Bezpečnost při elektronických platbách

Security of electronic payments

Bc. Michal Holík

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michal HOLÍK**
Osobní číslo:	**A09363**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost při elektronických platbách**

Zásady pro vypracování:

1. **Popište problematiku elektronických plateb.**
2. **Analyzujte existující řešení a aktuální trendy v problematice.**
3. **Vytvořte návrh doporučených postupů.**
4. **Prezentujte řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **MATYÁŠ, Vašek; KRHOVJÁK, Jan. Autorizace elektronických transakcí a autentizace dat i uživatelů. 1. vyd. Brno : Masarykova univerzita, 2008. 125 s. ISBN 978-80-210-4556-9.**
2. **MÁČE, Miroslav. Platební styk : klasický a elektronický. 1. vyd. Praha : Grada, 2006. 220 s. ISBN 8024717255.**
3. **KATSAROS, Panagiotis. A roadmap to electronic payment transaction guarantees and a Colored Petri Net model checking approach. Elsevier : Information and Software Technology [online]. 2009, Volume 51 Issue 2, [cit. 2011-02-02]. Dostupný z WWW: [http://delab.csd.auth.gr/katsaros/ePaymentsTechReport.pdf]. ISSN 0950-5849.**
4. **SHI-JEN, Lin; DING-CHYU, Liu. An incentive-based electronic payment scheme for digital content transactions over the Interne. Elsevier : JournalofNetworkandComputerApplications [online]. 2009, Volume 32 Issue 3, [cit. 2011-02-02]. Dostupný z WWW: [http://www.sciencedirect.com/science]. ISSN 1084-8045.**
5. **KNOSPE, Heiko; POHL, Hartmut. Information Security Tech. Report : RFID security . Elsevier Advanced Technology Publications Oxford, UK. 2004, Volume 9 Issue 4, s. 39-50. ISSN 1363-4127.**

Vedoucí diplomové práce: **Ing. Erik Král**
Ústav bezpečnostního inženýrství

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

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

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.
děkan

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

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá bezpečnostní při elektronických platbách. Rozebírá nejčastější formy elektronického styku, zejména oblast platebních karet, elektronického bankovnictví a elektronických peněženek. U těchto oblastí je rozebráno teoretické zabezpečení, praktické útoky na něj a možnosti implementace vhodného opatření.

Práce se dále zabývá trendy v problematice, jejich popisem a aktuální úrovní bezpečnosti. V praktické části jsou analyzovány možnosti a omezení vybraných elektronických peněženek se závěrečným porovnáním přístupů k jejich bezpečnosti.

Klíčová slova:

Platební karty, EMV, TLS, PKI, Autentizace, 3D Secure, Internetové bankovnictví, Super čipové karty, NFC, Elektronická peněženka.

ABSTRACT

This graduation theses deals with security of electronic payments. It analyzes the most common forms of electronic transaction, especially in the areas of payment cards internet banking and electronic wallets. In these areas is analyzed theoretical security, practical attacks on it and the possibility of implementing appropriate measures.

The work also deals with trends in the issue, their description and the current level of security. In a practical part there are analyzed possibilities and restriction of selected electronic purses with their final comparison in field of security.

Key words:

Payment cards, EMV, TLS, PKI, Authentication, 3D Secure, Internet banking, Super smart card, NFC, Electronic wallets.

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval své rodině za poskytnuté zázemí při studiu a panu Ing. et Ing. Eriku Královi za odbornou pomoc při zpracování této diplomové práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Elektronické platby jsou v dnešní době velice zajímavá a rychle se rozvíjející oblast, jak z pohledu uživatele, tak samotných poskytovatelů. Objem elektronických transakcí se prudce zvyšuje s rozmachem technologií a snadnému přístupu k nim. Toto má mnoho výhod jak pro zákazníka, tak pro poskytovatele. Zákazník má díky internetu okamžitý přístup ke svému účtu a může pohodlně zadávat příkazy a poskytovatel si tímto způsobem přístupu snižuje náklady na transakce. Pomocí platebních karet můžeme díky interoperabilitě platit na celém světě a nové technologie bezdotykových karet nám dále zvyšují pohodlí platby. Další možnost rychlých plateb představují elektronické peněženky, které díky využívání vlastní infrastruktury, bez účasti bank, dále snižují náklady na transakce.

Nedílnou součástí elektronických plateb je zajištění jejich bezpečnosti, které bývá často odsunuto na druhé místo v zájmu snížení nákladů nebo pohodlí pro uživatele.

Celou práci jsem koncipoval do několika oblastí realizace elektronických plateb, u kterých kromě popisu standardního zabezpečení uvádím jeho nedostatky, či popisuji již realizované útoky se zamyšlením nad možnostmi jejich eliminace.

V prvních dvou částech se věnuji zákonu v oblasti elektronických plateb, jejich rozdělení podle způsobu realizace a popisu základních pojmů, důležitých pro bezpečnost.

Ve třetí části se zabývám platebními kartami, jejich rozdělením, možnostmi zneužití jak za fyzické přítomnosti karty, tak na internetu a uvádím metody, jak se proti těmto útokům bránit. Také zde popisuji standardy vztahující se k čipovým kartám, procesy pro bezpečnou komunikaci a principy provedených útoků na ně. Pozornost jsem věnoval také terminálům pro akceptaci karet, které z pohledu snadnosti útoků patří k největším hrozbám.

Čtvrtá část je zaměřena zejména na internetové bankovnictví, principy jeho zabezpečení, autentizaci uživatele a popis doporučeného bezpečného chování uživatele.

V páté části se věnuji elektronickým peněženkám, jejich rozdělení a základním principům bezpečnosti.

V poslední teoretické části analyzuji současné trendy v elektronických platbách a to od Adaptivní autentizace, přes super-čipové karty, až k technologii NFC v mobilních telefonech. Zároveň uvádím úroveň zabezpečení těchto přístupů a jejich nedostatky.

V praktické části rozebírám možnosti elektronických peněženek a detailně popisuji přístup k bezpečnosti u vybraných zástupců se závěrečným porovnáním jejich úrovně.

Po přečtení této práce, by měl mít čtenář přehled o možnostech realizace elektronických transakcí, úrovni jejich bezpečnosti, rizikových faktorech, ale také o způsobech zvyšování bezpečnosti.

I. TEORETICKÁ ČÁST

1 ÚVOD DO ELEKTRONICKÝCH PLATEBNÍCH SYSTÉMŮ

1.1 Právní úprava platebního styku v ČR

Základem pro právní úpravu platebního styku je zákon č. 284/2009Sb. – o platebním styku [1]. V jeho čtvrté části jsou popsány následující úkony:

- Provádění převodů peněžních prostředků.
- Vydávání a užívání elektronických platebních prostředků.
- Vznik a provozování platebních systémů.

Nový zákon o platebním styku, který je odvozen ze směrnice EU, který nabyl účinnosti ke dni 1. 11. 2009, přinesl několik výhod pro klienty bank, či finančních institucí. Důležitou částí pro tuto práci je odpovědnost klienta při zneužití platební karty. Toto bylo dříve problematické v případě zneužití čipových karet a PINu, kdy banky neuznávaly nároky klienta na rozdíl od klasického podpisu. To bylo způsobeno tím, že čipová karta s PINem byla považována za maximálně bezpečnou, bez možnosti útoku ze strany pachatele.

Dnes zákon jasně definuje že: „*Při ztrátě nebo odcizení karty se její majitel na škodě podílí 150 eury za souhrn všech neoprávněných plateb, výjimkou jsou případy, kdy jedná podvodně nebo hrubě poruší smluvené podmínky se svým poskytovatelem*.“ [1]

1.2 Elektronické platební systémy

Jedná se o systémy bezhotovostních plateb, které jsou realizovány elektronicky a to jak pomocí internetu, tak dalšími prostředky komunikačních technologií. Spadají sem zejména [2]:

- Platby kartami.
- Internetové bankovnictví.
- Elektronické peněženky.

1.2.1 Rozdělení podle realizace platby

Podle realizace platby, můžeme elektronické platební systémy dělit následovně [2]:

- Offline platba – samotný clearing platby se uskuteční až se zpožděním (nejčastěji na konci dne).

  - Platební příkazy elektronického bankovnictví.
  - Platby platebními kartami kreditními a debetními.
  - Platby superCash na terminálech Sazky a České pošty.

- Online platba – platba i potvrzení o platbě pro odesilatele i adresáta proběhne okamžitě (v rámci několika sekund).
  - Prémiové SMS.
  - Platby elektronickou peněženkou.
  - Platby platebními kartami kreditními a debetními.

2 DŮLEŽITÉ POJMY PRO BEZPEČNOST ELEKTRONICKÝCH TRANSAKCÍ

2.1 Šifrování

Šifrování neboli kryptování je základním stavebním prvkem současné bezpečnosti elektronických transakcí. Šifrování se dá rozdělit na:

- Symetrické.
- Asymetrické.

2.1.1 Symetrická kryptografie

Používá se stejného tajného klíče jak pro šifrování, tak pro dešifrování dat. Výhodou je jejich nízká náročnost na výpočetní výkon. Nevýhodou je nutnost sdílet šifrovací klíč.

Symetrická kryptografie je často využívána spolu se asymetrickou kryptografii, kde se data zašifrují pomocí symetrické šifry náhodně vygenerovaným klíčem. Tento klíč se zašifruje asymetrickou šifrou pomoci veřejného klíče příjemce.

Symetrická kryptografie se rozděluje na [3]:

- Blokové šifry – šifrují data po blocích.
    - AES (nejpoužívanější, nahradil DES, klíče 128, 192, 256 bitů),
    - 3DES (3xDES, pomalejší než AES, klíče 168 bitů).
- Proudové šifry – šifrují data po bitech.
    - RC4 (generuje pseudonáhodný proud bitů – délka klíče odpovídá 40-128 bitů).

2.1.2 Asymetrická kryptografie

Bezpečnost je založena na náročnosti matematického problému, jako například prvočíselný rozklad násobku dvou velkých prvočísel.

Využívá rozdílných klíčů pro šifrování a dešifrování. Tyto klíče mají tu vlastnost, že nelze jeden z druhého odvodit. Přesto mají matematicky stejný základ, který dovoluje šifrování a dešifrování na základě dvojice těchto klíčů. Výhodou je, že se šifrovací klíče nemusí distribuovat. [4]

Tyto klíče se nazývají [4]:

- Veřejný klíč – tímto klíčem, který je veřejný a patří příjemci zprávy, se daná zpráva zašifruje.
- Soukromý klíč – soukromým klíčem příjemce zprávy (který je zná jen příjemce) rozšifruje zprávu, která byla zašifrována jeho veřejným klíčem.

Typy asymetrických šifer [4]:

- RSA (na principu faktorizace, klíče 1024, 2048, 3072 bitů),
- ElGamal (na principu výpočtu diskrétního logaritmu, klíče 1024 bitů),
- Diffie-Hellman (na principu výpočtu diskrétního logaritmu, klíče 1024, 2048, 3072 bitů).

