Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Bezpečnost platebních karet

DIPLOMOVÁ PRÁCE

Student: **Bc. Michal Fuchs**

Vedoucí: **Prof. Ing. Petr Doucek, CSc.**

Rok vypracování: **2014**

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze které jsem čerpal, dle normy ČSN ISO 690-2.

V Praze dne 1.5.2014

. . . . . .

Jméno a příjmení studenta

Poděkování

Tímto děkuji prof. Ing. Petru Douckovi, CSc., za cenné rady a připomínky při vedení práce.

Abstrakt

Práce se zabývá platebními kartami a riziky spojenými s jejich používáním. Hlavním zaměřením práce je analyzovat možnosti zneužití platební karty a případné způsoby ochrany. Nejdříve jsou analyzovány technologie, které jsou dnes s platebními kartami a jejich používáním spojeny. Následně jsou rozebrány jejich slabiny a jednotlivé typy útoků, které získávají údaje o kartě pro následné odcizení finančních prostředků. Poté je zpracováno porovnání následných útoků s cílem odcizit finanční prostředky v různých světových oblastech. Na statistických datech ECB je provedena kvalitativní analýza rizik spojených s využíváním platební karty vydané v České republice. Na tuto analýzu pak navazují doporučení s cílem omezit dopad nebo pravděpodobnost zneužití platební karty. Pro ověření stanovených doporučení je zpracováno dotazníkové šetření.

Klíčová slova

platební karty, analýza rizik, zneužití platebních karet, ochrana proti zneužití

Abstract

This thesis aims to identify and evaluate the risks related to payment cards and their use. The main focus is the methods used to commit card related fraud and possible methods of protection related to this topic. First of all, the technology that is nowadays used in relation with the payment cards is analyzed and its weaknesses and attacks used to gather card information are described. After that, statistical data related to card fraud are analyzed in relation with different world regions. Qualitative analysis of risk related to payment card use is performed on the statistical data of ECB for the cards issued in Czech Republic. The qualitative analysis is then followed by recommendations that are designed to limit the risk's impact or probability. To verify the recommendations, a survey is carried out.

Key words

payment cards, risk analysis, card fraud, card fraud protection

Obsah

Úvod

Platební karty jsou jedním z významných a oblíbených způsobů platby jak v kamenných obchodech, tak i při zprostředkovaných platbách na internetu, přes telefon nebo poštou. Rychlý vývoj informačních technologií posledních několika dekád znamenal jejich zavedení i v oblasti platebních karet, díky čemuž jsou stále rozšířenější a nabízejí širší množství funkcí. Spolu s jejich dalším rozvojem se však rozvíjí i kriminalita s nimi spojená, jejímž cílem je pomocí odcizených údajů o kartách nebo karet samotných získat přístup k finančním prostředkům jejich majitele.

Technologie karet do jisté míry na tato rizika reagovala, ale karty jsou stále zranitelné různými typy útoků. Je však možné se proti nim částečně bránit, případně snížit jejich dopad, pokud k útoku skutečně dojde. Vzhledem k tomu, že karty jsou napojeny na běžné účty klientů, hrozí při jejich zneužití poměrně vysoké ztráty, z tohoto důvodu je důležité jejich bezpečnosti nepodceňovat a snažit se riziko pokud možno minimalizovat.

Tato práce si klade za cíl tato rizika identifikovat a analyzovat a na základě této analýzy doporučit, jak se proti možným útokům co nejlépe bránit.

Cíle práce

Záměrem práce je nejdříve analyzovat fungování platebních karet, a to obzvláště s důrazem na jejich bezpečnost při běžném používání, a následně identifikovat a blíže definovat jednotlivé typy útoků, které jsou dnes proti platebním kartám vedeny, a to v kontrastu se zabezpečeními, která jsou nasazována ze strany bankovních domů a vydavatelů karet.

Primárním cílem práce je vyhodnotit nejvýznamnější rizika při použití platebních karet a navrhnout možnost, jak se proti nim bránit. V závislosti na identifikovaných typech útoků – rizicích při používání platební karty, budou daná rizika zhodnocena na základě statistických údajů odpovědných institucí. Na základě tohoto zhodnocení budou identifikována největší rizika spojená s využitím platební karty. Na tato vybraná rizika bude vypracováno doporučení, poskytujících návrh, jak se proti takto zaměřeným útokům přiměřeně bránit.

Doporučení a hodnocení rizik se zaměřuje primárně na skupinu studentů a přínos doporučení bude ověřen dotazníkovým šetřením na odpovídající skupině respondentů.

Vedlejším cílem je porovnání útoků v jednotlivých světových oblastech. Pro toto srovnání byly vybrány nejvýznamnější země z regionů Evropy, Severní Ameriky, Austrálie, Asie, Afriky.

Způsob dosažení cílů práce

Doporučení bezpečnostních opatření, která mají zmenšit nebo vyloučit možnost napadení platební karty, případně dopad takovéhoto útoku, bude založeno na dříve vybraných typech útoků. Prvotní výběr těchto útoků proběhne nejdříve na základě literatury, kdy budou vybrány nejčastěji zmiňované útoky.

Na těchto vybraných útocích pak bude na základě dostupných statistik vypracována kvalitativní analýza rizik, jejímž cílem bude vyhodnotit významnost jednotlivých rizik pro uživatele platební karty. Při této analýze budou využity hlavně informace o počtu útoků a finančních dopadech těchto útoků.

Na základě analýzy fungování platebních karet z teoretické části pak budou formulována doporučení. Doporučení bude zaměřeno především na skupinu studentů, kteří často využívají všechny možnosti plateb, jak platby přímo kartou, tak platby bez přítomnosti karty, čímž jsou tyto karty potenciálně vystaveny maximálnímu možnému riziku. Možnost uplatnění formulovaných doporučení bude následně ověřena dotazníkovým průzkumem na skupině studentů.

Mimo hlavního cíle bude provedeno porovnání statistických údajů o útocích na platební karty v různých světových oblastech. Toto porovnání by mělo určit, kde jsou které typy útoků nejběžnější a jaká rizika tak nejčastěji hrozí v různých regionech. Porovnání bude provedeno na základě statistických dat dostupných především od institucí monitorujících nebo regulujících bankovní sektor a finanční transakce.

Předpoklady a omezení práce

Předpokladem práce a hlavně formulovaného doporučení je vůle uživatele chránit se proti možnému útoku na jeho platební kartu. Její ochrana z velké části spočívá právě v této vůli a v tom, jak moc je obezřetný a uvědomělý v okamžicích, kdy kartu používá.

Omezením práce je zajisté sama podstata útoku a obrany. Obrana proti útokům je ve většině případů reakcí, která následuje po úspěšných útocích, které prolomily původní obranu. Formulovaná doporučení tak mohou mít omezenou dobu platnosti, stejně tak se ale mohou stát zbytečnými v okamžiku, kdy přijde nová technologie, která odstraní některé ze zranitelných míst platební karty.

Cílem doporučení není nahradit běžná pravidla zacházení s kartou pravidelně doporučovaná bankovními domy a finančními institucemi. Záměrem je navrhnout dodatečné možnosti obrany, které mapují veškeré dostupné možnosti. Cílem není ani zabývat se zločinností spojenou s kreditními kartami a nesplácením přečerpaných limitů způsobených vlastním majitelem karty, práce se zaměřuje pouze na útoky vedené proti kartě bez souhlasu jejího majitele.

Předpokladem porovnání statistik o útocích na platební karty v různých světových oblastech je očekávání, že nejčastěji využívané typy útoků se v různých částech světa liší, a to především na základě používaných technologií. Omezením v tomto ohledu je dostupnost statistik v různých regionech, kde některé poskytují vyčerpávající statistiky, zatímco jiné poskytují pouze základní či žádné.

Struktura práce

Práce je rozdělena na dvě hlavní části, část teoretickou a část praktickou. Teoretická část objasňuje vznik a historii platebních karet a vznik karetních asociací, které jsou dnes hlavními hráči na tomto trhu a nesou hlavní odpovědnost za tvorbu a implementaci bezpečnějších technologií v této oblasti. Dále teoretická část definuje jednotlivé typy karet jak podle způsobu užití, tak podle využívaných technologií, což je východiskem pro praktickou část.

Na závěr teoretické části jsou definovány nejčastější typy útoků na platební karty a tyto útoky jsou blíže analyzovány z hlediska zranitelnosti jednotlivých typů karet a snadnosti provedení takovéhoto útoku.

Praktická část je pak rozdělena na tři dílčí části. První část podává porovnání statistik z jednotlivých světových regionů a vyhodnocení nejčastějších útoků podle světových oblastí. Dále obsahuje zhodnocení rizikovosti jednotlivých typů útoků pomocí kvalitativní analýzy rizik pro karty vydané v České republice.

Na kvalitativní analýzu pak navazuje část s doporučeními, jak zmenšit nebo vyloučit možnost útoku na platební kartu nebo snížit jeho případný dopad.

Na závěr praktické části je zpracováno dotazníkové šetření, které si bere za cíl ověřit využitelnost těchto doporučení pro cílovou skupinu.

Výstupy a očekávané přínosy

Hlavním výstupem práce je zhodnocení rizik spojených s útoky na platební karty a formulace doporučení, které mohou snížit nebo vyloučit možnost útoku na platební kartu nebo snížit jeho dopad. Očekávaným přínosem doporučení oproti běžným radám je jeho širší zaměření, které umožňuje upozornit na technologie či produkty, které jsou vzhledem k bankám nebo platební kartám konkurenti, ale umožňují zvýšit bezpečnost při platbách kartou. Významná je celistvost práce od analýzy přes doporučení až po ověření využitelnosti doporučených opatření pro cílovou skupinu.

Zároveň je předpokládaným přínosem i analýza jednotlivých typů útoků a jejich bližší popis, který může pomoci případný útok snáze odhalit.

Dalším výstupem je porovnání statistik z jednotlivých světových oblastí. Jeho očekávaným přínosem je upozornění na nebezpečí, která mohou hrozit v různých světových oblastech, což může čtenáři umožnit větší ostražitost při konkrétních typech plateb v těchto oblastech.

1. Platební karty

1.1. Vývoj platebních karet

Za prvního předchůdce platebních karet, respektive karet kreditních, lze považovat tzv. metal charge plates, což byly kovové štítky hojně využívané v USA koncem 19. století. Tyto štítky sloužily hlavně k identifikaci klienta – každý štítek měl vyražené identifikační číslo, které bylo přiřazeno určitému klientovi. Většinou byly štítky vydávány movitým klientům a velmi dobrým zákazníkům. Ti pak místo platby za zboží předložili štítek a obsluha zaevidovala nákup a identifikační číslo štítku a zákazník potvrdil nákup podpisem. Platby za nakoupené zboží pak zákazník provedl vždy jednou za určité období, nemusel se tedy zabývat s hotovostí, jejíž přeprava byla v tehdejší době poměrně nebezpečná. Využití štítků však bylo limitováno pouze na konkrétní obchod.

Přibližně ve stejnou dobu vznikly další předchůdci platebních karet – cestovní šeky. Cestovní šeky, které později převzaly i významné dopravní společnosti jako American Express a Wells Fargo či Bank of America značně usnadnily cestování. Ve své podstatě cestovní šeky fungovaly jakou předplacené karty, klient si zakoupil cestovní šek v určité hodnotě, na který se podepsal. Dále získal doklad o zaplacení a telefonní spojení na klientské centrum pro případ problému. Při platbě nebo výběru hotovosti ve směnárně předložil klient šek a průkaz totožnosti a znovu se podepsal, přičemž podpis musel být shodný s podpisem na šeku. To zabránilo snadnému zneužití šeků, jako je tomu v případě peněz. Bez shodného podpisu a průkazu totožnosti byl šek bezcenný. Různé šeky však mohly být úspěšné pouze za předpokladu, že je akceptovalo dostatečné množství obchodníků.

Počátkem 20. století se začaly transformovat i stávající metal charge plates do své nové podoby, kdy je postupně začalo využívat čím dál tím větší množství obchodů. Většina velkých řetězců postupně nabízela vlastní kartu, ať již v podobě úvěrové karty, kdy klient mohl své nákupy postupně splácet, nebo přednabité karty, kterou si za určitou cenu zakoupil, a poté sloužila namísto platby v hotovosti. Tyto karty se rozšířily do širokého spektra různých odvětví, od obchodních řetězců jako byl Sears Roebuck přes telegrafní společnosti Western Union až po čerpací stanice Mobil a Shell.

Bylo tak běžným zvykem, že člověk u sebe nosil několik různých karet, každou pro jinou síť obchodů. Zároveň začínají vznikat skupiny obchodníků, kteří si navzájem uznávají své karty a tím rozšiřují možnost jejich využití. Kolem roku 1936 měla jen jedna z těchto sítí v Seattlu kolem tisíce obchodů, kde bylo kartou možné platit.

Druhá světová válka pozastavila vývoj platebních karet, jelikož vláda omezila čerpání spotřebních úvěrů, které odváděly finance potřebné na válku. Krátce po válce se však platební karty vrátily v plné síle jako v předválečném období. Roku 1947 byly vydány první úvěrové karty pod názvem Air Travel Card, které přijímalo všech 83 členů Mezinárodní asociace leteckých dopravců IATA. Díky tomu se Air Travel Card stala první mezinárodně uznávanou úvěrovou kartou.

1.1.1. Vznik Diners Club a American Express

První univerzální platební kartou, kterou bylo možné použít ve více různých oblastech, byla v roce 1950 Diners Club Identification Card. S kartou Diners Club bylo možné zaplatit v nasmlouvaných hotelích, restauracích, obchodech, či u přepravců. Z pohledu obchodníků měla velkou výhodu v tom, že riziko nesolventnosti zákazníka se přesunulo z obchodníka akceptujícího kartu na Diners Club. Ten ručil za své klienty a sám nesl riziko. Vzhledem k tomu si ale Diners Club také účtoval poplatek z částky, kterou zákazník u obchodníka zaplatil. Tento poplatek zpočátku tvořil 5-7% a zároveň se účtoval roční poplatek 5 dolarů za vydání karty a její správu.

Díky akvizicím a dobrému obchodnímu modelu se karta rychle rozšířila a roku 1956 již měla přes 250 000 klientů a více než 9 000 míst, kde bylo možné kartu využít. Kartou bylo možné platit po celých spojených státech, včetně Kanady. Mezinárodní charakter karty Diners Club ukázal, že mohou konkurovat cestovním šekům a nemusí se omezovat na konkrétní regiony nebo oblasti podnikání. Díky bezkonkurenčnímu počtu uživatelů a stále rostoucímu počtu obchodníků, kteří kartu akceptovali, se stala jakousi ikonou, díky čemuž se její využití nadále rozrůstalo.

Roku 1958 vstupuje na trh platebních karet American Express, jejíž cestovní šeky jsou podrobeny tvrdé konkurenci ze strany Diners Club Card. Tento fakt American Express nakonec přinutí ke vstupu na trh s vlastní kreditní kartou. Díky akvizici Universal Travel Card a vlastní síti míst, která přijímají cestovní šeky American Express, dokáže nová kreditní karta nabídnout již v prvním roce svého provozu na 17 500 akceptačních míst.

Aby získala další akceptační místa a napomohla rychlému rozšíření, požaduje American Express od obchodníků pouze 3-4% z transakce, tedy méně než Diners Club.

V této době se již běžně nevyužívají papírové karty, kde jsou údaje předtištěny nebo ručně napsány, ale stále více se využívá plastových karet, které mají vyraženy údaje o svém majiteli. Jednak je těžší tyto plastové karty padělat, ale zároveň se tím usnadňuje a zpřehledňuje zpracování transakce. K tomu se využívá tzv. imprinter, do kterého se karta vloží, a přes kopírovací papír se údaje vyražené na kartě otisknou přímo na účtenku, kterou pak klient podepíše.

Roku 1958 vstupuje po dlouhé přípravě na trh platebních karet i BankAmericard od největší americké banky, Bank of America. Bank of America nabízí dva druhy kreditních karet podle movitosti klientů, White Card s limitem 300 dolarů a Gold Card s limitem 500 dolarů. Klientovi jednou měsíčně odesílá vyúčtování všech jeho transakcí a dává bezúročné období 30 dní, pokud splatí celý úvěr. Pokud se rozhodne splácet postupně a přesáhnout bezúročné období, strhává si banka úroky.

Během dvou let měla BankAmericard více než 2 miliony držitelů po USA. Zároveň však začalo docházet k významným problémům, když úvěrové ztráty, které byly původně odhadovány na 4%, přesáhly 22%. Karty se staly terčem podvodníků, kteří je využívali k malým platbám, kde nebyla požadována autorizace, nebo jejich klienti nedokázali nebo nechtěli splácet své úvěry. Karta tak vlastně platila za svoji rozšířenost, kdy se dostala do rukou masám lidí, kteří však kreditní kartu nikdy získat neměli. Zákon navíc neznal zneužití kreditní karty a banka tak nemohla ani žádat o pomoc policii.

Reakcí bylo důkladné zpřísnění pravidel pro vydání kreditní karty. Banka začala dbát na důslednou kontrolu movitosti klienta a zpřísnila požadavky. Zároveň zavedla oddělení pro vymáhání pohledávek, které řešilo problémy s nesplácením úvěrů. Díky tomu sice klesl počet uživatelů karet na polovinu, ale v roce 1961 se BankAmericard dostala poprvé do zisku.

1.1.2. Problémy při zavádění platebních karet

Ostatní bankovní domy sledovaly nástup BankAmericard a viděly obtíže, se kterými se potýká největší americká banka. Mnohé se však i přesto pokusily v 60. letech zavést vlastní kreditní kartu, jelikož kreditní karta byla tehdy v módě. Aby tyto banky získaly akceptační místa, snažily se vytvořit kritickou masu uživatelů, která by obchodníky přilákala. Aby

toho dosáhly, stanovovaly nízké nebo zcela žádné nároky na vlastníka karty a vydávaly je všem klientům, kteří o ni požádali, ale i těm, kdo o ni ani nepožádali. Jsou známy i případy, kdy banky rozesílaly kreditní karty podle telefonních seznamů nebo některým klientům poslaly karet hned několik. Zároveň požadovaly nízké poplatky od obchodníků akceptujících karty, mnohdy nižší než 1%. Kreditní karty tak díky těmto faktorům generovaly masivní ztráty, například karta Citibank dosáhla v roce 1971 ztráty 11 milionů dolarů. Celkové ztráty amerického bankovního sektoru v roce 1970 způsobené kreditními kartami dosahovaly 115,5 milionu dolarů.

Zároveň se množily stížnosti klientů, kteří dostávali karty, které si nevyžádali. Ukradené nebo ztracené karty byly zdrojem mnoha problémů, jelikož banky neměly téměř žádná opatření, jak při krádeži či ztrátě postupovat. Tento přístup vedl ke vzniku zákona, který zakazoval rozesílat nevyžádané kreditní karty a ukončil tak stávající praktiky, při kterých bylo podle odhadů rozesláno až 100 milionů nevyžádaných kreditních karet.

1.1.3. Vznik MasterCard a VISA

Banky čelily při vydávání karet zásadním problémům – aby obchodníci jejich karty akceptovali, musely banky nabídnout dostatečné množství klientů. Předchozí přístup, kdy vydaly kartu všem svým klientům, se však neosvědčil a poukázal na druhý problém. Žádná banka nemůže vydat kartu klientům, kteří u ní nemají vedeny účty nebo nedosahují odpovídající bonity, tím se vystavuje neúměrnému riziku. Řešením těchto problémů se stalo budování asociací mezi různými bankami. Různé banky využívaly jednu kreditní kartu, čímž dosáhly dostatečného počtu klientů pro oslovení obchodníků a zároveň se vyvarovaly rizikových klientů.

V 60. letech došlo v přibližně stejné době ke vzniku dvou asociací, Western States Bankcard Association (WSBA), která měla za členy na 200 amerických bank, převážně ze západního pobřeží USA, a Interbank Card Association (ICA), která zahrnovala východní pobřeží USA. Po složitých jednáních došlo v roce 1967 ke spojení obou asociací, čímž bylo pokryto celé území USA jedinou asociací. Asociace využívala logo a označení Master Charge, nynější MasterCard. Roku 1971 zaznamenává Master Charge o třetinu vyšší obrat než konkurenční BankAmericard a téměř dvojnásobný obrat než American Express a Diners Club.

