteľovi). Tieto zoskupené údaje obsahujú meno držiteľa, číslo tejto karty a bezpečnostný kód CVV2/CVC2. Na prvý pohľad je takmer nemožné rozlíšiť tieto údaje od údajov, ktoré sú fyzicky vyobrazené na bežnej platobnej karte. Virtuálne platobné karty ponúkajú vyššiu bezpečnosť pri platbách v prostredí CNP, taktiež je výhodou, že tieto karty nie je možné použiť pri platbách mimo prostredia CNP. V prípadoch použitia tejto karty mimo prostredia CNP, či už v kamennom obchode alebo pokus o výber z bankomatu, nebudú tieto príkazy autorizované. V prípade, ak táto karta bude odcudzená, výrazne to znižuje možnosti zneužitia.

Bezpečnosť, ako taká, nie je odlišná od bežných platobných kariet. Pri riešení platby cez internet sú možnosti autorizácie skrz meno, bezpečnostný trojmiestny kód alebo pomocou 3-D Secure. Vzhľadom na nepoužívaný fyzický nosič je možnosť odcudzenia, straty alebo skimmingu nemožná. Samozrejme za predpokladu že klient, majiteľ údajov tieto informácie bezpečne uchová.

4.2.2 Typy platobných kariet v CNP a CP prostredí

Táto kapitola popisuje možnosti, ako znížiť prípadný dopad útokov. Možnosti, ako znížiť dopad môže byť používanie rôznych platobných kariet pre rôzne typy platobných kanálov. V dnešnej dobe síce moderné platobné karty ponúkajú maximálnu možnú flexibilitu. Týmto potom môže byť jedna karta použitá na všetky typy platieb. Avšak pri strate, krádeži alebo údajov z platobnej karty zvyšuje na druhú stranu aj širokú škálu možného zneužitia.

Ako možnosť obrany môže byť používanie dvoch rôznych kariet. Jedna karta pre platby v obchodoch a výbery z bankomatov, táto karta je zároveň blokovaná na internetové platby. Pri tomto prípade je zneužitie spôsobom prečítania údajov z karty obmedzené. Druhá zvolená karta by bola funkčná len pre internetové platby, čo zvyšuje jej bezpečnosť, kedže na kartu nie je možné použiť skimming alebo rýchle odčítanie údajov. Preto v tomto prípade je návrh na zníženie rizika zneužitia v používaní dvoch platobných kariet. Virtuálna karta a klasická platobná karta, ktorá má blokované používanie v CNP prostredí.

Odporúča sa virtuálnu kartu dobre uschovať a v rámci užívateľského záujmu ju aj uchrániť pred zneužitím.

4.2.3 Informovanie o zneužití platobnej karty

Všeobecným pravidlom býva, čím skôr sa na zneužitie platobnej karty príde, tým menší je negatívny dopad pre klienta a držiteľa karty. Dôležité je, čo najrýchlejšie zistenie prvých transakcií, ktoré neurobil držiteľ karty. V dnešnej dobe síce banky používajú systémy a softvéry, ktoré väčšinou odhalia neautorizovanú transakciu, avšak nebýva to pravidlo a nie všetky neautorizované transakcie sú odhalené včas.

Najlepší spôsob ako predchádzať zneužitiu je dôkladné a pravidelné sledovanie aktivity platobnej karty. Ak klient kontroluje platby až pri mesačnom výpise, častokrát už je príliš neskoro. Namiesto pravidelného kontrolovania je chytré využiť službu zasielania informačných správ za určitý poplatok alebo na základe podmienok účtu. Tieto informačné správy sú vo forme SMS alebo emailu. Klient si sám stanoví, ktoré transakcie mu budú pre istotu chodiť aj do SMS schránky v mobilnom telefóne. Odporúčané je informovanie aspoň všetkých debetných transakcií formou SMS správy. Banka, v čo najkratšom čase po transakcii bude klienta týmto spôsobom informovať. Príchod tejto informácie je spravidla do niekoľkých sekúnd alebo maximálne pár minút po vykonaní transakcie. Klient si následne sám analyzuje situáciu, či transakciu urobil on alebo osoba, ktorej kartu zveril. Pri následnom preverení a vážnom podozrení zo zneužitia jeho karty môže potom postupovať podľa postupu, ktorý je vo väčšine napísaný na karte alebo sám kontaktovať priamo banku, ktorá urobí následné opatrenia. Týmto klient zabráni opakovanému zneužitiu svojej platobnej karty.