2.1.3 Šifrovací klíč

Podle šifrovacího klíče se řídí průběh daného algoritmu. Při šifrování jím určuje transformace dat do šifrované podoby. V praxi se uvažuje, že používaný algoritmus je útočníkovi známý a spoléhá se tedy jen na bezpečnost daného klíče.

Pro symetrickou kryptografii se považuje za bezpečnou délka klíče od 128 bitů. Obecně se dá říci, že asymetrická kryptografie potřebuje pro stejnou míru bezpečnosti několika násobně delší klíč (cca 24x delší). [4]

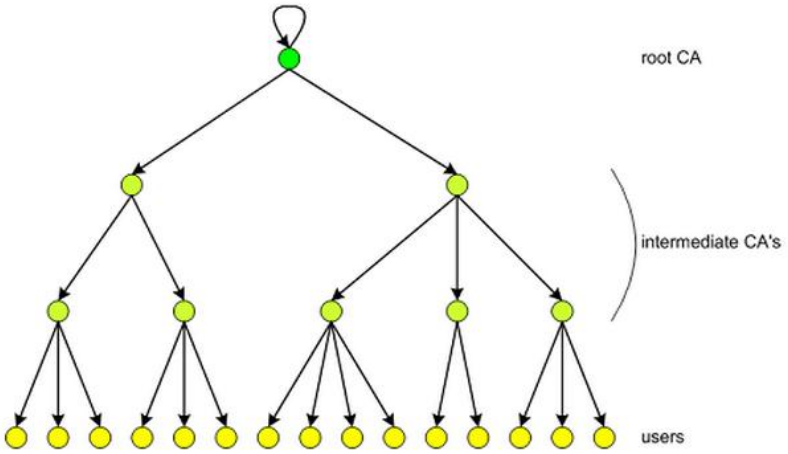
2.2 Public Key Infrastructure (PKI)

Při vzdálené autentizaci, kdy jsou data přenášena přes nezabezpečené prostředí, mohou být snadno odposlechnuta a dále zneužita. Proto je nutné data zabezpečit. Bohužel klasické postupy šifrování, či hashování dat nejsou účinné z toho důvodu, že sice zabezpečí obsah zpráv, ale mohou samy o sobě sloužit pro přístup do vzdáleného systému. Kvůli tomuto se využívá metod založených na asymetrické kryptografii. Aby toto v praxi fungovalo, je potřeba vytvořit infrastrukturu veřejných klíčů, neboli PKI. [5]

2.2.1 Certifikační autority

PKI sestává z řetězce důvěryhodných autorit, neboli certifikačních autorit (CA), kde se postupem „shora dolů“ certifikují veřejné klíče následujících autorit až po samotného

uživatele. Jednotlivé CA mají jasně definovanou úroveň a vztah k okolním CA. Nejvyšší je kořenová CA (root CA). Posledním článkem je uživatel. Princip certifikace následujících CA je zobrazen na obrázku (Obr. 1). [5]



Obr. 1. Struktura vydávání certifikátů [5]

Certifikát je vlastně digitálně podepsanou zprávu, která se skládá z identity vlastníka veřejného klíče a samotného veřejného klíče. Tímto se potvrdí, že daný veřejný klíč patří uvedenému vlastníkovy. V ČR jsou akreditovanými CA například První certifikační autorita nebo Česká pošta.

2.2.2 Certifikát X. 509

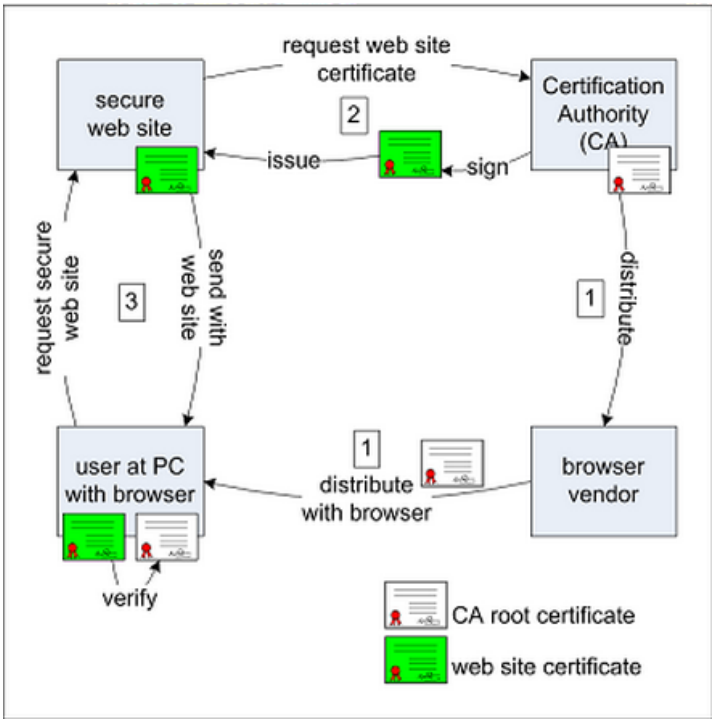
Jedná se o celosvětově uznávaný standard pro digitální certifikáty. V současné době se využívá X. 509 v3. Certifikát obsahuje následující části [6]:

- *Version: verze certifikátu.*
- *Serial Number: sériové číslo certifikátu.*
- *Signature Algorithm: označení algoritmu (ID).*
- *Issuer: vydavatel.*
- *Validity: platnost.*
- *Not Before: nepoužívat před datem.*
- *Not After: nepoužívat po datu.*
- *Subject: vlastník veřejného klíče.*
- *Subject Public Key Info: informace o veřejném klíči vlastníka.*
- *Public Key Algorithm: algoritmus pro veřejný klíč.*

- *Veřejný klíč (data).*
- *Issuer Unique Identifier: unikátní identifikátor vydavatele (volitelný.)*
- *Subject Unique Identifier: unikátní identifikátor vlastníka (volitelný).*
- *X509v3 extensions: rozšíření (volitelné.)*
- *Signature Algorithm: algoritmus pro certifikát (elektronický podpis).*
- *Certifikát (elektronický podpis).*

2.2.3 Funkce certifikátů

Certifikáty zajišťují jak ověřování jednotlivých uživatelů (například certifikáty vydané bankou pro přihlášení k IB), tak identitu internetových stránek (pravost stránek konkrétního IB). Cyklus funkce vydávání a ověřování certifikátů pro webové stránky je zobrazena na obrázku (Obr. 2).



Obr. 2. Cyklus funkce webových certifikátů [5]

1 – Certifikační autorita (CA) distribuuje své kořenové certifikáty přes prohlížeče. Ty jsou uloženy v seznamu důvěryhodných certifikátů v uživatelském PC. Tímto jsou všechny certifikáty vydané touto CA považovány za důvěryhodné, bez dalšího „online“ ověřování.

2 – Společnost požadující bezpečné stránky si od CA objedná certifikát, který je danou CA podepsán a garantuje uživateli identitu těchto stránek.

3 – Při přístupu uživatele na tyto stránky si webový prohlížeč vyžádá certifikát webového serveru (na kterém jsou stránky provozované) a jestliže může být tento ověřen pomocí seznamu důvěryhodných certifikátů uložených v PC, je webový certifikát přijatý. Poté může začít šifrovaná komunikace.

2.3 Identifikace, autentizace, autorizace

Nyní si popíšeme některé pojmy, které jsou důležité z pohledu ověření identity uživatele a autorizace transakce v dané aplikaci.

2.3.1 Identifikace

Při identifikaci se **určuje** identita uživatele. Toto se realizuje dvěma způsoby:

- Uživatel zadá svou identitu.
- Systém prohledává množinu záznamů v databázi podle zadaného (biometrického) vzorku.

2.3.2 Autentizace

Autentizace uživatelů – Při autentizaci se **ověřuje** identita uživatele. Toto se realizuje zadáním informace, která umožní daného uživatele ověřit (PIN). Tento proces je jednodušší než proces identifikace, protože již pouze ověřuje platnost daných informací.

Používají se zejména:

- Co uživatel zná – PIN, heslo apod.
- Co uživatel má – tokeny, platební karta.
- Co uživatel je – biometrické informace.

Autentizace dat – Při autentizaci dat se ověřuje pravost osoby, která data odesílá, spolu s ověřením integrity dat.

2.3.3 Autorizace

Autorizace uživatele – Autorizace obvykle následuje po autentizaci a udává, jaké práva má uživatel v systému. Toto se děje právě na základě autentizace a přiřazené bezpečnostní politiky

Autorizace transakcí – Autorizace transakcí se provádí na základě autentizace a autorizace uživatele a dále pak na autentizaci dat dané transakce.

2.4 Protokoly pro bezpečnou komunikaci

2.4.1 HTTPS

HTTPS je prakticky stejný jako HTTP, ale využívá defaultně TCP port 443, takže je separovaný od HTTP. HTTPS pracuje ve spojení s protokolem TLS pro bezpečný přenos dat.

V případě potřeby bezpečné komunikace, rozliší HTTPS odesilatele a adresáta.

HTTPS se stejně jako HTTP nestará o to, jak budou data doručena, ale pouze o korektní zobrazení.

2.4.2 TLS

TLS je nástupcem protokolu SSL a je v současné době nejpoužívanějším. Protokol SSL 3.0 a protokol TLS 1.0 jsou v podstatě stejné.

Bezpečný přenos dat zajišťuje TLS tím, že data šifruje. SSL propojuje jak ověřování autentizace serveru (jeho pravosti), tak šifrovací proces mezi klientem a serverem. Při vzájemné autentizaci stran je potřeba zavést PKI. [7]

Funkce TLS [7]:

- Po připojení na server je iniciováno zabezpečené připojení pomocí HTTPS (SSL, TLS).
- Strany se dohodnou na podporovaných algoritmech:
    - pro kryptografii s veřejným klíčem: RSA, Diffie-Hellman, DSA.
    - pro symetrické šifrování: RC2, RC4, IDEA, DES, Triple DES, AES, Camellia.

  - pro jednosměrné hašování: Message-Digest algorithm (MD2, MD4, MD5), Secure Hash Algorithm (SHA-1, SHA-2).
- Server odešle klientovy certifikát.
- Proběhne ověření certifikátu od serveru přes certifikační autoritu.
- Poté je prohlížečem vytvořen jedinečný klíč pro relaci se serverem, který je zašifrován veřejným klíčem serveru, takže data jsou čitelná pouze pro server.
- Nakonec se vytvoří symetricky šifrovaný komunikační kanál mezi serverem a klientem.

2.5 Hash

Hash je matematická funkce, která převádí vstupní data na relativně malý soubor znaků a vytváří jejich tzv. otisk. Důležitou vlastností je, že malá změna na vstupu vede k velké změně na výstupu.