V reakci na konkurenci ze strany Master Charge začala i Bank of America nabízet ostatním bankovním domům využití BankAmericard. Na rozdíl od Master Charge karta stále nesla

název BankAmericard, a banky tak na svých kartách měly obchodní značku svého hlavního konkurenta, což se později stalo značným problémem. Koncem šedesátých let začaly banky zapojené do BankAmericard požadovat decentralizaci vedení a nezávislost na Bank of America. Přes počáteční nesouhlas byla Bank of America nakonec nucena kapitulovat a v roce 1970 byla vytvořena National BankAmericard Inc. (NBI), dnešní VISA.

1.1.4. Zpracování transakce

S nástupem karetních asociací a významným postavením American Express a Diners Club začal upadat význam karet jednotlivých obchodních řetězců a sítí. Většině z nich se totiž nepodařilo expandovat mimo vlastní odvětví a přes vysoké počty klientů (Texaco mělo vydáno 35 milionů karet, Esso 45 milionů) nemohly konkurovat kartám, které bylo možné využít i jinak než při platbě v jednom konkrétním typu obchodu.

1.1.5. Kreditní karty v Evropě

Vznik kreditních karet v Evropě probíhal odlišně od USA. Část bank sice zpočátku vydávala vlastní kreditní karty, ale velké množství bank se raději přidalo k některé z karetních asociací. Příkladem může být anglická Bank of England, které přijala American Express, nebo italská Bank of America and Italy, která přijala BankAmericard. Úspěch slavila asociace EuroCard International, která vznikla spojením dvou konkurujících si karetních systémů Rikskort a Wallenberg. Její význam v Evropě byl natolik velký, že v roce 1969 uzavřela strategické spojenectví s Master Charge.

Odlišně postupoval vývoj ve Francii, kde se pod vedením Société Générale vytvořil karetní systém zvaný Carte Bleue, jenž zahrnoval nejvýznamnější francouzské banky. Do roku 1970 měly Carte Bleue na 437 000 klientů a disponovaly 39 000 akceptačními místy.

1.1.6. Kreditní karty v Japonsku

V Japonsku díky vlivu americké kultury a hospodářství začaly první kreditní karty vznikat již v roce 1960. První karty byly vydány pod značkou Nippon Diners Club, ale až v roce 1961 založila jedna z nejvýznamnějších japonských bank společnost Japan Credit Bureau (JCB). Jelikož japonské zákony nedovolovaly bankám vydávat kreditní karty, musely banky zakládat dceřiné společnosti, jako byla JCB. Od roku 1966 se vlastnictví JCB rozdělilo mezi další japonské banky a v pozdějších letech přibyly i obchodní společnosti a průmyslové firmy jako například Toyota Motors. JCB se zpočátku zaměřovala hlavně na

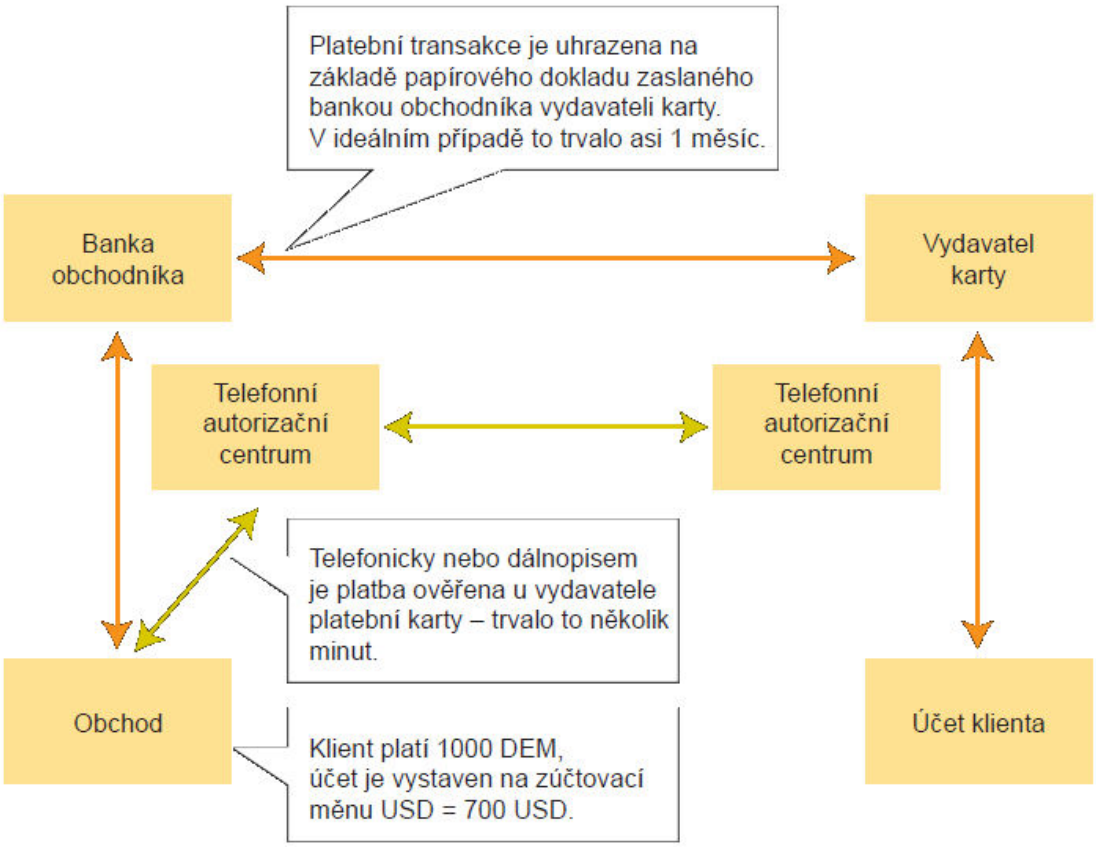
domácí trh, kde brzy získala 50% podíl. Posléze se však přesunula i na zahraniční trhy, aby svým klientům poskytla alternativu k „cizím“ kartám.

1.1.7. Automatizace v oblasti přijímání platebních karet

Od počátku 70. let tedy existují všechny dnešní mezinárodní karetní asociace, American Express, Diners Club/Discover, MasterCard, Visa a JCB. K dalšímu rozvoji karet pak přispěl hlavně technický pokrok, díky němuž jsou dnes natolik rozšířeným způsobem platby. Roku 1973 již bylo 85% platebních karet opatřeno magnetickým proužkem, který byl poprvé na platební kartě použit teprve o čtyři roky dříve a umožňoval strojové čtení údajů na kartě.

V přibližně stejnou dobu vstupují na světlo světa první bankomaty, nejdříve ve Spojených státech a Británii. Jejich provoz je zpočátku drahý a problémový a banky se jejich zavádění brání. O několik let později přichází i bankomaty, které umožňují provádět operace na účtu klienta nebo přijmout obálku s penězi.

V této době též dochází k nutnosti upravit současný autorizační systém fungující na základě telefonických hovorů a obíhajících papírových kopií prodejních dokladů. S rozvojem počítačů začínají všechny karetní asociace budovat vlastní počítačová centra, která autorizují transakce. Například pro VISA (dříve BankAmericard) znamenalo zavedení počítačů zkrácení doby autorizace na 56 sekund z původních pěti minut a ušetření 30 milionů dolarů jen za první rok provozu. Obrázek 1 popisuje provedení transakce před příchodem počítačových center.



Obrázek 1: Zpracování transakce platební kartou v 70. letech, zdroj: Juřík

70. léta též znamenala nástup platebních terminálů. Původní platební terminály sloužily v offline režimu, kdy přijaly údaje z karty a ověřením vůči vlastní databázi zablokovaných karet a platnosti karty schválily nebo odmítly transakci. Pravidelně, většinou jednou denně, se prováděla aktualizace databáze a přenos údajů o platbách z terminálu do zúčtovacího centra. Nejdříve se k tomu využívaly diskety, později telefonní a datové linky. Od roku 1979 VISA zavedla první terminály, které online ověřovaly každou transakci.

Rozšíření platebních terminálů a vznik bankomatových sítí po celém světě vedl banky k zamyšlení, zda by nebylo možné pomocí kreditních karet nahradit dosud používané šeky, jejichž vzájemné zaúčtování a zpracování vyžadovalo vysoké náklady. První offline debetní karty se nesetkaly s příliš velkým úspěchem, jelikož obchodníci neviděli důvod k jejich akceptaci. Z jejich pohledu se jednalo o náhradu šeku, za jehož zpracování však platili pouze malý poplatek, zatímco za transakci s debetní kartou si banky účtovaly stejné ceny jako za kartu kreditní. Až díky snížení poplatků v polovině 80. let se stala úspěšnou offline karta MasterCard II či online debetní karta VISA Check.

V devadesátých letech pak MasterCard přichází s debetní kartou Maestro, která se během několika let stává nejúspěšnější debetní kartou. Ve stejnou dobu přichází konkurenční VISA s VISA Debit, Electron a Interlink.

1.1.8. Vznik EMV

S příchodem mikroprocesorů a postupujícím technologickým pokrokem začínají v devadesátých letech vznikat první prototypy čipových karet. Předpokládané zvýšení bezpečnosti díky čipu a ochraně pomocí PIN kódu testují banky nasazením zkušební sady 115 000 kusů karet s čipem dle standardu EMV (Europay/MasterCard/Visa). Vzhledem k masivní úspěšnosti projektu je již po roce rozhodnuto o výměně všech platebních karet v Británii za karty s EMV čipem.

Příjem plateb pomocí čipu a PIN kódu dle standardu EMV však vyžaduje, aby byl obchodník vybaven odpovídajícím zařízení. Díky prokazatelně vyšší bezpečnosti čipových karet došlo v Evropě ke změně, kdy odpovědnost za podvodné transakce, kterým by bylo možné zabránit, kdyby měl obchodník zařízení umožňující platbu dle EMV, nese právě obchodník.

1.1.9. Moderní trendy v oblasti platebních karet

Nejnovějším trendem v oblasti platebních karet je využití tzv. bezkontaktních karet, které stačí přiblížit k odpovídajícím terminálu. MasterCard zahájila pilotní testování této technologie na konci roku 2002. Později se technologie MasterCard označovaná jako PayPass osvědčila natolik, že byla zavedena do běžného provozu. VISA experimentovala s rozdílným systémem, ale v roce 2005 došlo k dohodě mezi MasterCard a VISA o společném využívání systému MasterCard PayPass, též evidovaným jako ISO 14448. Tato dohoda na sjednocení technologie, stejně jako dřívější dohody na společném přístupu k magnetickému proužku či čipu umožnila plošné nasazení bezkontaktních karet.[1]

1.2. Druhy platebních karet

Existuje několik druhů platebních karet, které lze rozlišit podle způsobu, jakým mohou být užity. Stejně tak se liší i požadavky kladené na držitele jednotlivých karet. Debetní karty bývají vydávány k běžným bankovním účtům, zatímco u kreditních karet nebo charge cards nemusí být držitel karty majitelem konta v bance, která kartu vydává. Na rozdíl od debetní karty však musí být dostatečně důvěryhodný, aby mu banka kreditní kartu vydala.

[1] JUŘÍK, P. *Platební karty: 1870-2006 : velká encyklopedie*. 1. vydání, Praha: Grada, 2006.

Přednabité karty pak představují zcela zvláštní typ karty, který míří právě na klienty, kteří nemají u banky účet nebo nechtějí, aby s ním byla jejich karta spojena.

Podle společnosti MasterCard je možné platební karty rozlišit na následující druhy[2]:

1.2.1. Kreditní karty

Kreditní karty umožňují svému majiteli čerpat tzv. revolvingový úvěr. Ve své podstatě se jedné o koupi na úvěr, který držitel následně splácí, z tohoto důvodu je při vydávání kreditní karty posuzována schopnost klienta splácet úvěr.

Kreditní karta umožní čerpat úvěr až do částky, která je předem stanovena při vydání karty. Pro tento úvěr je stanovena doba, do které musí být splacena celá částka nebo její stanovená část. Pokud je v této lhůtě celý úvěr nebo požadovaná část splacena, je po držiteli karty požadován nulový úrok z úvěru. V případě, že tuto lhůtu překročí, je po klientovi již požadován předem dohodnutý úrok, který zpravidla přesahuje běžné úrokové míry.

V České republice je bezúročné období pro většinu kreditních karet 55 dní, v případě překročení bezúročného období se úroková sazba pohybuje v rozmezí 18,99% - 23,99% p.a.[3]

Charge karty

Charge cards jsou druhem kreditní karty, ale oba pojmy nejsou navzájem zaměnitelné. Charge cards na rozdíl od kreditních karet vyžadují do určitého časového rámce splatit celý úvěr, ne pouze jeho část. Na rozdíl od kreditních karet také není omezen limit, kterého je možné s kartou dosáhnout.

Charge cards míří především na bohatší klientelu, než jsou uživatelé kreditních karet. Jejich cílem jsou majetní lidé ochotní utrácet na dluh, ale zároveň natolik zodpovědní, že své závazky včas splatí v plné výši. Za odměnu charge cards zpravidla nabízejí slevové a věrnostní programy na základě objemu utracených prostředků.

---

[2] *MasterCard Worldwide - All about payment cards.* [on-line]. [cit. 2014-03-10]. <http://www.mastercard.com/us/company/en/docs/All_About_Payment_Cards.pdf>. (přeložil Fuchs, M.)

[3] *Kreditní karty online - Ušetřeno.cz* [online]. [cit. 2014-03-10]. Dostupné z: <http://www.usetreno.cz/kreditni-karty/>.

1.2.2. Debetní karty

Debetní karty jsou napojeny přímo na běžný účet klienta. Při platbě u obchodníka nebo výběru peněz je transakce okamžitě provedena a z klientova účtu jsou odepsány odpovídající prostředky. Debetní karty poskytují široké možnosti využití, od přímých plateb u obchodníků jak fyzicky, tak přes internet či po telefonu, po výběry z bankomatu a možnosti cashback.

1.2.3. Přednabité karty

Přednabité karty existují v mnoha různých variacích, ale jejich princip zůstává stejný. Jedná se o kartu, která není napojena na klientův běžný účet, místo toho je na ní nabita určitá konkrétní částka, kterou může klient uplatnit v závislosti na typu karty. Karty mohou být vydávány konkrétními společnostmi, jako jsou obchodní řetězce, a mohou pak být využity pouze při platbách v tomto řetězci, nebo se může jednat o nezávislé karty vydávané například ve spolupráci s MasterCard, které lze využít při jakékoliv platbě stejně jako klasickou debetní kartu.

Přednabité karty na jedno použití

Přednabité karty na jedno použití jsou většinou omezeny na platbu u konkrétního obchodníka a bývají též označovány jako dárkové poukazy nebo vouchery. Po jejich vyčerpání je není možné znovu použít a je nutné zakoupit nové.

Přednabité karty na více použití

Přednabité karty na více použití bývají vydávány ve spolupráci s karetní asociací, jakou je například MasterCard, a nesou její logo. Možnosti jejich využití jsou stejně široké jako u debetních karet, lze je použít kdekoliv, kde lze zaplatit debetní kartou, stejně tak je možné je využít k výběru z bankomatů. Jediným rozdílem je, že karta není napojena na běžný účet a disponuje pouze takovými prostředky, které jsou na ní momentálně uloženy. V případě vyčerpání těchto prostředků je nutné kartu znovu nabít.

Pro nabití karty zpravidla existuje množství způsobů, od převodu z účtu, přes přesun hotovosti pomocí debetní karty nebo pomocí SMS. Veškeré transakce spojené s nabíjením karty bývají obvykle náležitě zpoplatněny.

Výhodou předplacené karty je především ochrana klientova běžného účtu při případném zneužití karty, dále pak její dostupnost i pro klienty, kteří nemají běžný účet v bance.[4]

1.3. Technologie v oblasti platebních karet

Během poměrně dlouhého vývoje platebních karet existovalo množství typů a použitých technologií. Dnešní platební karty podléhají řadě standardizací, které zajišťují jejich přenositelnost a celosvětovou použitelnost. Zároveň ve většině případů kombinují několik různých technologií určených ke zjednodušení transakce a většímu zabezpečení karty.

Platební karty vycházejí ze standardu ISO/IEC 7810 ID-1, který charakterizuje jejich základní fyzické vlastnosti. Pro platební karty je využíván standard ID-1, který stanovuje rozměry 85,6 x 53,98mm s tloušťkou karty 0,76mm a zaoblenými rohy. Dále stanovuje požadavky na ohebnost karty, hořlavost, odolnost vůči chemikáliím a další podobné vlastnosti. [5]

ISO/IEC 7812 definuje způsob a provedení, jakým jsou karty popisovány. Definuje se způsob číslování i font, který se používá. ISO/IEC 7811 a 7813 určuje požadavky na magnetický proužek a embossing karty, ISO/IEC 8583 a 4909 pak definuje způsoby uložení informací a komunikace s magnetickým proužkem pro účel finančních transakcí. Novější standard ISO/IEC 7816 stanovuje požadavky na kontaktní čipové karty, ISO/IEC 14443 pak stanovuje požadavky na bezkontaktní čipové karty.

Díky široké mezinárodní standardizaci je možné využít karty od různých vydavatelů v jednom platebním terminálu. Díky tomu se snižují náklady obchodníka (nemusí pořizovat více terminálů) a pro držitele karty se tak zvětšuje množství míst, kde může kartu využít.

Většina platebních karet v Evropě odpovídá standardu EMV, jedná se tedy o karty čipové. Následující schéma popisuje konkrétní dispozice takovéto karty a význam jednotlivých technologických prvků:

---

[4] *MasterCard Worldwide - All about payment cards.* [on-line]. [cit. 2014-03-10]. <http://www.mastercard.com/us/company/en/docs/All_About_Payment_Cards.pdf>. (přeložil Fuchs, M.)

[5] *ISO 7810:2003 Identification cards -- Physical characteristics.*, [on-line]. 2003. [cit. 2014-03-10]. <http://www.iso.org/iso/catalogue_detail?csnumber=31432>. (přeložil Fuchs, M.)

Obrázek 2: Příklad platební karty s EMV čipem, zdroj: VISA

- Logo vydavatele karty (karta často obsahuje kromě loga vydávající karetní asociace i logo banky nebo partnera)
- Bezpečnostní hologram (slouží k ochraně karty proti padělání a určení její pravosti při manuální prohlídce)
- EMV čip
- Číslo karty (první číslo identifikuje sektor karty – 4 a 5 je bankovnictví a finance, prvních 6 čísel celkově identifikuje vydavatele karty. Na příkladu je vydavatel VISA, který má identifikátor 4. Další čísla jsou pak identifikátorem držitele karty a kontrolní součet)[6]
- Datum platnosti (vždy se uvádí datum, kdy platnost karty končí, může ale navíc obsahovat i datum, kdy platnost začíná)
- Jméno držitele karty

Zadní strana karty pak obsahuje magnetický proužek a podpisový proužek. Bez podpisu držitele není karta platná. Zpravidla na okraji podpisového proužku se pak uvádí trojciferný CVV2/CVC2 kód, který slouží k ověření držitele karty při platbách přes internet či po telefonu.

[6] *ISO 7812-1:2006 Identification cards – Identification of issuers.* [on-line]. 2006. [cit. 2014-03-10]. <http://www.iso.org/iso/catalogue_detail?csnumber=39698>. (přeložil Fuchs, M.)

1.3.1. Embossing

Embossing, neboli fyzické vyražení klíčových údajů (číslo karty, datum platnosti a jméno držitele karty) do plastické karty, byl jednou z prvních technologií, které měly usnadnit provádění transakce. Při platbě embossovanou kartou je možné využít tzv. imprinteru, do kterého se karta vloží, a přejetím válečkem se vyražené údaje na kartě otisknou na stvrzenku.

Zpracování imprinterem bylo rychlejší než původní přepisování údajů a zabraňovalo též chybám při opisování. V dnešní době se k tomuto zpracování transakce přistupuje pouze zřídkakdy, zpravidla je využíváno jako záloha při poruše platebního terminálu. Výhodou embosovaných karet je jejich využitelnost i v místech, kde jsou imprintery stále ještě využívány. Nevýhodou však je menší bezpečnost karty, kdy zablokování karty pro běžné transakce je provedeno téměř okamžitě po nahlášení držitelem, ale stoplistování pro platby přes vyražené údaje trvá zpravidla 24 hodin.[7]

Přestože je embossing na dnešních platebních kartách téměř přežitkem, je stále hojně využíván, částečně kvůli zajištění maximální zpětné kompatibility, částečně i kvůli větší důvěryhodnosti, kterou vyražené údaje na kartě údajně přinášejí.