4.2.4 Predplatené platobné karty

Jednou z možností, ako zabrániť prípadnému zneužitiu bežne používanej platobnej karty je používanie predplatenej karty, práve namiesto bežne požívanej karty, ako je napr. debetná alebo kreditná karta. Predplatenú platobnú kartu je možno použiť rovnako, ako ostatné karty. Je možné pomocou nej realizovať všetky bežné úkony ako napr. platba u obchodníka alebo výber z bankomatu či platba na internete. Rozdiel spočíva v tom, že od ostatných typov kariet nie je napojená na bežný debetný alebo kreditný účet klienta a môže disponovať len finančnými prostriedkami, ktoré na túto kartu klient sám vopred

vložil. V prípade zneužitia predplatenej karty, tak môže páchateľ vybrať maximálne sumu, ktorá bola na karte vložená.

Nevýhodou tejto karty je nízka pohodlnosť, keďže klient musí kartu pravidelne dobíjať a to sumou takou aby ho prípadné zneužitie karty zasiahlo, čo najmenej. Ďalšou nevýhodou sú vysoké poplatky, ktoré sú spojené s každým dobíjaním karty a aj správou a udržovaním. Predplatená platobná karta má svoje opodstatnenie a využívajú ju najmä klienti, ktorí cestujú do viacej rizikových krajín, kde je vyššia pravdepodobnosť krádeže karty alebo údajov z tejto karty.

4.3 Odporúčania pre zníženie a predchádzanie zneužitiu

Odporúčanie, ktorých cieľom je zníženie pravdepodobnosti zneužitia platobných kariet. Zameriavajú sa na ukrytie údajov a informácií, ktoré môžu byť kľúčové pre realizáciu neoprávnenej platby. K odcudzeniu týchto údajov môže prísť pri platbe napr. u obchodníka, preto je v záujme zákazníka aby tieto údaje nevystavoval možnosti predania ich akýmkoľvek spôsobom obchodníkovi. Čím zabráni aby obchodník vedome alebo nevedome poskytol predmetné kľúčové údaje páchateľovi. Ďalšou z možností ako zabrániť úniku údajov je kartu zamykať, tak aby sa k nim nedostala iná osoba, ktorá by údaje mohla zneužiť. Týmto spôsobom sa zabráni prípadnému úniku finančných prostriedkov.

4.3.1 Uzamknutie, blokácia platobnej karty

Niektoré banky poskytujú svojim klientom uzamykanie ich platobných kariet. Cez iný prístup ku karte môže klient samovoľne svoju platobnú kartu sám zablokovať alebo odblokovať. Tento spôsob sa osvedčil v prípade, ak klient zistí zneužitie alebo môže z akéhokoľvek dôvodu kartu zablokovať a potom na svojom rozhodnutí aj následne kedykoľvek odblokovať.

Konkrétne prevedenia tohto princípu môžu klientovi ponúknuť napr. odblokovania a zablokovanie za pomoci určitého limitu. Klient si môže nastaviť maximálny limit, ktorý určí napr. obmedzený počet transakcii, výšku transakcie a ďalšie priebehy transakcií. Tieto limity si klient môže nastaviť dočasne, vtedy ak doba nastaveného limitu vyprší sa následne prejde do štandardného režimu približne do niekoľkých hodín, v niektorých prípadoch to môže byť aj niekoľko dní z dôvodu prebiehajúcich transakcií.

Raiffeisen banka ponúka možnosti uzamknutia a odomknutia na základe príkazu klienta. Kartu môže klient odomknúť pomocou SMS správy, táto správa odomkne kartu

len na jednu transakciu alebo si môže klient zvoliť odomknutie na určitú dobu. Tento spôsob je veľmi bezpečný a nie je jednoduché prelomiť takto vyriešené bezpečnostné opatrenia.

Tieto dva spôsoby zvyšujú bezpečnosť zabezpečenia platobnej karty. Keďže umožňujú realizáciu platby len v čase, ktorý si klient sám určí. Týmto sa dá z veľkou pravdepodobnosťou zaručiť, že prebehnú len platby a príkazy, ktorých si klient bude vždy vedomý. Avšak ani toto opatrenie nemôže celkom zaručiť možnosť zneužitia, keďže blokovanie a odblokovanie je možné riešiť len reálne v čase pre online autorizované platby. Ak sa karta zneužije pre offline transakciu, vtedy nie je možné toto riešenie aplikovať. Pre offline platby je toto opatrenie nevyužiteľné.