Hashovací funkce není šifra, je jednosměrná, a proto ji po provedení není možné převést na původní text. Toto není možné ani teoreticky z důvodu, že hash se skládá z poměrně malého množství znaků bez ohledu na velikost původního souboru a neexistuje tu tedy poměr mezi hashem a původním souborem. Nevýhodou hashování je, že může docházet ke kolizím, kdy několik různých zpráv může mít stejný otisk. Toto je z důvodu, že počet vstupních zpráv je vždy větší než počet možných vygenerovaných otisků. [8]

2.5.1 MD5

Toto je velmi oblíbená hashovací funkce, která má ovšem své nedostatky. Generované hash kódy nejsou unikátní, pouze existuje malá pravděpodobnost, že dva různé soubory budou mít stejný hash. Z tohoto vyvstává otázka bezpečnosti, kdy se útočník při nalezení textu s odpovídajícím hashem může přihlásit k účtu oběti, bez faktické znalosti vlastního hesla. Výsledek MD5 má 32 znaků. Složitost prolomení je 2^32, MD5 byl již prolomen (bude popsáno dále v textu). [5]

2.5.2 SHA-1

Je považován za nástupce MD5. V současné době je nejpoužívanější. SHA-1 vytváří bitový obraz daných dat o maximální velikosti 160 bitů a maximální délkou 2^64 - 1 bitů. Tento

algoritmus vychází z algoritmů MD5. Složitost prolomení je 2^64. Výsledek SHA-1 má 40 znaků. [5]

Jeho nástupcem je SHA-2, na který nebyly realizovány ani teoretické útoky. Jeho nízké nasazení v praxi je zřejmě způsobeno nízkou podporou na operačních systémech Windows XP SP2 a starších. [8]

2.6 Typické útoky za účelem krádeže identity a citlivých údajů

2.6.1 Phishing

Jedná se o tzv. sociální inženýrství, které je založeno na důvěřivosti a neznalosti lidí. Nejčastěji se realizuje pomoci emailů. Útočník rozešle emaily, které vypadají jako např. od banky (loga, písmo, jména), ve kterých požaduje ověření osobních údajů spolu s pinem. Toto je nejčastěji spojeno s motivací, kterou je například vrácení peněz na účet apod.

Při zadání údajů požadovaných útočníkem je obratem vyrobena falešná karta, kterou je možné vybrat peníze z účtu.

Ochrana proti phishingu

Obecně žádné banky, ani jiné instituce nevyžadují žádné identifikační údaje ani PINy při komunikaci přes email. Proti zneužití údajů je důležité dodržovat několik zásad:

- Emaily s požadavky údajů, hesel, či pinů ignorovat (v případě potřeby je možné navštívit banku a daný email si ověřit, či jej ohlásit).
- Zobrazovat podrobnosti o emailech (adresa odesilatele, IP adresa, země…), které si v případě potřeby lze ověřit.
- Neklikat na žádné odkazy ve zprávě, protože můžou odkazovat na web útočníka se stejným vzhledem jako originální web. Pravou URL adresu si lze zkontrolovat podržením ukazatele nad odkazem, nebo zkopírováním do nového panelu prohlížeče.

2.6.2 Pharming

Pharming je sofistikovanější metoda sociálního inženýrství a má dvě základní podoby [9]:

Základní DNS útok

Počítač oběti je napaden škodlivým softwarem například v podobě trojského koně nejčastěji stáhnutého s obsahem „zdarma“, pornografií, či programem na zpřístupnění placeného obsahu uživatelem.

Při zadání URL adresy serveru uživatelem je tato přeložena pomocí DNS na skutečnou adresu IP (překlad z písmen na čísla). Aby toto probíhalo co nejrychleji, každý počítač si pamatuje již navštívené URL adresy a uchovává si i jejich IP adresy v mezi-paměti. Vir způsobuje přepsání některých IP adres u některých URL. Při zadání adresy uživatelem, počítač prohledá mezi-paměť a „vytočí“ již pozměněnou IP adresu, která je spojena s URL. Oběť poté nemá tušení, že je na stránce útočníka a ne na stránce originální.

Ochrana proti základnímu DNS útoku

Chránit se dá zejména aktualizací systémů, antiviru a programů na PC. Dále nestahováním neznámých dat z internetu, či neklikáním na bannery a jiné reklamní poutače na internetu.

Rozšířený DNS útok

Tento útok spočívá v napadení DNS serverů poskytovatele internetu, či legitimní organizace, které způsobí, že při zadání adresy do internetového prohlížeče, budete přesměrování na stránky útočníka.

Tyto servery jsou nejlépe zabezpečené, ale mají pro útočníka největší potencionální zisk. Se slabší ochranou se můžeme setkat u serverů např. menších organizací. V minulosti několik takových útoků proběhlo, ale pouze modifikovaly severy tak, že přidávaly vyskakovací okna s reklamou před originální stránky. Potenciál zneužití je nicméně velký.

Ochrana proti rozšířenému DNS útoku

Ochranou v tomto případě je pouze kvalitní zabezpečení serverů dané instituce. Proto je vhodné používat silné a důvěryhodné poskytovatele. Dále využívání dalších bezpečnostních opatření, které neumožní převod prostředků z vašeho účtu i při zjištění vašich identifikačních údajů. Například elektronické certifikáty, SMS kódy, pin kalkulátory atd.

2.6.3 Spoofing

Při Spoofingu se část sítě vydává za jinou identitu a zachytává síťový provoz, ze kterého se snaží vyfiltrovat citlivá data.

Ochrana proti Spoofingu

Obranou je používání šifrovaného přenosu. Velmi rozšířený je SSL (TLS) protokol, který využívá HTTPS.

2.7 Hardwarová bezpečnostní zařízení

Tato zařízení se nazývají Hardware Security Module (HSM) a jsou to bezpečné kryptoprocesory, jejichž účelem je provádět zabezpečené kryptografické operace v jinak nedůvěryhodném prostředí. Najdeme je i v bankovních centrech a poskytují mimo jiné následující funkce [10]:

- Bezpečné úložiště klíčů pro kryptografii.
- Bezpečné prostředí pro šifrování.
- Bezpečné prostředí pro verifikaci PINů atd.

Mezi HSM můžeme zařadit čipové karty, kryptografické akcelerátory, či bezpečnostní tokeny. Tyto HSM bývají nasazovány na hostitelských zařízeních, u kterých je předpoklad, že se nacházejí v nedůvěryhodném prostředí, a proto je nutné se zaměřit na bezpečnost HSM již při výrobě.

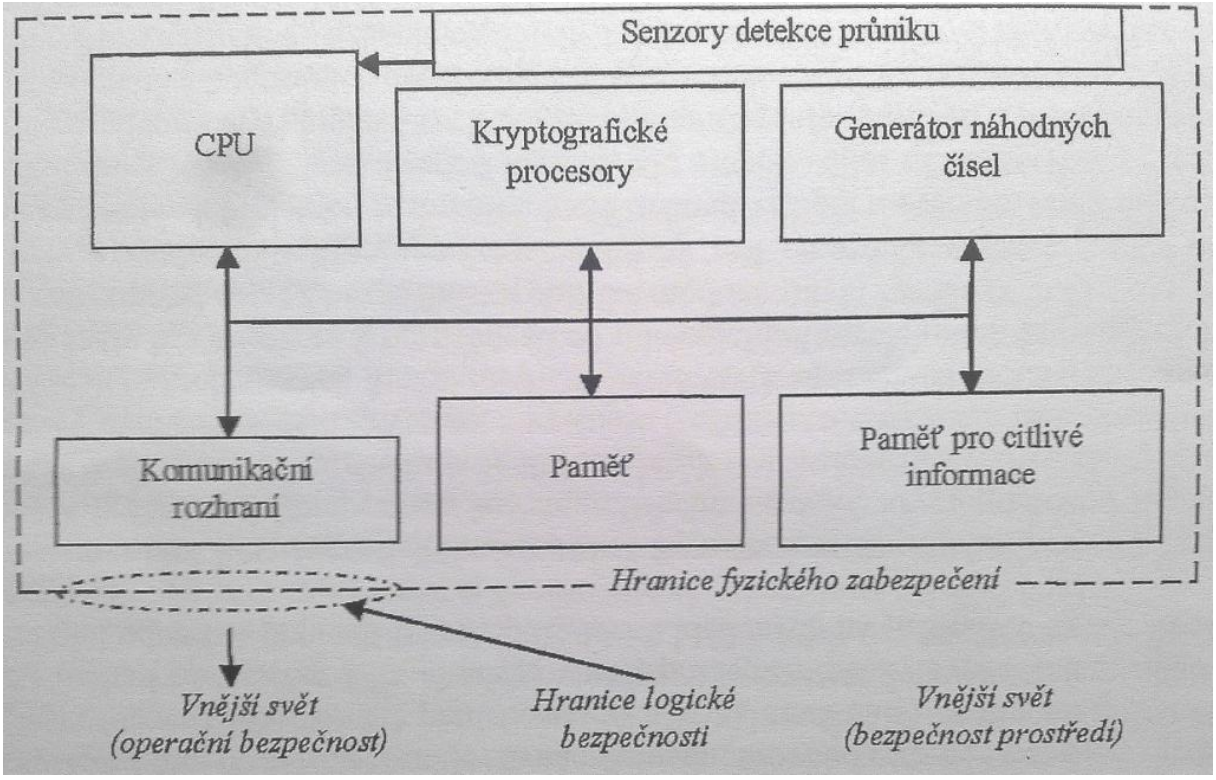
2.7.1 Architektura HSM

Vnitřní složení HSM záleží na jeho typu, ale obecně se skládá z následujících součástí [10]:

- **Procesor CPU** – je jádrem zařízení a řídí vstupně/výstupní operace, zpracovává přesušení a stará se o paměť.
- **Paměť** – uchovává citlivé informace, jako tajné klíče a je obvykle nezávisle napájena.
- **Generátory náhodných čísel** – využívá se pro generování tajných klíčů.
- **Koprocesory pro kryptografické operace** – využívá se pro zrychlení kryptografických operací.

- **Fyzická ochrana.**

Obecné schéma vnitřního uspořádání HSM je zobrazeno na obrázku (*Obr. 3*).



Obr. 3. Vnitřní uspořádání HSM [10]

2.7.2 Příklady HSM zařízení

- **Čipové karty** – jsou to kryptografické moduly s malým výpočetním výkonem. Hlavním úkolem je provádět kryptografické operace s tajným klíčem. Jejich výhoda oproti magnetickým kartám je ochrana uložených dat proti zkopírování. Podrobněji budou čipové karty rozebrány v samostatném oddílu.
- **Super čipové karty** – jsou čipové karty s rozšířením v podobě klávesnice, displeje a solárního panelu pro napájení, nebo čtečky otisků prstů. Podrobněji budou čipové karty rozebrány v samostatném oddílu.
- **Kryptografické routery** – routery, které jsou zabezpečeny pro síťový provoz v bankovních institucích.
- **Kryptografické akcelerátory –** koprocesory urychlující kryptografické operace.
- **USB čipy** – fungují na principu čipových karet s tím rozdílem, že komunikují přes rozhraní USB.

- **Platební terminály** – zařízení pro akceptaci platebních transakcí [10].

2.7.3 Příklady funkcí HSM

- Generování digitálních certifikátů včetně veřejných a soukromých klíčů.
- Šifrování a dešifrování zpráv těmito klíči.
- Generování hashů a podepisování zpráv digitálními podpisy.
- Ověřování digitálních podpisů.
- Zajišťování interoperability s aplikacemi třetích stran.
- Ochrana certifikátů a klíčů před fyzickými a síťovými útoky [10].