1.3.2. Magnetický proužek

Technologie ukládání dat na kovový proužek za pomoci magnetismu pochází již z dob druhé světové války. Do spojení s platebními kartami se dostala díky společnosti IBM, jejíž inženýři jako první přišli s plastovou kartou opatřenou magnetickým proužkem, který měl uchovávat data o kartě.

Magnetický proužek na platebních kartách umožňuje rychlou komunikaci s platebním terminálem nebo bankomatem, který obsahuje čtečku magnetického proužku. Projetím magnetické karty čtečkou tak získá veškeré potřebné informace pro provedení (nebo zamítnutí) transakce, což umožňuje její automatizaci.

Díky dohodě mezi karetními asociacemi je možné v platebních terminálech či bankomatech použít karty různých vydavatelů, jelikož mají stejný formát. Standard ISO/IEC 7813 určuje fyzické charakteristiky platební karty – velikost, tvar, umístění magnetického proužku a dále pak i strukturu, v jaké jsou data na proužku uložena.

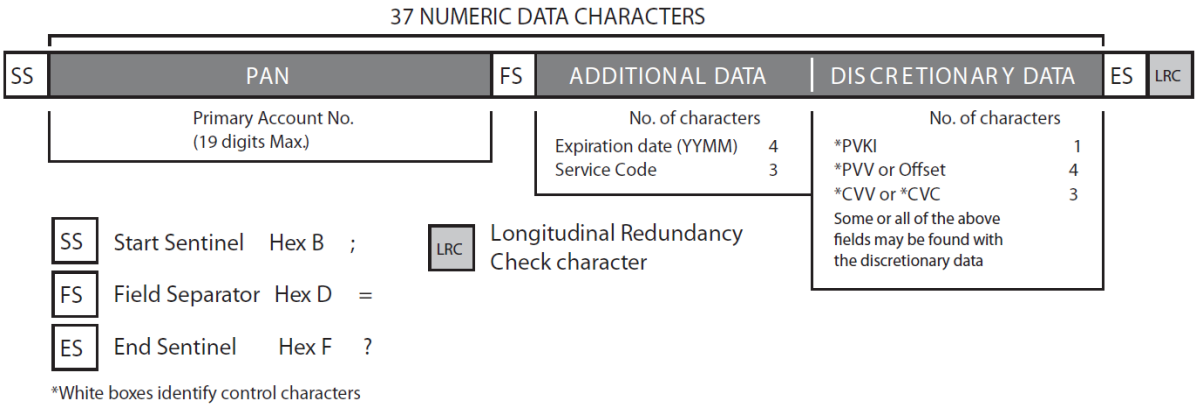
---

[7] JUŘÍK, P. *Platební karty: 1870-2006 : velká encyklopedie*. 1. vydání, Praha: Grada, 2006. ISBN 80-247-1381-0.

Magnetický proužek sestává ze tří stop, přičemž každá nese určité informace. První stopa obsahuje 79 alfanumerických znaků a jako jediná obsahuje i jméno držitele karty. Druhá stopa nese 40 numerických znaků. Obě dvě stopy dohromady zaznamenávají všechny potřebné informace pro provedení platby, číslo účtu, jméno držitele karty, dobu expirace karty a servisní kód nesoucí pokyny pro užití karty (za jakých okolností je možné s kartou platit a zda je vyžadován PIN). Třetí stopa je jedinou stopou, kterou je možné přepisovat. Mohou zde být například uvedeny informace o poslední transakci, které je možné využít při provádění offline transakcí. Ve většině případů však není třetí stopa využívána a u některých karet se ani nevyskytuje, pak se jedná o tzv. karty s tenkým proužkem.

Karty s magnetickým proužkem významně usnadnily placení kartou, ale v dnešní době je jejich technologie velmi zranitelná. Magnetický proužek lze snadno přečíst a takto získané údaje pak použít k platbám na internetu či k vytvoření kopie karty, se kterou pak podvodník zaplatí. Jako náhrada magnetického proužku tak nastoupila technologie čipových karet se standardem EMV, které jsou mnohem bezpečnější. Přesto jsou však i čipové karty opatřeny magnetickým proužkem, aby bylo dosaženo zpětné kompatibility a bylo s nimi možné platit i v oblastech, které ještě zcela nepřešly na novou technologii čipových karet.

Obrázek 3 popisuje rozložení údajů na druhé stopě magnetického proužku. První stopa obsahuje stejné údaje a navíc ještě jméno držitele karty.



Obrázek 3: Formát údajů na druhé stopě magnetického proužku, zdroj: MagTec

- PAN - číslo účtu identifikující vydavatele karty a kartu samotnou.
- Expiration code - datum platnosti, uvádí se, do kdy je karta platná.
- Service code - servisní kód, dává pokyny, jak s kartou zacházet. První číslice určuje, kde je možné kartu použít (národní/mezinárodní platby) a jak s kartou komunikovat (zda použít čip). Druhá číslice klade požadavek na online ověření u vydavatele. Třetí číslice určuje, k čemu je možné kartu použít (zboží, služby, hotovost, pouze pro bankomat, bez omezení), a klade požadavek na zadání PIN kódu.
- PVKI a PVV jsou kódy sloužící k ověření PIN kódu.
- CVV nebo CVC jsou kódy podobné CVV2/CVC2. Jejich účelem je ověřit, zda je při platbě u obchodníka skutečně přítomna existující platební karta.[8]

[8] *Magtek.com - Magnetic stripe cards standards* [on-line]. 2011. [cit. 2014-03-10]. <http://www.magtek.com/documentation/public/99800004-1.08.pdf>. (přeložil Fuchs, M.)

1.3.3. Čipové karty

Čipové karty, též známé jako smartcards, při komunikaci s platebním terminálem nebo bankomatem nespoléhají na zranitelný magnetický proužek, ale místo toho komunikují přes integrovaný čip. Stejně jako u magnetického proužku, i u čipových karet je využíváno mezinárodního standardu, který zaručuje akceptování karet od různých vydavatelů. Pro čipové karty se využívá standardu EMV (Europay, MasterCard, Visa), který je též standardizován jako ISO/IEC 7816 pro kontaktní karty a ISO/IEC 14443 pro karty bezkontaktní.

Čipová karta vyžaduje pro provedení transakce terminál, který odpovídá standardu EMV, jelikož komunikuje s terminálem pomocí šifrovaného spojení, což zabraňuje jednoduchému čtení a zaznamenávání informací, jako tomu bylo v případě magnetického proužku. Pro šifrovanou komunikaci s terminálem využívá integrovaný čip šifrovací algoritmy jako je 3-DES, RSA nebo SHA. [9]

Dalším stupněm zabezpečení čipové karty je nutnost zadání PIN kódu pro ověření držitele karty. Z tohoto důvodu se například v Británii používá označení technologie jako Chip and Pin. PIN kód nahrazuje podpis účtenky a manuální inspekci karty, jako tomu bylo u platebních karet dříve. V některých oblastech se však vydavatelé karet častěji přiklání k variantě Chip and Signature (hlavně z historických důvodů), kdy se držitel karty verifikuje stále pomocí podpisu. Tento způsob však není tolik bezpečný jako použití PINu. Chip and Pin karty jsou nejrozšířenější v Evropě, Chip and Signature jsou naopak běžnější v USA a Austrálii. Možná je i kombinace Chip, Pin and Signature.

EMV čipové karty jsou momentálně nejbezpečnějším typem platební karty. Jejich slabinou je však nutná přítomnost magnetického proužku, který stále nese informace nezbytné k provedení transakce a umožňuje tak zpětnou kompatibilitu v platebních systémech, které dosud nejsou kompatibilní s EMV standardem. Přestože okopírovanou kartu není zpravidla možné zneužít v EMV terminálu bez znalosti PINu, lze ji snadno zneužít u prodejců, kteří EMV terminál ještě nemají, nebo při platbách v internetových obchodech, které nevyžadují zadání bezpečnostního kódu CVV2/CVC2.

[9] *ISO 7816:2004 Identification cards – Integrated circuit cards.* [on-line]. 2004. [cit. 2014-03-10]. <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45144>. (přeložil Fuchs, M.)

Z tohoto důvodu se karetní asociace snaží o co nejrychlejší rozšíření EMV terminálů. K tomu se též využívá i tzv. liability shift, který byl poprvé uveden v roce 2005 v Evropě, a přenáší odpovědnost za škodu způsobenou zneužitím karty z vydavatele karty na prodejce, který ještě nedisponuje EMV terminálem, který by zneužití karty zabránil. Postup migrace platebních terminálů na EMV v Evropě se i díky tomuto rozhodnutí značně urychlil, a karetní asociace tak plánují zavedení podobného přístupu i pro další světové oblasti s cílem prosadit bezpečnější variantu platebních karet.

Původní myšlenka smartcard počítá i s jejím využitím v různých oblastech. Přestože momentálně jsou karty většinou využívány pouze pro účely placení, samotná podstata integrovaného čipu s vlastním operačním systémem a aplikacemi umožňuje, aby karta plnila různé funkcionality. Původně zamýšlenou funkcionalitou bylo například uchovávání uživatelských dat nebo třeba biometrických údajů uživatele. Stejně tak měla technologie čipové karty umožnit vlastnictví jedné karty, která by v sobě zahrnovala různé platební aplikace, například funkci kreditní karty, debetní karty nebo třeba elektronické peněženky či slevových kupónů, to vše na jednom fyzickém nosiči. Povětšinou však dnešní čipové karty plní převážně pouze jednu konkrétní funkci. [10]

1.3.4. Bezkontaktní karty

Bezkontaktní platební karty jsou dnes z velké části postaveny na systému PayPass od MasterCard, která systém poprvé vyzkoušela roku 2003. Od bezkontaktních platebních karet se vyžaduje kompatibilita se standardem ISO/IEC 14443, jak PayPass od MasterCard, tak PayWave od VISA ze standardu vychází.

Bezkontaktní platební karty jsou ve většině případů postaveny na standardu EMV čipové karty a jsou tak kompatibilní i s EMV platebními terminály. Bezkontaktní platba vyžaduje přítomnost terminálu kompatibilního s ISO/IEC 14443, který dokáže s kartou komunikovat.

Kromě EMV čipu obsahuje karta integrovaný čip pro rádiovou komunikaci a anténu. Čip zajišťuje stejné funkce jako v případě EMV, udržuje data o kartě a pomocí aplikací nahraných na čipu komunikuje přes anténu s platebním terminálem. Bezkontaktní karta neobsahuje zdroj energie, aktivně tedy nekomunikuje, dokud se nedostane do blízkosti

[10] JUŘÍK, P. *Platební karty: 1870-2006 : velká encyklopedie*. 1. vydání, Praha: Grada, 2006. ISBN 80-247-1381-0.

magnetického nebo elektromagnetického pole, které je natolik silné, aby napájelo integrovaný čip. Pro komunikaci s běžným terminálem je proto nutné kartu přiložit velmi blízko k terminálu, standardně uváděná maximální možná vzdálenost je 4 palce, mnohdy je však nutné kartu na terminál přímo přiložit.[11]

Nutnost přiblížit kartu k terminálu na krátkou vzdálenost má zabezpečit kartu proti nechtěnému přečtení, brání nevědomé platbě při průchodu kolem terminálu nebo snadnému přečtení karty třetí osobou s mobilním terminálem. Vzdálenost, na kterou je možné s kartou komunikovat, však záleží na různých faktorech, jako je například velikost antény, nebo síla, s jakou terminál vysílá. Technologie bezkontaktních plateb není zcela totožná s technologií RFID tagů, ale sdílí s ní základní principy. Díky tomu je možné využít například antény v rámu dveří (stejně jako bezpečnostní rámy v obchodech) a aktivovat tak jakoukoliv bezkontaktní kartu, která se ocitne mezi rámy.

Bezkontaktní karty však svým způsobem připomínají spíše EMV čipové karty, pouze používají jiný komunikační prostředek. Stejně jako EMV karty, i bezkontaktní karty umožňují šifrované spojení s terminálem pomocí různých šifrovacích metod, například šifry 3-DES. Stejně jako EMV karty, i bezkontaktní karty vyžadují ověření držitele karty pomocí kódu PIN. Z hlediska bezpečnosti je jejich hlavní nevýhodou nutnost zadat PIN až pro transakce přesahující stanovený limit. Limit obvykle bývá stanoven na 50 amerických dolarů, případně 25 Euro. V České republice je například pro karty PayPass stanoven limit do 500Kč na transakci. Platby do tohoto limitu nevyžadují ověření PIN kódem, platby přesahující tento limit ověření PIN kódem již vyžadují, jinak transakce neproběhne.[12][13]

Výhodou bezkontaktního placení je stálý dohled držitele karty, který ji nikdy neztrácí z očí, ani z ruky. Díky tomu není karta natolik ohrožena neoprávněným přečtením a zkopírováním magnetického proužku nebo informací, které jsou vytištěné přímo na kartě.

[11] *ISO 14443-1:2008 Identification cards – Contactless integrated circuit cards*. [on-line]. 2004. [cit. 2014-03-10]. <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39693>. (přeložil Fuchs, M.)
[12] *SMARD CARD ALLIANCE - About smard cards: Frequently asked questions.* [on-line]. [cit. 2014-03-10]. <http://www.smartcardalliance.org/pages/smart-cards-faq>. (přeložil Fuchs, M.)
[13] *MASTERCARD - Co je to MasterCard PayPass?.* [on-line]. [cit. 2014-03-10]. <http://www.paypass.cz/stranka/1/co-je-paypass/>.

Přesto ale existují spory ohledně zranitelnosti karty, obzvláště kvůli snadnému navázání komunikace s kartou bez jakéhokoliv vědomí jejího držitele. [14]

1.3.5. E-Commerce

Platby v internetových obchodech a další platby na dálku jsou specifické oproti standardním platbám tím, že při platbě nevstupuje do hry samotná platební karta, ale pouze informace o ní. Z tohoto důvodu se transakce tohoto typu označují jako CNP (card not present). Stejné označení se užívá i při platbách po telefonu, které jsou si s internetovými platbami velmi blízké.

Různé platební aplikace vyžadují různé údaje o kartách. Zatímco některé se spokojí pouze se základními údaji, jiné vyžadují z důvodu bezpečnosti důkladnější ověření držitele karty. CNP platby na rozdíl od plateb s přítomností karty neprošly tak rozsáhlou standardizací a existuje tak několik způsobů, jakými se obchody snaží ověřit držitele karty. Zároveň se karetní asociace, vzhledem ke stoupajícím objemům plateb přes internet, snaží přijít s bezpečnějšími způsoby, jak ověřit vlastnictví karty.

Většina platebních aplikací vyžaduje pouze zadání údajů o platební kartě, na základě kterých autorizuje transakci. Požadované informace mohou být následující:

Číslo karty

Číslo karty je při platbě požadováno vždy, jelikož se jedná o základní identifikační údaj. Během začátků plateb po internetu bylo původně vyžadováno pouze číslo karty, což však nese silnou bezpečnostní hrozbu, a to převážně pro obchodníka přijímajícího platbu. Čísla karet nejsou generována náhodně, ale vznikají podle určitého algoritmu. Při pokusu o falešnou platbu je tak možné podle tohoto algoritmu generovat čísla karet a je pouze otázkou času, kdy bude některé z nich číslo skutečně platné karty a obchod transakci autorizuje. Dříve navíc neprobíhaly autorizace mezi obchodem a vydavatelem karty okamžitě, ale číslo se ověřovalo pouze na základě algoritmu, nemuselo se tedy ani jednat o platnou kartu. Vzhledem k velké zranitelnosti byly požadované údaje rozšířeny a pouze samotné číslo karty se již nepoužívá.

[14] *MASTERCARD - Osobní karty MasterCard*. [on-line]. [cit. 2014-03-10]. <https://www.mastercard.com/cz/osobni-karty/cz/paypass.html>.

Číslo karty a jméno

Samotné číslo karty nahradily údaje o čísle a navíc ještě jméno držitele karty tak, jak je napsáno na kartě. Číslo karty stále slouží jako identifikace a jméno držitele slouží jako ověření pravosti karty. Při pokusu o platbu obchodník, respektive jeho platební aplikace, ověří u vydavatele karty shodnost jejího čísla a jména držitele. To odstraňuje předchozí zranitelnost generováním náhodných čísel karet, jelikož jméno a číslo karty jsou dva na sobě nezávislé údaje, pokud se shodují, pak taková karta existuje.

Požadavek na jméno držitele však neodstraňuje zranitelnost systému z pohledu vlastníka karty. Jak číslo karty, tak jméno jsou údaje, které je velmi jednoduché získat. Oba jsou na kartě fyzicky napsány nebo vyraženy a oba jsou zaznamenány na magnetickém proužku karty. V případě odcizení karty nebo zaznamenání údajů na magnetickém proužku tak hrozí zneužití.

Číslo karty a CVV2/CVC2

CVV2 nebo CVC2 je trojciferný bezpečnostní kód, který je zapsán zpravidla na zadní straně karty u podpisového proužku. Tento kód není zaznamenán na magnetickém proužku, nehrozí tedy jeho zneužití v případě, že dojde k úniku údajů na magnetickém proužku. Kód je náhodně generován pomocí tajného algoritmu, který zná pouze vydavatel karty, není tedy možné bez této znalosti přiřadit k číslu karty odpovídající kód. CVV2/CVC2 však neochrání kartu, pokud je fyzicky odcizena nebo si podvodník bezpečnostní kód manuálně zaznamená.

3D-Secure

3D-Secure systémy si berou za cíl zvýšit bezpečnost plateb v internetovém prostředí. Svým způsobem se jedná o variaci na technologii čipových karet s PIN kódem. VISA jako první přišla se systémem Verified by Visa, MasterCard nabízí MasterCard SecureCode, JCB J/Secure a American Express nejnověji přichází s American Express SafeKey.

Princip všech těchto systémů je stejný. Při platbě kartou u internetového obchodníka je do procesu vložen jeden dodatečný krok, který zákazníka přesměruje na stránku vydavatele karty. Zde klient navíc ještě zadá bezpečnostní kód, který ověří jeho totožnost. Jedná se o kód, který není nikde na kartě zaznamenán, a tudíž nemůže být získán ani při krádeži karty ani při získání dat, které jsou na kartě zaznamenány. Konkrétní implementace bezpečnostního kódu se může lišit, zpravidla se jedná o heslo, ale je možné využít i

externích čteček karet či bezpečnostních klíčů připojených k počítači. Nabízí se i možnost ověřit držitele karty pomocí SMS zprávy s jednorázovým bezpečnostním kódem.[15] [16]

Ověření zkušební platbou

Jedná se o velmi bezpečný způsob ověření držitele kreditní karty, který používá například platební portál PayPal. Klient zaregistruje u obchodníka svoji kartu, a ten provede transakci s nízkou sumou (PayPal používá 50Kč). Ve výpisu transakcí u své banky pak klient v informacích o transakci najde kód, který pro něj obchodník náhodně vygeneroval. Ten pak zadá na stránkách obchodníka a tím potvrdí, že je skutečně držitelem karty.

Tento způsob ověření je velmi silnou ochranou, jelikož potvrzuje klientův přístup k bankovnímu účtu. Není však využitelný v běžných obchodních podmínkách, jelikož je zde nutná lhůta pro zpracování transakce bankou.

[15] MONTAGUE, D. *Essentials of online payment security and fraud prevention*. New York: Wiley, 2010. ISBN 04-706-3879-6. (přeložil Fuchs, M.)
[16] MONTAGUE, D. *Credit card fraud: the professional's guide to preventing credit card fraud in e-commerce, mail order and telephone order sales*. Victoria, B.C: Trafford, 2004. ISBN 14-120-1460-3. (přeložil Fuchs, M.)

1.4. Útoky na platební karty

Útoky na platební karty lze rozdělit do dvou typů podle typů transakcí – CP a CNP. Při CP útocích je útok veden přímo proti fyzicky přítomné kartě. Při CNP útocích není karta přítomna a karta je tak napadena pouze zprostředkovaně přes informace, které o ní poskytne uživatel.