4.3.2 Odporúčania pri platbe na internete

Platobné portály na internete ponúkajú zvýšenú bezpečnosť, plnia rolu prostredníka medzi kupujúcim a predávajúcim. Tieto portály ochraňujú platobnú kartu a všetky údaje zadávané pre platbu skryjú pred predávajúcim. Tvoria týmto určitú záruku pred zneužitím. Obchodník nezíska kľúčové údaje platobnej karty od zákazníka, čím sa eliminuje únik týchto údajov na maximum.

Platobné portály, ktoré patria medzi najpoužívanejšie sú PayPal alebo TrustPay. Platobným portálom a zároveň sprostredkovateľským e-shopom, ktorý je v dnešnej dobe najviac používaný je AliPay a Aliexpress. Nevýhoda v tomto sprostredkovaní je akceptovanie tejto platby zo strany obchodníka. Nie každý obchodník akceptuje niektorý z platobných sprostredkovateľských portálov. Taktiež je nevýhodou možný poplatok, ktorý si tieto portály za sprostredkovanie transakcie zaúčtujú. Spravidla je tento poplatok vo výške 5%, kedy ale v prípade zneužitia, nedodania tovaru alebo služby následne rieši sprostredkovateľský portál a daný spor vyrieši. Zároveň daný prostredník ručí za to, že údaje o karte nebudú v žiadnom prípade mimo kontroly zákazníka a údaje cez neho nie je možné zneužiť obchodníkom ani treťou osobou, ktorá by sa mohla pokúsiť získať údaje na základe prebiehajúceho platobného styku.

ZÁVER

V teoretickej časti sa práca zaoberala spôsobmi, ktorými v dnešnej dobe prebiehajú operácie s platobnými kartami a následnými technológiami a bezpečnosťou. Ďalej boli detailne rozobrané slabiny jednotlivých typov technológií a aké typy útokov sú najčastejšie využívané s hlavným cieľom odcudzenia finančných prostriedkov.

V praktickej časti je prehľad neoprávnených získaní finančných prostriedkov pomocou krádeže, či už karty alebo údajov z karty. Taktiež je spracované porovnanie vybraných oblastí a krajín sveta, ktoré do určitej miery odrážajú aktuálny stav úrovne zabezpečení a hrozieb individuálne pre každú svetovú oblasť.

Následne boli navrhnuté odporúčania a opatrenia, ktoré sa zamerali na zníženie dopadu na rôzne spôsoby zneužitia a taktiež predchádzanie zneužitiu a znižovanie pravdepodobnosti. Pre zvýšenie je samozrejme možnosť navrhnuté odporúčania a opatrenia kombinovať medzi sebou a tým celkovú bezpečnosť zvýšiť. Niektoré opatrenia sú bohužiaľ z určitého pohľadu na systém poplatkov menej zaujímavé, avšak tie môžu byť naopak veľmi zaujímavé v budúcnosti, ak sa zmení poplatkový sadzobník predplatených kariet.

Cieľom bolo porovnanie informácií a dát o útokoch, ktoré boli vo vybraných oblastiach dosiahnuté. Na základe týchto štatistík bolo urobené vyhodnotenie, kedy sa určili najčastejšie využívané útoky podľa vybraných oblastí.

Možné rozšírenie tejto práce do budúcnosti môže byť spracovanie detailnejšieho porovnania svetových oblastí. Oblasti odpovedajú najmä podľa použitej EMV technológie a práve to rozdeľuje svet na Afriku, Ameriku, Európu a Áziu. Dané krajiny rozdeliť podľa použitej technológie EMV. K Ázii patrí aj oblasť Pacifiku a Austrálie. Európa je rozdelená na oblasť SEPA a krajiny mimo tohto priestoru. USA v tomto prípade môže byť zohľadnená na migráciu EMV technológie. Získanie viac informácií a detailnejšie údaje o kriminalite spájanej s platobnými kartami. Avšak toto je veľmi zložité hlavne vo vyspelejších krajinách, pri ktorých sú štatistiky a informácie skreslené hlavne dôvodom výberu len dominantnej krajiny z jednotlivej vybranej oblasti.

ZÁVER V ANGLIČTINE

The theoretical part of the work dealt with the ways in which nowadays underway operations with payment cards and downstream technologies and safety. There were also detail discussed groin different types of technology and what types of attacks are the most commonly used with the primary purpose of theft of funds.

