JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

PEDAGOGICKÁ FAKULTA

A

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

FAKULTA MANAGEMENTU V JINDŘICHOVĚ HRADCI

BAKALÁŘSKÁ PRÁCE

2011/2012 **autor: Karel Beneš**

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

PEDAGOGICKÁ FAKULTA

A

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

FAKULTA MANAGEMENTU V JINDŘICHOVĚ HRADCI

Skimming, scanning a padělání platebních karet

Autor: Karel Beneš

Vedoucí práce: doc. JUDr. Dr. Jan Hejda

Studijní program: Sociální pedagogika, specializace bezpečnostně právní

Termín odevzdání bakalářské práce : 31.3.2012

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: 2010/2011

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

Jméno a příjmení:	**Karel Beneš**
Osobní číslo:	**P09994**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Sociální pedagogika**
Název tématu:	**Skimming, scanning a padělání platebních karet**
Zadávající katedra:	**Katedra pedagogiky a psychologie**

Z á s a d y p r o v y p r a c o v á n í

Cílem práce je popsat a vysvětlit možnosti zneužití platebních karet podle jednotlivých metod se zaměřením na vytvoření metodicko didaktického průvodce občana v prevenci a ochraně platebních karet před jejich zcizením a zneužitím. V práci bude provedena komparace jednotlivých ochranných prvků u vybraných subjektů platebního styku.

Prohlášení

Prohlašuji, že bakalářskou práci na téma

„Skimming, scanning a padělání platebních karet“

jsem zpracoval samostatně a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal, způsobem ve vědecké práci obvyklým.

Dále prohlašuji, že v souladu s § 47b zákona č.111/1998 Sb. v platném znění, souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedením zákona č. 111/1998 Sb. zveřejněny posudky školitele i záznam o průběhu a výsledku obhajoby kvalifikační práce.

Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

České Budějovice, dne 4. března 2012

.....

Karel Beneš

Poděkování

Na tomto místě bych chtěl především poděkovat doc. JUDr. Dr. Janu Hejdovi za odborné podněty, rady a pomoc při zpracování mé bakalářské práce.

Anotace

Bakalářská práce se zabývá bezhotovostními platbami pomocí platebních karet a internetu. Práce je určena jako průvodce pro občana v prevenci a ochraně v bezhotovostním platebním styku. V první části práce jsem popsal základní rozdělení platebních karet, jejich možnosti a zabezpečení, upozornil jsem na jejich zneužitelnost a uvedl rady, jak se bránit proti zneužití. V druhé části práce jsem se věnoval elektronickému obchodování, zabezpečení pomocí elektronického ověřování a bezpečnostních protokolů a využitelnosti elektronických peněženek. Ve třetí části jsem popsal problematiku skimmingu. Ve čtvrté části jsem se zabýval finančním arbitrem, který plní úlohu ochrany spotřebitele před poskytovateli platebních služeb. V páté části jsem uvedl doporučení, jak s platební kartou zacházet, aby nedošlo k jejímu zneužití.

Annotation

This thesis deals with non-cash payments using credit cards and the Internet. This work is meant as a guide for a citizen in prevention and protection for non-cash payments. In the first part of the work I described the basic dividing of credit cards, their capabilities and security. I pointed out the possibility of their misuse and gave advices how to defend against the misuse. In the second part I devoted to electronic trading, security through electronic verification and safety protocols and serviceability of electronic wallets. In the third part I described the problems of skimming. In the fourth part I dealt with financial arbiter, who plays the role of protecting consumer against providers of payment service. In the fifth part I gave recommend dations how to handle credit card to provide its unauthorized use.

Obsah

Úvod

Platební karta, jako nástroj bezhotovostní platby, se čím dál více stává součástí našeho života. Největší výhoda používání tohoto platebního prostředku spočívá v jeho bezpečnosti oproti držení peněz v hotovosti. Držitel platební karty má možnost se díky množství bankomatů a platebním terminálům dostat téměř kdykoliv a kdekoliv bez problémů ke svým financím.

V návaznosti na masový rozvoj nových informačních a telekomunikačních technologií došlo k řadě významných změn právě v oblasti bankovnictví, a to jak v nabídce služeb ze strany bankovních ústavů, tak i celkového přístupu ke klientovi. Téměř všechny bankovní ústavy po celém světě nabízí svým klientům možnost spravovat své účty pomocí moderních komunikačních prostředků, jako je například mobilní telefon nebo počítač s připojením na internet. Tento způsob komunikace je pro klienty velmi pohodlný a také časově výhodný, na druhé straně přináší však také určitá rizika a nebezpečí, která se týkají zejména technických zabezpečení elektronického bankovnictví. Elektronické bankovnictví se neustále vyvíjí, zvyšují se také nároky klientů bankovních ústavů a ty musejí na tyto nároky reagovat.

V době internetu lidé přecházejí od plateb svých závazků na poštách k platbám přes elektronické bankovnictví, od placení v hotovosti k platbám kartami, od nákupů v kamenných obchodech k nákupům v internetových obchodech, od návštěv bank k úpravám svých účtů přes online bankovnictví. Důvody těchto kroků jsou zřejmé a pochopitelné. Lidé se vždy snaží ušetřit co nejvíce času a věci si usnadnit. Je mnohem rychlejší a pohodlnější zadat platební příkaz u svého počítače, než běžet na poštu nebo banku a zde ho vyplňovat.

I přes všechny zmiňované výhody si lidé neuvědomují, jaká jim vznikají rizika používáním platebních karet v bankomatech, využíváním platebních terminálů a realizováním platebních transakcí přes internet. Zlepšení informovanosti a zvýšení bezpečí při realizaci bezhotovostního styku je hlavním cílem této bakalářské práce. Ve své práci popíši a vysvětlím možnosti využití platebních karet, ale také upozorním na rizika, která hrozí při používání platebních karet a jak těmto rizikům předcházet.

Troufám si říci, že každý člověk dnes ví, co je to platební karta a k čemu slouží. Běžní zákazníci bank se však již hůře orientují v jednotlivých druzích platebních karet a jejich zabezpečení ze strany banky. Přitom každý spotřebitel může učinit kroky k tomu, aby jeho karta, případně informace uložené na platební kartě, nebyly zneužity.

1 Platební karty

Několik faktů týkajících se platebních karet. V současné době je v České republice vydáno celkem 9,85 milionu platebních karet. Z tohoto množství je 7,4 milionu debetních karet, 2,5 milionu kreditních karet a přes 290 000 charge karet. Počet obchodních míst akceptujících platební karty je 67 324 a počet bankomatů na území České republiky je 4 022. Lidé v současné době dávají přednost placení platební kartou na obchodních místech před výběrem finanční hotovosti z bankomatu.

Na konci 90. let 19. století někteří obchodníci ve Spojených státech amerických zavedli kovové štítky, na kterých bylo vyraženo číslo klienta. Při placení zákazník předložil štítek, obchodník opsal číslo ze štítku na účet a nakonec klient stvrdil transakci podpisem.

V roce 1914 začala vydávat americká telefonní a telegrafní společnost Western Union Telegraph Company platební kartu, pomocí které mohli zákazníci telefonovat a zasílat telegrafy bez okamžitého zaplacení. Zákazník na konci každého měsíce obdržel soupis zaslaných telegrafů a uskutečněných telefonátů, jejich jednotlivé ceny a jejich součet, které pak jednorázově zaplatil šekem nebo příkazem z banky. Společnost se tímto způsobem snažila udržet klienty a přimět je k častějšímu používání svých služeb s možností bezhotovostního placení. Tento příklad následovaly další telegrafní a obchodní společnosti např. Mobil Oil, AT&T, Sears Roebuck nebo letecké společnosti. Karty byly vyrobeny z plechu.

Jedny z prvních platebních karet byly vyráběny z tvrdého papíru nebo plechu. Plechové karty s papírkovým textem na lícové straně si nechala patentovat společnost Farrington. Tyto karty se používaly až do 50. let 19. století. Zákazník podepisoval účty, které se shromažďovaly v účtárně společnosti a následně se klientům rozesílaly faktury. Klienti od společnosti získali bezúročný úvěr. Tyto karty se nazývají Charge Card.

Použití prvních „pravých bankovních“ platebních karet se uskutečnilo v roce 1951. Tuto kartu vydala Franklin National Bank v New Yorku. Karty byly vydávány důvěryhodným klientům banky, kdy obchodníci platili bance poplatek za provedené platby. Klienti byli povinni uhradit provedené nákupy do 30, 60 nebo 90 dnů. Použití platebních karet bylo velmi jednoduché a tento základní princip funguje do současné

doby. Klient u obchodníka předložil kartu a podepsal účet. Obchodník si zkontroloval platnost platební karty a porovnal podpis se vzorovým podpisem na kartě, případně s dokladem totožnosti, pokud na kartě nebyl vzorový podpis.

Co se týká věrnostních karet, tak jejich velkou nevýhodou bylo jejich omezené použití v obchodní síti společnosti, která je vydávala.

V roce 1958 vydala Bank of America platební kartu, která již byla vyrobena z plastu. Placení touto kartou bylo možné pomocí mechanických snímačů – imprinterů (hovorově žehlička).

V České republice byla vydána první platební karta v roce 1988 Živnostenskou bankou jako dispoziční karta k tuzexovému účtu. Od poloviny roku 1989 vydávala Česká státní spořitelna svým klientům ke sporožirovým účtům karty k výběru z bankomatů.[1]

1.1 Druhy platebních karet

Platební karty lze rozdělit podle mnoha kritérií. Cílem této práce však není popisovat podrobné rozdělení platebních karet, proto popíši pouze základní rozdělení karet a podrobněji se budu věnovat zabezpečení platebních karet, jejich možnostem a využití.

Rozdělení podle způsobu zúčtování

Debetní karty

Debetní karty jsou u nás nejběžnější používanou platební kartou. Jsou spojeny s účtem klienta. Z debetních karet jsou čerpány finanční prostředky, které jsou uloženy na účtu, jinými slovy, jsou čerpány peníze majitele účtu. Vybrané finanční prostředky

[1] Juřík, P., 2003, *Encyklopedie platebních karet Historie, současnost a budoucnost peněz a platebních karet*, Grada Publishing, a.s., s.312. ISBN 80-247-0685-7

jsou strženy z účtu ihned nebo během několika dnů. Pokud na účtu není dostatek finančních prostředků, není výběr nebo transakce povolena. Debetní karty jsou převážně využívány k výběrům z bankomatů. Lze je využít i k platbě do zahraničí, častěji jsou však k tomuto účelu využívány karty kreditní.

Kreditní karty

Zásadní rozdíl v kreditní kartě oproti debetní kartě je, že peníze, které držitel platební karty čerpá, nejsou jeho, ale bankovního ústavu, který kreditní kartu vydal, tudíž si je klient půjčuje. U banky, která vydala kartu, však nemusí být zřízen ani účet. Před vydáním platební karty však bankovní ústav požaduje předložení potvrzení o výši příjmu, na jehož základě stanoví limit výše čerpání úvěru. Výhodou kreditní karty je placení v obchodech, kdy je následně možné využít bezúročného období. Každý měsíc banka klientovi zašle výpis plateb provedených kreditní kartou, na němž je uvedena celková čerpaná částka a minimální povinná splátka. Zde má klient na výběr, buď splatí celou dlužnou částku najednou v rámci bezúročného období, anebo se rozhodne splácet postupně a zaplatí prozatím jen minimální splátku. Minimální částka splátky se pohybuje ve výši 5 – 10% z čerpaného úvěru. Pokud klient splatí celou dlužnou částku do konce bezúročného období, nezaplatí nic navíc a mezitím mohl své peníze na splátku úročit na spořicím účtu a dosáhnout tak malého zisku. Pokud se však rozhodne jít cestou splátek, musí si uvědomit výši úroků. Dokud nesplatí celou dlužnou částku, je z dlužné částky účtován poměrně vysoký úrok. Kreditní kartu je tedy výhodnější využívat jen v bezúročném období a splatit celou dlužnou částku. Bezúročné období se většinou pohybuje od 45 do 55 dní od data transakce. Naopak výběry finančních prostředků z bankomatů jsou u těchto typů karet velmi nevýhodné. Za výběr z bankomatu si bankovní ústav zpravidla ihned strhne několik procent z vybrané částky a navíc ihned po výběru nabíhají úroky. Kreditní karty jsou vydávány dobrým klientům banky nebo podle ohodnocení bonity klienta.