Ve většině případů není cílem útoku zmocnit se samotné karty, jelikož odcizení karty bývá zpravidla brzy odhaleno a klient kartu nahlásí jako ztracenou nebo odcizenou a po stoplistaci vydavatelem se stává bezcennou. Cílem je naopak získat data o kartě bez vědomí jejího majitele a ta pak využít k vytvoření padělané karty (counterfeit card) nebo k CNP nákupům pouze za pomoci takto získaných dat.

Banky a vydavatelé karet se nezaměřují pouze na prevenci útoků, ale aktivně se snaží o jejich včasné odhalení. Automatizované systémy za pomoci různých algoritmů a dataminingu hledají v údajích o provedených transakcích podezřelé údaje, které vyhodnotí jako možné zneužití karty. V tomto případě pak mohou být údaje o konkrétních transakcích ověřeny u klienta a v případě potvrzeného zneužití je karta stoplistována. Tyto systémy mohou díky své efektivitě odhalit zneužití dříve, než ho zaznamená sám klient a zkracují tak dobu, po kterou může pachatel kartu zneužívat. [17]

1.4.1. Cíle útoku

Útoky lze též rozlišit podle jejich cíle. Existují dva typy, které se však v některých případech mohou překrývat. První typ útoku si bere za cíl data o kartě. Jeho cílem není odcizit přímo finanční prostředky, ke kterým má karta přístup. Cílem je naopak získat dostatek informací o kartě, aby pomocí nich mohly být finanční prostředky odcizeny v budoucnu. Pro tento typ útoku je typická snaha zamaskovat ho před majitelem karty tak, aby v ideálním případě ani nepostřehl, že karetní data byla odcizena. V některých případech proto mezi odcizením a následným zneužitím údajů proběhne delší doba, místy i v řádech měsíců, čímž se pachatelé snaží zamést stopy po útoku, který data odcizil. Typické příklady těchto útoků jsou uvedeny níže, patří mezi ně skimming, phishing, krádeže karet, krádeže údajů o kartách v CNP prostředí nebo krádeže identity.

[17] *Computer Weekly.com: IT Security. 2008 - How banks are detecting credit fraud.* [on-line]. [cit. 2014-03-10] <http://www.computerweekly.com/feature/How-banks-are-detecting-credit-fraud>. (přeložil Fuchs, M.)

Druhým typem útoku je pak samotný pokus o odcizení finančních prostředků za pomoci nelegálně získaných informací o kartě nebo jejím uživateli. Těchto typů útoků je méně, povětšinou se jedná o využití padělané karty (nově vytvořené karty, která obsahuje předem získané informace), ukradené nebo ztracené karty, nebo o využití získaných informací v internetových obchodech, kde si pachatel na kartu objednává většinou dobře a rychle zpeněžitelné zboží, jako je například elektronika. Při tomto útoku je již téměř jisté, že bude odhalen, ať již bankou, nebo samotným uživatelem. Otázkou tak zůstává pouze čas, po který bude možné pomocí karty čerpat peníze, než banka kartu zablokuje.

Ve statistických údajích o kriminalitě spojené s platebními kartami se obvykle sledují právě údaje o druhém typu útoků. Získat informace o tom, kde byly zneužité údaje získány je totiž v mnoha případech velmi obtížné, ne-li zcela nemožné. Proto nejsou takové údaje většinou ani uváděny, pokud se nejedná o odhalení významného množství těchto útoků.

1.4.2. Skimming

Skimming je patrně nejznámějším typem útoku na platební kartu, jelikož bývá pravidelně medializován. Přesto jsou však některé formy skimmingu, které jsou při správném provedení téměř neodhalitelné. Jedná se o útok, při kterém jsou během provádění transakce odcizeny údaje o kartě a to bez vědomí jejího držitele. Zpravidla se tak děje pomocí čteček magnetického proužku, které jsou pachatelem umístěny na platební terminál nebo bankomat a zamaskovány tak, aby nevzbudily pozornost. Často je též na takto napadeném zařízení nainstalována miniaturní kamera, které snímá oblast klávesnice a zaznamenává zadávaný PIN kód. Pachatel tak získává veškeré údaje o kartě a navíc disponuje i PIN kódem.

Skimming se však neomezuje pouze na úpravu platebního terminálu nebo bankomatu, formou skimmingu je i neoprávněné získání údajů za pomoci obsluhy terminálu, ať již fyzickým přepsáním údajů z karty nebo pomocí čtečky. V České republice podle policie ČR k podvodům za pomoci obsluhy dochází nejčastěji v barech, restauracích, čerpacích stanicích nebo hotelech. Z tohoto důvodů je důležité si kartu při platbě hlídat a nikdy nedovolit obsluze, aby ji odnesla do zázemí nebo mimo dohled držitele.

Skimmovací zařízení

„Skimmovací zařízení je technické zařízení umožňující zkopírování elektronických údajů z platební karty. Taková zařízení bývají nejčastěji montována na bankomaty v místech pro vkládání karty. Skládá se z části, která načítá data z platební karty vložené do bankomatu a části, která umožňuje získat číselný PIN kód. Pouze získání obou těchto údajů umožní osobám, které nelegálně kopírují údaje z platební karty, následnou výrobu padělků karet a nelegální výběry z finančních účtů v ČR i v cizině.

Kopírovací zařízení jsou nejčastěji montována na štěrbinu pro vkládání karty formou různých nástavců napodobujících originál nebo formou panelu, který bývá montován na originální součást bankomatu. Zařízení pro odpozorování PIN kódu bývá umísťováno do horního panelu bankomatu (kamera, mobilní telefon) nebo bývá používána falešná klávesnice, která je samostatně nebo formou celého panelu montována na originální klávesnici nebo panel bankomatu.

Kopírovací zařízení a krycí lišty kopírovacích prostředků na bankomatech jsou vesměs provedeny v barvě a kovu velmi podobných materiálů, ze kterých je bankomat vyroben. Při zběžném pohledu jsou tato zařízení od originálu téměř nerozpoznatelná.

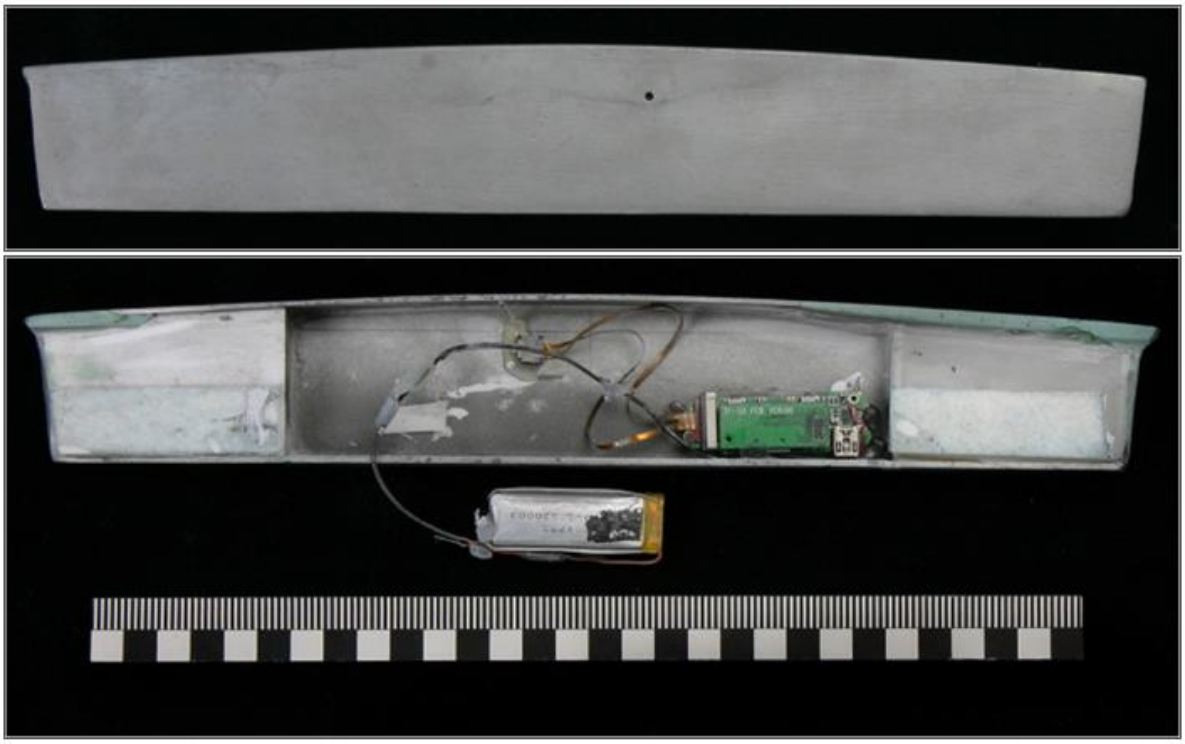
Před časem začaly bankovní společnosti v reakci na nárůst tohoto typu podvodů používat ochranný prvek proti skimmingu tzv. antiskimmovací nástavec, který je montován na štěrbinu pro vkládání platební karty a měl by zabránit montáži skimmovacího zařízení, nejnovější případy však potvrzují, že i tato ochrana je překonatelná, neboť byly zajištěny modely kopírovacích zařízení mající shodné provedení s bezpečnostním antiskimmovacím nástavcem.

Vedle údajů z magnetického proužku je dalším důležitým údajem pro pachatele skimmingu PIN kód. K jeho zjištění (odpozorování) využívají pachatelé v případě bankomatů kamery, mobilní telefony nebo speciální klávesnici, která bývá umísťována na klávesnici nebo místo klávesnice původní. V případech, kdy je pro snímání PIN kódu použita kamera, je pak umístěna většinou v liště nad rámem obrazovky.“[18]

[18] *Policie české republiky - SKIMMING.* [on-line]. 2010. [cit. 2014-03-20]. <http://www.policie.cz/clanek/skimming.aspx>.

Obrázek 4: Antiskimmovací nástavce, zdroj: Policie ČR

Obrázek 5: Falešné antiskimmovací nástavce, zdroj: Policie ČR



Obrázek 6: Falešná lišta s kamerou pro snímání PIN kódu, zdroj: Policie ČR

1.4.3. Ukradené karty nebo karty ztracené v poště

Krádež platební karty je nutné neprodleně nahlásit bance a kartu stoplistovat, aby se snížilo nebezpečí jejího zneužití. I přes technologii čipových karet a ochranu PIN kódem je totiž možné kartu zneužít, například při platbě přes internet, jelikož z karty je možné vyčíst veškeré nezbytné informace.

Krádež a následné zneužití nově vydaných karet, které byly teprve poslány poštou klientovi, bylo velmi oblíbené v době, kdy se platební karty teprve zaváděly a byly posílány klientům v obrovském množství, často aniž by o tom sami klienti věděli. Princip spočívá v tom, že pachatel odcizí zásilku s kartou, ať již z poštovní schránky klienta nebo například během transportu poštou. Ve výsledku tak získá originální platební kartu s nevyplněným podpisovým proužkem, do kterého může podle jména pravého držitele doplnit vlastnoruční podpis, který pak může vydávat za pravý a podepisovat se s ním při platbě touto kartou. Podpis na účtence se ověřuje vůči podpisu na kartě, není tudíž možné zjistit, že samotný podpis na kartě je podvrh.

S rozmachem těchto útoků přišla i opatření ze strany bankovních domů, které jsou obvykle tím, kdo komunikuje s klientem ohledně nové karty. Existuje několik způsobů, jak je možné kartu přiměřeně chránit, a většinou se využívá alespoň jeden z nich.

Datum platnosti

Nově vydaná platební karta je bankou odeslána klientovi se značným předstihem a klient je informován, že karta je na cestě. Je vyrozuměn, že pokud mu nebude karta doručena do určité doby, má kontaktovat banku. Aby do této doby nemohla být karta zneužita, tak se kromě data, do kdy je karta platná, uvádí i datum, od kdy je karta platná, viz. obrázek č.2. Kartu nelze použít před tímto datem a do té doby by měl klient nedoručení karty nahlásit bance, která ji stoplistuje.[19]

Vyzvednutí na pobočce

Další možnou obranou je nezasílání samotné karty poštou. Zvykem při tomto typu obrany je zasílat poštou pouze obálku s PIN kódem ke kartě a vyrozuměním, že karta je k vyzvednutí na stanovené pobočce banky. Klient si pak musí kartu osobně vyzvednout na pobočce, kde je jeho totožnost ověřena zpravidla vůči průkazu totožnosti, případně mohou být vyžadovány například dva různé doklady. Samotný PIN kód je případném pachateli bez karty zbytečný a kartu si může vyzvednout pouze ten, kdo má platný průkaz totožnosti.[20] [21]

Aktivace karty

Klient též může obdržet platební kartu poštou, ale musí poté provést její aktivaci. Při aktivaci karty bankou je identita klienta ověřena sérií otázek zaměřených tak, že by je měl znát pouze právoplatný majitel karty. V případě, že je držitel karty pomocí otázek ověřen, je karta aktivována a je možné ji využít.[22]

---

[19] JUŘÍK, P. *Platební karty: 1870-2006 : velká encyklopedie*. 1. vydání, Praha: Grada, 2006. ISBN 80-247-1381-0.
[20] Tamtéž.
[21] *Česká Spořitelna - Zasílání karet poštou.* [on-line]. [cit. 2014-03-20]. <http://www.csas.cz/banka/nav/osobni-finance/visa-classic/zasilani-platebnich-karet-postou-d00018807>.
[22] SAKHAROVA, I. *Payment Card Fraud: Challenges and Solutions*. [on-line]. 2011. [cit. 2014-03-20]. <https://www.utdallas.edu/~bxt043000/Publications/Technical-Reports/UTDCS-34-11.pdf>. (přeložil Fuchs, M.)

1.4.4. Krádež identity

Krádež identity je útok, jehož cílem není získat klientovu platební kartu nebo informace o ní. Cílem krádeže identity je za pomoci informací získaných o jejím oprávněném držiteli, přesvědčit banku, že pachatel je právě oním oprávněným držitelem. V případě úspěchu mohou pachatelé převzít kontrolu nad účtem bez vědomí jeho majitele. Například změnou doručovací adresy zajistí, že výpisy se nedostanou k majiteli a poté nahlásí pravou kartu jako ztracenou nebo ukradenou a nechají si vydat novou, se kterou pak mají neomezený přístup k účtu. Krádež identity se nemusí omezovat pouze na platební kartu, stejně tak si může pachatel sjednat půjčku nebo úvěr. Poškozený se o tomto zneužití s velkou pravděpodobností dozví až poté, co po něm budou vymáhány splátky.[23]

K získávání informací, potřebných pro provedení takovéhoto útoku, existuje několik možných způsobů.

Dumpster diving

Dumpster diving je v podstatě prohledávání odpadu budoucího cíle. Vychází z předpokladu, že všichni lidé dostávají dopisy a oznámení z bank, obchodů, úřadů či zaměstnání, ze kterých je možné získat potřebné informace. Zároveň se počítá s tím, že málokdo tyto materiály před vyhozením zničí nebo jinak znehodnotí a při prohledávání odpadu je tak mohou pachatelé získat. Opačným přístupem může být naopak vybírání poštovní schránky. Nevýhodou však může být zvýšená ostražitost poškozeného, pokud zaznamená chybějící dopisy nebo pravidelně vykradenou poštovní schránku.[24]

Jedinou možnou ochranou proti tomuto útoku je dbát na to, aby žádné dokumenty neopouštěly domácnost ve stavu, ve kterém je možné z nich něco vyčíst. Běžné doporučení je veškeré takové dokumenty skartovat nebo roztrhat, aby údaje na nich byly nečitelné. Takovými údaji mohou být rodná čísla, různá identifikační čísla či třeba výpisy z účtů.

---

[23] *VISA - Identity Theft.* [on-line]. [cit. 2014-03-20]. <http://usa.visa.com/personal/security/learn-the-facts/identity-theft.jsp>. (přeložil Fuchs, M.)
[24] SAKHAROVA, I. *Payment Card Fraud: Challenges and Solutions*. [on-line]. 2011. [cit. 2014-03-20]. <https://www.utdallas.edu/~bxt043000/Publications/Technical-Reports/UTDCS-34-11.pdf>.

Social Networking

S rozmachem sociálních sítí přichází i obrovská příležitost pro získání klíčových osobních informací. Významným znakem sociálních sítí je sdílení všemožných informací o sobě samém, což je přesně to, co případný pachatel hledá. Je tedy nezbytně nutné, aby si uživatel i na sociálních sítích uvědomoval, jaké informace sdílí a zda nemohou být zneužity.

Pro jednoduché získání údajů od uživatelů mohou být využity například různé kvízy a hry, které pokládají otázky, jejichž cílem je lépe poznat majitele účtu. Jméno matky za svobodna, základní škola, kterou vystudoval, jméno nejlepšího přítele, oblíbený film/herečka/seriál, to vše jsou v mnoha případech bezpečnostní otázky pro verifikaci uživatele, pokud zapomene heslo. Veškeré tyto informace jsou pak dostupné pro případného pachatele.

Nejslabším článkem hesla a bezpečnosti vůbec bývá často uživatel. Mnohá upozornění varují, že pro bankovnictví by se měla používat bezpečná a unikátní hesla, která uživatel pravidelně mění a nepoužívá je nikde jinde. Množství uživatelů ale stejně používá stejné heslo pro více různých přihlášení a v případě, že se pachateli podaří získat heslo například k sociální síti, tak existuje pravděpodobnost, že stejné heslo bude fungovat například i do internetového bankovnictví.[25]

1.4.5. E-Commerce

S rozšířením internetových plateb přichází též rozvoj kriminality zaměřené právě na internetové platby. Existují různé útoky na platební karty v internetovém prostředí, na některých z nich se může podílet sám prodejce, jiné jsou naopak provedeny za pomoci prolomení bezpečnosti prodejcova platebního systému, například nabouráním se do databáze obsahující informace o platebních kartách. Transakce přes internet mají velmi blízko k transakcím prováděným přes telefon nebo poštu, pro všechny je možné použít jak stejné útoky, tak stejné způsoby obrany.

Podvodné obchody

Cílem podvodných e-shopů a zprostředkovatelů služeb je získat informace o platebních kartách svých „zákazníků“. Takto získané informace mohou pachatelé buďto přímo sami

[25]SAKHAROVA, I. *Payment Card Fraud: Challenges and Solutions*. [on-line]. 2011. [cit. 2014-03-20]. <https://www.utdallas.edu/~bxt043000/Publications/Technical-Reports/UTDCS-34-11.pdf>.

zneužít, nebo je mohou prodat dál. Nejbezpečnějším způsobem ochrany je nakupovat pouze v obchodech, které má uživatel ověřené z nějakého důvěryhodného zdroje.[26]

Odcizení údajů zaměstnancem

Při platbě kartou v CNP prostředí klient neví, kdo má na straně příjemce přístup k poskytnutým informacím. Na způsoby zabezpečení internetových plateb ze strany obchodů jsou kladeny požadavky například od PCI DSS, která stanovuje, jak mají být data chráněna a jak má být zabezpečen přístup k nim. Reálně však není možné, aby si klient ověřil, zda konkrétní obchod stanovená pravidla skutečně dodržuje.[27]

Krádež údajů z databáze

Ne ve všech případech musí být údaje o kartě ukradeny z podvodné stránky. Internetové obchody a další subjekty, které akceptují elektronické platby, si zpravidla udržují databázi klientských účtů, ke kterým bývají přiřazeny údaje o kreditních kartách. Hlavním účelem je zvýšení komfortu pro klienta, protože nemusí při každé transakci znovu zadávat veškeré potřebné údaje. V případě prolomení bezpečnosti a odcizení těchto dat, obzvláště pak u velkých společností, může dojít k ohrožení bezpečnosti tisíců karet. Příkladem je například krádež dat o účtech společnosti Sony Corporation v roce 2011, při které unikly informace o více než 100 milionech účtů, včetně údajů o platebních kartách.[28]

Takto citlivá data uložená v databázích bývají často navíc ještě dodatečně šifrována, tudíž jejich odcizení nemusí nutně znamenat jisté zneužití těchto údajů. Přesto je však v případě takovéhoto úniku nutné přinejmenším pozorněji sledovat aktivitu na kartě, případně kartu rovnou vyměnit.