The practical part is an overview of improperly obtaining funds through theft, either the card or on the card. It is also prepared a comparison of selected region countries in the world and, to some extent reflects the current state-level security and threat individually for each world region. Subsequently, the proposed recommendations and measures that focus on reducing the impact the various methods of abuse as well as preventing and reducing abuse probability. The increase is of course the possibility to propose recommendations and measures to combine with each other and thus enhance overall security. Some measures are unfortunately from a certain perspective on the charging system less interesting, but those can be large-on the contrary it interesting in the future if changes charged tariff prepaid cards.

The aim was to compare the information and data on attacks that have been achieved in selected areas. On the basis of the evaluation it was made player when determined the most common attacks used by selected areas.

The possible extension of this work in the future can be more detailed processing the comparison of areas. The field respond mainly used by EMV technology, and this is what divides the world into Africa, America, Europe and Asia. The country divided by usage EMV technology. The Asia region includes the Pacific and Australia. Europe is divided into SEPA country and outside this space. US in this case, the reflected the migration of EMV technology. Getting more information and detailed data on crime associated with credit cards. However, this is very difficult especially in more advanced countries for which statistics are distorted information and mainly because of the choice only the dominant countries of the individual selected areas.

ZOZNAM POUŽITEJ LITERATÚRY

[3] JUŘÍK, P. *Platební karty: 1870-2006 : velká encyklopedie. 1. vydanie,* [cit. 2016-05-09]. Praha: Grada, 2006. ISBN 80- 247-1381-0.

[2] JUŘÍK, P. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet 1. vydanie,* [cit. 2016-05-09] Praha: Grada Publishing, a.s., 2003. 312 s. ISBN 80-247-0685-7.

[3] MÁČE, Miroslav. *Platební styk: klasický a elektronický*. 1. vydanie, [cit. 2016-05-09] Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.

[4] Platebné karty a ich druhy. *Penize.cz* [online]. [cit. 2016-05-09]. Dostupné z: http://www.penize.cz/15744-platebni-karty-a-jejich-druhy

[5] Platební karty - magnetický proužek. *IDnes.cz* [online]. 2005 [cit. 2016-05-09]. Dostupné z: http://finance.idnes.cz/platebni-karty-magneticky-prouzek-dt3-/bank.aspx?c=A051130_173803_fi_osobni_zal

[6] Čipové karty. *SystemOnline* [online]. 2013 [cit. 2016-04-05]. Dostupné z: http://www.systemonline.cz/it-security/cipove-karty.htm

[7] EMV technológia. *Evertecinc* [online]. 2016 [cit. 2016-05-09]. Dostupné z: http://www.evertecinc.com/es-es/solucionesparacomerciantes/emv.aspx

[8] Nové komunikačné technológie. *Bezkontaktné platobné karty.* [online]. 2012 [cit. 2016-05-09]. Dostupné z: http://www.derivat.sk/files/casopis%202012/2012_Dec_Napolitano_Tkacova.pdf

[9] MONTAGUE, D. *Credit card fraud: the professional's guide to preventing credit card fraud in ecommerce, mail order and telephone order sales.* [online]. 2016 [cit. 2016-05-09]. Dostupné z: http://ijcsi.org/papers/IJCSI-10-3-2-172-179.pdf

[10] Platební karty - embosovaná. *Nové služby* [online]. 2013 [cit. 2016-05-09]. Dostupné z: http://www.novesluzby.cz/pojisteni-afinance.201/platebni-karty-debetni-kreditni-embosovana.20496.html

[11] Dumpster Diving Identity Theft. *The Value of Your Trash* [online]. 2016 [cit. 2016-05-09]. Dostupné z: http://www.spamlaws.com/dumpster-diving.html

[12] Social Networks. *Payments and Banking Intersect* [online]. 2012 [cit. 2016-05-09]. Dostupné z: https://www.kansascityfed.org/publicat/psr/briefings/psr-briefingdec2012.pdf

[13] Skimming. *Policie České Republiky* [online]. 2010 [cit. 2016-05-09]. Dostupné z: http://www.policie.cz/clanek/skimming.aspx

[14] Blog. *Mysmas.cz* [online]. 2013 [cit. 2016-05-09]. Dostupné z: http://mysmas.cz/blog-mizi-vam-z-uctu-penizeneznamo-kam

[15] MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů.* 1. vydanie. Brno: Masarykova univerzita, 2008 [cit. 2016-05-09], 125 s. ISBN 978-80-210-4556-9.