Charge karty

Charge karta je velmi podobná kreditní kartě. S touto kartou je také možné platit v obchodech a provádět výběry v bankomatech, aniž by klient měl dostatek finančních prostředků na svém účtu. Stejně jako u kreditní karty si klient od bankovního ústavu finanční prostředky půjčuje. Výše úvěru je však podstatně vyšší než u kreditní karty a může činit i více než půl milionu korun. Tuto kartu však může získat jen klient, který

má opravdu velkou důvěru banky a vysokou bonitu. Žádná banka by nepůjčila tak vysokou finanční hotovost klientovi, u kterého by si nebyla jista, že jí bude tato hotovost navrácena. Rozdíl oproti kreditní kartě je také v době splácení úvěru. Úvěr v tomto případě nelze splácet několik měsíců. Princip této karty je takový, že úvěr se čerpá během jednoho kalendářního měsíce. Klient obdrží výpis, kde se dozví, v jaké výši čerpal úvěr a do kdy ho musí splatit. Na úhradu dlužné částky má pak zpravidla 14 dní až měsíc. Velmi důležité je zdůraznit, že klient za úvěr neplatí žádné úroky. Za vydání této karty a vedení účtu se můžou však poplatky ročně vyšplhat i na několik tisíc korun. Taktéž výběry z bankomatů jsou u tohoto typu karet velmi nevýhodné, stejně jako u kreditních karet. Je nutné si uvědomit, že charge karta je spíše prestižní záležitostí a klienta, který má tuto kartu k dispozici, většinou výše poplatků nezajímá.

S charge kartou jsou spojeny i určité výhody, které se týkají například cestovního pojištění, které se vztahuje jak na držitele karty, tak až na tři jeho spolucestující. Další výhodou vztahující se k cestování je pojištění na hrazení léčebných výloh, zpoždění letu, ztráty či odcizení zavazadel apod. Díky této kartě může držitel získat různé slevy, například na ubytování v hotelech nebo jsou mu umožněny volné vstupy do letištních salónků nebo některých klubů.

Nákupní úvěrové karty

Nákupní úvěrová karta umožní klientovi čerpat úvěr. Úvěr poskytuje úvěrová společnost. Tento úvěr slouží výhradně k nákupu spotřebního zboží. Pro využití v praxi je nutná smlouva mezi obchodníkem a úvěrovou společností. Kartu si lze objednat v obchodě nebo přes internet. Obvykle stačí vyplnit dotazník a karta je klientovi doručena poštou. Tyto karty často využívají nízkopříjmové skupiny, které nemají jinou, výhodnější možnost získání finančních prostředků. Pokud ji již klient musí použít, doporučení zní, jen v nejnutnějších případech, a to při náhlé a neočekávané potřebě řešení finančních nedostatků. V případě, že takovou kartu bude klient používat k běžné denní potřebě a nákupům, pomalu se dostane do začarovaného kruhu placení splátek a vysokých úroků. Výhodou úvěrové karty je její vydání zpravidla zdarma, rychlost vyřízení, jednoduchost schvalování a při nepoužívání karty absence poplatků. Mezi nevýhody této karty patří vysoké úroky ihned od okamžiku transakce, skryté poplatky a výpisy.

Rozdělení karet podle způsobu provedení

Elektronické platební karty

Elektronické karty jsou nejrozšířenější v České republice. Do této skupiny jsou zařazeny karty asociací VISA Electron a Maestro. Karty jsou použitelné pouze pro transakce, které jsou on-line ověřeny v kartovém centru, tedy pro výběry z bankomatů a platby u obchodníků disponujících elektronickým platebním terminálem. Výhodou těchto karet je, že jsou většinou vedeny zdarma v balíčku produktu příslušné banky (účet). Další výhodou jsou nízké poplatky za blokaci ztracené či odcizené karty a téměř nulová možnost zneužití zablokované karty.

Embosované platební karty

Mají plasticky (reliéfně) vytištěny veškeré údaje o majiteli karty, platnosti, číslu karty. Kromě platby přes elektronický terminál, umožňují platbu tak, že obchodník vloží kartu do imprinteru a otiskne veškeré údaje z karty na účet, který pak zákazník podepíše. Každý obchod má nastavenou výši útraty, tzv. floor limit, kterou mohou zákazníci provést bez nutnosti platbu ověřit. Pokud chce zákazník provést u obchodníka vyšší platbu, provádí se telefonické ověření. Embosované karty je možno použít na více místech než karty elektronické. Daní za tuto výhodu embosované platební karty je vyšší cena za vydání, vedení či blokaci karty a jistá možnost zneužití karty i po nahlášení její ztráty či odcizení. U této karty je problematické její zablokování v případě ztráty. Karta je pak zařazena na tzv. stoplist, neboli listinu ztracených či odcizených karet, kterou banka rozešle obchodníkům a bankovním partnerům. Celý proces však trvá řádově i dny a banku stojí nemalé finanční náklady. S embosovanou platební kartou lze provádět i elektronické operace. V takovém případě se na ni vztahují stejná pravidla jako u elektronických platebních karet.

Rozdělení podle druhu záznamu

Karty s magnetickým proužkem

Magnetický proužek se nachází na zadní straně karty. Tento proužek nese veškeré nutné informace k provedení dané platby nebo výběru z bankomatu, tedy údaje o kartě a jejím držiteli. Po držiteli karty je pak při vlastní transakci vyžadován většinou pouze podpis. Na magnetickém proužku není uložen PIN (personální identifikační číslo), proto tento typ karet není tak bezpečný jako karty čipové. Blíže o magnetickém proužku bude uvedeno v problematice padělání platebních karet.

Čipové karty

Paměťovým médiem u čipových karet je zabudovaný mikroprocesor (čip), do kterého lze bezpečně uložit informace potřebné k ověření osobního kódu klienta. Do těchto čipů je možné nejen vpisování údajů, ale i jejich mazání a přepisování. Nevýhodou čipových karet je méně obchodních míst, na kterých s nimi lze platit, ale zato jsou mnohem bezpečnější. Průkopníkem v zavádění čipových karet byla Francie, kde jsou karty úspěšně používány už od 90. let. V České republice se první čipová karta objevila teprve v prosinci 2002 u Komerční banky. V dubnu 2003 následovala ČSOB. V budoucnu by měly být všechny elektronické karty vybaveny čipem. Banky potom ponesou větší odpovědnost za zneužití karty.

Protože karta s magnetickým proužkem již svůj potenciál vyčerpala, rozhodly se bankovní platební systémy vytvořit potřebnou infrastrukturu pro zavedení čipových karet. Dlouho však banky váhaly, zda novou technologii zavést, protože některé analýzy ukazovaly, že řídit riziko zneužití platebních karet lze efektivně i bez čipu a náklady na jejich celosvětové zavedení se odhadovaly na 40 miliard USD.

Po 30 letech, kdy byly magnetické karty součástí infrastruktury platebních karet, banky došly k poznání, že musí být proveden další technologický skok. Magnetický proužek již vyčerpal své technické možnosti, takže se stal nepoužitelným pro nové distribuční kanály (e-commerce, m-commerce).[2]

[2] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.104

Důvody pro zavedení čipových karet v bankovnictví:

1. Úspora provozních nákladů – významnou položkou provozních nákladů magnetických karet jsou telekomunikační a autorizační náklady na ověření transakcí. Čipové karty umožní bezpečně uložit důvěrná data přímo v paměti mikroprocesoru, a tím snížit potřebu on-line autorizací a s nimi spojených telekomunikačních poplatků přibližně o 80 – 90%.

2. Ochrana proti podvodníkům – čipové karty nabízejí díky svému technickému řešení zvýšenou aktivní i pasivní ochranu proti zneužití karty neoprávněnou osobou, podvodným duplicitním transakcím a proti výrobě padělků. V paměti karty může být bezpečně uložen PIN klienta nebo jeho digitalizovaný podpis, fotografie apod.

3. Úvěrový management – vydavatel karty může do paměti čipové karty vložit finanční limity transakcí, které mohou být ověřeny off-line. Tyto limity je možné kdykoliv změnit, během on-line transakce (např. v bankomatu), podle vývoje finanční situace klienta. Transakce se autorizují on-line jen při překročení stanovených parametrů, při náhodně vybrané platbě a u podezřelých transakcí (z podnětu obchodníka).

4. Doplňkové služby – čipové karty mohou přinést vyšší užitnou hodnotu bankám a uživatelům platebních karet. Paměť čipové karty umožní její souběžné použití pro bankovní i nebankovní aplikace (např. bonusy obchodních domů, identifikace zdravotních pojišťoven, GSM aj.)

5. Dálková změna aplikací – je možné dodatečně doplňovat, měnit, mazat, aktivovat a zmrazovat jednotlivé aplikace karty.[3]

Podle použité technologie, stupně zabezpečení, počtu aplikací a míry flexibility rozdělujeme tři základní druhy čipových karet. Na základě těchto skutečností je rovněž závislá i výrobní cena karty.

1. Paměťová karta – u této karty není kladen důraz na bezpečnost, jedná se především o předplatní karty. Tyto karty obsahují program a mají jednoduchý mechanismus k identifikaci jeho držitele. Výrobce těchto karet již ve výrobě programuje jejich využití.

[3] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.104

2. Paměťová karta s autentizační logikou - tyto karty jsou bezpečnější než karty předchozí a to vložením tajného kódu, který potvrzuje právo na přístup k datům uloženým v paměti. Funkce karet je taktéž programována již ve výrobě.

3. Mikroprocesorová karta – tyto karty jsou již vybaveny tzv. aktivní inteligencí. Karty vybavené mikroprocesorem již umožňují přístup k uloženým datům, případně jejich změnám. Změny může provádět oprávněná osoba, která se prokáže přístupovými kódy. Programové vybavení takovéto karty je již schopno rozpoznat i pokus o neoprávněný zásah a v takovém případě je možné veškerá data a programy z karty vymazat a kartu zablokovat – je to však závislé na naprogramování karty.[4]

Karty s mikroprocesorem se skládají z těchto částí:

– Vstup/Výstup (Input/Output) – spojuje čip s okolním světem.

– Centrální řídicí jednotka (Central Processing Unit - CPU) – je řídicí jednotkou procesoru pracující na základě 8, 16 nebo 32 bitové architektury. Centrální řídicí jednotka řídí a kontroluje veškeré operace, které na kartě probíhají.

– I/O Controller – řídí tok dat mezi terminálem nebo bankomatem a procesorem.

– Paměť ROM (Read Only Memory) – jeden z hlavních typů paměti sloužící k uložení operačního systému karty. Program je do karty zaznamenán výrobcem a již není možné ho změnit.

- Paměť RAM (Random Acces Memory) – druh paměti, která se používá k uložení výsledků ověřujících vstupní kódy. Data se po odpojení od zdroje ihned smažou.

- Paměť EEPROM (Electronically Erassable Programmable Read Only Memory) – jedná se o paměť, na kterou se ukládají data dle druhu karty (bankovní karta, věrnostní karta apod.). Tuto paměť lze kdykoliv využít i přepsat. Vkládání dat je omezeno pouze životností karty. Informace v této paměti mohou být jak volně přístupné, jako je např. číslo karty, jméno držitele, tak i utajené, jako je PIN, digitální podpis apod.

- Crypto Processor – doplňuje prvek určený pro provádění bezpečnostních a šifrovaných výpočtů.

[4] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.101

– Chip Operating System (COS) – používá informace uložené v ROM a provádí operace podle zadání aplikace. Existují dva druhy COS – obecný, používaný většinou čipů a dále speciální, který používají jen vybrané aplikace.[5]

Přesto, že mají čipové karty tzv. logické zabezpečení, šifrování a autentizaci a je takto velmi ztíženo podvodníkům zneužití těchto karet, jsou navíc tyto karty zabezpečeny i fyzickými překážkami. Zejména se jedná o tzv. speciální krycí štíty, které jsou umístěny přímo na čipu. Jejich velikost lze vyčíslit řádově v μm. Speciální krycí štíty zabraňují zejména pozorování činnosti mikroprocesoru za využití elektronických mikroskopů, nežádoucí elektromagnetické stimulaci a interferenci a zásahu založeném na manipulaci se strukturou čipu změnou logických bloků.[6]

Podle způsobu komunikace čipových karet s okolním prostředím rozeznáváme karty kontaktní a bezkontaktní. Bezkontaktní karty pracují na principu rádiových vln za využití aktivní nebo pasivní antény, která je zapuštěna po obvodu do povrchu karty. Komunikace mezi kartou a přijímačem může být šifrována. Bezkontaktní karty jsou velmi výhodné v případech, kdy dochází k velmi častému využití, jako jsou např. vstupní systémy, permanentky na lyžařských vlecích apod., nebo pokud potřebujeme využít kartu na více služeb, jelikož na karty je možné nahrát více aplikací. Životnost čipových karet výrobci garantují podle provedení na 100 000 až 1 milión transakcí a dobu uchování dat kolem 10 let. Čipová karta je schopna fungovat v teplotním rozmezí od -25°C do 85°C.[7]

Hybridní karty

Obsahují čip i magnetický proužek. Tyto karty tedy mají výhody obou předchozích karet. Lze je použít na všech obchodních místech a navíc jsou bezpečnější. Z výše zmíněného lze usoudit, že v budoucnu bude většina platebních karet vydávána jako hybridní.

[5] Juřík, P., 2003, *Encyklopedie platebních karet Historie, současnost a budoucnost peněz a platebních karet*, Grada Publishing, a.s., s.312. ISBN 80-247-0685-7, s.256
[6] Juřík, P., 2003, *Encyklopedie platebních karet Historie, současnost a budoucnost peněz a platebních karet*, Grada Publishing, a.s., s.312. ISBN 80-247-0685-7, s.257
[7] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.102

Laserové karty

U laserových karet je použit stejný princip záznamu dat jako u kompaktních disků. Mají vysokou kapacitu paměti, ale nedokážou účinně zabezpečit vložená data před neoprávněným přístupem. Laserová karta je velmi drahá.