1.4.6. Phishing

Phishing je stále rozšířenějším typem útoku, který nabývá na intenzitě s rozmachem online bankovnictví, e-mailů a plateb přes internet. V případě útoků na platební karty je cílem phishingu získat údaje o kartě, které jsou nezbytné pro provedení transakcí. Zpravidla se tak jedná o číslo karty, jméno držitele karty, platnost karty a CVV2 a PIN kód. Pachatelé zasílají podvodné e-mailové zprávy, které na sebe berou podobu oficiální zprávy od banky, státní

[26] *VISA* - Online shopping. [on-line]. [cit. 2014-03-20]. <http://usa.visa.com/personal/security/learn-the-facts/online-shopping.jsp>. (přeložil Fuchs, M.)
[27] *PCI SECURITY STANDARDS COUNCIL - Co je PCI DSS?* [on-line]. [cit. 2014-03-20]. <http://www.pcistandard.cz/index.php?cat=7>.
[28] *Information Week: Security - Sony Says PlayStation Credit Card Data Was Encrypted.* [on-line]. 2011. [cit. 2014-03-20]. <http://www.informationweek.com/attacks/sony-says-playstation-credit-card-data-was-encrypted/d/d-id/1097464>. (přeložil Fuchs, M.)

instituce nebo jiného důvěryhodného odesílatele. Kvalita takovýchto zpráv se může lišit, ale nejkvalitnější z nich obsahují loga dané instituce a stejný formát zprávy.

Tato podvodná zpráva pak klienta vyzývá, aby se přihlásil na určitou stránku a ověřil údaje o kartě, případně je jakýmkoliv jiným způsobem odeslal na zadanou adresu. Zpravidla je též uveden dodatek o nezbytnosti ověření nebo uvedení těchto údajů v určitém časovém limitu, jehož nesplnění povede ke zrušení konta, sankcím, ohrožení apod. Adresa nebo podvodná stránka se pak vydává za oficiální stránku dané instituce, ale ve skutečnosti slouží pouze ke shromáždění potřebných informací. U sofistikovanějších phishingových zpráv může být uvedeno i telefonní číslo pro ověření zprávy, kterým se klient dostane např. na automatický záznamník, jenž mu potvrdí autenticitu zprávy. [29]

Phishing je též poměrně známým typem útoku, který se netýká zdaleka jen platebních karet, ale i dalších údajů, které je možné zneužít. Může se tak týkat například informací o účtu apod. Banky pravidelně nabádají své klienty, aby nikdy nesdělovali údaje o kartě, a upozorňují, že banka je po nich nikdy nebude vyžadovat. Vzhledem k rozšiřujícímu se povědomí o phishingu tak vznikají nové formy útoku, které používají jiné, na první pohled bezpečnější komunikační kanály. Příkladem je smishing, který má podobu SMS zpráv, případně vishing, který využívá telefonních hovorů. [30]

1.4.7. Bezkontaktní karty

Bezkontaktní karty jsou jednou z nejnovějších technologií mezi platebními kartami, díky čemuž se brzy po svém nasazení staly terčem obzvláště pro odborníky z oblasti bezpečnosti, kteří demonstrovali některé jejich slabiny, které byly později opraveny, nebo označeny za nízkou hrozbu, jelikož bezkontaktní kartou je možné platit bez použití PIN kódu pouze v případě menších obnosů. Díky tomu společnosti vydávající tyto karty nepředpokládají významný zájem zločinců o prolomení jejich bezpečnosti.

Šifrování karet

První série karet PayPass a PayWave obsahovaly významnou bezpečnostní trhlinu, která umožňovala případnému pachateli jednoduché získání údajů o kartě. Karta komunikuje s terminálem pomocí šifrovaného spojení, ale první série karet nešifrovaly některé klíčové

[29] *VISA - Phishing.* [on-line]. [cit. 2014-03-20]. <http://usa.visa.com/personal/security/learn-the-facts/phishing.jsp>. (přeložil Fuchs, M.)
[30] SAKHAROVA, I. *Payment Card Fraud: Challenges and Solutions*. [on-line]. 2011. [cit. 2014-03-20]. <https://www.utdallas.edu/~bxt043000/Publications/Technical-Reports/UTDCS-34-11.pdf>.

údaje, jako bylo například číslo karty, díky čemuž bylo možné se k těmto údajům dostat. Dnešní bezkontaktní karty však již bezpečně šifrují veškeré údaje.[31]

Relay útoky

Relay útoky nejsou považovány pouze za teoretickou možnost, ale byly odborníky v oboru vyzkoušeny i v praxi. Princip relay útoku spočívá ve zprostředkované komunikaci mezi terminálem a bezkontaktní kartou. Využívá toho, že s kartou není nutné při platbě nijak manipulovat, stačí ji přiblížit dostatečně blízko k terminálu. Za pomoci zařízení, ideálně mobilního telefonu, který simuluje kartu, se pachatel přiblíží k terminálu. Terminál komunikuje s telefonem, jako kdyby se jednalo o bezkontaktní kartu (telefon obsahuje čip pro bezkontaktní platby). Telefon ve skutečnosti ale přeposílá údaje od terminálu do jiného zařízení, které se za pomoci jiného pachatele přiblíží k něčí bezkontaktní kartě. Ta odpoví falešnému terminálu, který přepošle informaci zpět do telefonu a ten s ní odpoví pravému terminálu. Pokud není vyžadován PIN, proběhne transakce standardním způsobem, protože údaje, které terminál i karta získávají, jsou autentické. [32]

[31] DUBINSKY, Z. *CBC News: Technology & Science - New credit cards pose security problem*. [on-line]. 2010. [cit. 2014-03-20]. <http://www.cbc.ca/news/technology/new-credit-cards-pose-security-problem-1.904220>. (přeložil Fuchs, M.)

[32] FRANCIS, L. *Practical Relay Attack on Contactless Transactions*. [on-line]. 2011. London. [cit. 2014-03-20]. <https://eprint.iacr.org/2011/618.pdf>. (přeložil Fuchs, M.)

2. Analýza rizik

Analýza rizik obsahuje dvě části. První částí je porovnání statistik o útocích v různých regionech, které analyzuje a následné vyhodnocuje statistická data od odpovědných orgánů a institucí v různých zemích světa. Druhou částí je pak kvalitativní analýza rizik spojených s využívání platebních karet vydaných v České republice. Na základě jejího vyhodnocení jsou pak navržena doporučení pro snížení rizik.

2.1. Analýza statistik o útocích v různých regionech

Cílem porovnání statistik o útocích na platební karty podle jednotlivých zemí je získat přehled o nejčastěji využívaných typech útoků v závislosti na regionu, do kterého daná země spadá, případně vyhodnocení, kde jsou jednotlivé typy útoků nejčastěji využívány.

Objektem analýzy jsou útoky, jejichž cílem je přímo odcizit finanční prostředky klienta, nikoliv útoky, které se zaměřují pouze na získání údajů o kartě nebo klientovi. Tyto útoky nemusí nutně probíhat v dané zemí ani regionu a na rozdíl od útoků, kdy jsou odcizeny finanční prostředky, jsou velmi těžko odhalitelné.

2.1.1. Metoda srovnání

Prvním krokem analýzy je identifikace klíčových zemí. Pro jednotlivé regiony nejsou ve většině případů dostupné celkové přehledy ani data (s výjimkou oblasti SEPA), mnohdy však nejsou data běžně dostupná ani pro jednotlivé země. Pro různé regiony jsou tedy stanoveny klíčové země, které jsou brány jako reprezentant daného regionu.

Druhým krokem je výběr dat pro srovnání tak, aby byla všechna data z korespondujícího období a rozlišovala útoky na stejné typy. Data pak budou převedena do stejných formátů, například dopočtem změny v útocích vůči předchozímu roku na základě statistiky z roků 2012 a 2011, dále pak přepočtem dopadu v měně jednotlivých států na jednotnou měnu pro srovnání celkového dopadu (jako společná měna bylo vybráno Euro s kurzem k 31.12.2012 podle kurzovního lístku ECB[33]). Podle vybraných typů útoků pak bude provedeno srovnání.

[33] *European Central Bank - Euro foreign exchange reference rates*. [on-line]. [cit. 2014-04-12]. <http://www.ecb.europa.eu/stats/exchange/eurofxref/html/index.en.html>. (přeložil Fuchs, M.)

2.1.2. Identifikace dat

Pro analýzu byly identifikovány následující země, USA a Kanada zastupující Severní Ameriku, oblast SEPA zastupující Evropu, dále pak Austrálie a na závěr Jihoafrická republika, zastupující oblast Afriky. Pro země z Asie a Jižní Ameriky se nepodařilo získat srovnatelná data, tudíž nejsou do analýzy zahrnuty.

Veškerá analyzovaná data jsou z roku 2012, zdrojem dat pro jednotlivé země jsou buď státní úřady, nebo bankovní asociace jednotlivých zemí.

Typy útoků

Jakožto nejčastější typy rozpoznávaných útoků byly vybrány následující:

Kradené nebo ztracené karty (Lost or Stolen) – zde jsou uvedeny jak karty ztracené nebo odcizené během jejich užívání, tak karty, které nebyly nikdy doručeny majiteli.

Padělané karty (Counterfeit Cards) – pro padělané karty rozlišují některé země kanál, přes který ke zneužití došlo – bankomat/platební terminál. V rámci této analýzy jsou uváděny statistiky pro padělané karty jakožto celek.

CNP transakce (Card not present) – veškeré podvodné transakce zahrnující e-commerce, platby přes telefon i platby poštou za využití platební karty.

Data pro jednotlivé země

Data pro jednotlivé země jsou uvedena v tabulkách a rozdělena podle typů útoků (kradené/ztracené karty, padělané karty, CNP transakce a ID theft pro země, které tuto kategorii sledují). První sloupec vždy zaznamenává celkové ztráty za rok 2012 pro každý z typů útoků a to v domácí měně. Sloupec procento vyjadřuje procentuální podíl daného typu útoku na útocích vedených proti platebním kartám v dané zemi. Sloupec změna sleduje změnu vůči minulému, s kladným znaménkem znamená nárůst dopadu daného útoku vůči roku 2011, se záporným znaménkem znamená pokles. Kurz měny informuje o převodním kurzu mezi domácí měnou a eurem koncem roku 2012. Poslední sloupec pak zaznamenává celkové ztráty pro jednotlivé útoky v přepočtu ne společnou měnu (euro) pro následné porovnání.

SEPA

Do zemí SEPA spadá celkem 28 zemí Evropské unie a 6 zemí mimo EU. Cílem SEPA je zajištění stejných podmínek pro platby v celé oblasti, jako kdyby platby probíhaly uvnitř jednoho státu. Pro oblast platebních karet je SEPA významným evropským činitelem, jelikož stanovuje různé požadavky na provádění těchto plateb. Například rozšířenost EMV technologie v prostředí SEPA, která dosahuje téměř sta procent, je z velké části připisována právě inciativě ze strany SEPA.

Pro země SEPA udržuje statistiku ECB[34] [35], která každoročně zveřejňuje statistiky ohledně využití platebních karet a s nimi spojené kriminality. Tyto statistiky obsahují jak detailní informace pro jednotlivé země, tak i souhrnné informace pro celou oblast SEPA.

Mezi identifikovanými útoky jsou kradené a ztracené karty, padělané karty a útoky v CNP prostředí. Krádež identity statistiky ECB nerozlišují.

SEPA	Celkem (EUR)	Procento	Změna	Kurz měny	Celkem (EUR)
Kradené / Ztracené	198 225 907	16,02%	-5%	1 EUR = 1 EUR	198 225 907
Padělané	266 579 668	21,54%	-1,6%	1 EUR = 1 EUR	266 579 668
CNP	772 397 499	62,43%	+12%	1 EUR = 1 EUR	772 397 499
ID theft	-	-	-	-	-

Tabulka 1: Statistika zneužití karet v oblasti SEPA pro rok 2012, zdroj: autor

Kanada

Pro Kanadu jsou statistiky[36] týkající se platebních karet a s nimi spojené kriminality dostupné přes Canadian Bankers Association, která zastupuje kanadské bankovní domy a udržuje souhrnné statistiky.

[34] *EUROPEAN CENRAL BANK - Second report on card fraud: July 2013* [on-line]. 2013 [cit. 2014-04-07]. <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf>. (přeložil Fuchs, M.)
[35] *EUROPEAN CENRAL BANK - Third report on card fraud: February 2014* [on-line]. 2014 [cit. 2014-04-07]. <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf>. (přeložil Fuchs, M.)

Mezi identifikovanými typy útoků jsou kradené a ztracené karty, padělané karty, zneužití v prostředí CNP a jsou vedeny i statistiky o převzetí účtů a karet pomocí osobních údajů a informací, což splňuje definici krádeže identity.

Kanada (Ca)	Celkem (CAD)	Procento	Změna	Kurz	Celkem (EUR)
Kradené / Ztracené	26 986 687	6,31%	-16,79%	1 EUR = 1,3137 CAD	20 542 503,62
Padělané	118 109 538	27,64%	+10,10%	1 EUR = 1,3137 CAD	89 906 019,64
CNP	268 573 473	62,87%	+3,50%	1 EUR = 1,3137 CAD	204 440 491,00
ID theft	13 543 195	3,17%	+0,64%	1 EUR = 1,3137 CAD	10 309 199,21

Tabulka 2: Statistika zneužití karet v Kanadě pro rok 2012, zdroj: autor

Austrálie

Pro Austrálii jsou statistiky[37] týkající se platebních karet a s nimi spojené kriminality dostupné přes Australian Payments Clearing Association (APCA), organizaci, která zajišťuje dohled a regulaci nad platebními systémy v Austrálii. Zároveň též udržuje a pravidelně vydává statistiky pro jednotlivé platební kanály.

Mezi identifikovanými typy útoků jsou kradené a ztracené karty, padělané karty a zneužití v prostředí CNP. Krádež identity statistiky APCA nerozlišují a není tudíž uvedena.

[36] *CANADIAN BANKERS ASSOCIATION - Credit Card Fraud and Interac Debit Card Fraud Statistics - Canadian Issued Cards.* [on-line]. [cit. 2014-04-12]. <http://www.cba.ca/contents/files/statistics/stat_creditcardfraud_en.pdf>. (přeložil Fuchs, M.)

[37] *Australian Bankers Clearing Association - Fraud Statistics 2012 Calender Year.* [on-line]. [cit. 2014-04-12]. <http://www.apca.com.au/payment-statistics/fraud-statistics/2012-calendar-year?SchemeCredit,DebitandChargeCardFraud>. (přeložil Fuchs, M.)

Austrálie (Au)	Celkem (AUD)	Procento	Změna	Kurz	Celkem (EUR)
Kradené / Ztracené	21 247 776	19,84%	+80,54%	1 EUR = 1,2712 AUD	16 714 738,83
Padělané	13 065 989	12,20%	-21,7%	1 EUR = 1,2712 AUD	10 278 468,38
CNP	72 761 292	67,95%	-1,24%	1 EUR = 1,2712 AUD	57 238 272,50
ID theft	-	-	-	-	-

Tabulka 3: Statistika zneužití karet v Austrálii pro rok 2012, zdroj: autor

Jihoafrická republika

Pro Jihoafrickou republiku jsou data o platebních kartách a s nimi spojené kriminalitě[38] dostupné přes SABRIC, South African Banking Risk Association, která udržuje statistiky a informuje o nebezpečích spojených s bankovními službami v zemi.

Mezi identifikovanými typy útoků jsou kradené a ztracené karty, padělané karty, zneužití v prostředí CNP a identifikovány jsou i krádeže identity vedoucí ke zneužití pomocí platebních karet.

JAR	Celkem (ZAR)	Procento	Změna	Kurz	Celkem (EUR)
Kradené / Ztracené	15 600 000	5,63%	-15%	1 EUR = 11,1727 ZAR	1 396 260,53
Padělané	105 100 000	38%	-45%	1 EUR = 11,1727 ZAR	9 406 857,79
CNP	154 800 000	55,97%	+16%	1 EUR = 11,1727 ZAR	13 855 200,62
ID theft	1 100 000	0,003%	+38%	1 EUR = 11,1727 ZAR	98 454,27

Tabulka 4: Statistika zneužití karet v JAR pro rok 2012, zdroj: autor

[38] *The Banking Association South Africa - 2012 Sabric Card Fraud Statistics*. [on-line]. [cit. 2014-04-12]. <http://www.banking.org.za/index.php/media-events/new-noteworthy/2012-sabric-card-fraud-statistics/>. (přeložil Fuchs, M.)

Spojené státy americké

Pro USA udržuje data o platbách a kriminalitě spojené s platebními kartami[39] organizace FED, Federal Reserve System. Statistiky však neposkytují veškeré potřebné informace. Další informace poskytuje Federal Trade Commission, která udržuje statistiky o stížnostech klientů[40]. Ani kombinace obou statistiky však neposkytuje veškeré údaje.

Statistiky identifikují zneužití za pomoci kradených a ztracených karet, padělaných karet, a zneužití v prostředí CNP, krádeže identity spojené s bankovními službami nejsou uvedeny.

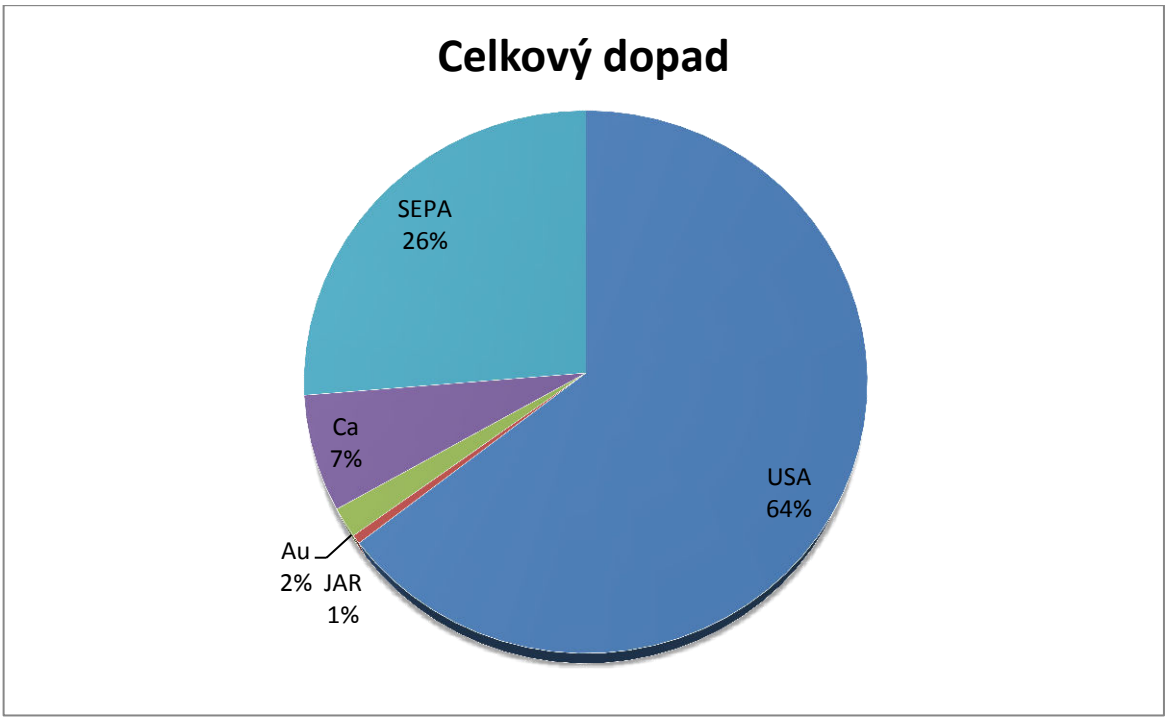
USA	Celkem (USD)	Procento	Změna	Kurz	Celkem (EUR)
Kradené / Ztracené	923 000 000	23%	-	1 EUR = 1,3194 USD	699 560 406,2
Padělané	1 477 000 000	37%	-	1 EUR = 1,3194 USD	1 119 448 234
CNP	1 600 000 000	40%	-	1 EUR = 1,3194 USD	1 212 672 427
ID theft	-	-	-	-	-

Tabulka 5: Statistika zneužití karet v USA pro rok 2012, zdroj: autor

[39] *The 2013 Federal Reserve Payments Study*. [on-line]. [cit. 2014-04-12]. <http://fedpaymentsimprovement.org/wp-content/uploads/2013_payments_study_summary.pdf>. (přeložil Fuchs, M.)