2.7.4 Úroveň zabezpečení a typy útoků na bezpečný hardware

V této části budu vycházet hlavně z [10][11][12][13].

Bezpečnost HSM můžeme dělit do následujících úrovní:

- Fyzická bezpečnost.
- Logická bezpečnost.
- Bezpečnost prostředí.
- Operační bezpečnost.

Fyzická bezpečnost

Jejím úkolem je ochránit vnitřní výpočetní systém před fyzickým přístupem. Běžně používané metody zabezpečení HSM jsou následující:

- ***Průniková odolnost*** – zajišťuje co možná největší odolnost proti fyzickému průniku do systému. Toto je realizováno chemikáliím odolnými materiály. U čipových karet jsou tímto myšleny ochranné vrstvy na čipu, plastový obal čipu apod.
- ***Evidence průniků*** – zajišťuje zaznamenání stop, při průniku, nebo narušení bezpečnosti HSM. Realizuje se chemickými, či mechanickými prostředky jako:
    - Označovací barviva.
    - Holografické nálepky.
    - Pečetě apod.

- ***Detekce průniků*** – zajišťuje detekci pomocí čidel připojených k ochranným prvkům zařízení.
- ***Reakce na průnik*** – zajišťuje reakci při detekci průniku, která zabrání získání citlivých informací uložených v modulu. Nejčastěji se využívá smazání paměti, nebo zničení čipu chemikáliemi.

Logická bezpečnost

Jejím úkolem je zabránit pomoci operačního systému, nebo jiného software neoprávněnému přístupu k citlivým informacím. Mechanizmy, které se využívají lze rozdělit následovně:

- ***Kryptografické algoritmy*** **–** matematické funkce k zajištění důvěrnosti, integrity, autentizace a nepopiratelnosti dat. Jsou hlavním pilířem současné kryptografie.
- ***Kryptografické protokoly*** **–** popisují komunikaci mezi jednotlivými zařízeními v prostředí mimo HSM.
- ***Řízení přístupů*** **–** řídí přístup k prvkům systému v prostředí HSM.

Bezpečnost prostředí

Jejím úkolem je ochrana samotného zařízení před možností provést na něj útok. Toto je realizováno například fyzickou stráži, omezením fyzického přístupu, instalací bezpečnostních kamer apod.

I když se toto zdá nejméně podstatné, je zanedbání bezpečnosti prostředí jedním z nejčastějších důvodů selhání systému jako celku. Jako příklad můžeme uvést krádeže celých bankomatů, instalaci kamer a kopírovacích zařízení na bankomaty atd.

Operační bezpečnost

Do této oblasti spadá bezpečná manipulace a používání konkrétního zařízení. Uživatelé by měli být informování o možných typech útoků na jejich zařízení a jak se proti nim bránit. Toto zahrnuje široké spektrum informací od technických prvků až po principy sociálního inženýrství. Dále postupy při manipulaci se zařízeními jako platební karty a zadávání PINů, či aplikace bezpečnostních tokenů jen v prověřeném prostředí apod.

2.7.5 Útoky na fyzickou bezpečnost

Tyto útoky jsou náročné na přípravu a nejsou provozovaný amatéry. Můžeme je rozdělit do následujících podskupin podle druhu použité technologie.

Invazivní – jsou podmíněny přístupem k částem zařízení, jako je například paměť. Toto si v případě vysokého stupně integrace obvodů vyžaduje velmi drahé vybavení, srovnatelné s tím, které je použito při výrobě. Při tomto útoku se odstraní ochranné kryty, pomocí reverzního inženýrství se zjišťuje struktura čipu a dále díky přístupu ke křemíkové vrstvě čipu se útočníci snaží pomocí mikrosond modifikovat chování čipu, pro přímý přístup k datům.

Polo-invazivní – jsou méně náročné na vybavení, protože nevyužívají přímý přístup ke komponentám čipu. Útočníci odstraňují ochranné části čipů a samotný čip dále ozařují. Pro ozařování se používají nejčastěji rentgenové, UV, nebo mikrovlnné záření. Toto se kombinuje s velkými výkyvy teplot aplikovanými na čip, což má za cíl způsobit nestandardní chování čipu, či vyřadit bezpečnostní pojistky a odhalit tak uložené údaje.

Neinvazivní – využívá se vystavení čipu extremním vlivům okolního prostředí a sledují se jeho vlastnosti při zpracovávání dodávaných dat. Tento útok, v případě nezničení obvodů, nezanechává na zařízení stopy, a proto je těžko detekovatelný.

Dále sem můžeme zařadit:

- Útoky postranními kanály.
- Útoky pomocí elektromagnetické analýzy.

Útoky postranními kanály – využívá se informací z postranních kanálů, které je možno získat v průběhu činnosti daného zařízení. Tímto je možno získat tajné parametry, které jsou součástí konkrétního výpočtu. Zejména se využívají informace o čase prováděné instrukce, spotřebě energie pro danou operaci, apod.

- ***Chybová analýza*** – ve zkoumaném zařízení se úmyslně generují chyby a výstup z daného zařízení se zkoumá pro odpozorování informací o tajných parametrech výpočtu. Tyto chyby se obvykle generují následujícími způsoby:
    - Změna napětí.
    - Změna taktovací frekvence.
    - Změna teploty.

  - Aplikace určitého druhu záření.
- ***Časová analýza*** – zkoumá se čas, který je nutný k provedení kryptografické operace pro odhalení tajného klíče. Útočník vysílá do kryptografického zařízení množinu zpráv ke zpracování a zaznamenává čas potřebný k jejich zpracování, z čehož vyvozuje další závěry o použitých algoritmech apod. Pro zachování bezpečnosti je důležité, aby čas provádění algoritmu nebyl závislý na vstupu.
- ***Odběrová analýza*** – množství spotřebované energie závisí na prováděných instrukcích.
  - SPA (Simple Power Analysis) přímé vyhodnocování spotřebované energie.
  - DPA (Differential Power Analysis) odstraňuje šum vznikající u SPA pomocí několikanásobného měření.

  Ochranou proti tomuto typu útoku může být implementace šumu přidaného při provádění operací nad daty.

Útoky pomocí elektromagnetické analýzy

Střídavé magnetické pole, které zařízení generuje, může být detekováno pomocí cívky a později útočníkem analyzováno. Tímto se zabývají vojenské standardy TEMPEST, které stanovují limity pro elektromagnetické záření elektronických zařízení a mají zabránit tomuto typu zneužití.

Ochrana proti útokům

Pro zlepšení odolnosti proti popsaným útokům, se používají například následující metody:

- Generátory šumu.
- Náhodné časování instrukcí
- Vkládání prázdných instrukcí.
- Náhodné přejmenování registrů.
- Šifrování sběrnice dat.
- Vnitřní nezávislé generátory hodinového taktu.
- Zkoumání a optimalizace vyzařovacích charakteristik apod.
- Používání nových typů výroby čipů.

Těmito opatřeními se zvyšuje náročnost provedení útoku, pomocí metod analýzy postranních kanálů elektromagnetického vyzařování apod., ale při dostatečném množství

analýz daného procesu se dají šumy vzniklé aplikací těchto opatření odstranit. Řešením jsou speciální obvody, které jsou konstruovány s ohledem na tyto typy útoků, kde se například maskuje spotřeba energie pomocí zdvojených vodičů. Nevýhodou je, že tato řešení mají jen poloviční rychlosti, zvýšenou celkovou spotřebu, nebo zabírají vetší prostor.

Ochranou proti invazivním útokům je například použití nových metod při výrobě čipů, kde pokročilá miniaturizace neumožňuje útočníkům rozeznávat základní stavební prvky daného čipu a tím zabraňuje i jejich následné analýze. Dále se aplikují nové materiály na paměťové bloky, které jsou citlivé na některé typy záření, což zabraňuje použití polo-invazivních metod pro analýzu čipu.

2.7.6 Útoky na logickou bezpečnost

Tento útok spočívá v odhalení slabosti kódu daného software. Typy útoků můžeme rozdělit podle typů chyb, které využívají

- **Integrita klíčů a jejich kompatibilita** – tyto útoky využívají vlastností API, které jsou nezbytné pro zajištění kompatibility mezi novými a staršími zařízeními.
- **Nedostatečná kontrola parametrů při práci s PINy** – využívá se chyb, které vznikají kvůli velkému množství podporovaných standardů a tím obrovskému množství parametrů funkcí.
- **Nízké požadavky na bezpečnostní politiku** – některé API si nevynucují použití bezpečnostní politiky při transakci. Tohoto je využito například v útoku na čipové karty, popsaného dále v textu.

2.7.7 Útoky na bezpečnost prostředí

Tento útok spočívá v odcizení celého zařízení, nebo prvků obsahujících kýžený obsah. Příkladem, který je poměrně často k vidění i u nás v ČR je vytrhnutí a odvezení celého bankomatu.

Další nebezpečí spočívá v přístupu administrátorů k systému, ti mohou systém do značné míry ovládat a případně nastavit pro usnadnění zamýšleného útoku. Toto nebezpečí se dá zmírnit současným přístupem vždy alespoň dvou operátorů při manipulaci s funkcemi systému.

2.7.8 Útoky na provozní bezpečnost

Tyto typy útoků jsou založeny na neznalosti, či chybném užívání daného zařízení uživatelem. Spadají sem odpozorování PINů, sociální inženýrství apod. Samotná zařízení mohou být navrhována s ohledem na nejčastější hrozby provozní bezpečnosti. Příkladem mohou být krycí pouzdra na PINpadech bránící odpozorování pinu. Hlavní část provozní bezpečnosti ale leží na koncovém uživateli, jeho znalostech problematiky a důslednosti dodržování doporučených postupů s manipulací se zařízeními.

3 PLATEBNÍ KARTY

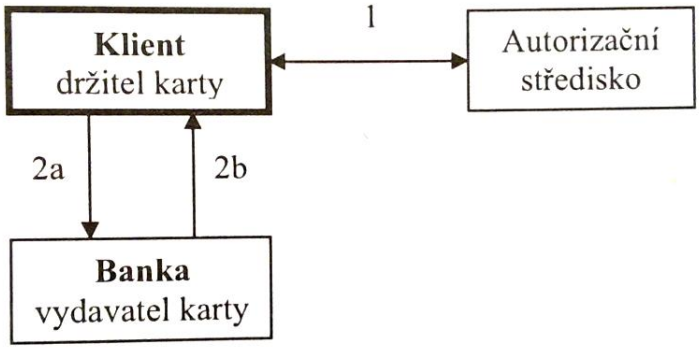
Platební karty jsou fyzické prostředky pro bezhotovostní styk. Zejména se jimi realizují [14]:

- Výběry hotovosti.
- Bezhotovostní platby.

Banky, jako vydavatelé platebních karet, se řídí pravidly mezinárodních asociací pro platební karty. Podmínky užívání platebních karet jsou dány obchodními podmínkami vydávající banky.