1.2 Druhy rizik

Úvěrové ztráty – Představují ztrátu způsobenou nesolventností držitele karty. Jde o případy, kdy klient není schopen uhradit výdaje, které realizoval platební kartou (nejčastěji úvěrovou). Výše tohoto rizika je závislá na způsobu, jakým vydavatel karty (banka) provádí ověření bonity klienta, na míře rizika, které při tomto hodnocení vědomě akceptuje (obchodní riziko).[8]

Zneužití karty cizí osobou – Největší ztráty vydavatelů tvoří zneužití ztracených nebo odcizených platebních karet. Velmi důležité je, aby držitel karty kontroloval, zda ji stále vlastní a v případě její ztráty nebo krádeže, aby neprodleně informoval svoji banku. Banka provede tzv. stoplistaci karty[9] (pouze v případě embosovaných karet). Jedná se o trvalé a nezvratné zrušení práva používat platební kartu. Identifikační údaje klienta jsou zapsány na stoplist (mezinárodní databáze blokovaných karet). Tento seznam je rozšiřován mezi obchodníky, kteří používají mechanickou čtečku. Stoplistace je poměrně organizačně náročná, proto je poplatek za blokaci až 10x vyšší než blokace elektronické karty. Pokud dojde k odcizení elektronické karty je zapotřebí jí co nejdříve zablokovat, a to buď osobně na nejbližší pobočce banky, nebo telefonicky.

Zneužití nedoručené karty – Většina bank v rozvojových zemích zasílá platební karty klientům poštou v oddělené zásilce od PIN. Některé z takto doručených karet jsou během poštovní přepravy odcizeny a následně zneužity. Platební karta má čistý podpisový proužek, takže podvodník může podle jména klienta vytvořit svůj vlastní

[8] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.90

[9] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.90

vzorový podpis. V České republice naopak naprostá většina bank vydává platební karty na své pobočce.[10]

Padělky karet – Paděláním platebních karet se zabývají spíše velmi dobře organizované skupiny pachatelů. Výrobu padělků velmi ztěžují ochranné prvky na platebních kartách, které musejí společnosti vyrábějící karty neustále zdokonalovat, a to zejména z důvodu činnosti padělatelů.

Objednávkové služby – Zaplatit za zboží nebo služby je možné vybranými druhy platebních karet i prostřednictvím telefonu, dopisu, faxu nebo internetu. Jedná se o tzv. služby Mail/Telephone Order, kdy držitel karty sděluje dodavateli písemně, elektronicky nebo telefonicky číslo své karty a konec její platnosti. Dodavatel pak provede ověření transakce (autorizaci) a své zúčtovací bance předá prodejní doklad. Asi 26% všech podvodů s platebními kartami tvoří právě tento druh transakcí, kdy jsou zneužity údaje získané z platební karty. Dodavatelé jsou zúčtovacími bankami upozorněni na riziko ztrát, pokud držitel karty transakci odmítne a většina obchodníků s tímto rizikem i počítá. Jako jeden z prostředků prevence tohoto druhu podvodů je v některých zemích používán systém ověření adresy příjemce služby, tzv. Adress Verification System. Zboží nebo služby mohou být poskytnuty pouze na adresu držitele karty, nikoliv cizí osobě. Při telefonní nebo poštovní objednávce zboží (včetně internetu) musí být ověřena nejen platnost karty, ale i shoda jména a adresy příjemce s údaji držitele karty.[11]

1.3 Zabezpečení platebních karet

Nejrozšířenějšími platebními kartami jsou karty s magnetickým proužkem na rubové straně. Na ten lze zapisovat data na tři stopy, tzv. Tracky. Vydavatelé karet využívají k zápisu převážně dva z těchto Tracků.

Tento typ karet lze nejsnadněji padělat. Vyšší stupeň zabezpečení mají čipové karty, které mají na lícové straně čip a data jsou zapsána v čipu. Zde rozlišujeme karty

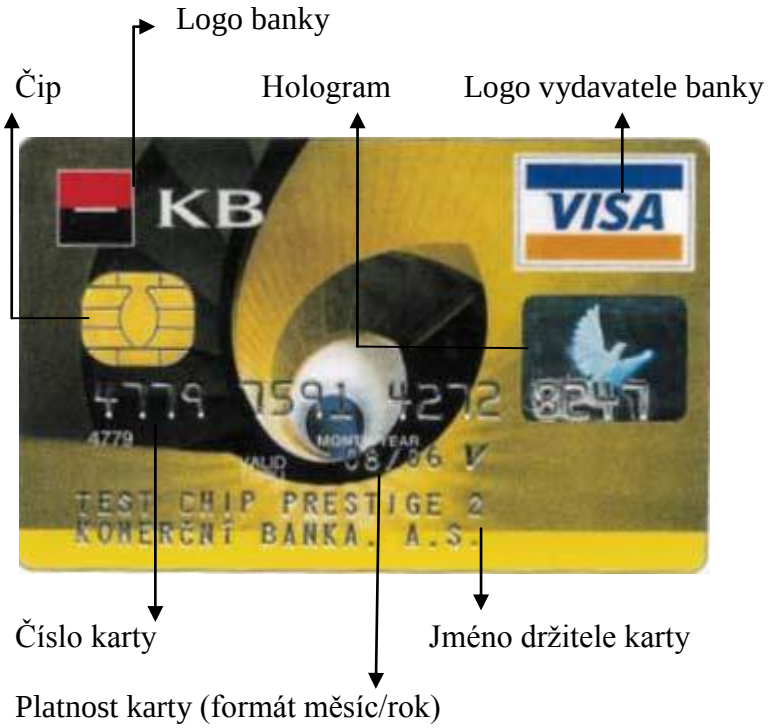
[10] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.91

[11] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.91,92

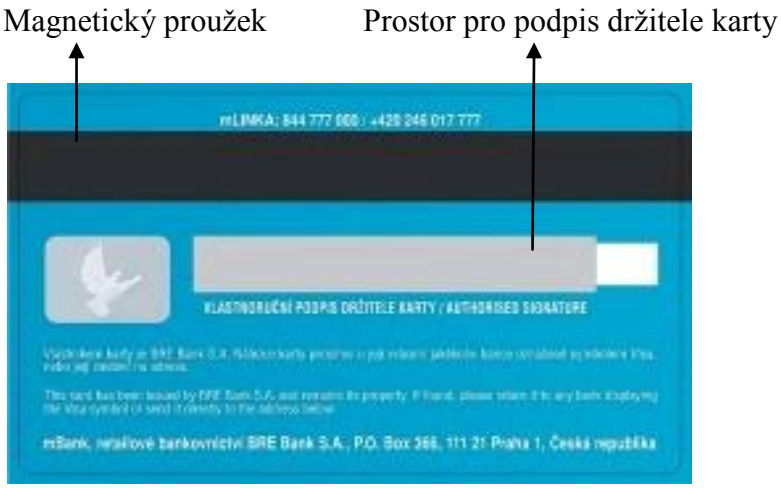
kontaktní a bezkontaktní. Kontaktní karty musíme vždy při provádění transakce zasunout do terminálu. U bezkontaktních karet lze kartu s čipem pouze přiložit k terminálu. Čipové karty jsou finančně náročnější na výrobu než karty s magnetickým proužkem.

Vydavatelské společnosti platebních karet se zaměřují na bezpečnost těchto zařízení, aby zabránily okrádání svých klientů. Mají však před sebou velmi nelehký úkol, protože každé další zavedené bezpečnostní opatření se projeví až po dlouhé době, nezřídka až po výměně veškerých vydaných platebních karet, což může trvat i roky. Až do ukončení celkové výměny platebních karet musí navíc být i nadále přijímány a musí fungovat i karty stávající. Pachatelé tak využívají vzniklé chyby v zabezpečení ve svůj prospěch.

Při platbách přes internet jsou zadávány informace, které jsou uvedeny čitelně na platební kartě společně s informacemi o majiteli karty, naopak při platbách přes terminály nebo při použití karty v bankomatu jsou načítána data, která jsou uvedena buď na magnetickém proužku, nebo čipu. Z důvodu bezpečnosti platebních karet se v budoucnu můžeme dočkat toho, že společnosti vydávající platební karty budou ukládat na platební karty biometrické údaje držitele, aby nedocházelo k neoprávněným manipulacím s finančními prostředky.



Obr. č. 1 Přední strana platební karty



Obr. č. 2 Zadní strana platební karty

Číslo karty

Vydavatelské společnosti používají svůj specifický formát zápisu čísla karty. U VISA karet začíná číslo karty vždy číslicí 4, u karty MasterCard číslicí 5. Karty VISA mají 13 místné číslo ve skupinách číslic 4-3-3-3 nebo 16 místné číslo ve 4 skupinách 4 číslic. Nápis vždy zasahuje do hologramu. Prvních 6 čísel identifikuje vydavatelskou banku. Společnost MasterCard používá pouze 16 místná čísla, jinak je systém zápisu stejný.[12]

Hologram

Jedná se o vizuální bezpečnostní prvek, díky kterému lze padělanou platební kartu odhalit na první pohled. Hologram je dvourozměrný nebo třírozměrný obraz, který se mění při pohybu karty.

Společnost MasterCard používá jako hologram své logo, které se během vývoje několikrát změnilo. V současné době se na platebních kartách objevují dvě propojené polokoule v pozadí s nápisem MasterCard a zároveň jsou polokoule lemovány

[12] HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání*, 2008. s. 160, ISBN 80-7312-055-0, s.75

mikrotextem MC. Hologram se umísťuje buď na přední stranu platební karty, nebo na zadní stranu vedle podpisového proužku. Hologram lze využít také jako magnetický proužek. Od září roku 2005 používá VISA hologram s letící holubicí, která představuje mezinárodní symbol míru. Zpravidla bývá umístěn na přední straně karty pod posledním čtyřčíslím čísla karty. Nově se však objevuje i na zadní straně jako u karet MasterCard.

Ultrafialové prvky

Dalším kvalitním ochranným prvkem jsou ultrafialové prvky, které jsou viditelné pod ultrafialovým světlem. Jedná se buď o znak asociace na přední straně karty, nebo o její název v podpisovém proužku.

Na platebních kartách MasterCard jsou ultrafialovým inkoustem vytištěna písmena MC ve spodní části přední strany. U karet VISA se na přední straně ve středu karty objeví letící holubice. Na novějších kartách VISA je holubice nahrazena písmenem V umístěným pod logem asociace.

Obr. č. 3 Ultrafialové prvky

Obr. č. 4 Ultrafialové prvky

Podpisový proužek

Všechny platební karty s magnetickým proužkem i čipem jsou opatřeny podpisovým proužkem. U platebních karet s magnetickým proužkem je nutný vlastnoruční podpis držitele platební karty, jelikož platební transakce je ověřována pouze na základě podpisového vzoru na kartě. Karta, která je bez podpisu, je považována za neplatnou. Také na platebních kartách opatřených čipem je nutný podpisový vzor, protože ne všichni obchodníci jsou vybaveni přístrojem s čipovou technologií a transakce pak probíhá za využití magnetického proužku. Podpisový proužek je vyroben ze speciálního materiálu, díky kterému jsou odhalitelné jakékoliv

změny původního podpisu. U karet je na podpisovém proužku poslední čtyřčíslí čísla karty.

Magnetický proužek – bude blíže popsán v kapitole padělání platebních karet.

1.4 Padělání platebních karet

V této části se budu krátce vracet k předchozím kapitolám, aby došlo k podrobnému vysvětlení. Pokud se pachatelům podaří získat záznamy z magnetického proužku karty, je zapotřebí tato data zapsat na jinou platební kartu. Data, která se nachází na magnetickém proužku, jsou specificky vygenerované řetězce, které se označují jako Track 1, Track 2 a Track 3 (Track 3 však nemusí být na kartě nahrán). Tyto řetězce identifikují kartu a umožňují systému ověřit, o který účet se jedná, aby mohl vydat požadované finanční prostředky a tyto prostředky odepsat z účtu. Jako další ochrana je na platební kartě umístěn PIN kód, případně čip. Pachatelé se převážně zaměřují na země, kde bankomaty, popřípadě platební terminály, nevyžadují jako ochranu čip, ale pouze magnetický proužek a PIN kód. Na výrobu padělané karty se převážně využívají tzv. čisté bílé plasty s magnetickým proužkem na rubové straně nebo se jedná o karty s jednoduchým nápisem na lícní straně, potiskem ve stříbrné nebo zlaté barvě a magnetickým proužkem na rubové straně. Tyto polotovary jsou snadno dostupné například jako klubové nebo vstupní karty, tudíž není problém si je opatřit. Mají standardizované rozměry jako pravé karty. Není však problém sehnat na „černém trhu“ i polotovary originálních karet. K nahrávání dat na platební karty existuje mnoho zařízení, která umožňují nahrávat data na všechny druhy platebních karet, a to do všech tří Tracků. Tyto zařízení je možné zakoupit bez potíží ve specializovaných prodejnách, kde však požadují ověření totožnosti. Tato zařízení umožňují opakovaně nahrát data na platební karty. Nákup těchto přístrojů je možné uskutečnit prostřednictvím internetu, kde v mnoha případech zákazník nemusí prokazovat svou totožnost. K dokončení padělané platební karty je dále zapotřebí software. Výhodou pro padělatele je, že samotný software není nutné instalovat a nezanechává tedy v počítači žádné stopy. Počítač tedy funguje pouze jako propojení mezi CD mechanikou a samotným přístrojem, který zapisuje potřebná data na platební karty.