[40] *Federal Trade Commission - Consumer Sentinel Network Data Book for January - December 2012.* [on-line]. [cit. 2014-04-12]. <http://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2012>. (přeložil Fuchs, M.)

2.1.3. Srovnání podle celkového dopadu zneužití platebních karet



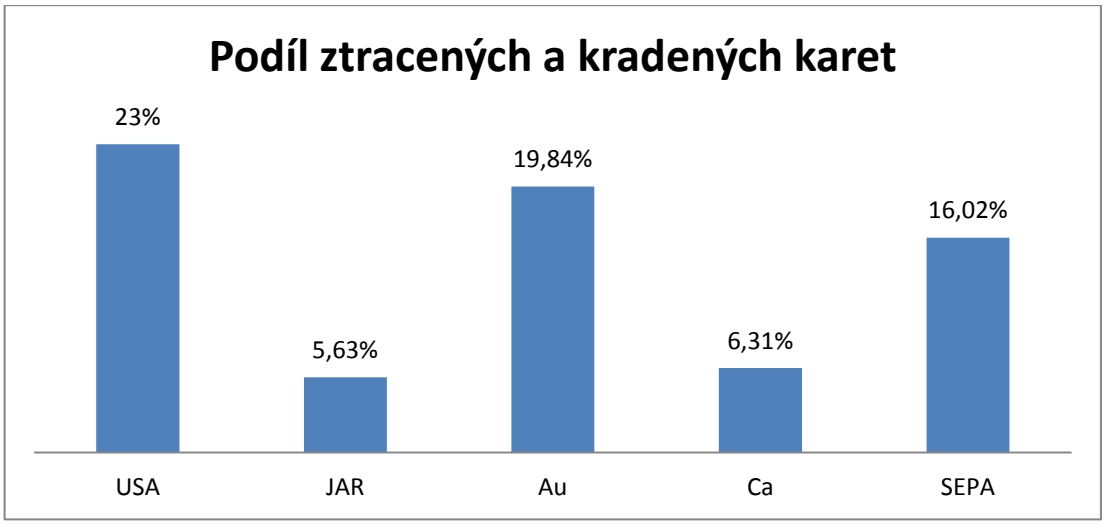
Graf 1: Srovnání celkového dopadu dle jednotlivých zemí, zdroj: autor

Celkový dopad zneužitých platebních karet pro sledované země ukazuje, že největší podíl ze všech sledovaných zemí drží USA. Toto zjištění koresponduje s údaji některých zpravodajských stanic, podle kterých USA drží téměř poloviční podíl z celosvětového dopadu zneužití platebních karet[41]. Tento stav může být způsoben jednak vysokou oblíbeností platebních karet na území USA, tak i menším zájmem o bezpečnost platebních karet v kontrastu s ostatními zeměmi. Zatímco migrace karet i terminálů v oblasti SEPA na technologii EMV dosahuje již téměř 100%, migrace v USA nebyla doposud masivně vyžadována ani propagována tak, jako je tomu v Evropě.

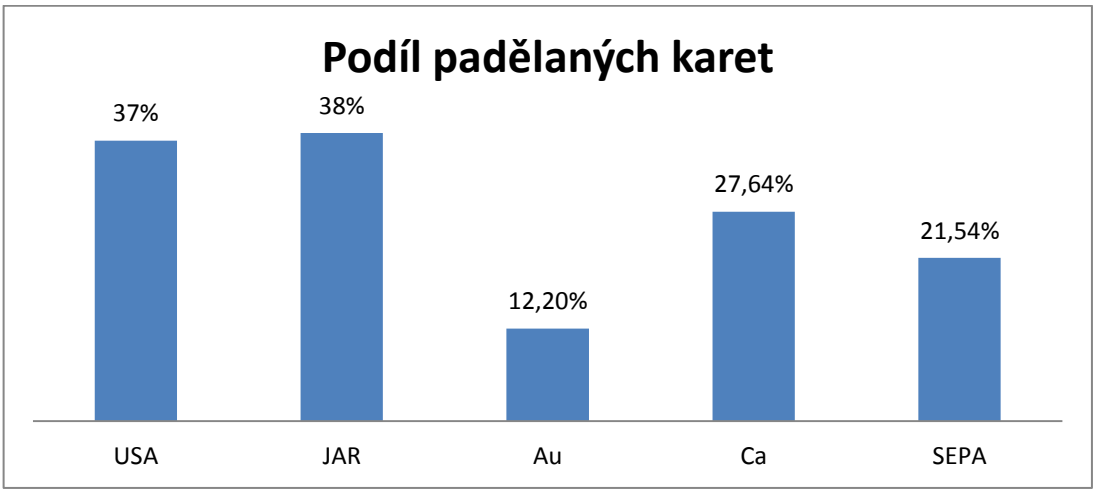
Celková úroveň dopadu však neposkytuje bližší informace, jelikož se jedná o trhy rozdílné velikost, kdy JAR nebo Austrálie a Kanada mohou těžko vyrovnat množství plateb probíhajících v oblastech jako je USA nebo SEPA. Možným řešením by bylo očištění údajů pomocí počtu platebních karet na daném trhu a přepočtem dopadu na jednu kartu. Informace o počtu karet na daném trhu jsou však ještě nedostupnější, než údaje o kriminalitě spojené s kartami.

[41] *CARDHUB – Credit card & debit card fraud statistics* [on-line]. 2013. [cit. 2014-04-12]. <http://www.cardhub.com/edu/credit-debit-card-fraud-statistics>.(přeložil Fuchs, M.)

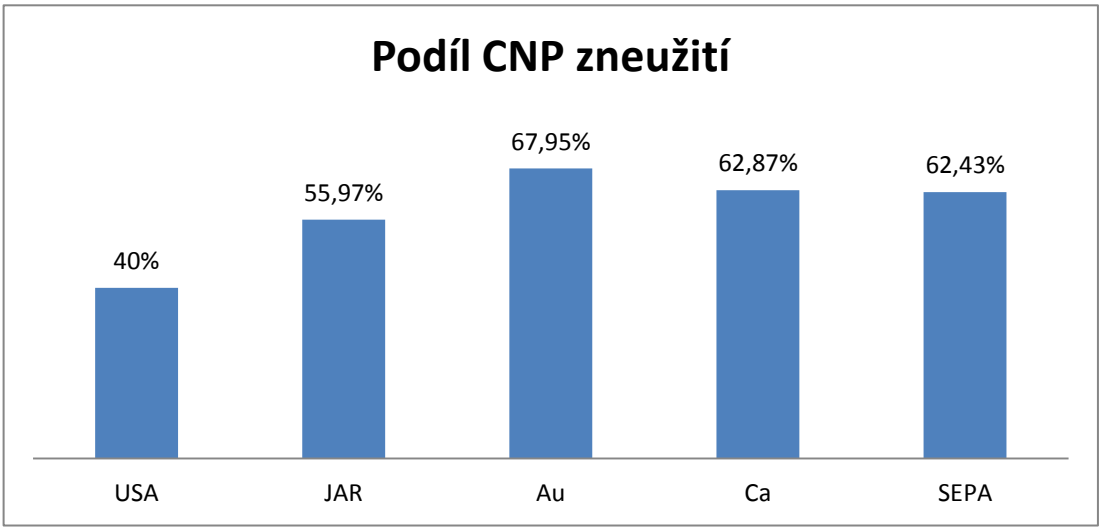
2.1.4. Srovnání podle nejčastějších typů útoku



Graf 2: Podíl ztracených a kradených karet, zdroj: autor



Graf 3: Podíl padělaných karet, zdroj: autor



Graf 4: Podíl CNP zneužití, zdroj: autor

Nejvyšší procento zneužití pomocí padělaných karet si drží země, kde ještě neproběhla migrace na EMV technologie[42], případně probíhá pomalu. USA a oblast Afriky přechází jak na EMV karty, tak na EMV terminály velmi pomalu, zatímco oblasti jako je SEPA nebo Kanada se snaží co nejvíce urychlit přechod na tuto technologii. K roku 2013 dosahuje například úroveň pokrytí EMV technologií pro SEPA jak v oblasti terminálů, tak v oblasti karet, téměř sta procent. Při přechodu na EMV obvykle dochází ke snížení podílu padělaných karet, jelikož se jejich zneužití stává složitějším, jelikož padělané karty musejí být použity v zemích, kde je nižší úroveň zabezpečení. Část pachatelů se tak přesouvá na hůře zabezpečená území, jako jsou například USA nebo Afrika.

Dalším z trendů při přechodu na bezpečnější technologie při kontaktních platbách je přesun kriminality do CNP prostředí, což je možné pozorovat i na statistikách z vybraných zemí. Země s nejmenším podílem padělaných karet mají zároveň nejvyšší podíl CNP útoků, zatímco země s vyšším podílem padělaných karet mají nejnižší podíly útoků v CNP prostředí. Celkově má však počet útoků v CNP prostředí spíše stoupající tendenci, a to ve všech oblastech, což může být připisováno hlavně stoupající oblibě těchto plateb a jejich narůstajícímu počtu.

Z hlediska ztracených a kradených karet dochází spíše k pravidelnému poklesu jejich podílu na zneužití, jelikož jsou karty čím dál více chráněny PINem, což omezuje možnosti zneužití. Dalším faktorem je též snadnější odhalení, zatímco získání údajů o kartě projde ve velkém množství případů bez povšimnutí, dokud nedojde k samotnému útoku, odcizení nebo ztráta karta bývá zaznamenána v mnohem kratší době a karta pak může být zablokována. Výjimkou v tomto ohledu je Austrálie, kde podíl zneužití kradených a ztracených karet mezi lety 2011 a 2012 vzrostl o 80%.

Novým typem zneužití se stává krádež identity. Jak je patrné ze statistik, mnohé instituce její existenci zatím nerozlišují, ale podle změny vůči předchozím rokům je zřejmé, že dochází k nárůstu počtu těchto zneužití. Toto může být způsobeno jak snadnějším přístupem k osobním údajům a informacím lidí, tak i potenciálně velkým výnosem, který může pachatel získat, jelikož odhalení tohoto typu útoku je složitější než v případě prostého zneužití karty.

[42] *EMVCo.com - Worldwide EMV Deployment and Adoption.* [on-line]. [cit. 2014-04-12]. <http://www.emvco.com/documents/EMVCo_EMV_Deployment_Stats1.pdf>. (přeložil Fuchs, M.)

2.2. Kvalitativní analýza rizik pro ČR

Cílem této analýzy je vyhodnotit nejvýznamnější rizika pro bezpečnost platebních karet a na základě tohoto vyhodnocení zpracovat návrh na zvýšení bezpečnosti platební karty. K analýze budou využita data Evropské centrální banky ze zprávy z počátku roku 2014, která analyzuje situaci v oblasti SEPA pro rok 2012[43], případně data z analýzy pro rok 2011[44].

Při analýze je nutné rozlišit mezi útokem na platební kartu, při kterém je prolomena její bezpečnost, ale jsou získána pouze data o kartě, a samotným útokem, při kterém jsou odcizeny finanční prostředky. Útoky mohou být provedeny různými osobami v různých zemích bez zjevného spojení a mohou mezi nimi být delší časové intervaly až v řádech měsíců. Útoky, při kterých jsou odcizena pouze data o kartě, projdou velmi často bez povšimnutí. Z tohoto důvodu neexistují dostatečně detailní statistiky, které by jasně identifikovaly, které útoky vůči datům na kartě jsou nejčastější. Zároveň je zde širší škála útoků na data než v případě samotného odcizení prostředků.

V případě útoku, při kterém jsou přímo odcizeny finanční prostředky, se dá hovořit o třech různých kanálech, které jsou k tomu využívány. První dva útoky probíhají s fyzickou kartou, ať již odcizenou nebo padělanou, a jsou provedeny pomocí bankomatu nebo terminálu v prodejně. U těchto útoků je třeba rozlišit, zda se jedná o padělané karty nebo karty, které jsou následně nahlášeny jako odcizené nebo ztracené. V případě padělaných karet však existuje množství zdrojů, odkud mohou zneužitá data pocházet, a ve většině případů není možné určit, kde k získání dat došlo. Třetím kanálem pro využití získaných dat jsou CNP platby. Zde též není možné jasně identifikovat zdroj dat, ale je možné snížit okruh případných podezření v závislosti na zabezpečení platby z pohledu internetového obchodu (například CVV2/CVC2 se nenachází na magnetickém proužku a nelze je tak získat při skimmingu).

Na útoky vedené vůči platebním kartám lze dále nahlížet ze dvou různých stran z hlediska postižených zemí. Je možné studovat útoky vedené proti kartám, které byly vydány v konkrétní zemi, nebo je možné se zaměřit na útoky, které byly provedeny v dané zemi proti všem kartám.

[43] *EUROPEAN CENRAL BANK - Third report on card fraud: February 2014* [on-line]. 2014 [cit. 2014-04-07]. <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf>.
[44] *EUROPEAN CENRAL BANK - Second report on card fraud: July 2013* [on-line]. 2013 [cit. 2014-04-07]. <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf>.

Při analýze útoků proti kartám vydaným v určité zemi jsou do statistiky zahrnuty i útoky, které byly provedeny v zahraničí, ale terčem byla karta vydaná ve zkoumané zemi. K tomuto jevu často dochází v například v Evropě, kde je nejvyšší míra zastoupení EMV terminálů a bankomatů a pro pachatele je tak jednodušší využít padělanou kartu v jiné zemi, kde není jejich zastoupení tak vysoké.

Analýza z pohledu karet zneužitých přímo v dané zemi naopak zahrnuje i veškeré zahraniční karty, které jsou v dané zemi zneužity, ale nezahrnuje útoky proti vlastním kartám, které proběhly mimo území dané země. V případě Evropy jsou tak mezi oběma pohledy významné rozdíly, jelikož například padělání evropských karet a jejich zneužití v bankomatu nebo terminálu je stále významnou hrozbou, ale na rozdíl od CNP transakcí je mnohem častěji prováděno mimo oblast Evropy. Při analýze zneužití karet v dané zemi by se tak toto riziko mohlo zdát neúměrně malé. K analýze byla proto vybrána první možnost, jelikož je směrodatnější pro cílovou skupinu, na kterou je práce zaměřena.

2.2.1. Metoda hodnocení

K analýze byla vybrána metodika založená na třech dále popsaných hodnotících kritériích. Podle statistik ECB bylo vybráno 5 typů útoků – ztracené nebo ukradené karty zneužité v bankomatech (dále ATM), padělané karty zneužité v ATM, ztracené nebo ukradené karty zneužité v platebních terminálech u obchodníka (dále POS), padělané karty zneužité v POS a zneužití v prostředí plateb přes internet, telefon nebo mail (dále CNP). Každý typ útoku bude bodově ohodnocen podle jednotlivých kritérií. Výsledné hodnocení pro každý útok pak bude provedeno na základě součtu dílčích hodnocení pro každé kritérium. Výsledkem bude stanovení největších rizik pro platební kartu na základě nejvyššího bodového hodnocení.

2.2.2. Kritéria hodnocení

Pravděpodobnost útoku

Pravděpodobnost útoku vychází z rozdílu ve statistikách ECB mezi roky 2011 a 2012. Záměrem je zohlednit změny v rozložení jednotlivých typů útoků na karty vydané v České republice, kdy některé jsou s postupem času využívány více, zatímco jiné jsou kvůli zvyšující se bezpečnosti vytlačeny do pozadí.

Hodnota vychází ze statistiky ECB pro roky 2011 a 2012, které identifikují změnu ve využití daného útoku vůči předchozímu roku. Hodnota je stanovena jako průměr změny z roku 2011 a 2012.

Pravděpodobnost je bodově ohodnocena na stupnici o škále 10 bodů. Pro rozsah mezi -100% a + 100% je pro -100% bodové ohodnocení 0, pro +100% je 10 bodů. Každých 20% navíc vůči minimu je hodnoceno +1 bodem. Jedná se o minimalizační kritérium, čím menší hodnota, tím méně významné se dané kritérium stává.

Dopad útoku

Dopad útoku je vyjádřen přímo v průměrných hodnotách podle typu útoku uvedených ve statistikách ECB pro rok 2012. Je vyjádřen v průměrné peněžní hodnotě ztráty v eurech, přepočtené na jednu kartu vydanou v České republice a platnou v daném období.

Celkový dopad na jednu kartu v roce 2012 je pro Českou republiku 0,32 Eur. Na stupnici o škále 10 bodů je každých 0,032 Eur navíc vůči minimu hodnoceno +1 bodem. Dopad 0 až 0,032 je tedy hodnocen 0 body, zatímco dopad 0,32 je hodnocen 10 body. Jedná se minimalizační kritérium, čím menší hodnota, tím menší je dopad daného útoku.

Zranitelnost

Zranitelnost symbolizuje náchylnost karty vůči útokům, které mohou být využity pro získání dat.

Zranitelnost je hodnocena na základě 4 typů útoků využívaných pro získání potřebných dat. Každý z nich je hodnocen na stupnici od jedné do tří. Bodové ohodnocení 0 pro daný útok na data znamená, že jej nelze využít pro tento způsob zneužití karty. Ohodnocení 1 znamená, že je možné jej využít pouze v omezených případech, ohodnocení 2 pak znamená využitelnost téměř bez překážek. Jedná se o minimalizační kritérium, čím menší je počet možných útoků, tím lépe je karta proti zneužití zabezpečena.

2.2.3. Identifikace dat

Pravděpodobnost útoku

Změna vůči předchozímu roku / rok	Kradené / ztracené karty v ATM	Padělané karty v ATM	Kradené / ztracené karty v POS	Padělané karty v POS	CNP
2011	-3%	142%	104%	19%	198%
2012	-31%	-5%	-74%	-35%	-49%

Tabulka 6: Změna v útocích vůči předchozímu roku, data ECB pro roky 2012,2011, zdroj: autor

Dopad útoku

Dopad podle útoku jako podíl všech transakcí / rok	Kradené / ztracené karty v ATM	Padělané karty v ATM	Kradené / ztracené karty v POS	Padělané karty v POS	CNP
2012	0,0002%	0,0025%	0,0002%	0,0014%	0,0045%

Tabulka 7: Dopad útoků, data ECB pro rok 2012, zdroj: autor

2.2.4. Zpracování dat

Pravděpodobnost útoku

Pravděpodobnost útoku vychází z průměrné změny vůči předchozímu roku z let 2011 a 2012 pro jednotlivé typy útoků. Hodnoty pro oba roky zvlášť jsou uvedeny v tabulce č. 1. Následující tabulka zobrazuje průměrné hodnoty pro jednotlivé útoky:

Změna vůči předchozímu roku / rok	Kradené / ztracené karty v ATM	Padělané karty v ATM	Kradené / ztracené karty v POS	Padělané karty v POS	CNP
2011	-3%	142%	104%	19%	198%
2012	-31%	-5%	-74%	-35%	-49%
průměr	-17%	68,5%	15%	-8%	74,5%
Bodové ohodnocení	4	8	5	4	8

Tabulka 8: Hodnocení pravděpodobnosti útoku, zdroj: autor

Dopad útoku

Dopad útoku identifikuje přímý finanční dopad daného typu útoku rozpočítaný na jednu kartu vydanou v České republice a platnou v době záznamu dat. ECB pro rok 2012 počítá v České republice s počtem 10 068 863[45] platných karet.

[45] *European Central Bank - Statistical Data Warehouse - Czech Republic - Number of cards - For cards issued in the reporting country, cards with a cash function - Number - Non-MFIs counterpart.* [on-line]. [cit. 2014-04-07]. <http://sdw.ecb.europa.eu/quickview.do?node=3447411&SERIES_KEY=169.PSS.A.CZ.S101.I11.Z00Z.NT.X0.20.Z0Z.Z>. (přeložil Fuchs, M.)