3.1 Výběr hotovosti v bankomatech

Výběr hotovosti z bankomatu probíhá výhradně elektronicky v on-line režimu. Toto umožňuje okamžitou autorizaci realizovaných transakcí. Průběh transakce s popisem úkonů je vidět na obrázku (Obr. 4).



Obr. 4. Průběh transakce při výběru z bankomatu [14]

1 – autorizace platby v případě přesažení daného limitu

2a – odečtení částky transakce z účtu držitele karty

2b – vydání částky transakce v hotovosti

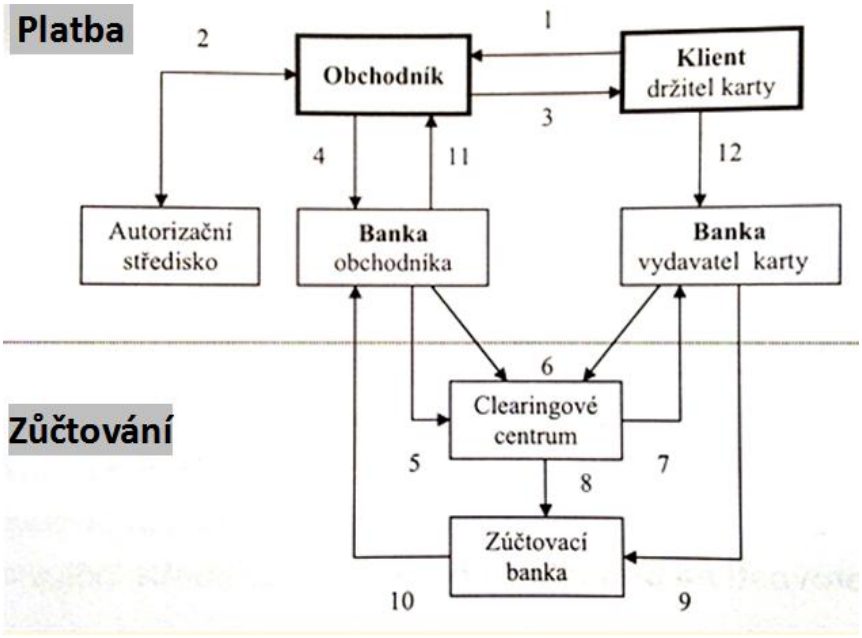
3.2 Bezhotovostní platby kartou

Bezhotovostní platba se skládá z následujících úkonů [14]:

- Autorizace transakce.

- Přenos transakce.
- Clearing transakce.

Průběh celé transakce s popisem úkonů je zobrazen na obrázku (Obr. 5).



Obr. 5. Průběh transakce při platbě kartou [14]

1 – předložení karty obchodníkovi, který ověří ochranné prvky karty

2 – autorizace platby v případě přesažení určeného limitu

3 – vystavení prodejního dokladu

4 – předání informace o platbě bance obchodníka

5 – předání informací o provedených platbách

6 – clearingové zúčtovaní mezi napojenými bankami

7 – předání informace o provedených platbách

8 – příkaz k vyrovnání sald mezi bankami

9 – odečtení částky z účtu banky, která kartu vydala

10 – převedení částky na účet banky obchodníka

11 – připsání částky transakce snížené o bankovní provize

12 – zatížení účtu držitele karty částkou transakce

3.3 Ochranné prvky platebních karet

Platební karty se vyrábí ze tří vrstev netoxického PVC se standardními rozměry 85,6 x 54 x 0,76 mm podle mezinárodní normy ISO 3554. Karty jsou chráněny několika bezpečnostními prvky [15]:

- Logo vydavatele, banky.
- Hologram.
- Číslo platební karty.
- EMV čip (u čipových karet).
- Platnost karty.
- Jméno majitele.
- CVV (Card Verification Value) kód.
- Podpisový vzor.

3.4 Kriteria dělení platebních karet

Základní typy platebních karet můžeme rozdělit podle několika hledisek uvedených v tabulce (Tab. 1).

Tab. 1. Druhy platebních karet

Hledisko třídění	**Druh platební karty**
podle způsobu zúčtování transakcí	debetní karta
	kreditní karta
podle záznamu dat	karta embosovaná
	karta s magnetickým záznamem
	karta čipová
podle platnosti	tuzemské karty
	mezinárodní karty

Z hlediska bezpečnosti, které se budu dále věnovat, je nejdůležitějším kritériem typ technologie záznamu dat na kartě.

3.5 Nejčastější útoky na platební karty

Nyní popíšu nejtypičtější útoky na platební karty. Data získaná těmito metodami jsou buď zneužita přímo pachatelem, zkopírováním na falešnou kartu, nebo předána třetím stranám na černém trhu. [16]

3.5.1 Skimming

Karty s magnetickým proužkem jsou jak snadno „programovatelné“, tak snadno kopírovatelné. Při skimmingu jsou data z karty kopírována přes zařízení, které se připojí ke vstupnímu otvoru bankomatu a které se jeví jako jeho součást. Ukládají se do připojeného datového úložiště. Odtud můžou být data dále odeslána bezdrátově, nebo fyzicky odejmuty pachatelem.

Tímto nejsou kopírovány všechny ochranné prvky karty jako CVV kód, takže není možné padělanou kartu použít k výběru z bankomatu v ČR. Ovšem v některých zemích lze realizovat výběr bez CVV, zejména v Americe a Asii. [16]

Obrana proti Skimmingu

Technologie magnetického proužku už je dávno překonaná a lehce napadnutelná, ale důvodem jejího stále masivního nasazení je zpětná kompatibilita karet.

Proti nejčastějšímu druhu útoku – Skimmingu je třeba se bránit hlavně ostražitostí. Při výběru si zakrývejte zadávání pinu rukou, i když kolem Vás nikdo nestojí – zabráníte tak sejmutí pinu kamerou. Zdá se Vám bankomat pozměněný, přibyly na něm nové lišty, má přelepenou klávesnici? Raději peníze vyberte jinde, nejlépe v bankomatech co nejblíže bank.

V ČR není Skimming příliš častý, podle České spořitelny se řeší několik desítek případů ročně, ale například v Německu bylo za rok 2010 zaevidováno cca 4000 krádeží dat z platebních karet. Řešením je přechod na platební karty pouze s čipem, kdy jsou údaje na čipu kryptovány a obtížněji přístupné pro útočníka. Tím ovšem vzniká problém s kompatibilitou. Dalším možným řešením je podle šéfa německého Spolkového kriminálního úřadu Jörge Ziercke zablokování magnetického proužku bankou a jejího budoucího odblokování pouze pro cestu do zahraničí. [17]

3.5.2 Skrytá kamera

Kamera se umisťuje na bankomat nejčastěji v podobě lišty, či zařízení připojeného přímo k falešnému vstupu pro kartu s přímou viditelností na klávesnici. Používá se v kombinaci se skimmingem.

3.5.3 Dotykový senzor

Na klávesnici bankomatu se přidělá falešní klávesnice, která snímá PINy. Zadané piny se odesílají bezdrátově, nebo jsou fyzicky odebrány i s falešnou klávesnicí pachatelem stejně jako v předchozích případech. Používá se v kombinaci se Skimmingem.

3.5.4 Lisabonská smyčka

Technické zařízení, (používají se magnetické pásky)které je vsunuto do otvoru bankomatu a kvůli kterému se karta nedostane ani do bankomatu, ani zpět k majiteli. Pachatel se obvykle nabídne s pomocí a doporučí zadat pin pro vyproštění a poté poradí jít problém řešit přímo do banky. Jakmile se oběť vzdálí od bankomatu, pachatel kartu vyprostí a může ji zkopírovat, nebo zneužít. Tento způsob krádeží je již spíše historický. V ČR jsou již všechny bankomaty proti tomuto útoku odolné.

3.6 Embosovaná karta

3.6.1 Popis

Embosovaná karta je specifická tím, že její identifikační údaje jsou vyraženy reliéfním písmem a lze ji použít i u obchodníků, kteří používají mechanické snímače – imprintery. U nás je zažité také pojmenování „žehlička“. Pro potvrzení transakce je vyžadován pouze podpis vlastníka karty. V dnešní době je většina karet kombinovaná, tj. obsahují reliéf, čip i magnetický proužek. [15]

3.6.2 Výhody

Zdálo by se, že embosovaná karta nemá větší užití než čipová, protože imprintery jsou na ústupu a setkat se s nimi můžeme převážně jen v restauracích, či u malých obchodníků. Nicméně embosované karty jsou nenahraditelné například v USA, kde jsou nezbytné pro možnost půjčení auta. Stejně to funguje například v síti auto-půjčoven Europcar. Před

několika lety také nebylo možné zřídit si účet u společnosti PayPal s jinou, než embosovanou kartou.

3.6.3 Bezpečnostní rizika a jejich eliminace

Ochrana při platbě embosovanou kartou je prováděna na základě fyzické přítomnosti karty a podpisu vlastníka karty, který musí být shodný se vzorem na kartě. Při ztrátě karty je toto velmi slabá ochrana, protože v praxi je podpis kontrolován velmi zběžně, či vůbec. Při nahlášení ztráty navíc trvá bance až 3 dny, než rozešle aktualizované seznamy zakázaných karet svým prodejcům. Zloděj má tedy dostatek času kartu zneužít. [14]

Bezpečnostní doporučení

V případě ztráty, či krádeže existuje vysoké riziko zneužití karty, kvůli možnosti placení bez zadávání pinu. Toto lze zejména u čerpacích stanic – např. Benzina, Shell. Velmi důležité je sjednat si pojištění proti zneužití karty a aktivovat si SMS upozornění při čerpání z karty. Dále neprodleně kontaktovat banku pro blokaci karty. Jak již bylo uvedeno, karta zpravidla obsahuje i ostatní technologie záznamu dat, a proto je možné ji zneužít i jinými způsoby, které budou popsány dále.

3.7 Karta s magnetickým proužkem

3.7.1 Popis

Identifikační údaje a data o provedených transakcích jsou zaznamenána na magnetickém proužku karty, což umožňuje elektronické transakce.

Magnetický proužek je definován normou ISO a obsahuje tři datové stopy, na které jsou uloženy následující identifikační údaje až do velikosti 1288 bitů:

- Číslo karty.
- Platnost karty.
- Tuzemská/mezinárodní karta.
- Povolené použití (bankomaty, terminály).

Jak data vypadají a jaký mají význam, je zobrazeno v následujících tabulkách (Tab. 2, Tab. 3, Tab. 4, Tab. 5) [15].

Tab. 2. Konstrukce dat na magnetickém proužku karty

1. stopa:	%B4406160384321844^NOVOTNY/ZDENEK.MR ^02125211652600000000001910000000?;
2. stopa:	4406160384321844=02125211652619120?+
3. stopa:	014406160384321844=2030…030501200571310020000212 2= 20316216181471803==1=7000...0?