Track na platební kartě:

Track 1

B4548767125007684^ Jan/Novak^1106101000000000012345678909874563 21

Základním zápisem je Track 1, který je určen pro zápis osobních karet. Číselný řetězec se skládá z několika částí. První část „B4548767125007684“. Na začátku řetězce je písmeno B, které obsahuje každý Track 1 jakékoliv společnosti vydávající platební karty. Za ním následuje číslo karty. Jedná se o stejné číslo, které je uvedeno na přední straně platební karty. Stříškami oddělený řetězec „^Jan/Novak^“ obsahuje jméno a příjmení majitele platební karty. Na závěr je uveden dlouhý řetězec „1106101000000000012345678909874563 21“. První čtyřčíslí označuje platnost platební karty ve tvaru rok a měsíc – YYMM. Další trojčíslí je servisní kód. Zbývající číselná řada je vygenerována v příslušné bance.

Track 2

4548767125007684=11061011234567890123

Na Tracku 2 je méně informací než na předchozím Tracku. Jedná se o starší zápis na karty a je zejména vydáván společnostem. První část „4548767125007684“ se skládá opět z čísla platební karty, které je odděleno znaménkem „=“. Na začátku druhé části je opět uvedena doba platnosti platební karty, dále servisní kód. Závěr číselné kombinace je opět vygenerován bankou stejně jako u Tracku 1. Tento zápis používají společnosti Visa a MasterCard. U ostatních společností se může formát zápisu lišit. Například u platebních karet AMEX je uvedeno pouze 15 čísel místo 16, jinak je formát řetězce stejný.

Track 3

014548767125007684==0302000000000000005000000000000006020===0=

U karet, které mají na magnetickém proužku nahraný i Track 3, začíná kód číslem 01 a pak je opět uvedeno číslo platební karty. Další část je oddělena symboly „==“ a následuje číselný kód, jehož kombinace není zveřejnitelná, ten je zakončen tvarem „===0=“.

Servisní kód na Tracku 1, případně na Tracku 2, určuje, zda karta vyžaduje ověření za pomoci čipu. Pokud je servisní kód 101, jedná se o starší typ platební karty a ověření čipu není podporované. V případě, že bude servisní kód 201, tak ověření za pomoci čipu je podporované, ale není vyžadováno. Pokud by bylo nutné vyžadovat ověření za pomoci čipu, muselo by být zařízení, které kartu zpracovává tímto vybaveno a podporovat ho.

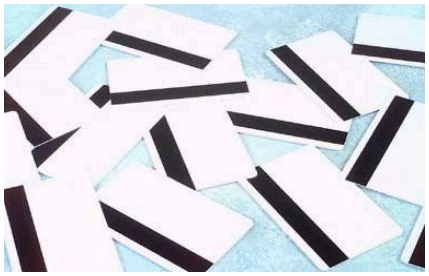
Na základě číselných kombinací uložených na Tracku 1, Tracku 2, a Tracku 3, je možné odlišit i jednotlivé zákazníky dle typů vydaných platebních karet. Banky vydávají více druhů platebních karet na míru jednotlivým zákazníkům, například společnost VISA vydává karty Electron, Classic, Gold, Platinum, Signature, Business. Podle prvních šesti čísel platební karty je možné zjistit, o jaký typ platební karty se jedná. Podle těchto informací se dá určit hodnota karty a zároveň se dá odhadnout i množství finančních prostředků, které jsou uloženy na účtu majitele platební karty. Na základě těchto informací se dá stav konta pouze odhadnout, není rozhodně zaručený. Je však pravděpodobné, že pokud klient obdrží od banky platební kartu VISA Business, tak nebude mít na účtu pár tisíc korun, ale stav konta bude řádově v desetitisících, spíše ve statisících korun.

U čipových karet bylo zabezpečení pomocí čipu brzy po jeho zavedení prolomeno. Rozdíl je však v tom, že pořízení platebních karet, které jsou opatřeny čipem, je mnohem nákladnější, než získání platební karty opatřené pouze magnetickým proužkem. Taktéž koupě zařízení sloužící k dekódování čipu a následně zařízení sloužící k nahrání dat získaných z čipu je pro pachatele velmi nákladná. Proto se padělatelé spíše soustředí na platební karty opatřené magnetickým proužkem. Pro přiblížení: cena zařízení pro dekódování platebních karet s čipem a zařízení sloužící k přenesení dat na tyto karty je přibližně 7 krát vyšší než u zařízení potřebného k padělání platebních karet s magnetickým proužkem.

Data získaná zneužitím platebních karet se dají využít mnoha způsoby. Dříve však musí pachatel získaná data stáhnout ze zařízení, na které je nahrál. Nejčastěji tak učiní pomocí mini USB připojení. Tato zařízení mají jednoduchý software, který je schopen přečíst flash paměť. Stejný způsob se používá i u PinPadu nebo kamery. K datům z platebních karet přiřadí PIN kódy a následně se rozhodne, jak s nimi naloží dál. Data lze prodat prostřednictvím internetu na „černém trhu“, nebo lze nahrát získaná

data na nové platební karty a díky tomu provádět výběry finanční hotovosti, popřípadě jiné finanční transakce. Kde vybírat finanční hotovost z padělaných platebních karet se musí pachatel rozhodnout podle mnoha kritérií. Ve zvolené lokalitě se musí nacházet terminály nebo bankomaty, které umožňují podporu platebních karet, které byly padělané. V některých zemích není možné platit s určitými druhy platebních karet. Dalším kritériem je uskutečnit co možná nejvyšší možný výběr z padělku karty.[13]

Obr. č. 5 Padělky platebních karet



Obr. č. 6 Padělky platebních karet

Obr. č. 7 Padělek platební karty

Obr. č. 8 Padělek platební karty

1.5 Plánovaný vývoj a použití platebních karet

Budoucí vývoj platebních karet směřuje k bezkontaktnímu placení. Princip tohoto placení spočívá v tom, že platební karta je pouze přiblížena k platebnímu zařízení, nebude nutné jí do terminálu zasouvat, taktéž se nebude zadávat PIN kód. Tento způsob placení je již rozšířen v některých slovenských, polských a německých obchodech. V České republice se tento způsob placení připravuje a během posledního

[13] HRADECKÝ, M. *Platební prostředky jejich ochrana a padělání*, 2008. s. 160, ISBN 80-7312-055-0, s.74

čtvrtletí roku 2011 bude spuštěn. Rychlejší odbavení bude zákazníky motivovat k platbám kartou. Obchodní řetězce ani banky za tyto platby nebudou, stejně jako u standardních plateb platební kartou, účtovat klientům žádné poplatky. Platby budou omezeny do výše 500 Kč za každý nákup, v případě placení vyšší částky bude i nadále nutné zadat PIN kód. Dle vyjádření bank spočívá hlavní těžiště plateb na hypermarketech, supermarketech, lékárnách, drogeriích, restauracích, kavárnách a dalších místech, kde dochází spíše k nižším platbám. Pro zavedení nového způsobu plateb bude zapotřebí, aby banky vydaly nové platební karty, které budou vybaveny potřebnou technologií. V České republice jsou však banky, které se tomuto typu placení příliš nepřiklánějí. Jedním z důvodů je zneužitelnost karty při odcizení. Jakmile dojde k odcizení platební karty a držitel karty ihned nezjistí krádež, pachatel může nakupovat s využitím bezkontaktního placení až do výše limitu, který má držitel karty nastaven, nebo do doby zablokování karty. Pachateli však stačí zpravidla velmi krátká doba ke zneužití karty.

V České republice byl také spuštěn nový zkušební projekt placení, a to pomocí mobilního telefonu. K tomuto projektu bylo vybráno cca 400 respondentů, kteří tímto způsobem mohou platit ve čtyřech hypermarketech Globus. Projekt byl spuštěn v červenci roku 2011.

2 Elektronické obchodování

E-commerce – je poměrně široký pojem používaný k označení veškerých obchodních transakcí realizovaných za pomoci internetu a dalších elektronických prostředků. Definice e-commerce podle Asociace pro elektronickou komerci (APEK) zní: *„Způsob obchodování, kde komunikace a transakce mezi účastníky obchodu je prováděna formou elektronické výměny dat.“*[14]

Při platbě platební kartou, či platbě za pomoci dat uvedených na platební kartě bychom měli být velmi obezřetní, jelikož sdělujeme velmi důvěrná data ke svému účtu. Při placení přes internet chybí účinný ověřovací mechanismus. Zaplatit kartou může kdokoliv, nemusí to tedy být oprávněný držitel karty. Karta nemusí být držena fyzicky, stačí zadat pouze údaje, které jsou na kartě. Proto je velmi důležité dodržovat určitá pravidla a postupy. Platební kartu nikomu nepůjčovat, nikomu nesdělovat údaje o kartě, vybírat si takové obchody, které jsou důvěryhodné a jsou vybavené bezpečnostními systémy.

Při platbě kartou přes internet je zapotřebí uvést údaje o platební kartě (číslo karty, datum ukončení platnosti, třímístný číselný kód CVC2/CVV2, který se nachází na zadní straně platební karty). Platební proces je realizován bankou, se kterou má obchodník uzavřenou smlouvu. Banka po zpracování platby informuje o výsledku transakce zákazníka a obchodníka současně pomocí e-mailu. Obchodník následně dodá zákazníkovi zboží.[15]

Proti získání, případnému zneužití dat na platební kartě se zejména používají níže uvedená zabezpečení.

[14] Stejskal, O. 2007. *E-kommerce*. Bakalářská práce, Masarykova univerzita v Brně, Ekonimicko –správní fakulta, Brno, s.15

[15] Džaferagič, A. 2008. Aplikace pro obchodování na internetu. Bakalářská práce, Masarykova univerzita v Brně, Fakulta informatiky, Brno, s.9

2.1 Zabezpečení za využití elektronického ověřování

V současné době je mnoho druhů zabezpečení týkajících se elektronického bankovnictví a je pouze na klientovi, který ze způsobů si vybere. Samozřejmě nejlepší jsou různé kombinace těchto zabezpečení. Nejčastější metody zabezpečení jsou založeny na moderní asymetrické kryptografii.

Z pohledu bezpečnosti má běžná internetová komunikace dva podstatné nedostatky. Odesílatel a příjemce dat nemají jistotu, že si data po cestě nepřečte třetí osoba. Příjemce zároveň postrádá záruku, že přijatá data opravdu pocházejí od deklarovaného odesílatele. Jako řešení obou jmenovaných problémů se nabízí asymetrické šifrování garantující pravost identity odesílatele a diskrétní přenos dat. Ačkoli historicky myšlenka asymetrické kryptografie vedla k vytvoření pestré škály technologií, její základní principy se nemění. Rámcem pro její efektivní použití je pak infrastruktura veřejných klíčů.

Lokálně ukládaná elektronická data bývají chráněna prostřednictvím tajného šifrovacího klíče. S jeho pomocí lze data zašifrovat i rozšifrovat. Šifrovací klíč má k dispozici majitel těchto dat, případně omezený okruh uživatelů, kteří ho udržují v tajnosti. Popisovaný způsob ochrany dat nazýváme symetrickou kryptografií. Pro lokální použití je ideální, s její aplikací na vzdálenou výměnu dat je to složitější. Strany komunikace musí mít předem k dispozici šifrovací klíč, takže vzniká problém jeho bezpečné distribuce. Jak roste počet účastníků komunikace, zvyšuje se riziko vyzrazení klíče.