[16] Information Security. *Sony Says Credit Card Data Was Encrypted.* [on-line]. 2011 [cit. 2016-05-09]. Dostupné z: http://www.informationweek.com/attacks/sony-says-playstation-credit-carddata-was-encrypted/d/d-id/1097464

[17] DUBINSKY, Z. CBC News. *Technology & Science - New credit cards pose security problem.* [online]. 2010. [cit. 2016-05-09]. Dostupné z: http://www.cbc.ca/news/technology/new-credit-cards-pose-securityproblem-1.904220

[18] BROT, J., HRADECKÝ, M. *Platební prostředky, jejich ochrana a padělání. Praha: Ministerstvo vnitra, odbor vzdělávání a správy policejního školství a Policie ČR, Útvar pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování,* 2008 [cit. 2016-05-09], 160 s. ISBN: 80-7312-055-0.

[19] SVOBODA, J. *Placení kartami je v ČR bezpečnější neţ v EU* [online]. Právo, 2008 [cit. 2016-05-09]. Dostupné z WWW: http://www.novinky.cz/clanek/140974-placeni-kartami-je-v-cr-bezpecnejsi-nez-v-eu.html

[20] EUROPEAN CENRAL BANK. *Second report on card fraud.* [on-line]. 2016 [cit.2016-05-09]. Dostupné z: https://www.ecb.europa.eu/stats/html/index.en.html

[21] CANADIAN BANKERS ASSOCIATION. *Credit Card Fraud and Interac Debit Card Fraud Statistics - Canadian Issued Cards.* [on-line]. 2016 [cit. 2016-05-09]. Dostupné z: http://www.cba.ca/en/component/content/publication/69-statistics

[22] Federal Trade Commission. *Consumer Sentinel Network Data Book for January* [on-line]. 2016 [cit. 2016-05-09]. Dostupné z: https://www.ftc.gov/policy/reports

[23] Australian Bankers Clearing Association. *Fraud Statistics Calender Year*. [on-line]. 2016 [cit. 2016-05-09]. Dostupné z: http://www.apca.com.au/payment-statistics/fraud-statistics/2015-financial-year

[24] The Banking Association South Africa. *Sabric Card Fraud Statistics*. [on-line]. 2016 [cit. 2016-05-09]. Dostupné z: http://www.banking.org.za/news-media/new-noteworthy/economy-and-finance

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

Atď.	A tak ďalej
ATM	Automated Teller Machine
A pod.	A podobne
CNP	Card Not Present
CP	Card Present
CVC/CVV	Bezpečnostný kód prítomný aj na magnetickom prúžku
CVC2/CVV2	Bezpečnostný kód, ktorý nie je na magnetickom prúžku
EÚ	Európska únia
EMV	Europay Mastercard Visa
ECB	Európska centrálna banka
Napr.	Napríklad
JAR	Juhoafrická republika
POS	Point Of Sale
SEPA	Platobná únia pre 28 krajín EÚ a 6 krajín mimo EÚ
USA	Spojené štáty americké

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: ANALÝZA TRHU S BANKOVÝMI ČIPOVÝMI A HYBRIDNÝMI KARTAMI VO SVETE (DOKUMENT NBS)

Národná banka Slovenska

PODSTATA ČIPOVEJ KARTY

Historicky pojem "čipová karta" je známy od r. 1972 a pochádza z Francúzska. Je to platobná karta, ktorej princípom je záznam údajov do programovateľného mikroprocesora umiestneného na karte. Ide o druhú generáciu platobných kariet po platobných kartách s magnetickým prúžkom. V súčasnosti existuje veľké množstvo druhov mikročipov pre najrôznejšie oblasti použitia (telefónne, bankové, zdravotné..). Môžeme ich zaradiť do troch základných skupín:

- pamäťová karta (Memory Card) - karta má pamäť, ale žiadnu "inteligenciu", funkcie karty sú naprogramované pri výrobe, nespĺňa požiadavky bezpečnosti, preto jej použitie je možné v oblastiach, pre ktoré táto podmienka nie je nutnosťou (napr. predplatné telefónne karty).
- logická karta (Hard-Wind Logic Card) - na rozdiel od pamäťovej karty zvyšuje úroveň bezpečnosti vložením tajného kódu, ktorý potvrdzuje právo na prístup k údajom uloženým v pamäti.
- mikroprocesorová karta (Microprocesor Card, Smart Card) - karta s "aktívnou inteligenciou". Čip umožňuje prístup k údajom a prevádzať ich zmeny len subjektom, ktoré sa preukážu prístupovými kódmi. Používajú sa v oblastiach vyžadujúcich vysokú bezpečnosť napr. bankové platobné karty.