Tab. 3. Popis dat první stopy magnetického proužku karty

Zástupný znak	**Význam znaku**
%	Začátek stopy
B	Formát (pro platební karty "B")
4,40616E+15	Základní číslo karty (natištěno i na kartě)
^	Oddělovač
NOVOTNY/ZDENEK.MR	Majitel karty, titul
^	Oddělovač
212	Datum platnosti (12/2002)
521	Servisní kód VISA Electron
1	PVKI: Indikátor čísla PIN
6526	PVV: (PIN Verification Value) Hash pinu
0	Výplň
?	Konec stopy

Tab. 4. Popis dat druhé stopy magnetického proužku karty

Zástupný znak	**Význam znaku**
4,40616E+15	Základní číslo karty (natištěno i na kartě)
=	Oddělovač
212	Datum platnosti (12/2002)
521	VISA Electron
1	PVKI: Indikátor čísla PIN
6526	PVV (PIN Verification Value) - Hash pinu
20	Rozšiřující data
?	Konec stopy

Tab. 5. Popis dat třetí stopy magnetického proužku karty

Zástupný znak	Význam znaku
1	Formát
4,40616E+15	Základní číslo karty (natištěno i na kartě)
=	Oddělovač
203	Země
0	Kód měny
0	Exponent měny
2000	Částka schválená na cyklus
0	Zbývající částka tohoto cyklu
305	Zahájení cyklu (den)
1	Délka cyklu (dnů)
2	Počet opakování
5713	Kontrolní parametr PIN
1	Interchange control
0	PAN - servisní omezení
2000	FSAN - servisní omezení
212	Datum platnosti (12/2002)
2	Pořadové číslo karty vydané k účtu
=	Oddělovač
2,03162E+16	Primární číslo účtu
=	Oddělovač
	Sekundární číslo účtu (není)
=	Oddělovač
1	Relay marker
=	Oddělovač
700000	Šifrovací kontrolní data
0	Výplň
?	Konec stopy

3.7.2 Výhody

Výhodou je nízká cena pro vydavatele a snadné „programování“ karty. Další výhodou a hlavním důvodem neustálého masového nasazení je zpětná celosvětová kompatibilita.

3.7.3 Bezpečnostní rizika a jejich eliminace

Při útocích na tento typ karet se využívá zejména Skimmingu, neboli kopírování. Dále se pro zjištění pinu využívá skryté kamery a dotykové senzory. Dříve se pro zadržení karty

v bankomatu a pozdější zneužití používal útok zvaný Libanonská smyčka. Tyto metody jsou podrobně popsány na začátku kapitoly.

3.8 Zneužití platebních karet na internetu

Údaje z platební karty může pachatel získat několika způsoby. Při krádeži či ztrátě je obvykle daná karta rychle zablokována a riziko zneužití je minimální.

Při Skimmingu můžou být získané data použita pro platbu na internetu. Toto riziko je částečně minimalizováno používáním CVV kódu uvedeného na zadní straně, ovšem existují i internetové obchody s možností plateb kartou bez ověřování CVV kódu, zejména v zahraničí. [18]

Další možností je zneužití obchodníkovy databáze s evidencí zákaznických karet a to jak interně, tak externím útokem. Toto riziko je v ČR a obecně v Evropě řešeno využíváním technologie 3D SECURE. Nebezpečí zneužití údajů z karty zadáním na internetu je ovšem vysoké u Amerických a Asijských obchodníků. Zde je vhodné využívat například virtuální platební kartu, či rozšířenou elektronickou peněženku Paypal.

3.8.1 Virtuální platební karta

Virtuální karta je určena k platbám na internetu. Karta není fyzická, takže s ní nelze realizovat elektronické transakce v terminálech. [19]

Její výhody jsou zejména:

- Nastavení limitu transakce.
- Možnost uzamknutí karty.

Kartu je vhodné odemykat pouze z důvodu realizace transakce.

Virtuální karty vydávají například Raiffeisen bank, Komerční banka, GE MoneyBank.

3.8.2 3D SECURE

Popis

Struktura 3D SECURE je založena na 3 prvcích [20]:

- Obchodník a jeho banka.

- Vydavatel platební karty.
- Struktura podpory 3D SECURE protokolu – ACS(Access Control Server).

Jedná se o technický standard vytvořený společností Visa a MasterCard pro bezpečné platby kartou v prostředí internetu. Je založený na XML protokolu jako další vrstva bezpečnosti online transakcí.

MasterCard označuje tento systém logem „*MasterCard SecureCode*“ a Visa „*Verified by Visa*“.

Hlavní rozdíl mezi MasterCard a Visa spočívá v metodě vytvoření UCAF(Universal Cardholder Authentication Field) kterým se realizuje autentizace držitel karty.

V ČR nabízí platbu pomocí 3D SECURE tyto banky (I/2011).

- ČSOB.
- Komereční banka.
- Česká spořitelna.
- Raiffeisenbank.
- Unicreditbank.
- Citibank.

Na obrázku (Obr. 6) jsou zobrazena loga zabezpečení Visa a MasterCard.

Obr. 6. Logo zabezpečení 3D SECURE [21]

MasterCard

Pro přihlášení se používá hodnota AVV (Accountholder Authentication Value), což je vlastně číslo účtu držitele karty.

Visa

Visa pro přihlášení používá hodnotu CAVV (Cardholder Authentication Verification Value), která reprezentuje číslo karty zákazníka.

Princip

Bezpečnost platby přes 3D SECURE je založena na faktu, že uživatel neposkytuje informace o své kartě na stránkách prodejce, ale přímo bance obchodníka díky přesměrování. Toto spojení je šifrováno a znemožňuje přečtení dat útočníkem. Informace o platební kartě jsou ověřeny bankou obchodníka zařazenou v programu 3D SECURE. Banky komunikují mezi sebou a obchodníka informují pouze o autorizaci, či zamítnutí transakce. Tímto je zamezeno styku obchodníka s údaji na platební kartě a tím i jak úmyslného, tak neúmyslného (nabourání obchodníkovy databáze) zneužití. [20]

Po registraci 3D SECURE je možné si nastavit personalizovaný login. Toto dále zvyšuje ochranu i v případě jiného druhu získání informací útočníkem jako je např. Skimming.

Funkce

Protokol využívá XML zprávy zaslané přes zabezpečené spojení SSL. Autentizace mezi serverem a klientem je zabezpečena pomocí digitálních certifikátů. Transakce je přesměrována na stránky vydavatele karty pro její autorizaci. Vydavatelé karet (banky) můžou používat libovolnou metodu autentizace – toto není v protokolu 3D SECURE specifikováno, ale obvykle se užívá metoda založená na heslech. Nejčastěji se používá následující [20]:

- Autentizační kalkulátor. Vygenerovaný kód se zadá do formuláře dané transakce.
- SMS kód na registrované číslo mobilního telefonu.
- Vygenerování autentizačního kódu platební kartou s displejem, nebo klávesnicí.

ACS (Access Control Server)

ACS se jako přístupový server používá na straně banky. Umožňuje kontrolu přístupu k aplikaci. Většina bank pro tuto činnost využívá outsourcing.

MPI (Merchant Plug-In) providers

MPI je platební brána pro realizaci transakce.

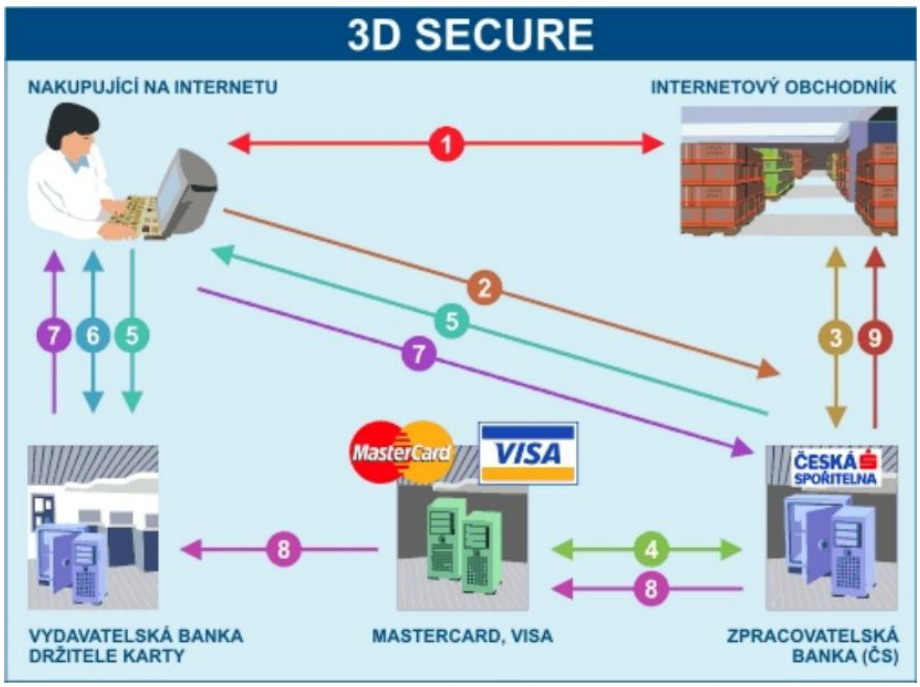
Transakce realizované přes 3D SECURE zahrnují dva základní páry typu výzva – odpověď.

- Verification request/ Verification response.
- Autorization request/Autorization response.

Tyto žádosti jsou odesílány na servery banky, ale protože Visa a MasterCard nedovolují obchodníkům odesílat požadavky přímo na jejich servery, je toto řešeno pomocí prostředníka v podobě licencovaného softwaru Merchant Plug-In (MPI). Tyto jsou nejčastěji pronajímány. V ČR využívají banky KB, ČSOB a Raiffeisenbank outsourcing firmy GPE, a.s., která zajišťuje technické řešení MPI. Marketingový název je GP WebPay / Pay MUZO. Česká spořitelna provozuje vlastní MPI.

Schéma 3D SECURE

Schéma průběhu transakce přes systém 3D SECURE je zobrazeno na obrázku (Obr. 7). Všechny požadavky na Validation a Confirmation musí být zabezpečeny protokolem SSL. [20]



Obr. 7. Schéma průběhu transakce pomocí 3D SECURE [22]

1) Zákazník navštíví internetový obchod a vybere si zboží, nebo službu.
2) Po potvrzení vybraného zboží je nakupující přesměrován na zpracovatelskou banku (banka obchodníka), kde zadá platební údaje.
3) Odsouhlasení objednávky mezi bankou a obchodníkem.
4) Obchodníkova banka vyšle dotaz na kartovou asociaci. Asociace (VISA, MasterCard) potvrdí zařazení/nezařazení držitele karty do systému 3D SECURE a odešle odpověď zpět do banky obchodníka.
5) Banka obchodníka pošle žádost na autentizaci karty do vydavatelské banky přes prohlížeč držitele karty.
6) Vydavatelská banka požádá držitele karty o heslo. Držitel karty vyplní heslo a banka toto heslo potvrdí.
7) Banka zákazníka pošle odpověď zpátky do banky obchodníka přes prohlížeč držitele karty zabezpečeným spojením.
8) V případě, že autentizace proběhla úspěšně, je internetová platba dále zpracována jako běžná platební transakce.
9) Banka obchodníka zašle obchodníkovi informaci o výsledku transakce.