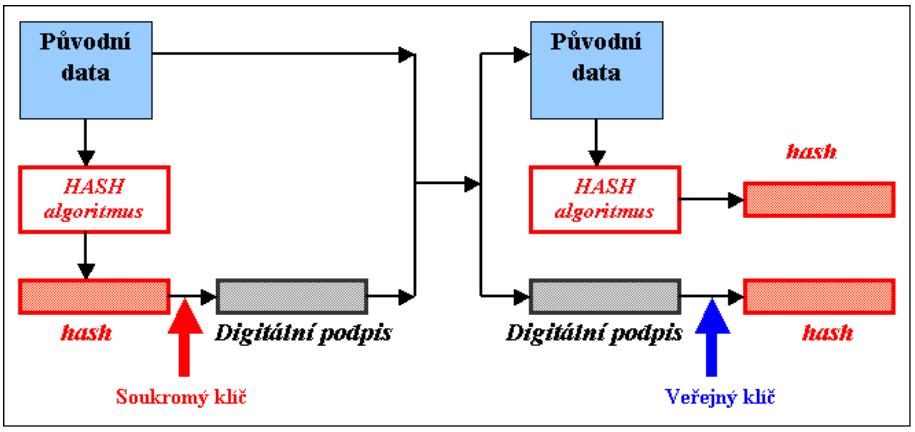
Asymetrické šifrování bylo navrženo právě proto, aby tyto potíže vyřešilo. Na rozdíl od symetrického šifrování se v něm nepracuje s jedním klíčem, ale s klíčovým párem. V tomto páru je jeden klíč soukromý a jeden veřejný. Klíče mezi sebou mají určitou matematickou souvislost, nicméně soukromý klíč prakticky nelze odvodit z klíče veřejného. Podstata asymetrické kryptografie spočívá v tom, že k zašifrování dat se používá jeden klíč a k jejich rozšifrování druhý klíč. Zatímco soukromý klíč jeho držitel uchovává v tajnosti, veřejný klíč lze volně distribuovat otevřenými

komunikačními kanály. Tím odpadá nutnost si předem bezpečnou cestou vyměnit společný šifrovací klíč a vysoké riziko jeho kompromitace.[16]

K nejpoužívanějším technologiím v dnešní době řadíme:

Digitální podpis

Digitální podpis je složený ze dvou algoritmů. První algoritmus se používá pro podepisování a druhý pro ověřování podpisu. Digitální podpis je implementován pomocí asymetrického šifrování. Při podepisování dat je nejdříve vypočten tzv. hash (digitální obdoba otisků prstů). V dalším kroku je hash zašifrován pomocí tajného klíče, čímž je vytvořen digitální podpis. Příjemce zprávy hash dešifruje za využití veřejného klíče, následně je z přijaté zprávy vypočítán hash kód a tento je porovnán se zaslaným. V případě, že se oba hash kódy shodují, došlo k ověření podpisu a zpráva je považována za důvěryhodnou.[17]



Obr. č. 9 Šifrování s digitálním podpisem

Elektronický certifikát

Elektronickým (digitálním) certifikátem se rozumí soubor dat v mezinárodně stanoveném formátu. Slouží k identifikaci osoby a při komunikaci dvou stran slouží k autentizaci komunikujících stran nebo k zajištění šifrování přenášených informací. Prvním krokem k získání certifikátu je zažádání. Zákazník si na svém počítači vygeneruje dvojici klíčů a elektronicky požádá o certifikát u dané certifikační autority.

[16] Thruschka, J., 2009, *Asymetrická kryptografie v praxi*, IT Security 2009, s. 6-7
[17] Kučerová, P. 2010. *Elektronické bankovnictví*. Diplomová práce, Masarykova univerzita v Brně, Ekonimicko –správní fakulta, Brno, s.59

Tuto žádost podepíše svým soukromým klíčem. Jakmile certifikační autorita ověří přijaté údaje, vystaví zákazníkovi digitální certifikát. Tento certifikát certifikační autorita podepíše svým soukromým klíčem a soukromý klíč připojí k certifikátu.[18]

Autorizační kalkulátor

Autorizační kalkulátor je elektronické zařízení, které dokáže generovat jednorázová hesla pro přístup k bankovní aplikaci. Tato zařízení bývají synchronizována se systémy banky tak, aby obě strany generovaly stejné klíče. Ty pak uživatel opisuje do aplikace a ověřuje tak svou totožnost jednoduše tím, že dokáže, že je majitelem příslušného kalkulátoru. Generovaná hesla mívají obvykle návaznost na operace, které jsou pomocí klíče generovány a uživatel je tak nucen do kalkulátoru uvádět informace jako je číslo účtu, částka se kterou je manipulováno a podobně. Z tohoto důvodu je velmi obtížné podvrhnout uživateli falešné formuláře k potvrzení, protože pokud nejsou na obou stranách zadány stejné údaje, klíče jsou neplatné. Jedná se o jednu z nejbezpečnějších metod autorizace uživatele.[19]

Autorizace pomocí SMS

Jedná se o metodu, která bývá běžně používána u většiny bank. Základem této metody je vygenerování jednorázového hesla. Tato služba je pevně spjata s mobilním telefonem, bez kterého by nemohla fungovat. Banka při požadavcích o autorizaci zašle klientovi SMS s potvrzovacím kódem, který je potřeba opsat zpět do aplikace. Jedná se o velmi bezpečnou metodu, která má ovšem také svá omezení. Součástí SMS bývají také stručné informace týkající se dané transakce jako je například částka, číslo účtu apod. Pokud uživatel tyto informace nekontroluje, je poměrně snadné mu podvrhnout falešnou webovou stránku a provést úplně jiný krok než ten, který uživatel očekává.

Uživatelské jméno a heslo

Obecně nejznámější a nejběžnější způsob autorizace uživatele. K potvrzení identity stačí znát uživatelské jméno a heslo klienta. Výhodou je snadná implementace tohoto autorizačního procesu a jeho nenáročnost na samotného uživatele. Bohužel

[18] Kučerová, P. 2010. *Elektronické bankovnictví*. Diplomová práce, Masarykova univerzita v Brně, Ekonimicko –správní fakulta, Brno, s.60

[19] Krčmář, P., *Autorizace v internetovém bankovnictví* [online]. 24.8.2006 [cit. 2011-11-17]. Dostupné z:< http://www.root.cz/clanky/autorizace-v-internetovem-bankovnictvi/>

autorizační údaje se mění jen zřídka a proto je možno je získat velmi jednoduše. Ve chvíli, kdy se pachateli podaří tyto údaje získat, ať už odposlechem nebo je vyloudí z uživatele, má neomezený přístup. Spolehlivost autorizace je navíc velmi závislá na zvoleném hesle.[20]

2.2 Bezpečnostní protokoly

SSL (Secure Socket Layer)

Jedná se o bezpečnostní protokol pro přenos dat internetem, který šifrováním znemožní, aby údaje z platební karty při transakci mohl někdo přečíst. Aplikaci tohoto protokolu lze rozeznat podle přidaného „s“ za *https://* nebo zobrazením symbolu „zavřeného zámku“ v prohlížeči.

SET (Secure Electronic Transaction)

Je systém zajišťující bezpečnost finančních transakcí na internetu. Jeho vývoj sahá do druhé poloviny 90. let. Na jeho vzniku se podílely největší karetní asociace VISA a MasterCard, IBM, Microsoft a další. SET je definován jako robustní protokol zajišťující maximální míru bezpečnosti a nezávislosti na použitých komunikačních prostředcích. Transakce je prováděna za využití digitálních certifikátů a ověřována pomocí kombinace digitálních certifikátů a digitálních podpisů mezi kupujícím, obchodníkem a bankou kupujícího. Podrobně lze toto zabezpečení vysvětlit tak, že SET umožnil, aby objednatel služby nebo zboží vložil číslo své platební karty do „uzavřené digitální obálky“ a tu společně s objednávkou poslal dodavateli (např. zásilkový obchod). Ten tuto „obálku“ odešle k ověření do autorizačního centra, které ověří platnost digitálního podpisu zákazníka i obchodníka a finanční krytí transakce. Poté potvrdí transakci obchodníkovi, který odešle klientovi zboží. Obchodník odešle informaci o platební transakci své zúčtovací bance, která zajistí její úhradu

[20] Krčmář, P., *Autorizace v internetovém bankovnictví* [online]. 24.8.2006 [cit. 2011-11-17]. Dostupné z:< http://www.root.cz/clanky/autorizace-v-internetovem-bankovnictvi/>

prostřednictvím clearingového a zúčtovacího centra.[21] Díky komplikovanosti a nákladnosti na implementaci se však systém příliš nerozšířil.

3D SET

Rozdíl oproti SET spočívá v tom, že software a digitální certifikáty nejsou umístěny v počítači klienta a obchodníka, ale na serveru banky (vydavatel karty, zúčtovací banka). Klient obdrží nebo si z internetu stáhne malý program (plug-in), který se při každé transakci spojí se serverem vydavatele a vyžádá si transakční certifikát. Aby tento certifikát získal, musí být klient registrovaným a verifikovaným uživatelem. Systém 3D SET podporuje také čipové transakce ve virtuálním světě, kde pak digitální podpis nahrazuje certifikát SET.[22]

3D-Secure

Každý, kdo typ e-commerce používá za využití platebních karet ví, že není možné ověřit si kupujícího a nahrát si data z magnetického proužku. Internetové transakce jsou anonymní a velmi rizikové. Z tohoto důvodu představila společnost Visa na počátku roku 2001 bezpečnostní protokol nazvaný 3D-Secure, kterým chtěla zlepšit bezpečnost transakcí v on-line režimu a urychlit rozvoj internetových plateb za využití platebních karet. Hlavním cílem 3D-Secure je možnost vydavatelů platebních karet skutečně si ověřit držitele během on-line nákupu s cílem snížit pravděpodobnost podvodného použití platební karty a zlepšit výkon transakce ve prospěch obchodníků, spotřebitelů a vydavatelů karet. Společnost MasterCard brzy následovala příkladu společnosti Visa. Společnosti Visa a MasterCard představují svůj program pod názvy „Verified by Visa“ a „SecureCode™“.

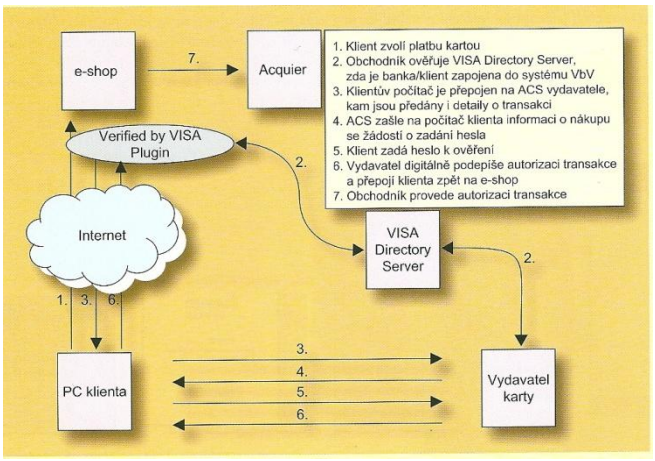
Obr. č. 10 Logo společnosti Visa

Obr. č. 11 Logo společnosti MasterCard

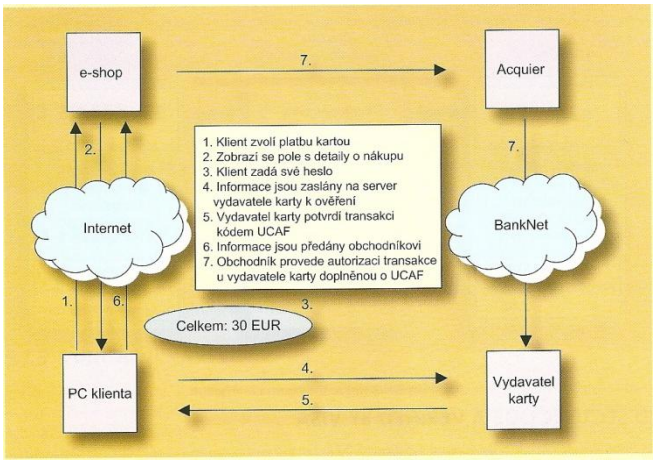
[21] Juřík, P., 2003, *Encyklopedie platebních karet Historie, současnost a budoucnost peněz a platebních karet*, Grada Publishing, a.s., s.312. ISBN 80-247-0685-7, s.239

[22] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.71Strana 71

Způsob platby je takový, že pokud se zákazník rozhodne platit za využití této služby, tak vyplní údaje z platební karty na internetových stránkách banky. Banka následně zajistí bezpečný zakódovaný přenos dat a obchodníkovi pouze sdělí výsledek autorizace. Tímto způsobem je zamezena možnost zneužití dat ze strany obchodníka a dále nedojde k přenosu chráněných dat přes nezabezpečenou veřejnou síť. Klientům bankovního ústavu plyne z této služby několik výhod, jako jsou vysoká bezpečnost a transparentnost probíhající transakce, vysoká důvěryhodnost obchodníků podporujících zabezpečení 3D-Secure služby a v neposlední řadě skutečnost, že veškerá komunikace probíhá mezi zákazníkem a bankovním ústavem bez prostředníka. Pro obchodníka spočívají hlavní výhody v bezpečnosti nabízeného řešení, ve vysoké důvěře držitelů platebních karet, zvýšení počtu uskutečněných transakcí a v rychlosti provedení platby. Bezpečnou komunikaci mezi klientem a obchodníkem zajišťuje služba SSL.



Obr. č. 12 Schéma transakce Verified by VISA



Obr. č. 13 Schéma transakce MasterCard SecureCode

Obecně platí, že pokud internetový obchodník nemá na svých webových stránkách uvedenou podporu 3D-Secure, jedná se o nedůvěryhodného obchodníka a nedoporučuje se s ním obchodovat.