Celkový objem transakcí za rok 2012 pro karty vydané v České republice činil 3 591 Eur na jednu kartu. Celkem se tak jedná o částku 36 157 287 033 Eur. Následující tabulka uvádí hodnoty pro jednotlivé typy útoků přepočtené na jednu kartu:

Dopad podle útoku	Kradené / ztracené karty v ATM	Padělané karty v ATM	Kradené / ztracené karty v POS	Padělané karty v POS	CNP
Procenta	0,0002%	0,0025%	0,0002%	0,0014%	0,0045%
Částka	0,0071 Eur	0,0898 Eur	0,0071 Eur	0,0502 Eur	0,1615 Eur
Bodové ohodnocení	0	2	0	1	5

Tabulka 9: Hodnocení dopadu útoku, zdroj: autor

Dopad na jednu kartu se může zdát nízký (přibližně 32 centů na jednu kartu), jedná se však o přepočet na všechny karty a transakce, kde je zneužito pouze malé procento z nich. Při celkovém pohledu je však dopad zneužití karet pro Českou republiku 3 254 155 Eur.

Zranitelnost

Zranitelnost reprezentuje možnosti, kterých se dá využít pro získání údajů potřebných k provedení daného typu útoku. Zranitelnost je hodnocena na základě 4 typů útoků využívaných pro získání potřebných dat. Každý z nich je hodnocen na stupnici od jedné do tří. Bodové ohodnocení 0 pro daný útok na data znamená, že jej nelze využít pro tento způsob zneužití karty. Ohodnocení 1 znamená, že je možné jej využít pouze v omezených případech, ohodnocení 2 pak znamená využitelnost téměř bez překážek. Maximální zranitelnost pro daný typ útoku je tak rovna 8.

Využitelné zdroje údajů o kartě:

Skimming: Pro účel tohoto srovnání je skimmingem myšleno strojové zaznamenání údajů na magnetickém proužku karty bez vědomí jejího majitele, přičemž další zařízení zaznamenává zadávaný PIN kód. V tomto případě je zranitelnost pomocí padělané karty v ATM nebo POS terminálu ohodnocena 2 body, jelikož pachatel disponuje všemi údaji potřebnými pro vytvoření padělku karty, tak i PIN kódem pro autorizaci transakce.

Zranitelnost pomocí CNP transakcí je hodnocena 1 bodem, protože využitelnost v CNP prostředí se omezuje na internetové obchody vyžadující pouze základní ověřovací informace o kartě (konkrétně jméno majitele a číslo karty). Při strojovém záznamu údajů nelze načíst CVV2/CVC2 kód, který není na magnetickém proužku zaznamenán, takto získané údaje tedy nemohou být využity v obchodech požadujících tento kód, nebo autorizaci pomocí 3-D Secure.

Kradené / Ztracené karty: Předpokladem je, že při krádeži nebo ztrátě karty majitel nezíská i PIN kód ke kartě. Karty je možné využít jak v ATM nebo v POS terminálech, ale musí se jednat o takový typ, který nebude požadovat zadání PIN kódu. Z tohoto důvodu je jejich využitelnost omezena. Vzhledem k vlastnictví karty a tedy i magnetického proužku je možné vytvořit i padělek karty, ale se stejným omezením ohledně PIN kódu. Z pohledu CNP prostředí je možné kartu využít v širší škále obchodů než v případě skimmingu, jelikož fyzické držení karty poskytuje pachateli CVV2/CVC2 kód. Karta i nadále není využitelná v případě autorizace přes 3-D Secure, ale počet obchodů vyžadujících tuto autorizace je stále velmi omezený.

Phishing: V případě Phishingu se mohou lišit údaje, které pachatel o kartě získává. Může získat PIN kód, jméno uživatele a číslo karty, nezíská však přesný otisk magnetického proužku, který by mohl snadno použít pro padělek karty. Zbylé údaje na magnetickém proužku by bylo nutné rekonstruovat, čímž se omezuje zranitelnost v ATM nebo POS.

Větší nebezpečí však hrozí pro CNP prostředí, kde pachatel může získat jak základní údaje, tedy jméno a číslo karty, tak i CVV2/CVC2 kód, ale může získat i bezpečnostní heslo pro ověření systémem 3-D Secure a kartu tak zneužít v libovolném obchodě v CNP prostředí.

E-Commerce: Jakožto zdroj dat E-Commerce uvažujme buďto podvodný obchod v CNP prostředí, jehož cílem je získat informace od uživatelů, případně prolomení bezpečnosti korektního obchodu v prostředí CNP a získání uložených dat. Pachatel v tomto případě znovu nedisponuje otiskem magnetického proužku ani PIN kódem a využitelnost pro padělanou kartu je tak omezená. Disponuje však potřebnými údaji pro zneužití v CNP prostředí, a to s velkou pravděpodobností jak základními informacemi, tak i CVV2/CVC2 kódem.

Využitelnost zdroje údajů o kartě pro jednotlivé útoky	Kradené / ztracené karty v ATM	Padělané karty v ATM	Kradené / ztracené karty v POS	Padělané karty v POS	CNP
Skimming	0	2	0	2	1
Kradené / ztracené karty	1	1	1	1	2
Phishing	0	1	0	1	2
E-Commerce (odcizení údajů o kartě)	0	1	0	1	2
Bodové ohodnocení	1	5	1	5	7

Tabulka 10: Hodnocení zranitelnosti vůči útoku, zdroj: autor

2.2.5. Ohodnocení rizik

Následující tabulka zobrazuje ohodnocení jednotlivých typů útoků podle stanovených kritérií. Celkové hodnocení pro daný typ útoku je součtem hodnocení podle každého z kritérií. Nejmenší možné ohodnocení je 0, maximální možné ohodnocení je 28, čím vyšší je ohodnocení, tím větší riziko tento typ útoku představuje.

Typ útoku / kritérium	Kradené / ztracené karty v ATM	Padělané karty v ATM	Kradené / ztracené karty v POS	Padělané karty v POS	CNP
Pravděpodobnost útoku	4	8	5	4	8
Dopad útoku	0	2	0	1	5
Zranitelnost	1	5	1	5	7
Ohodnocení	5	15	6	10	20

Tabulka 11: Ohodnocení rizik, zdroj: autor

Bodové ohodnocení ukazuje, že největšími riziky pro platební karty je zneužití v CNP prostředí, případně padělky karet, které jsou zneužity v bankomatech nebo platebních terminálech. Zároveň se ukazuje, že bankomaty jsou z hlediska padělaných karet preferovanější než platební terminály. Zneužití ztracených karet jak v bankomatech, tak v terminálech, je nejmenším rizikem ze všech sledovaných.

2.2.6. Vyhodnocení

Závěry tohoto hodnocení odpovídají i závěrům ECB, která považuje CNP platby za vrůstající hrozbu, obzvláště kvůli rychle se zvyšujícímu objemu transakcí v tomto prostředí a velmi rozdílnému stupni zabezpečení, které je na rozdíl od bankomatů a platebních terminálů celkově spíše na nízké úrovni. Naopak hrozbu z pohledu padělaných karet považuje za klesající a to převážně kvůli stále se zvyšujícímu pokrytí EMV terminálů a bankomatů jak v evropských zemích, tak i celosvětově.

V budoucnu lze očekávat stále vyšší zájem pachatelů o internetové platby, jelikož podle statistik jejich objem neustále stoupá. Spolu s dostupnějším internetovým připojením a rostoucím počtem obchodů, které své služby nabízejí online, jsou platby v CNP prostředí nejvýznamnějším rizikem. Toto prvenství si pravděpodobně udrží do doby, dokud i toto prostředí neprojde stejnou standardizací a přesunem odpovědnosti z bank na prodejce, jako tomu bylo u platebních terminálů a bankomatů.

Přestože význam padělaných karet klesá, udržují si stále poměrně silné zastoupení mezi typy útoků a je tedy nutné s nimi počítat a reagovat přiměřenou ochranou. Přetrvávající význam této hrozby lze připisovat převážně jednoduchosti, s jakou lze pomocí skimmingu získat důležité údaje o kartě, které lze následně prodat.

3. Návrh doporučení

Cílem doporučení je představit dodatečné možnosti, které mohou pomoci snížit pravděpodobnost zneužití karty, nebo snížit jeho dopad v případě, kdy ke zneužití skutečně dojde. Navržená doporučení nejsou náhradou za běžná bankovní desatera bezpečnosti platebních karet a respektování těchto základních pokynů je nezbytné k ochraně karty.

3.1. Cílová skupina pro doporučení

Jako cílová skupina pro navrhovaná doporučení byli vybráni studenti, tedy osoby ve věku přibližně 15-26 let, kteří aktivně studují. Podle průzkumů ohledně využívání platebních karet jsou karty studentů pravidelně využívány pro širokou škálu operací, od pravidelných plateb u obchodníka po výběry z bankomatu. Podle průzkumu GE-Money 51% jejích klientů mezi studenty alespoň jednou měsíčně vybírá z bankomatu a 48% alespoň jednou měsíčně platí kartou u obchodníka. Dalším omezením bylo zaměření převážně na studenty vysokých škol, kteří mají v drtivé většině přístup k internetu a očekává se tak u nich i vyšší zájem o platby na internetu, s čímž jsou též spojena specifická rizika, na která navrhovaná doporučení reagují.[46]

3.2. Doporučení pro snížení dopadu v případě zneužití

Doporučení pro snížení dopadu počítá s tím, že údaje o kartě již byly nějakým způsobem odcizeny. V případě využívání následujících doporučení je šance na snížení dopadu na finance majitele karty tím, že se omezí možné způsoby provedení podvodných transakcí nebo se zajistí včasné informování majitele o neautorizované aktivitě na kartě.

3.2.1. Virtuální karty

Virtuální karty, též známé jako e-cards, nejsou jako ostatní typy platebních karet na fyzickém plastovém nosiči, ale místo toho se jedná pouze o souhrn údajů potřebných k platbám v CNP prostředí. Tyto údaje obsahují jméno držitele karty, číslo karty a CVV2/CVC2 kód. Na první pohled nelze údaje rozlišit od údajů z běžné platební karty.

Virtuální karty nabízí zvýšenou bezpečnost pro platby v CNP prostředí a to hlavně tím, že je nelze mimo toto prostředí využít. V případě plateb mimo CNP prostředí, ať již u obchodníka nebo při pokusu o výběr z bankomatu, nebude transakce autorizována, což omezuje možností zneužití odcizených údajů.

[46] *Měšec.cz - 93 % studentů s účtem Genius Student využívá přímého bankovnictví* [on-line]. 2007 [cit. 2014-04-07]. < http://www.mesec.cz/tiskove-zpravy/93-studentu-vyuziva-primeho-bankovnictvi/>.

Samotné zabezpečení karty není vyšší než v případě běžných karet s povolenou platbou přes internet, poskytuje možnost autorizace jménem, CVV2/CVC2 kódem nebo pomocí 3-D Secure. Vzhledem k absenci fyzického nosiče však odpadá možnost krádeže a ztráty (za předpokladu, že klient informace o kartě bezpečně uschová) nebo skimmingu.

3.2.2. Různé karty pro platby v CP a CNP prostředí

Možností, jak snížit případný dopad útoku, je využívání různých platebních karet pro různé platební kanály. Moderní platební karty sice umožňují maximální možnou flexibilitu a jedna karta tak může být využita při veškerých typech plateb, ale v případě odcizení karty nebo jejích údajů se tak zároveň zvyšuje počet možností, jak je kartu možné zneužít.

Možnou obranou je využívání dvou různých karet, jedné pro platby v obchodech a výběry v bankomatech, která je ale blokována pro platby na internetu. V tomto případě se při krádeži či ztrátě, případně při skimmingovém útoku, omezí možnosti jejího zneužití.

Druhou kartu je naopak vhodné využívat pouze pro nákupy v CNP prostředí, což zvýší její bezpečnost, jelikož nehrozí skimming. Ideální kombinací je využití klasické platební karty a virtuální karty, kterou ani nelze využít jinde než pro CNP transakce.

3.2.3. Informování o použití karty

Obecným pravidlem je, že čím dříve se na zneužití karty přijde, tím nižší je dopad na klienta. Problémem je včasné zachycení prvních transakcí, které neprovedl klient. Banky sice využívají systémy pro odhalení neautorizovaných transakcí, ty ale nemusí odhalit všechna zneužití, případně dojde k varování příliš pozdě.

Nejjistějším způsobem tak zůstává důkladné monitorování aktivity na kartách. V případě kontroly měsíčního výpisu však může být příliš pozdě. Místo kontroly pravidelných výpisů je možné využít informativních zpráv, které banky nabízejí. Klient si stanoví, o jakých transakcích chce být informován (vybere kartu, minimální částku transakce či způsob, jakým bude informace zaslána), a banka ho poté bude informovat, že takováto transakce proběhla. Pokud transakce proběhla bez jeho vědomí, tak má větší šanci kontaktovat banku a zablokovat kartu dříve, než bude opětovně zneužita.

3.2.4. Předplacené karty

Možností, jak snížit dopad případného zneužití, je využívání předplacené karty místo běžné debetní či kreditní karty. Předplacenou kartu je možné využít stejně jako ostatní karty, provést výběr z bankomatu, platbu u obchodníka nebo nákup v e-shopu. Na rozdíl od ostatních karet

však není napojena přímo na běžný nebo kreditní účet klienta a disponuje tak pouze prostředky, které na ní klient sám uložil. V případě zneužití tak klient může přijít maximálně o částku, kterou měl na kartě uloženu.

Slabou stránkou karty je však ztráta komfortu, kdy je nutné kartu pravidelně dobíjet. Podstatným záporem jsou i poměrně vysoké poplatky, které jsou spojeny jak s dobíjením karty, tak s jejím udržováním. Kartu má však své opodstatnění, například při cestování do rizikových zemí, kde je vyšší riziko odcizení karty nebo jejích údajů.

3.3. Doporučení pro snížení pravděpodobnosti zneužití

Doporučení pro snížení pravděpodobnosti zneužití se zaměřují na skrytí klíčových údajů o kartě před obchodníkem, čímž se zamezí tomu, aby obchodník vědomě či nevědomě poskytl tyto informace případnému pachateli. Další možností obrany je uzamykání karty, které nezabrání úniku dat o kartě, ale může zabránit jejich využití k odcizení finančních prostředků.

3.3.1. Uzamykání karty

Uzamykání karty je možnost, kterou některé české banky poskytují svým klientům. Přes rozdílný přístup ke konkrétnímu provedení je princip stejný, klient může okamžitě kartu sám zablokovat nebo odblokovat.

Konkrétní provedení u České spořitelny nabízí možnost blokování a odblokování za pomoci limitů. Klient si nastaví maximální limit, který pak může na omezenou dobu zvýšit na stanovenou částku a povolit tím průběh transakce. Po uplynutí klientem stanovené doby (od 1 hodiny do 5 dní) se limit automaticky vrací na původní hodnotu.

Raiffeisenbank oproti tomu nabízí možnost zamčení a odemčení karty podle příkazu klienta. Karta může být odemčena pomocí SMS zprávy pro provedení jedné transakce nebo ji může klient odemknout na stanovenou dobu.

Oba způsoby zvyšují zabezpečení karty, jelikož umožňují provést transakce pouze v okamžiku, kdy si to klient přeje. Tím se dá s poměrně velkou pravděpodobností zaručit, že budou probíhat pouze transakce, kterých si je klient vědom. Ani toto řešení však nedokáže zcela vyloučit možnost zneužití, jelikož je možné využít odblokování nebo zablokování karty v reálném čase pouze pro online autorizované transakce, v případě, že se provádí offline, nemůže být odblokování nebo zablokování provedeno.

3.3.2. Použití prostředníka v případě platby na internetu

Zvýšení bezpečnosti při platbách na internetu nabízí platební portály, které plní roli prostředníka mezi obchodníkem a klientem. Poskytovanou ochranou pro platební kartu je skrytí veškerých údajů. Obchodník nezískává údaje o kartě ani o bezpečnostních kódech, čímž je karta odstíněna a zamezí se tak možnému úniku těchto informací.

Příkladem mohou být systémy PayPal nebo PaySec, které platbu zprostředkují. Nevýhodou je podmínka, aby obchodník platbu přes tyto systémy akceptoval, a také určitý poplatek za provedení transakce, které si tyto systémy účtují. V případě použití však poskytují jistotu, že údaje o kartě se nemohou žádným způsobem dostat mimo kontrolu klienta.

4. Dotazníkové šetření

4.1. Metoda šetření

Prvním krokem šetření bylo zpracování dotazníku, který může ověřit využitelnost navržených doporučení v praxi. Klíčovým bylo stanovení otázek, které ověřují povědomí o jednotlivých způsobech ochrany platební karty a následně zjišťují, zda jsou tato doporučení pro uživatele využitelná. Z tohoto důvodu je dotazník rozdělen na dvě hlavní části, první z nich ověřuje povědomí o způsobech ochrany, druhá zjišťuje zájem o využití jednotlivých způsobů ochrany.

4.2. Soubor respondentů

Cílová skupina pro doporučení byla stanovena jako studenti, čímž se předpokládá přibližně věkové rozmezí 15 – 26 let a aktivní studium, převážně pak na vysoké škole. Z tohoto důvodu bylo dotazníkové šetření zaměřeno na stejnou cílovou skupinu. Bylo prováděno na studentech VŠE v Praze a to ve dvou fázích. V první fázi bylo prováděno pomocí online průzkumu, na který byli respondenti odkázání buďto přímo e-mailem nebo pomocí sociálních sítí. Druhá fáze šetření probíhala pomocí osobního rozhovoru se studenty VŠE. Osobní oslovení studentů zajišťuje naplnění podmínky, kdy respondenty jsou pouze osoby spadající do skupiny studentů.

Pro zajištění co nejvyšší míry objektivity byly vybrané osoby jak z informatických oborů, tak i z oborů mimo informatiku, jelikož u studentů informatických oborů by bylo možné očekávat lepší povědomí o možných rizicích a na ně reagujících způsobech ochrany. Ověřit toto tvrzení však není cílem šetření a není tak dále zkoumáno.

Celkový počet dotazovaných činil přibližně 200 osob, z čehož 54 osob obdrželo online formu průzkumu. Návratnost odpovědí u online průzkumu činila 18 odpovědí, tedy 33%. U osobního rozhovoru byla návratnost ještě nižší, průměrně odpověděl každý čtvrtý dotazovaný.

Dotazník je dostupný v příloze 1.

4.3. Zpracování a výklad dat

Získaná data z obou fází průzkumu byla sjednocena do společné tabulky. Ze získaných dat lze vyčíst, že studenti přikládají bezpečnosti karet poměrně vysokou důležitost, při hodnocení nikdo neuvedl, že by bezpečnosti karty přikládal nízkou důležitost. Naopak 77% respondentů uvedlo, že na stupnici důležitosti je pro ně bezpečnost karty nejvyšší nebo druhá nejvyšší možná. Odpovědi na důležitost přikládanou bezpečnosti platební karty jsou zobrazeny v následující tabulce:

Jako přikládáte důležitost bezpečnosti vaší platební karty?	1	2	3	4	5
(1 nejnižší, 5 nejvyšší)	0	5	7	22	20

Tabulka 12: Jakou důležitost přikládáte bezpečnosti platební karty?, zdroj: autor

Z možností, jak zabezpečit kartu proti riziku zneužití, je mezi respondenty známá možnost informativních zpráv o použití karty nebo funkce prostředníků pro platby na internetu, jako je PayPal nebo PaySec. Tyto způsoby ochrany zná nadpoloviční většina respondentů. Ostatní způsoby ochrany patří naopak mezi málo známé. Následující tabulka zobrazuje získané informace ohledně znalosti jednotlivých typů ochrany:

Znáte ochranu?	virtuální karty	různé karty pro různá prostředí	informativní zprávy	předplacené karty	zamykání karty	prostředník pro platby na internetu
ano	13	28	45	15	18	40

Tabulka 13: Znáte následující způsoby ochrany?, zdroj: autor

Nejčastěji zmiňované možnosti ochrany, o kterých studenti uvažují, jsou informativní zprávy o použití karty a využití prostředníka pro platby na internetu. Dále je často zmiňována možnost využívat různé karty pro různá prostředí, kde je velký podíl odpovědí ano a spíše ano. Oproti tomu studenti málo uvažují o využití virtuálních karet a karet, které je možné zamykat. To může být též způsobeno nutností pořídit si tyto karty u konkrétní banky, jelikož jsou poskytovány pouze některými bankovními domy. Nejméně oblíbenou možností jsou pak předplacené karty, o kterých nadpoloviční většina studentů ani neuvažuje. Tento výsledek je možné předpokládat, obzvláště kvůli vysokým poplatkům, které jsou s jejich užíváním spojeny. Následující tabulka zobrazuje odpovědi na otázku týkající se využitelnosti jednotlivých způsobů ochrany:

Uvažujete o využití následujících?	ano	spíše ano	spíše ne	ne	nevím
virtuální karty	7	8	17	15	7
různé karty pro různá prostředí	17	15	4	13	5
informativní zprávy	35	5	3	8	3
předplacené karty	5	6	11	30	2
zamykání karty	6	8	13	20	7
prostředník pro platby na internetu	30	10	9	2	3

Tabulka 14: Uvažujete o využití následujících způsobů ochrany?, zdroj: autor

4.4. Vyhodnocení

Ze získaných dat lze usuzovat, že navržená doporučení mohou být využita v praxi. Některá doporučení jsou pro cílovou skupinu již poměrně známá a velká část studentů je má v úmyslu využívat nebo o této možnosti uvažuje (například informativní zprávy, prostředník pro platby na internetu). Jiné možnosti ochrany jsou naopak méně atraktivní, což může být též způsobeno jejich horší dostupností a nutností zajistit si platební kartu u konkrétních bankovních domů, případně platit poměrně vysoké poplatky za její užívání.