Částečná implementace 3D SECURE

Jestliže není karta zařazena do systému 3D SECURE, proběhne při platbě přímé přesměrování na stránky obchodníkovy banky, bez autentizace majitele karty vydavatelskou bankou. V tomto případě nese odpovědnost za případné zneužití karty vydavatelská banka. [14]

3D SECURE v České republice

Plnou podporu pro 3D SECURE začala v ČR nabízet jako první **Citibank** od 15. 4. 2011. Autentizační kód pro transakci je po registraci zasílán pomocí registrovaného mobilního telefonu. [23]

Ostatní banky plnou podporu 3D SECURE chystají.

Česká spořitelna – považuje systém bez autentizačního kódu za dostatečný, o zavedení uvažuje do budoucna. [24]

Komerční banka – využívá službu Pay MUZO, který pracuje následovně:
Při přijetí požadavku na provedení platby platební kartou předává Pay MUZO požadavek na prověření autentičnosti držitele karty do 3-D systému asociací VISA a MasterCard a na základě obdržených výsledku, povoluje, nebo zamítá, možnost dalšího zpracování objednávky. [25], [26]

ČSOB – připravuje spuštění v druhé polovině roku 2011. [27]

UniCredit Bank – plánuje zavedení v brzké době. [28]

Bezpečnostní rizika 3D SECURE

I přes to, že většina bank nepodporuje plnou podporu pro 3D SECURE je tato technologie velkou výhodu pro zákazníka, který se již nemusí tolik obávat o údaje z platební karty zadávané na internetu.

Systém se potýkal i s některými nedostatky, jako například pop-up (vyskakující) okno, který se objevuje během transakce pro zadání autentizačního PINu zákazníkově bance. V tomto případě je pro zákazníka těžké posoudit, jestli je toto okno opravdu od jeho banky, nebo „nastrčeno“ od útočníka. Některé z těchto pop-up oken postrádají přístup k bezpečnostnímu certifikátu stránky, což znemožňuje ověření pravosti okna. Důvodem je, že pop-up okno je zajišťováno doménou, která není:

- Stránkou obchodníka.
- Stránkou banky zákazníka.
- Stránkou Visa, či Mastercard.

Novější bezpečnostní doporučení obsahuje „inline frame“, který umožňuje otevírání nové stránky uvnitř hlavní stránky. Toto zlepšuje orientaci zákazníka, ale některé prohlížeče mají problém s jednoduchým ověřením bezpečnostního certifikátu pro obsah v „inline frame“. Zde je stále možnost útoků typu MITM, protože zákazník si nemůže ověřit certifikát SSL serveru. Řešením je využití celé stránky prohlížeče pro autentizaci místo „inline frame“, což ovšem snižuje přehlednost. [20]

Závěr

Systém 3D SECURE má řadů výhod a je to velký krok pro zvýšení bezpečnosti při platbách kartami na internetu. I když je na českém trhu již od roku 2004, stále není kompletně implementován.

Zavádění tohoto systému, také není pro všechny obchodníky ekonomicky výhodné. I přes zvýšení prestiže a pravděpodobnost zvýšení obratu se nemusí zavádění vyplatit. Ceny MPI se pohybují okolo 15 000,-Kč s tím, že je obvyklý měsíční poplatek za technickou údržbu cca 150,-Kč a odvádění procentuální částky z každého realizovaného obchodu.

Naopak výhodou pro obchodníka je, že vzhledem k tomu, že užívá platební bránu, která splňuje požadavky 3D SECURE, ztrácí vydavatel platební karty nárok na reklamaci případného zneužití karty a náhradu tak neplatí obchodník, jako ve většině případů bez 3D SECURE, ale vydavatelská banka.

3.9 Čipové platební karty

Čipová karta je označení pro karty obsahující čip. Anglicky také Integrated Circuit Card (ICC). Tyto mohou být realizovány od nejjednodušších pamětí až po 32bitové procesory s frekvencí 30MHz. Čipové karty mohou mít rozličné využití. Čipovou kartou je například i SIM karta.

Na čipovou kartu můžeme také nahlížet jako jednoduchý kryptografický modul s malou výpočetní silou. Hlavním účelem je vykonávání kryptografických operací, vyžadujících tajný klíč.

Hlavní výhodou čipových karet je možnost chránit data, která jsou na čipu uložena před případným útokem za účelem neautorizovaného přístupu, nebo modifikace dat.

Na konci roku 2010 bylo 97% všech vydaných karet v ČR čipových. [29]

3.9.1 Rozdělení čipových karet

Čipové karty můžeme rozdělit následovně [10]:

- Kontaktní – vyžadovaný fyzický kontakt čipu se čtečkou.
- Bezkontaktní – komunikace probíhá pomocí antény a snímače na krátkou vzdálenost.
- Kombinované – čip obsahuje kontaktní i bezkontaktní rozhraní.
- Hybridní – obsahuje dva nezávislé čipy, každý pro jednu technologii a případně i magnetický proužek. Tímto je dosaženo vysoké flexibility.

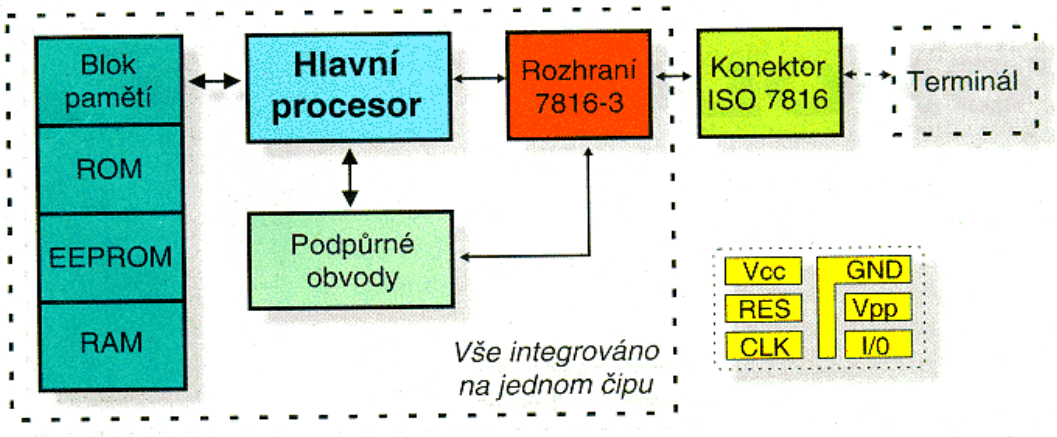
Bezkontaktní karty jsou z hlediska technologie složitější a zejména je potřeba řešit problém s napájením, ale mají přidanou hodnotu pro zákazníka, který může provést autentizaci i pouhým přiblížením. Toto sebou ovšem nese rizika autentizace bez vědomí majitele. Bezkontaktní karty budou popsány dále v textu.

Současné čipové karty fungují jako počítač.

Obsahují tyto části [30]:

- ROM (Read Only Memory) pamět o velikostech v řádech desítek až stovek KB.
- EEPROM o velikostech v řádech desítek KB.
- RAM o velikostech několika KB – provádění výpočtů.
- Procesor.
- Koprocesory – v případě potřeby speciálních výpočtu např.: kryptování.
- Vstupně/výstupní rozhraní.

Architektura karty je zobrazena na obrázku (Obr. 8).



Obr. 8. Architektura čipové karty [30]

ROM (Read Only Memory) – Je zde trvale uložen operační systém. Dále paměť řídí ukládání a načítání dat z EEPROM.

EEPROM (Electrically Erasable Programmable Read-Only Memory) – Je možné ji až 10000krát přeprogramovat. Obsahuje různé aplikace. Využívá ji procesor pro ukládání zašifrovaných dat.

RAM (Random Access Memory) – Paměť je využívána procesorem pro výpočty a mezi-výpočty.

PROCESOR – Hlavní procesor je důležitý pro bezpečnost. Provádí autentizaci, šifrování komunikace karty s terminálem a výpočty důležité pro digitální podpis.

Vcc – napájení karty.

Vpp – volitelné napájení karty.

GND – uzemnění.

I/O – vstupně, výstupní kontakt pro přenos dat mezi kartou a terminálem.

RES – funkce reset pro možnost zjištění typu karty terminálem v základním režimu.

CLK – vstup pro hodinový signál z terminálu, podle kterého se poté řídí rychlost komunikace.

3.9.2 FIPS 140-3

Dokument Federal Information Processing Standard (FIPS) specifikuje požadavky pro akreditované kryptografické moduly. Je vydáván za účelem koordinovat požadavky a standardy pro kryptografické moduly, které zahrnují jak hardwarové, tak softwarové komponenty. [31]

Změny oproti verzi FIPS 140-2 jsou následující [32]:

- 5 bezpečnostních úrovní namísto 4 původních ve verzi FIPS 140-2.
- Zpřísněné požadavky proti neinvazivním útokům při ověřování vyššího bezpečnostního stupně.
- Zavedení pojmu „veřejné bezpečnostní parametry“.
- Zvýšení požadavky na ověření uživatele a testování integrity.

Z pohledu čipových karet je zajímavý oddíl věnující se odběrové analýze jednočipových procesorů, včetně čipových karet.

„*Teoreticky analýza jednoho čipu číst klíče jakýchkoliv identických čipů.*

Tato pravděpodobnost, že dva čipy budou zcela totožné, je ale velmi malá. Nicméně odběrová analýza jednoho čipu může dramaticky snížit množství analýz potřebných k prolomení bezpečnosti čipů vycházejících ze stejného standardu.“ [32]

Tento typ analýzy byl zmíněn již v předchozí normě FIPS 140-2, ale protože v době vydávání této normy byl poměrně nový, byl zmíněn v části “ostatní útoky”, bez povinné aplikaci ochrany proti němu. (V této práci je tento druh útoků rozebrán v oddílu HSM.)

Cesta, jak se proti tomuto bránit, je přidávání náhodnosti, či šumů do funkce procesorů. Toto může být realizováno několika způsoby:

- Zavádění dodatečné energie pro obvody.

- Náhodné přeskakování některých cyklů procesoru.
- Přerušování procesů a přesměrování dokončení akce na jiné okruhy procesoru.

Samozřejmě i zde musí existovat kompromis mezi bezpečností, cenou a výkonem. Jakýkoliv dodatečně implementovaný šum vede ke zvýšení spotřeby, či snížení výkonu.

Toto řešení není dokonalé, protože s dostatečným vzorkem a počtem analýz lze šum odfiltrovat. Ovšem právě přidaný čas, úsilí a potřebné vybavení zvyšuje obtížnost proveditelnosti útoku pro „náhodné útočníky“.

3.9.3 EMV

Specifikace EMV byla vytvořena společnostmi Europay International, MasterCard International a Visa Internationl za účelem interoperability platebních systémů založených na čipových kartách. EMV je dominantní protokol užívaný pro platby čipovými kartami ve světě. V září 2010 dosáhl počet čipových karet ve světě počtu přes 1 bilion kusů. Počty karet a terminálů podporujících standard EMV a procento z celkového počtu, jsou zobrazeny na obrázku (Obr. 9). [33]

Použití čipových karet s kompatibilními platebními terminály také zaručuje mnohem lepší zabezpečení, kterým se budeme zabývat dále.