2.3 Elektronické peněženky

Elektronické peněženky jsou určeny k bezpečným platbám menších částek na internetu. Při využití elektronické peněženky se nemusí vyplňovat údaje, které je nutné uvést při platbě kartou, tedy číslo karty, datum platnosti a kontrolní číslo. Elektronickou peněženku lze kdykoliv dobít z účtu v libovolné bance. Platba prostřednictvím elektronické peněženky je velmi rychlá a jednoduchá. Elektronická peněženka je bezpečná zejména ze dvou základních důvodů: 1. elektronickou peněženku lze dobít pouze takovou částkou, jakou potřebujeme k běžným platbám. Na platební kartě, je oproti tomu plný objem finančních prostředků. 2. při platbě z elektronické peněženky se nemusí, na rozdíl od platby kartou, zadávat žádná citlivá a zneužitelná data, pouze se zadává přihlašovací jméno a heslo. Systém PaySec využívá ještě důkladnější zabezpečení, a to prostřednictvím mobilního telefonu, kdy je zapotřebí platbu ještě autorizovat.

PayPal

PayPal je celosvětově používaný internetový systém, který se začal používat v roce 1998. V současné době je PayPal používán ve 190 zemích světa a podporuje platby v 25 měnách. Ve službě PayPal je možné platit i českými korunami.

PayPal má tři základní varianty, které jsou závislé na tom, o jaký druh služby bude mít zákazník zájem:

- Personal – slouží pro jednotlivce nakupující on-line
- Premier – slouží pro jednotlivce kupující a prodávající on-line
- Business – slouží pro právnické osoby

Vstup a využívání služeb PayPal je podmíněno registrací. Po registraci si zákazník zvolí jednu z výše uvedených tří variant. Rozdíly v jednotlivých variantách

jsou jak v ceně, tak v dalších dodatkových službách. Jedna z největších výhod tohoto systému je jeho zabezpečení. Zákazník si svůj účet dobijí dle vlastních potřeb. Tento systém je využíván jako platební brána pro bankovní karty. V praxi to vypadá tak, že zákazník si zašle na svůj účet PayPal potřebné finanční prostředky a následně z PayPalu zaplatí za požadované zboží prodejci. PayPal tedy působí jako zprostředkovatel. Zákazník prodejci nesdělí žádná důvěrná data týkající se jeho účtu ani jeho platební karty.[23]

PaySec

PaySec jako internetový platební systém začal fungovat v roce 2008 na základě spolupráce mezi Československou obchodní bankou a Poštovní spořitelnou. Služba PaySec byla založena na podobném principu jako služba PayPal. Jedná se o český internetový platební systém a jedná se o první platební systém zaměřený na mikroplatby prováděné bankou. V systému PaySec je možné platit pouze českou měnou. Mikroplatby jsou určeny na nákup drobného zboží v hodnotě stokorun, nanejvýš několika tisícikorun, není určen na nákup za několik desítek tisíc.

PaySec funguje na předplaceném principu. Při platbách nejsou finanční prostředky strženy z účtu přes platební kartu. Pro uskutečnění platby je nutné si nejprve založit konto, to se provádí přes internet. Pokud má zákazník založený účet u Československé obchodní banky nebo Poštovní spořitelny, probíhá převod pohodlněji. Není to však podmínkou. Systém PaySec může využívat zákazník kteréhokoliv bankovního ústavu.

PaySec má dvě základní varianty, které jsou závislé na tom, o jaký druh služby bude mít zákazník zájem:

- **Konto PaySec** - tato varianta je určena pro spotřebitele. Při registraci k této službě je podmínkou uvést pouze přihlašovací jméno, heslo, e-mailovou adresu a telefonní číslo. Pokud však zákazník zadá jen tato povinná data, je limitován vybitím a nabitím konta jen do určité výše. Pokud by zákazník nechtěl toto omezení akceptovat, musel by udat další osobní údaje, aby mohla být ověřena jeho identita.

U konta PaySec jsou zpoplatněny pouze tři služby:

[23] Školkay, E. 2011. *Platební systémy na internetu*. Bakalářská práce, Masarykova univerzita v Brně, Ekonimicko –správní fakulta, Brno, s.27

- nabití kartou on-line – poplatek 2% z částky,
- vybití na běžný účet u jakékoliv jiné banky v České republice - 2 Kč,
- příjem peněz přes platební tlačítko PaySec - 1 Kč.

- **Konto PaySec pro podnikatele** – u této varianty musí obchodník při registraci zadat mimo jiné i identifikační číslo organizace, tzv. IČO. Registrace u této varianty je o něco složitější, než u varianty předchozí. Taktéž poplatky za využívání služby jsou odlišné. Podnikatel mimo výše uvedené poplatky platí i procenta z přijaté platby od zákazníka.

Z důvodu vyšší bezpečnosti existuje i další varianta zabezpečení. V případě realizace vyšší platby je prováděno ověření transakce zasláním sms s kódem na uvedený telefon. Zákazník musí opsat kód, aby došlo k autorizaci platby. Zákazník si tuto doplňkovou službu může zřídit u platby jakékoliv výše, i když nízké platby nejsou touto autorizací podmíněny.[24]

2.4 Virtuální karty (e-card)

Nejedná se o plastovou platební kartu, ale pouze tzv. papírek, který obsahuje 16 místné číslo platební karty, dále časovou platnost a kód CVC2, který je obdobou PINu. Virtuální kartou nelze platit v obchodech a vybírat finanční hotovost z bankomatů, lze s ní pouze provádět nákupy prostřednictvím internetu. Zabezpečení při nákupu přes internet je zajištěno pomocí SSL. V pořadí platebních metod, seřazených dle bezpečnosti, se nachází na předposledním místě před samotnou platební kartou, ale i přesto zajišťuje dostatečnou bezpečnost.

[24] Školkay, E. 2011. *Platební systémy na internetu*. Bakalářská práce, Masarykova univerzita v Brně, Ekonimicko –správní fakulta, Brno, s.32

3 Skimmovací zařízení

Skimming – Ačkoliv má anglický výraz skimming mnoho různorodých významů, jako jsou: lízání smetany, přelétající, odpěňování, odstřeďování, odstruskování, oddestilování, stahování, sbírání, stírání, stěr, rychlé čtení, pěna nebo odpěnění, v oblasti padělání platebních karet označuje tento pojem podvodné jednání, při kterém pachatelé (padělatelé platebních karet) zkopírují údaje z magnetického proužku nebo čipu karty bez vědomí majitele platební karty. Pachatelé data získají pomocí zařízení, které je umístěno na bankomatech, pokladních terminálech v obchodech nebo na zařízeních kde se k platbě používají platební karty. Pachatel tak získá veškerá data z platební karty, a to z magnetického proužku i čipu, včetně PIN kódu. Cílem pachatele je nezákonné odčerpání finanční hotovosti z účtu majitele platební karty nebo prodej informací pocházejících z platební karty.

Pachatelé této trestné činnosti bývají považováni za špičku organizovaného zločinu, jejich techniky jsou dokonale připravené, taktéž vybavení je na perfektní úrovni a jsou velmi dobře organizovaní.

Jeden ze způsobů jak získat neoprávněně platební kartu je za pomoci tzv. libanonské smyčky. Libanonská smyčka je zařízení, které pachatel umístí na bankomat do prostoru vstupního otvoru platební karty. Zařízení umožní vstup platební karty do bankomatu, kde však platební kartu zadrží a znemožní její výstup. Zákazník se domnívá, že mu bankomat z nějakého důvodu kartu zadržel. V té chvíli přichází osoba, která vystupuje jako pomocník. Jedná se však o podvodníka. Ten nabídne občanovi pomoc v nepříjemné situaci. Vyzve majitele karty, ať opětovně zadá svůj PIN kód, který si zapamatuje, či někam zaznamená. Po neúspěšném pokusu o získání karty doporučí zákazníkovi, aby se obrátil na pobočku banky. Když poškozený odejde, podvodník kartu vyjme a použije k výběru hotovosti.

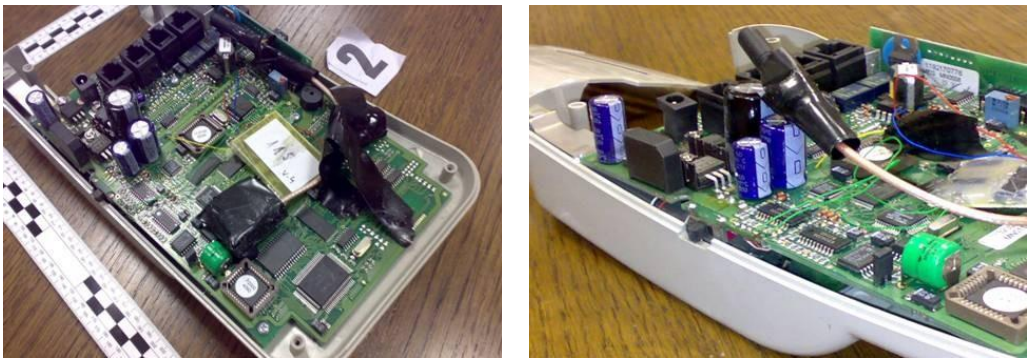
Obr. č.14 Ukázka Libanonské smyčky

Obr. č. 15 Ukázka Libanonské smyčky

Další způsob, jak neoprávněně získat data z platební karty je tehdy, když občan, platící například v restauraci, předloží platební kartu. Podvodník však přinese svou vlastní čtečku, pomocí které zaznamená data z magnetického proužku. Tato data poté nahraje na platební kartu, kterou si opatřil. Ve většině případů se jedná o tzv. čisté bílé plasty, které jsou opatřeny magnetickým proužkem na zadní straně. V tomto případě může být čtečka v obchodním místě umístěna bez vědomí prodejce nebo může prodejce s podvodníkem spolupracovat.

Obr. č. 16 Originál terminál

Obr. č. 17 Terminál s upraveným PinPadem

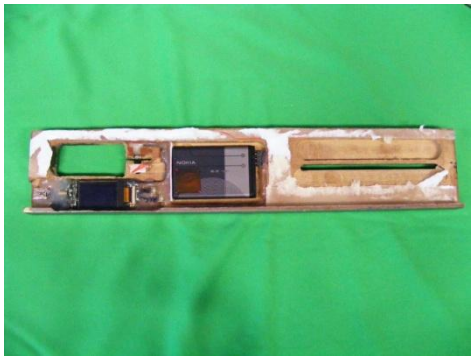


Obr. č. 18,19 Terminál osazený skimmovacím zařízením

Promyšlenějším a složitějším způsobem jak získat potřebná data z platební karty a PIN kód je za pomoci zařízení, která se umísťují na bankomat. Rozměry a vzhled těchto zařízení jsou různé, vždy však musejí vzbuzovat dojem, že zařízení na bankomat patří (je jeho součástí), aby klient banky nepoznal, že je na bankomatu umístěno nějaké cizí těleso. Tato skimmovací zařízení mívají takové rozměry, které přesně pasují do otvorů bankomatu. Taktéž barva zařízení je totožná s barvou bankomatu. Tyto přístroje jsou schopné nahrát, případně bezdrátově přenést, data z platební karty, a to jak z magnetického proužku, tak i z čipu. Na bankomat může pachatel umístit mikrokameru, která snímá číselnou klávesnici s cílem získat PIN kód. Získání PIN kódu je možné i umístěním falešné klávesnice na bankomat nebo přiložením speciální fólie na klávesnici. Zařízení, která nahrazují klávesnici, se nazývají PinPady. Skimmovací zařízení je na bankomat připevněno buď za pomoci suchého zipu, nebo oboustranné lepicí pásky, popřípadě použitím speciálních lepidel. Umístění tohoto zařízení na bankomat je otázkou několika vteřin. Sejmout ho však je trochu složitější než ho umístit, jelikož je vyráběno s co největší přesností, aby vzbudilo dojem originálu bankomatu (jedná se však také o vteřiny). Sejmutí je prováděno za pomoci ostřejších předmětů, například nožů nebo šroubováků a na bankomatu zanechává rýhy a vrypy (mechanoskopické stopy). Zařízení bývá na bankomatu připevněno několik hodin, ve výjimečných případech několik dní, aby pachatelé získali co nejvíce dat. Často se pohybují v bezprostředním okolí bankomatu a sledují bankomat. V některých případech již stahují přes mobilní telefon za pomoci bluetooth nebo prostřednictvím MMS a SMS zpráv získaná data, která lze zaslat kamkoliv ve světě. Využití takto získaných dat je možné více způsoby. Jsou to nákupy přes internet, při kterých nelze ověřit fyzické držení karty, přitom pachatel má k dispozici jak data z karty, tak PIN kódy. Jedná se

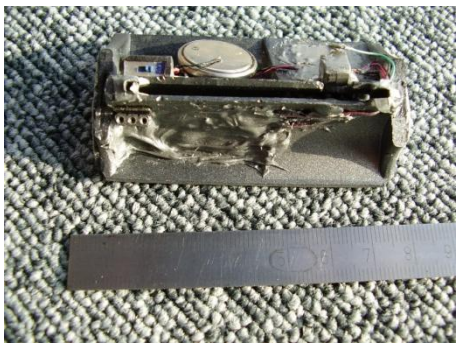
často o objednávky pobytů v hotelu, které jsou následně stornovány s tím, že zbytek částky po stržení stornopoplatku má být zaslán např. na účet v bance Western Union nebo Barclays Bank. Dalším ze způsobů je nákup zboží, které je následně zasíláno na adresy, kde ho mohou vyzvedávat tzv. bílí koně. Pachatelé mohou také získaná data z platebních karet prodávat přes internet. Tato data si dále zakupují osoby, které je následně nahrávají na tzv. bílé plasty a poté používají. Skimmingem se především zabývají dobře organizované skupiny pocházející z Moldavska, Bulharska a Rumunska. Pachatelé z těchto organizovaných skupin po získání potřebných dat z platebních karet často odcestují do Afrických zemí, kde vybírají z bankomatů finanční prostředky za pomoci takto padělaných platebních karet. Majitel platební karty se o neoprávněném výběru finanční hotovosti dozví se značným zpožděním buď z výpisu z účtu, nebo přímo od pracovníků banky. Obětem skimmingu v těchto případech banky škodu hradí.