Celkové výsledky ukazují, že polovina z navržených doporučení je pro studenty zajímavá a jejich využívání zvažují. U těchto tří doporučení více jak 50% studentů uvedlo, že o jejich využití uvažují. O zbylých třech doporučeních spíše neuvažují, pravděpodobně hlavně z výše uvedených důvodů.

Závěr

Práce se v teoretické části zabývala způsoby, jakými probíhají v dnešní době operace s platebními kartami, a obzvláště pak jejich technologickým zabezpečením. Dále pak teoretická část poskytla přehled o tom, jaké slabiny jednotlivé technologie mají a jaké typy útoků jsou nejčastěji využívány pro odcizení údajů o kartě, ideálně bez toho, aby si tohoto aktu její majitel všiml.

Praktická část pak poskytuje pohled na samotné neoprávněné získání finančních prostředků pomocí odcizených údajů o kartách. Je zde zpracováno porovnání pro různé země z klíčových světových regionů, které alespoň částečně odráží stav zabezpečení a nejakutnější hrozby v jednotlivých světových oblastech.

Důležitou součástí této části je zpracování kvalitativní analýzy rizik pro ČR, kde jsou identifikována a na základě statistických dat ohodnocena rizika spojená s používáním platební karty vydané v České republice. Na toto hodnocení následně navazuje návrh doporučení, která mají za úkol snížit pravděpodobnost nebo dopad zneužití platební karty pro jejího majitele. Na závěr je zpracováno dotazníkové šetření, které si klade za cíl ověřit využitelnost těchto doporučení v praxi na odpovídající skupině respondentů.

Míra dosažení stanovených cílů

Primárního cíle - zpracovat kvalitativní analýzu rizik spojených s užíváním platební karty a následně navrhnout doporučení, které tato rizik snižuje, bylo dosaženo. Kvalitativní analýza byla zpracována pro karty vydané v České republice na základě statistických údajů ECB pro roky 2011 a 2012. Analýza identifikovala největší rizika, která mohou vést k odcizení finančních prostředků pomocí platebních karet.

Následná doporučení se zaměřila na snížení dopadu takovéhoto zneužití a také na snížení jeho pravděpodobnosti. Pro vyšší bezpečnost je možné doporučení kombinovat a zabezpečení tak dále zvýšit. Na závěr byla využitelnost navržených doporučení otestována pomocí dotazníkového šetření, které prokázalo, že část doporučení je pro cílovou skupinu zajímavá a v praxi využitelná. Naopak některá z doporučení jsou méně atraktivní, což se však může změnit v budoucnu, pokud se změní například systém poplatků spojených s předplacenými kartami.

Vedlejší cíl, tedy porovnání dat o útocích v jednotlivých světových oblastech bylo též dosaženo. Na základě statistických údajů bylo provedeno srovnání nejčastěji využívaných útoků podle zemí v různých regionech.

Možnosti rozšíření práce

Možným rozšířením do budoucna je zpracování detailnějšího porovnání zemí nebo světových regionů. Porovnané země odpovídají spíše regionům podle rozdělení EMV, které monitoruje přechod platebních karet na EMV technologie, neodpovídá však běžnému geografickému členění na regiony. EMV rozděluje svět na Ameriku, Afriku, Asii a Evropu. Do Asie počítá i Austrálii a oblast Pacifiku, Amerika naopak nezahrnuje Spojené Státy Americké, které EMV nesleduje vůbec, zejména kvůli jejich specifickému postoji k migraci na EMV technologie. Evropa je pak rozdělena na dvě části, země prostoru SEPA a země mimo SEPA. Získání detailnějších informací o kriminalitě spojené s platebními kartami je však poměrně obtížné, obzvláště v méně vyspělých zemích, z tohoto důvodu může být porovnání zkresleno tím, že byly vybrány převážně nejvyspělejší státy z jednotlivých regionů.

Platnost kvalitativní analýzy má též pouze dočasný charakter, jelikož situace na poli bezpečnosti platebních karet a platebních systémů obecně se nadále vyvíjí a vyvíjet bude. Typy útoků se postupně mění s tím, jak jsou proti nim poskytovatelé služeb lépe bráněni. Dá se tedy očekávat, že postupně budou vznikat nová rizika a jejich významnost se bude postupem času měnit. Je možné, že některá rizika postupem času zaniknout, například v okamžiku, kdy přestanou mít platební karty v základu magnetický proužek. Tato skutečnost by s největší pravděpodobností vedla k rapidnímu snížení hrozby skimmingu. Naopak je ale možné, že v té době dojde k prolomení bezpečnosti EMV čipu nebo jinému typu útoku, který údaje získá stejně dobře, jako dnes skimming.

Terminologický slovník a použité zkratky

ATM	Automated Teller Machine, bankomat.
CNP transakce	Card Not Present transakce, jedná se o veškeré transakce, při kterých není karta fyzicky přítomná, tedy platby po internetu, po telefonu, poštou.
CP transakce	Card Present transakce, jedná se o veškeré transakce, při kterých je karta fyzicky přítomná, tedy výběry z bankomatů, platby v terminálech u obchodníků.
EMV	Europay Mastercard Visa, jedná se o nejpoužívanější standard čipových platebních karet.
POS	Point Of Sale, jedná se o platební terminál u obchodníka, v případě POS plateb probíhá platba přes terminál vložením nebo přiložením karty.
ECB	Evropská centrální banka.
CVC/CVV kód	Bezpečnostní kód pro ověření pravosti karty, je přítomen přímo na magnetickém proužku.
CVC2/CVV2 kód	Bezpečnostní kód pro ověření pravosti karty, není přítomen na magnetickém proužku, ale na zadní straně karty, zpravidla na podpisovém proužku.
SEPA	Platební unie pro 28 zemí Evropské unie a 6 zemí mimo EU, stanovuje pravidla pro platby v rámci SEPA, včetně platebních karet.

Seznam tabulek, grafů a obrázků

Seznam tabulek

Seznam grafů

Seznam obrázků

Zdroje

Knižní zdroje

DOUCEK, P. a kol. *Řízení bezpečnosti informací.* 2. vydání, Praha: PROFESSIONAL PUBLISHING, 2011. ISBN 978-80-7431-050-8.

JUŘÍK, P. *Platební karty: 1870-2006 : velká encyklopedie*. 1. vydání, Praha: Grada, 2006. ISBN 80-247-1381-0.

JUŘÍK, P. a kol. *Platební styk.* Praha: Bankovní institut, 1998.

MONTAGUE, D. *Credit card fraud: the professional's guide to preventing credit card fraud in e-commerce, mail order and telephone order sales*. Victoria, B.C: Trafford, 2004. ISBN 14-120-1460-3.

MONTAGUE, D. *Essentials of online payment security and fraud prevention*. New York: Wiley, 2010. ISBN 04-706-3879-6

Elektronické zdroje

Australian Bankers Clearing Association - Fraud Statistics 2012 Calender Year. [on-line]. [cit. 2014-04-12]. <http://www.apca.com.au/payment-statistics/fraud-statistics/2012-calendar-year?SchemeCredit,DebitandChargeCardFraud>.

CANADIAN BANKERS ASSOCIATION - Credit Card Fraud and Interac Debit Card Fraud Statistics - Canadian Issued Cards. [on-line]. [cit. 2014-04-12]. <http://www.cba.ca/contents/files/statistics/stat_creditcardfraud_en.pdf>.

CARDHUB – Credit card & debit card fraud statistics [on-line]. 2013. [cit. 2014-04-12]. <http://www.cardhub.com/edu/credit-debit-card-fraud-statistics>.

Computer Weekly.com: IT Security. 2008 - How banks are detecting credit fraud. [on-line]. [cit. 2014-03-10] <http://www.computerweekly.com/feature/How-banks-are-detecting-credit-fraud>.

Česká spořitelna - Odemknutí / zamknutí karty. [on-line]. [cit. 2014-04-07]. <http://www.csas.cz/banka/nav/osobni-finance/visa-classic/odemknuti--zamknuti-karty-d00018934>

Česká spořitelna - Zasílání karet poštou. [on-line]. [cit. 2014-03-20]. <http://www.csas.cz/banka/nav/osobni-finance/visa-classic/zasilani-platebnich-karet-postou-d00018807>.

DUBINSKY, Z. CBC News: Technology & Science - New credit cards pose security problem. [on-line]. 2010. [cit. 2014-03-20]. <http://www.cbc.ca/news/technology/new-credit-cards-pose-security-problem-1.904220>.

EMV - EMV 4.3. EMVCo. [on-line]. [cit. 2014-03-20]. <http://www.ecuait.com/attachments/article/8/EMV%20v4.2%20Book%204%20Other%20Interfaces%20CR05.pdf>.

EMVCo.com - Worldwide EMV Deployment and Adoption. [on-line]. [cit. 2014-04-12]. <http://www.emvco.com/documents/EMVCo_EMV_Deployment_Stats1.pdf>.

EUROPEAN CENRAL BANK - Second report on card fraud: July 2013. [on-line]. 2013 [cit. 2014-04-07]. <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf>.

EUROPEAN CENRAL BANK - Third report on card fraud: February 2014. [on-line]. 2014 [cit. 2014-04-07]. <https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf>.

European Central Bank - Euro foreign exchange reference rates. [on-line]. [cit. 2014-04-12]. <http://www.ecb.europa.eu/stats/exchange/eurofxref/html/index.en.html>.

European Central Bank - Statistical Data Warehouse - Czech Republic - Number of cards - For cards issued in the reporting country, cards with a cash function - Number - Non-MFIs counterpart. [on-line]. [cit. 2014-04-07]. <http://sdw.ecb.europa.eu/quickview.do?node=3447411&SERIES_KEY=169.PSS.A.CZ.S101.I11.Z00Z.NT.X0.20.Z0Z.Z>.

Federal Trade Commission - Consumer Sentinel Network Data Book for January - December 2012. [on-line]. [cit. 2014-04-12]. <http://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2012>.

FRANCIS, L. Practical Relay Attack on Contactless Transactions. [on-line]. 2011. London. [cit. 2014-03-20]. <https://eprint.iacr.org/2011/618.pdf>.

Information Week: Security - Sony Says PlayStation Credit Card Data Was Encrypted. [on-line]. 2011. [cit. 2014-03-20]. <http://www.informationweek.com/attacks/sony-says-playstation-credit-card-data-was-encrypted/d/d-id/1097464>.

ISO 14443-1:2008 Identification cards – Contactless integrated circuit cards. [on-line]. 2004. [cit. 2014-03-10]. <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39693>.

ISO 7810:2003 Identification cards -- Physical characteristics., [on-line]. 2003. [cit. 2014-03-10]. <http://www.iso.org/iso/catalogue_detail?csnumber=31432>.

ISO 7812-1:2006 Identification cards – Identification of issuers. [on-line]. 2006. [cit. 2014-03-10]. <http://www.iso.org/iso/catalogue_detail?csnumber=39698>.

ISO 7816:2004 Identification cards – Integrated circuit cards. [on-line]. 2004. [cit. 2014-03-10]. <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45144>.

Komerční banka - E-Card. [on-line]. [cit. 2014-04-07]. <http://www.kb.cz/cs/lide/obcane/ucty-a-platby/internet-telefon-mobil/e-card.shtml>.

Kreditní karty online - Ušetřeno.cz [online]. [cit. 2014-03-10]. Dostupné z: <http://www.usetreno.cz/kreditni-karty/>.

Magtek.com - Magnetic stripe cards standards [on-line]. 2011. [cit. 2014-03-10]. <http://www.magtek.com/documentation/public/99800004-1.08.pdf>.

MASTERCARD - Co je to MasterCard PayPass?. [on-line]. [cit. 2014-03-10]. <http://www.paypass.cz/stranka/1/co-je-paypass/>.

MASTERCARD - Osobní karty MasterCard. [on-line]. [cit. 2014-03-10]. <https://www.mastercard.com/cz/osobni-karty/cz/paypass.html>.

MasterCard Worldwide - All about payment cards. [on-line]. [cit. 2014-03-10]. <http://www.mastercard.com/us/company/en/docs/All_About_Payment_Cards.pdf>.

Měšec.cz - 93 % studentů s účtem Genius Student využívá přímého bankovnictví [on-line]. 2007 [cit. 2014-04-07]. < http://www.mesec.cz/tiskove-zpravy/93-studentu-vyuziva-primeho-bankovnictvi/>.

PaySec - nejčastější otázky. [on-line]. [cit. 2014-04-07]. <http://www.paysec.cz/CmsPage.aspx?Id=faq>.

PCI SECURITY STANDARDS COUNCIL - Co je PCI DSS? [on-line]. [cit. 2014-03-20]. <http://www.pcistandard.cz/index.php?cat=7>.

Policie české republiky - SKIMMING. [on-line]. 2010. [cit. 2014-03-20]. <http://www.policie.cz/clanek/skimming.aspx>.

Raiffeisen Bank - Užitečné rady a tipy k debetním kartám. [on-line]. [cit. 2014-04-07]. <http://www.rb.cz/osobni-finance/platebni-karty/debetni-karty/debetni-karty-tipy/>.

SAKHAROVA, I. Payment Card Fraud: Challenges and Solutions. [on-line]. 2011. [cit. 2014-03-20]. <https://www.utdallas.edu/~bxt043000/Publications/Technical-Reports/UTDCS-34-11.pdf>.

SEPA Cards Framework, version 2.1. [on-line]. 2009. [cit. 2014-03-20]. <http://www.europeanpaymentscouncil.eu/documents/Cards%20SCF%20006%2009%20v%202%201.pdf>.

SMARD CARD ALLIANCE - About smard cards: Frequently asked questions. [on-line]. [cit. 2014-03-10]. <http://www.smartcardalliance.org/pages/smart-cards-faq>.

The 2013 Federal Reserve Payments Study. [on-line]. [cit. 2014-04-12]. <http://fedpaymentsimprovement.org/wp-content/uploads/2013_payments_study_summary.pdf>.

The Banking Association South Africa - 2012 Sabric Card Fraud Statistics. [on-line]. [cit. 2014-04-12]. <http://www.banking.org.za/index.php/media-events/new-noteworthy/2012-sabric-card-fraud-statistics/>.

VISA - Identity Theft. [on-line]. [cit. 2014-03-20]. <http://usa.visa.com/personal/security/learn-the-facts/identity-theft.jsp>.

VISA - Online shopping. [on-line]. [cit. 2014-03-20]. <http://usa.visa.com/personal/security/learn-the-facts/online-shopping.jsp>.

VISA - Phishing. [on-line]. [cit. 2014-03-20]. <http://usa.visa.com/personal/security/learn-the-facts/phishing.jsp>.

Why PayPal?. [on-line]. [cit. 2014-04-07]. Dostupné z: <https://www.paypal.com/webapps/mpp/why>.

Přílohy

Příloha 1: dotazník

Dotazník pro diplomovou práci - Bezpečnost platebních karet (Michal Fuchs)

Následující dotazník je vytvořen pro diplomovou práci pro ověření využitelnosti navržených doporučení, jejichž cílem je zvýšit bezpečnost platebních karet. Cílovou skupinou dotazníku jsou studenti. Prosím o vyplnění, pokud máte pár volných okamžiků, velmi mi to pomůže. Před vyplněním si prosím přečtěte krátké informace o navržených doporučeních:

Virtuální karty

Virtuální karty jsou určené pouze pro platby na internetu, přes telefon nebo poštou. Fyzicky jsou přítomné pouze jako údaje o kartě na papírovém podkladě, nejedná se o plnohodnotnou kartu a nelze ji použít k platbám v kamenném obchodě nebo výběru z bankomatu, čímž se snižují možnosti, kterými lze kartu zneužít.

Různé karty pro různá prostředí

Je možné využívat dvě různé karty, jednu pro platbu v kamenných obchodech a bankomatech, která je blokována pro platby na internetu. Druhou pak využívat pouze pro platby na internetu (zde je ideální právě virtuální karta). Pokud se pachatel dostane k údajům o jedné z karet, pak má pouze omezenou možnost jak kartu zneužít, s první kartou nemůže využít internetových obchodů, s virtuální kartou naopak nevybere z bankomatu.

Informování o použití karty

Banky poskytují možnosti nastavit si informativní zprávy o využití platební karty. V případě, že s kartou kdokoliv zaplatí, bude majitel informován pomocí zvoleného kanálu o této transakci (v řádu minut) a má tak mnohem větší možnost uvědomit banku a zablokovat kartu dříve, než budou odcizeny další prostředky.

Předplacené karty

Tyto karty nejsou spojeny s běžným účtem majitele, naopak se musí pravidelně nabíjet. Z hlediska poplatků se jedná o poměrně drahou záležitost, ale v případě zneužití nehrozí odcizení všech prostředků na běžném účtu, pouze prostředků, které jsou právě uloženy na kartě.

Zamykání karty

Zamykání poskytují na českém trhu pouze Česká spořitelna a Raiffeisen Bank a každá aplikuje jiný přístup. Obecně se však jedná o možnost, kdy platební kartu trvale zamknete, a v případě, že chcete s kartou platit,

odešlete SMS zprávu, která kartu na předem stanovenou dobu odemkne. V případě zneužití je tak karta bezcenná, jelikož je zamčená a pachatel nemůže odcizit prostředky z účtu.

Prostředník pro platby na internetu

Odcizení údajů při platbách na internetu je stále častějším jevem. Možnou obranou je využít při platbách platebních systémů, které slouží jako prostředníci, například PayPal nebo PaySec. Díky nim se obchodník ani jiná nepovolaná osoba nemůže dostat k údajům o kartě, kterou platíte, a karta je tak zabezpečenější.

---

* Required

Vlastníte platební kartu? *

- Ano
- Ne

Jakou důležitost přikládáte její bezpečnosti? (Na stupnici 1-5, kde 1 je nejméně, 5 nejvíce) *

	1	2	3	4	5	
Nízkou						Vysokou

Znáte následující možnosti ochrany karty? (Zaškrtněte ty, které znáte) *

- [ ] Virtuální karty
- [ ] Různé karty pro různá prostředí
- [ ] Informování o použití karty
- [ ] Předplacené karty
- [ ] Zamykání karty
- [ ] Prostředník pro platby na internetu

Uvažujete o využití virtuálních karet pro zvýšení bezpečnosti? *

- Ano
- Spíše ano
- Spíše ne
- Ne

- Nevím

Uvažujete o využití různých karet pro různá prostředí pro zvýšení bezpečnosti? *

- Ano
- Spíše ano
- Spíše ne
- Ne
- Nevím

Uvažujete o využití informativních zpráv o použití karty pro zvýšení bezpečnosti? *

- Ano
- Spíše ano
- Spíše ne
- Ne
- Nevím

Uvažujete o využití předplacených karet pro zvýšení bezpečnosti? *

- Ano
- Spíše ano
- Spíše ne
- Ne
- Nevím

Uvažujete o využití zamykatelných karet pro zvýšení bezpečnosti? *

- Ano
- Spíše ano
- Spíše ne
- Ne
- Nevím

Uvažujete o využití prostředníka pro platby na internetu pro zvýšení bezpečnosti? *

- Ano
- Spíše ano
- Spíše ne
- Ne
- Nevím