Cieľom pre zavedenie čipových kariet je znížiť potrebu overovania transakcií v obchodnej sieti a bankomatoch v bankových centrálach. Ich základné vlastnosti určuje medzinárodná norma ISO 7816, na ktorú nadväzujú svojimi špecifikáciami jednotliví užívatelia.

V bankovníctve sa používajú mikroprocesorové karty, ktoré umožňujú bezpečne uložiť informácie potrebné k overeniu osobného kódu klienta PIN alebo iný overovací prvok (napr. fotografia), prípadne aj finančnú čiastku, ktorú má klient k dispozícii. Výška finančnej čiastky sa postupným používaním karty znižuje až do ďalšieho doplnenia v banke alebo v zákaznickom termináli. Použitie karty pri operáciách s menšími finančnými čiastkami nevyžaduje spojenie s bankomatom alebo platobným terminálom v reálnom čase s autorizačným systémom.

Jednou formou čipových kariet sú tzv. hybridné karty - kombinácia kreditných a debetných kariet, ktoré by mali byť orientované na malé a stredné platby a elektronické peňaženky, ktoré slúžia predovšetkým pre malé transakcie.

Perspektívne čipové karty nahradia karty a magnetickým prúžkom.

VÝHODY PLATOBNEJ KARTY

Používanie **hotovosti** pri úhradách má nevýhodu anonymity, nízkej bezpečnosti, nákladovosti na spracovanie, úschovu a dopravu ako pre obchodníka tak pre banku, nepohodlnosti pre obchodníka a zákazníka, nákladovosti na tlač a ochranu proti falšovaniu, nutnosť zmeny na požadovanú menu pri zahraničnom styku, je bez úrokového výnosu.

Pri **platobných kartách** odpadá anonymita klienta a možnosť straty alebo odcudzenia peňazí. Poznanie platcu - klienta má marketingovú hodnotu, ktorú využívajú banky hlavne a USA a Veľkej Británii.

Výhody pre držiteľov karty - jednoduché použitie, vyššia bezpečnosť, disponibilnosť s peňažnými prostriedkami na účte, celoštátne alebo medzinárodné použitie, zúčtovanie prebehne až po prevzatí tovaru alebo služby, odpadajú zmenárenské poplatky a kurzové straty, osobný predstih, doplnkové služby (napr. poistenie), núdzové služby pri strate alebo krádeži karty, prehľad transakcií.

Výhody pre obchodníkov - jednoduché použitie, vyššia bezpečnosť, viac zákazníkov, väčší obrat, zaručená platba, väčší predstih, udržanie sa v konkurenčnom prostredí.

Výhody pre vydavateľov karty - zníženie hotovostného obratu, získanie nových klientov, marketingové delenie klientov, udržanie sa v konkurenčnom prostredí, odstránenie nákladných prevádzok, ponuka komplexných služieb pre organizácie a podnikateľov, poplatok za kartu, poplatky za transakcie s kartou, u úverových kariet úrok.

Hlavnou výhodou mikroprocesorových kariet oproti kartám s magnetickým prúžkom je zníženie rizika nelegálneho zásahu do údajov. Zároveň dávajú možnosť lokálne overiť totožnosť držiteľa karty (napr. pomocou zadania číselného kódu). Mikroprocesorové karty umožňujú spojenie viacerých aplikácií do jednej karty (banková, predplatná, bonusová karta).

SÚČASNÝ TRH

Francúzsko - aj keď princíp záznamu údajov do programovateľného mikroprocesoru umiestneného na karte bol patentovaný vo Francúzsku v r. 1972, francúzske banky

sa rozhodli používať pre domáce transakcie čip od r. 1992 z bezpečnostných dôvodov. V r. 1993 bolo vo Francúzsku vydaných viac ako 21,8 mil. čipových kariet, ktoré sa mohli použiť v sieti 530 000 obchodných miest a 18 735 bankomatov. Bolo nimi prevedených 2,188 miliardy transakcií. Zavedením čipových kariet sa znížili straty z podvodov, rástol obrat, znížili sa telekomunikačné náklady.