Obr. č. 20 Přední strana skimmovacího zařízení



Obr. č.21 Zadní strana skimmovacího zařízení

Obr. č. 22 Přední strana skimmovacího zařízení



Obr. č. 23 Zadní strana skimmovacího zařízení

Obr. č. 24 Bankomat osazen skimmovacím zařízením

Obr.č.25,26 Bankomat osazen skimmovacím zařízením

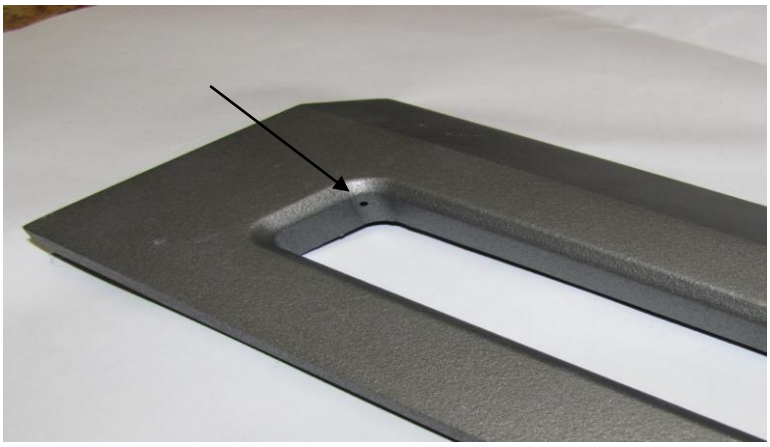
PinPady - jedná se o nejlepší náhradu mikrokamer a kamer. Proto se na bankomaty umísťují, aby nedošlo k odhalení kamery. PinPady bývají asi tak dvakrát větší než platební karta. Vypadají jako skutečná klávesnice, která je PinPadem překryta. PinPady jsou uzpůsobené tak, aby při zadávání údajů klientem na klávesnici zaznamenávaly tyto údaje. PinPad musí umožňovat fungování i originál klávesnice,

která je pod ním. Zařízení má velkou výdrž, jelikož se na ní dá nahrát několik tisíc záznamů. PinPady mají velkou úspěšnost pro jejich perfektní autentičnost, výbornou funkčnost a spolehlivost. Značnou nevýhodou pro pachatele je, že jsou vyráběny různé druhy bankomatů, které mají samozřejmě rozdílné klávesnice, tudíž pachatel nejprve musí nalézt bankomat, který má totožnou klávesnici, na kterou má PinPad. PinPad je vyráběn z plastu nebo kovu.

Obr. č. 27 Bankomat osazen PinPadem

Obr. č. 28 Zadní strana PinPadu

Kamery – kamery používané na skimmování bývají velmi malé, velikost čočky může být jako špendlíková hlavička. Je umístěna tak, aby zaznamenala plochu celé klávesnice. V případě použití takto malých kamer bývá záznam velmi nekvalitní a černobílý, avšak postačující, aby byl zaznamenán PIN kód a pachatel ho následně mohl identifikovat. Pachatelé mohou bankomat opatřit i větší kamerou a to pokud jim to situace dovolí. Jedná se zejména o případy, kdy je bankomat umístěn v rohu, anebo si poblíž bankomatu umístí falešnou krabičku s letáky, ve které je připojena kamera a otvor na čočku. Tyto záznamy již bývají mnohem kvalitnější a mohou být už i barevné.



Obr. č. 29 Bankomat osazen kamerou v prostoru výběru hotovosti

Obr. č. 30 Bankomat osazen kamerou v prostoru výběru hotovosti

Zařízení, která jsou používána ke skimmovanání mohou být vyráběna ručně nebo se jedná o výrobky vyráběny továrně. Pokud je zařízení vyráběno ručně, bývá pravidlem, že není tak kvalitní jako zařízení vyrobeno továrně. V případě, že má pachatel zájem si nechat vyrobit zařízení sloužící ke skimmingu, tak výroba v Evropě i USA bývá velmi riziková z důvodu odhalení. Proto k tomuto účelu často bývá využívána Čína. Jak je již známo, v Číně je možné vyrobit téměř cokoliv a ceny takového zařízení nejsou nijak drahé.

Černý trh - je místo, kde se setkávají lidé, aby zakoupili materiály, které nebyly zajištěny legálně, nejsou legální a tyto nebudou využívány k legálním účelům. V dnešní době se k těmto účelům často využívá internet. Skupiny, které se zabývají skimmingem, již na internetu fungují velmi dlouho. Na černém trhu je možné zakoupit téměř vše, co

se týká jak technického zařízení, návodů, informací, popřípadě schémat. Dají se sehnat i technické popisy vybraných bankomatů.

Celková suma zařízení sloužící ke skimmingu, které je možné sehnat na internetu, se pohybuje kolem 17 000 Kč až 85 000 Kč. Jedná se však o podprůměrné zařízení. Cena je velmi závislá na úrovni zařízení, tedy na typu, kvalitě a schopnosti zařízení. Plastový PinPad je možné sehnat za částku 25 000 Kč až 43 000 Kč, kovový se bude pohybovat kolem částky 100 000 Kč. Prázdné platební karty je možné sehnat za částku od 170 Kč za kus, za embosovanou od 500 Kč za kus. Za zlaté, platinové, bussines a další specifické karty se platí částka kolem 850 Kč za kus. Holografické karty se pohybují ve výši kolem 1 400 Kč za kus.

Nejžádanější na černém trhu jsou odcizené záznamy z platebních karet. Na ceně se velmi projeví fakt, zda prodávané záznamy obsahují i PIN kód. Rozhodující je také, z jaké země byla data odcizena. Pokud se jedná o záznamy bez PIN kódů, tak se cena pohybuje kolem 800 Kč, pokud je k záznamu i PIN kód a jedná-li se o platební kartu Gold, Bussines, Platinum, může se cena pohybovat i kolem částky 8 500 Kč za kus.

Kamery a mikrokamery se na černém trhu objevují jen ve velmi malém množství, spíše vůbec ne, jelikož je tyto možné zakoupit normální legální cestou od specializovaného prodejce a nikdo nepojme podezření, že by je chtěla osoba použít na nelegální účely.

Není však zaručeno, že odcizené záznamy, které mají být opětovně nelegálně použity, budou stále aktuální. Mohlo dojít k zablokování karty nebo není na kartě dostatek finančních prostředků. K tomuto účelu je možné sehnat bližší informace a to jak o aktuálním stavu účtu, případně funkčnosti karty. Cena této služby je v hodnotě kolem 170 Kč za kus. Pokud si však pachatel - nakupující nenechá tyto informace ověřit a odcizená zaslaná data jsou nefunkční, prodávající ve většině případů po reklamaci odešle nová data bezplatně.

Co se týká zařízení, kterým je možné odcizená data nahrát na novou platební kartu, tak tyto se pohybují v částce kolem 8 500 Kč a dosahují částky až kolem 150 000 Kč. Opět je cena závislá na více kritériích. Záleží, zda je k zařízení přiložen software a jaký, na jaké druhy karet je možné data zapisovat, kolik je schopné zapisovat

Tracků, zda je možné zapisovat na karty pouze s magnetickým proužkem nebo i vybavené čipem apod.

3.1 Zabezpečení bankomatů před skimmingem

Bankovní ústavy se snaží bankomaty před skimmovacím zařízením chránit. Jeden ze způsobů je vložit plastový nástavec do prostoru, kde se vkládá platební karta, bohužel pachatelé již na toto antiskimmovací zařízení nasazují svá skimmovací zařízení. Další ze způsobů jsou alarmová čidla, která jsou na bankomatu umístěna a v případě neoprávněného zásahu do bankomatu vyšlou signál. Další z opatření je výbava nového softwaru – ve chvíli, kdy bankomat rozpozná, že je na něj umístěno skimmovací zařízení nebo je proveden jiný neoprávněný zásah, bankomat se vypne. Bankovní ústavy však z pochopitelných důvodů nechtějí o dalším zabezpečení mluvit a to zejména právě z bezpečnostních důvodů.

Obr. č. 31,32 Nástavec protiskimmovacího zařízení tzv. „zelený zobák“

Obr. č. 33 Originální vzhled bankomatu

Obr. č. 34 Bankomat osazen antiskimmovacím zařízením

3.2 Postup při neoprávněném výběru finanční hotovosti z účtu

Jako první rada je, pokud se Vám na bankomatu nebo okolí zdá něco podezřelého, neprovádějte na bankomatu transakci a celou věc oznamte bance nebo policii. Jestli jste již bankomat použili a vybrali jste z něho finanční hotovost, raději platební kartu zablokujte a kontrolujte si výpisy z účtu. Pokud na výpisu z účtu zjistíte transakce, které jste neprovedli, podejte v bance reklamaci a věc oznamte na policii. Banka reklamaci prověří a pokud by vám byly z účtu odčerpány finanční prostředky za využití skimmovacího zařízení na bankomatu, banka vám bude škodu kompenzovat v plné výši.

Pokud se banka o skimmovacím zařízení na bankomatu dozví dříve než vy a vy jste v době, kdy bankomat byl osazen skimmovacím zařízením prováděli na bankomatu transakci, banka vám preventivně platební kartu zablokuje a následně vás o této skutečnosti vyrozumí.

4 Finanční arbitr

Funkce finančního arbitra je zvýšit ochranu spotřebitelů u poskytovatelů platebních služeb a vydavatelů elektronických peněz a usilovat o smírné vyřešení sporu. Finanční arbitr by měl zajistit rychlé, bezplatné a efektivní vyřízení sporů, mimosoudní cestou, mezi poskytovateli platebních služeb a uživateli platebních služeb při poskytování platebních služeb, mezi vydavateli a držiteli elektronických peněz, při vydávání a zpětné výměně elektronických peněz. Spadají sem spory, které se týkající převodů peněžních prostředků, problémů spojených s platební kartou a elektronickou peněženkou a to jak v tuzemsku, tak i v zahraničí v rámci Evropské unie. Finanční arbitr neřeší spory týkající se oblasti hypoték, úvěrů a spory mimo členské státy Evropské unie.

Řízení před finančním arbitrem se zahajuje pouze na návrh navrhovatele. Lhůta pro vyřešení sporu je 30 dnů, v případě složitějšího sporu je lhůta 60 dnů. Lhůtu lze prodloužit. Výsledkem řízení je vydání nálezu v písemné formě. Nález obsahuje výrok, odůvodnění a poučení o námitkách. Námitku proti rozhodnutí mohou podat obě dvě strany řízení. Proti rozhodnutí o námitce není možné další námitky uplatnit a rozhodnutí je konečné.

Spory, které řeší finanční arbitr, jsou bezplatné a rychlejší, než řízení před soudem. Spory jsou financovány z peněz všech daňových poplatníků a to i přes to, že se jedná o soukromoprávní spor. Na druhou stranu je nutné zdůraznit, že se jedná o ochranu spotřebitele proti velkým obchodním institucím.[25]

Pro zajímavost uvedu dva případy, které řešil finanční arbitr a s jakým výsledkem.