Rok	1987	1988	1989	1990	1991	1992	1993
% z obratu (CB)	0,27	0,17	0,16	0,13	0,11	0,08	0,04

Vývoj podvodných transakcií s platobnými kartami vo Francúzsku

Zdroj: Groupement doe Cartes Bancaires - Ten years of the "CB" interbanking system, 1994

Príklad Francúzska dokazuje, že najväčšími užívateľmi čipových kariet budú banky. Medzinárodné bankové platobné systémy Europay/MasterCard a VISA spolupracujú od r. 1994 na tvorbe normy pre bankové platobné karty. Táto spolupráca je nutná predovšetkým z dôvodu zjednotenia požiadaviek na čipy a ich snímače, ktoré sa používajú v bankomatoch a platobných termináloch (aby prechod k novému záznamovému médiu bol čo najľahší a najlacnejší). Aj keď náklady na výmenu alebo obmenu zariadenia sú veľmi vysoké, v budúcnosti by sa mali prejaviť ako výhodná investícia tým, že sa

- znížia telekomunikačné náklady (nemusia sa overovať údaje v bankovom centre. Finančný limit a PIN budú bezpečne uložené v pamäti karty)
- zvýši sa bezpečnosť (banka stanoví podmienky, za ktorých môže klient kartu použiť, v závislosti na jeho finančnej situácii a zároveň má zabudované zabezpečovacie čipy proti zneužitiu)
- vzniká nová úžitková hodnota pomocou zabudovania doplnkových služieb, čím sa zvýši komfort pre klienta a znížia sa náklady na vydávanie karty.

  Väčšia časť špecifikácie pri medzinárodnej normotvorbe bola ukončená.

Zostáva stanoviť vnútorné normy pre karty Eurocard/MasterCard, edc/Maestro, VISA, Electron a pre medzinárodné elektronické peňaženky.

V **Českej republike** sa uskutočnil prvý pilotný test s predplatnou čipovou kartou na čerpacích staniciach spoločnosti Tank-Plus v spolupráci I.S.C.MUZO a Komerční banky

v r. 1995. Podobné testy uskutočňuje Česká sporiteľňa a ČSOB. Združenie pre bankové karty v súčasnosti jedná s ČSOB o podmienkach vydávania tohto druhu bankovej karty.

V rozvoji technológie platobných kariet bol v r. 1993 v Českej a Slovenskej republike inštalovaný prvý platobný terminál, ktorého dodávateľom bola americká spoločnosť VeriFone, ktorá sa na svetovom trhu platobných terminálov podielu cca 40 %. Terminály VeriFoneTranz 330 pracujú v režime on-line, využívajú sa k prenosu údajov verejnej údajovej siete EuroTel, alebo bežnej telefónnej siete. K terminálom môže byť káblom pripojená klávesnica pre zadávanie osobného kódu PIN. Od r. 1995 je v ponuke výkonnejší terminál VeriFoneTranz 395 a klávesnica pre PIN, 5 kombinovaná so snímačom čipových kariet (bankových, zákazníckych a predplatných). Tým sa vytvárajú podmienky pre pripojenie sa k medzinárodnej norme čipových kariet Europya/Master Card - VISA, ktorá by mala vstúpiť do platnosti v tomto roku. Bariérou pre rozšírenie platobných terminálov u nás je však nízka kvalita telekomunikácií.

Česká republika predpokladá v r. 1996 vybaviť bankomaty a platobné terminály hybridnými snímačmi, t.j. magnetický prúžok/čip, zaviesť medzinárodné platobné karty EuroCard/Master Card, edc/Maestro a VISA vybavené čipom, realizovať pilotný projekt elektronickej peňaženky združenia pre bankové karty.

ODPORÚČANIA PRI ZAVÁDZANÍ ČIPOVÝCH KARIET

Na základe doterajších praktických skúseností krajín, ktoré zaviedli používanie platobných čipových kariet sa odporúča:

- vytvoriť spoločnú bankovú organizáciu, ktorá bude koncentrovať špecialistov a techniku,
- zamerať sa na jednoduchosť projektu, £ zaistiť, aby vedenie bánk bolo dobre informované a schopné správne rozhodovať o problematike platobných kariet,
- nespoliehať sa na výrobu,
- monitorovať skúsenosti a návrhy užívateľov.