1. Neoprávněné odčerpání finančních prostředků přes internet

Navrhovatel se obrátil na finančního arbitra s tím, že mu bylo v ranních, v době mezi 02.00 hodin až 03.00 hodin odcizena peněženka, ve které měl mimo jiné i platební kartu. Krádež peněženky navrhovatel zjistil až ve večerních hodinách téhož dne a celou

[25] Procházková, M., *Bezhotovostní platební styk*, Bakalářská práce, Masarykova univerzita v Brně,Právnická fakulta, 2010, s.36

věc ihned oznámil na policii. Pachatel však provedl s platební kartou dvě transakce na internetu a to v časech 06.20 hodin a 06.21 hodin. Transakce byly provedeny bez použití PINu u internetové sázkové společnosti. Transakce byly provedeny v celkové výši 20 000 Kč. Jakmile navrhovatel zjistil, že byla provedena neoprávněná transakce, věc oznámil na policii a u bankovního ústavu podal reklamaci. Bankovní ústav však reklamaci neuznal, ačkoliv se navrhovatel odvolal na § 18 zákona č. 124/2002 Sb., podle kterého měl nárok na okamžité vrácení peněz. Během řízení před finančním arbitrem bankovní ústav uznal, že tento spor měl řešit dle výše uvedeného ustanovení zákona č. 124/2002 Sb., jestliže bylo užito elektronického platebního prostředku, aniž byl fyzicky předložen nebo bez identifikace držitele osobním identifikačním číslem (PIN), má držitel právo na neprodlené vrácení takto odčerpaných peněžních prostředků.[26]

2. Chybně vyplnění příkaz k úhradě ze strany klienta

Navrhovatel, který se obrátil na finančního arbitra, podával u bankovního ústavu platební příkaz k úhradě, ale u příkazu vedl špatné číslo účtu plátce. Později se dověděl, že k převodu nedošlo a to z důvodu špatného zadání čísla plátce. Tím, že nedošlo k převodu finančních prostředků, nebyl navrhovateli připsán státní příspěvek ze stavebního spoření a zároveň mu nebyl připsán úrok z částky převodu. Finanční arbitr k případu provedl šetření a zjistil, že navrhovatel na platebním příkazu k úhradě zadal špatné číslo účtu. Navrhovatel příkaz tento příkaz stvrdil vlastnoručním podpisem, tudíž souhlasil s údaji uvedenými na platebním příkazu. Finanční arbitr v dané věci rozhodl ve prospěch bankovního ústavu, jelikož chyba byla na straně navrhovatele.[27]

[26] *Finanční arbitr: příklady řešených sporů* [online]. Změněno 2011 [cit. 2011-11-12]. Dostupné z:< http://www.finarbitr.cz/cs/spory-priklady-resenych-sporu.html>

[27] *Finanční arbitr: příklady řešených sporů* [online]. Změněno 2011 [cit. 2011-11-12]. Dostupné z:< http://www.finarbitr.cz/cs/spory-priklady-resenych-sporu.html>

5 Doporučení při používání platební karty

Téměř každá banka vydává pro své klienty tzv. desatero bezpečnosti, které informuje o tom, jak používat platební kartu. Doporučení jednotlivých bankovních ústavů se od sebe nijak významně neliší. Jedná se především o rady, které lze shrnout do těchto základních bodů:

1. Při převzetí platební karty od bankovního ústavu si ji hned podepište v prostoru podpisového proužku a pořiďte si kopii. Tato kopie může později posloužit při případné reklamaci plateb odcizenou kartou. V dnešní době je na většině platebních karet podpis v podpisovém proužku už přežitek a ochrannou funkci postupně ztrácí, jelikož naprostá většina dnes používaných terminálů již vyžaduje autorizaci za využití PIN kódu a podpis již není zapotřebí.

2. Platební karta je nepřenosná a jakékoliv použití jinou osobou, než je držitel karty není v žádném případě povoleno. Pokud dojde k porušení tohoto pravidla, banky to považují za hrubé porušení podmínek a reklamace je v takovém případě zamítnuta.

3. PIN kód je velmi důvěrný údaj a každý klient by ho měl uchovávat v bezpečí a nikomu dalšímu ho nesdělovat. Platby, které jsou autorizované použitím PIN kódu, se velmi těžce reklamují, jelikož banky považují neoprávněnou platbu autorizovanou za využití PIN kódu za hrubé porušení podmínek. Všeobecně je doporučováno nezapisovat si PIN kód na lístek, který nosíte v blízkosti platební karty.

4. Velmi opatrní buďte při používání bankomatů. Při zadávání PIN kódu u bankomatu nebo u platebního terminálu si dávejte pozor, aby kód někdo nemohl odpozorovat. Nenechte se při provádění transakce od nikoho rušit, řiďte se pouze pokyny, které bankomat zobrazuje na displeji. Nikdo nemá právo vaši transakci přerušit, ani ochranka nebo personál banky či obchodního centra. Pokud je bankomat v nočních hodinách špatně osvětlen, raději ho nepoužívejte. Po dokončení transakce si nezapomeňte vzít platební kartu, hotovost a stvrzenku. Hotovost si přepočítejte, zda souhlasí s požadovanou transakcí.

5. Při placení platební kartou trvejte na tom, aby obchodník s kartou nikam neodcházel a prováděl transakci před vámi. Při placení si ověřte správnost údajů a výši částky na stvrzence. Po platbě zkontrolujte, zda vám obchodník vrátil vaši kartu.

6. Při placení kartou přes internet nebo po telefonu buďte velmi opatrní. Pokud by někdo nepovolaný zjistil číslo vaší platební karty, jméno a dobu platnosti, nic mu nebrání v jejím zneužití. Při platbách přes internet preferujte obchody, které využívají systém bezpečného placení MasterCard SecureCode a Verified by Visa. V případě jakýchkoliv pochybností o internetovém nebo telefonním obchodníkovi využijte systém MasterCard SecureCode nebo Verified by Visa nebo raději zvolte jiný způsob úhrady.

7. Pravidelně kontrolujte výpisy z účtu. Pokud zjistíte jakoukoli nesrovnalost, ihned informujte svou vydavatelskou banku a spornou transakci reklamujte. V případě, že máte pocit, že při placení kartou nebo při vybírání hotovosti z bankomatu nebylo vše v pořádku, informujte o tom svou vydavatelskou banku.[28]

8. V případě ztráty nebo krádeže karty je nutné bez prodlení tuto skutečnost ohlásit jejímu vydavateli. Hlášení je možné podat přímo zákaznickému centru dané instituce, které často funguje nepřetržitě nebo prostřednictvím nejbližší pobočky členské banky VISA nebo Europay/MasterCard, příp. cestovních kanceláří Thomas Cook a American Express. Většina bank v zahraničí akceptuje telefonické hlášení, české banky většinou trvají na písemném potvrzení. Ztrátu nebo krádež karty je nutno hlásit co nejdříve po zjištění této skutečnosti jejímu vydavateli a pak následně podle okolností i místní policii.

Podle podmínek banky je možné kartu buď dočasně zablokovat, nebo uvést na stoplis. Blokace zajišťuje odmítnutí všech autorizovaných transakcí a je ji možné zrušit. Stoplistace je nevratné ukončení její platnosti. Při jakékoliv žádosti bankomatu nebo obchodníka o autorizaci transakce je vydán pokyn zadržet kartu.[29]

Nouzové služby – při ztrátě, či odcizení platební karty není podmínkou, že se dostanete do okamžitých nesnází, tak jak se to stává při ztrátě či odcizení finanční

[28] *Desatero bezpečnosti* [online]. [cit. 2011-11-11]. Dostupné z: <http://www.mastercard.com/cz/personal/cz/sluzby/desatero_bezpecnosti.html>

[29] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.97

hotovosti. Bankovní ústavy jsou schopny klientovi poskytnout rychlou a účinnou pomoc. V případě, že klient bankovní ústav o takovou pomoc požádá, bankovní ústav mu zajistí tyto služby:

Vydání nouzové hotovosti – jednorázově nebo opakovaně může klient obdržet do 24 hodin nouzovou hotovost do částky 1 000 USD, ve většině případů v nejbližší pobočce banky i v cestovních kancelářích Thomas Cook.

Vydání náhradní karty – pokud se klient banky plánuje zdržovat delší dobu v zahraničí nebo předpokládá, že bude mít vyšší výdaje, může mu být vydána nouzová platební karta, a to do 48 hodin. Tato karta je opatřena jménem klienta a identifikačním číslem přiděleným bankou a její výrobu provádí nejbližší regionální nouzové centrum příslušného karetního systému. Platební karta má jednotný design bez jména banky, není opatřena magnetickým proužkem a její platnost je časově omezena na dobu 2 měsíců. Kartu lze doručit kurýrem, popřípadě je možné si ji vyzvednout na pobočce banky.[30]

[30] Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2, s.97

Závěr

V dnešní moderní době je bezhotovostní platební styk naprostou součástí našeho života. S rostoucím množstvím platebních karet, jejich využitím, množství zboží, které je jimi možno platit, počtem míst, kde je možné platební kartou platit, úměrně roste i riziko jejich zneužití. Držitelé jsou ohroženi dobře organizovaným mezinárodním zločinem. Jedná se především o získání dat z platební karty za využití skimmovacího zařízení. Díky skimmovacímu zařízení jsou pachatelé schopni během krátké doby (řádově hodiny) provést nezákonné finanční operace z účtu držitele platební karty, která byla zneužita. K neoprávněným finančním operacím však nemusí dojít jen za využití skimmovacích zařízení. Může se jednat i o neopatrnost držitele karty, který dostatečně nechrání svá data na kartě a osoba, která tyto data získá, je využije k neoprávněným transakcím. Jelikož držitelé a uživatelé platebních karet si často ani neuvědomují možnosti zabezpečení svých platebních karet a rizika, které jim hrozí používáním platebních karet, rozhodl jsem se vybrat si jako téma bakalářské práce právě tuto problematiku. Ve své bakalářské práci jsem se pokusil vysvětlit možnosti zneužití platebních karet a vytvořit manuál pro občany, kteří používají platební karty, který přispěje k prevenci a ochraně platebních karet před jejich zcizením a zneužitím.

Ve své práci jsem popsal základní rozdělení platebních karet, aby si byl klient banky schopen vybrat takovou platební kartu, která bude splňovat jeho požadavky.

Když už v práci bylo popsáno rozdělení karet, bylo nutné vysvětlit i jejich zabezpečení a možná rizika spojená s jejich používáním. S pokrokem doby už se mezi námi nenajde téměř nikdo, kdo by nepoužíval internet. A spojení internetu a elektronického bankovnictví je jako spojení pohodlí a rychlosti, ale to jen v případě, že klient bude dodržovat určitá pravidla. Proto je další část určena pro ty, kteří využívají elektronické obchodování. Elektronické obchodování má mnoho druhů zabezpečení, jen si klient opět musí vybrat o jaký druh obchodu má zájem a následně podle toho zvolit druh a úroveň zabezpečení. Bezpečnostní prvky se dají různé kombinovat a propojovat.

Taktéž ke každodennímu životu dnes patří využívání bankomatů a platebních terminálů, na které mohou pachatelé umístit skimmovací zařízení, díky kterým lze

získat data na platební kartě. Proto je další část práce věnována této problematice a jsou zde znázorněny obrázky, jak samotné skimmovací zařízení vypadá a nač si dát pozor.

Banky v některých případech se svými klienty jednají z mocenské pozice a jejich ochota vracet peníze, které jim byly neoprávněně odčerpány z účtu neoprávněnou transakcí, není příliš vysoká. Proto se může nespokojený klient obrátit na finančního arbitra, který má za úkol spor mezi klientem banky a bankou rozhodnout.

Seznam použité literatury

Juřík, P., 2001, *Svět platebních a identifikačních karet*, Grada Publishing, spol. s.r.o., s.210. ISBN 80-247-0195-2

Juřík, P., 2003, *Encyklopedie platebních karet Historie, současnost a budoucnost peněz a platebních karet*, Grada Publishing, a.s., s.312. ISBN 80-247-0685-7

Hradecký, M. *Platební prostředky jejich ochrana a padělání*, 2008. s. 160, ISBN 80-7312-055-0

Závěrečné práce:

Džaferagič, A. 2008. *Aplikace pro obchodování na internetu*. Bakalářská práce, Masarykova univerzita v Brně, Fakulta informatiky, Brno

Kučerová, P. 2010. *Elektronické bankovnictví*. Diplomová práce, Masarykova univerzita v Brně, Ekonomicko –správní fakulta, Brno

Procházková, M., *Bezhotovostní platební styk*, Bakalářská práce, Masarykova univerzita v Brně,Právnická fakulta, 2010

Stejskal, O. 2007. *E-kommerce*. Bakalářská práce, Masarykova univerzita v Brně, Ekonomicko –správní fakulta, Brno

Školkay, E. 2011. *Platební systémy na internetu*. Bakalářská práce, Masarykova univerzita v Brně, Ekonomicko –správní fakulta, Brno

Elektronické zdroje:

Krčmář, P., *Autorizace v internetovém bankovnictví* [online]. 24.8.2006 [cit. 2011-11-17].
Dostupné z:< http://www.root.cz/clanky/autorizace-v-internetovem-bankovnictvi/>

Desatero bezpečnosti [online]. [cit. 2011-11-11]. Dostupné z: <http://www.mastercard.com/cz/personal/cz/sluzby/desatero_bezpecnosti.html>

Finanční arbitr: příklady řešených sporů [online]. Změněno 2011 [cit. 2011-11-12]. Dostupné z:< http://www.finarbitr.cz/cs/spory-priklady-resenych-sporu.html>

Odborné časopisy

Thruschka, J., 2009, *Asymetrická kryptografie v praxi*, IT Security 2009, s. 6-7

Obrázky

Použity z archivu Policie České republiky