EMV se skládá z funkcí, které jsou potřebné pro komunikaci platební karty s terminálem obchodníka a také systému pro autentizaci držitele platební karty.

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Caribbean	182,185,043	26.4%	2,000,000	55.6%
Asia Pacific	305,126,927	26.6%	3,200,000	41.6%
Africa & the Middle East	16,841,874	13.7%	348,000	62.5%
Europe Zone 1	555,688,434	65.4%	9,400,000	84.7%
Europe Zone 2	22,817,271	11.5%	457,800	61.2%
United States[1]				
TOTALS	1,082,659,549	36.0%	15,405,800	65.0%

Obr. 9. Celosvětové zavedení specifikace EMV a míra její adaptace (IX 2010) [34]

Poslední úprava specifikace je EMV 4.2, která je platná od VI/2008. Tato úprava je dělena do čtyř „knih“, které definují všechny komponenty v systému platby EMV. [16]

Kniha 1: Application Independent ICC to Terminal Interface Requirements

- Požadavky na elektromechanické vlastnosti.
- Specifikace přenosových protokolů.
- Mechanismus volby aplikací.
- Struktura souborů.

Kniha 2: Security and Key Management

- Bezpečnostní požadavky offline autentizace.
- Bezpečnostní požadavky šifrování PINů.
- Kryptografické požadavky a management kryptografických klíčů.

Kniha 3: Application Specification

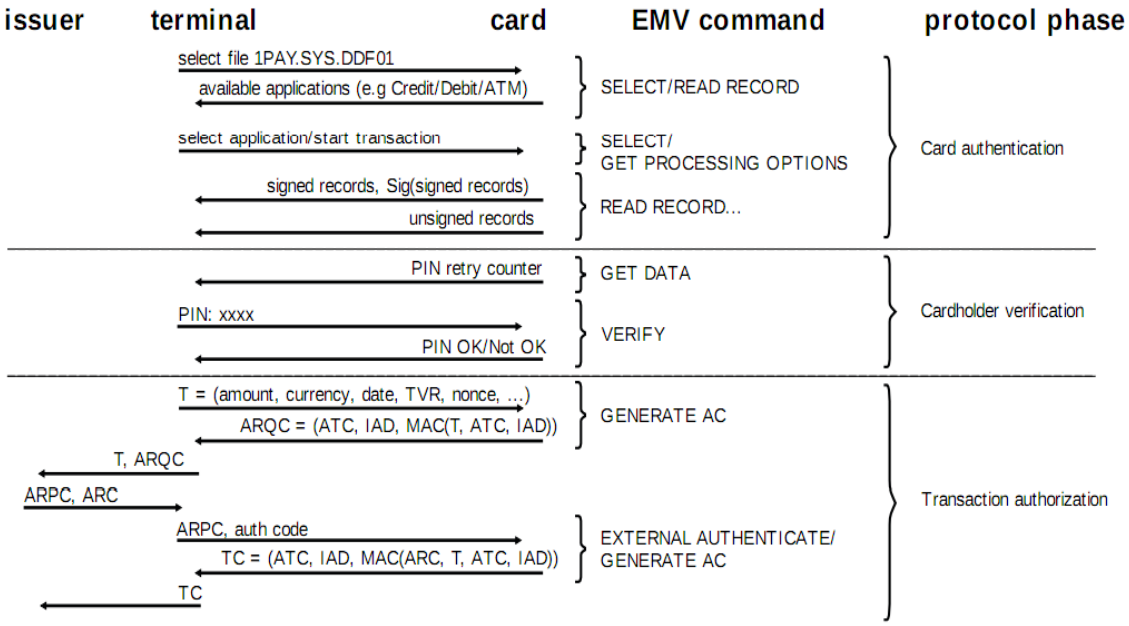
- Požadavky na jednotlivé aplikace.

Kniha 4: Cardholder, Attendant, and Acquirer Interface Requirements

- Požadavky pro zajištění kompatibility.

3.9.4 Analýza bezpečnosti čipových platebních karet

Kompletní průběh protokolu EMV při kontaktu čipové karty s terminálem je znázorněn na obrázku (Obr. 10). Jednotlivé kroky a jejich bezpečnost si rozebereme dále. [10]



Obr. 10. Průběh protokolu EMV při kontaktu čipové karty s terminálem [35]

3.9.4.1 Autentizace karty offline metodou

Offline autentizace karty je prvním bezpečnostním mechanizmem, který umožňuje detekci falešné, pozměněné, či zkopírované karty vložené do platebního terminálu či bankomatu (terminál). Při této metodě není vyžadováno spojení s bankou a princip ověření spočívá ve užití PKI (Public Key Infrastructure), která se stará o správu a distribuci veřejných klíčů pro asymetrickou kryptografii. Toto vyžaduje součinnost s certifikační autoritou (CA), která podepisuje veřejné klíče vydavatelů čipových karet. Existují dva typy Offline autentizace:

- Statická autentizace dat (SDA).
- Dynamická autentizace dat (DDA).

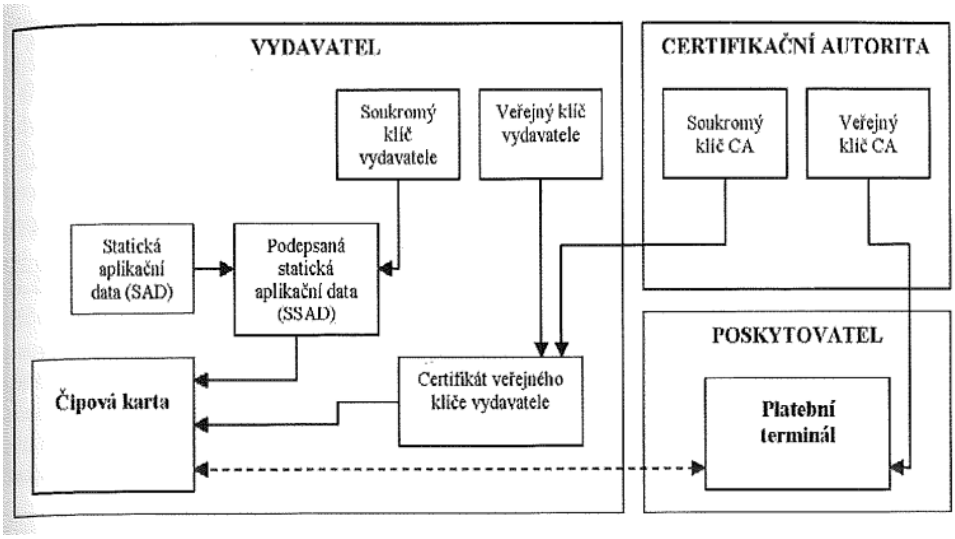
Statická autentizace dat

Static Data Authentication (SDA) umožňuje ověření statických aplikačních dat uložených na čipové kartě. Tato data jsou podepsána soukromým klíčem vydavatele. Na kartě je také uložen certifikovaný (ověřený důvěryhodnou certifikační autoritou) veřejný klíč vydavatele.

Terminál si z karty načte data společně s veřejným klíčem, který si následně ověří u CA. Poté si tímto již ověřeným klíčem ověří samotná statická aplikační data.

Využívá se algoritmu RSA a bezpečnost celého systému je závislá na utajení soukromých podepisovacích klíčů. Při jejich získání útočníkem by bylo možné vytvářet nové platební karty a podepisovat jejich nový obsah. Schéma SDA je zobrazeno na obrázku (Obr. 11)

Jelikož se při této metodě odesílají citlivá data mimo kartu, lze aplikovat útoky typu Skimming.



Obr. 11. Offline autentizace dat u EMV pomocí SDA [10]

Dynamická autentizace dat (DDA)

Dynamic Data Authentication (DDA) řeší problém ověření pravosti samotné karty u metody SDA. Rozšiřuje SDA o ověření samotné karty pomocí jedinečného páru RSA klíčů, které jsou bezpečně uloženy na samotné kartě a jelikož soukromý klíč nikdy neopouští kartu, není možné jej přečíst a zkopírovat.

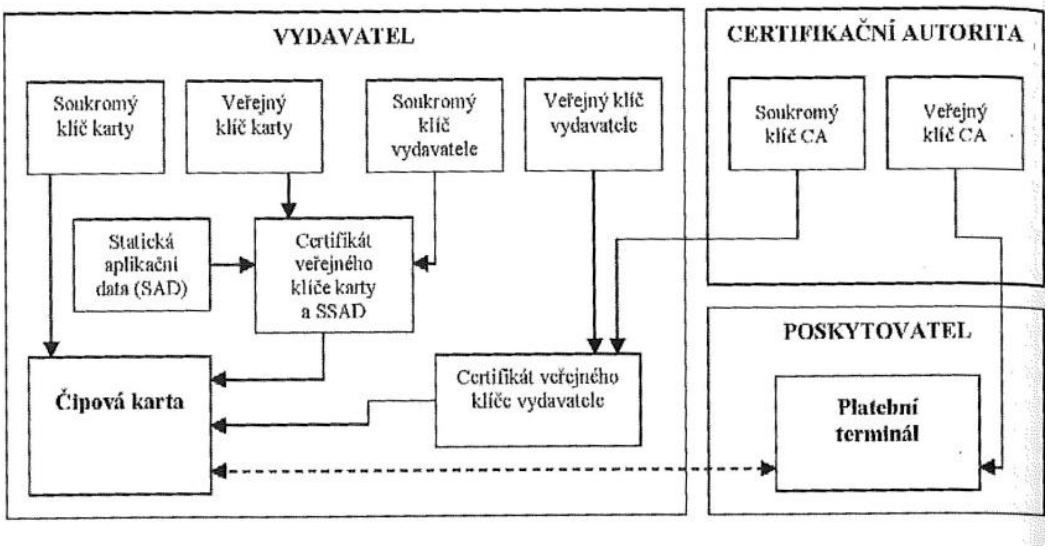
Aplikační data jsou spolu s veřejným klíčem karty podepsána soukromím klíčem vydavatele karty a jako celek jsou odeslány do terminálu společně s certifikovaným veřejným klíčem vydavatele karty. Terminál si ověří pravost veřejného klíče vydavatele karty. Je-li pravý, ověří jím aplikační data a veřejný klíč karty.

Bezpečnost karty je dále zvýšena náhodným zasíláním dat z terminálu kartě, která je podepisuje soukromým klíčem, a po následném přijetí terminálem jsou data ověřena důvěryhodným veřejným klíčem karty. Schéma DDA je zobrazeno na obrázku (Obr. 12).

Při aplikaci musíme řešit tyto problémy:

- Bezpečnost tohoto systému závisí na utajení podepisovacích klíčů RSA.
- Potřeba zajistit bezpečnost soukromého klíče karty.
- Karta musí obsahovat koprocesory pro asymetrickou kryptografii.

Toto vede k závěru, že DDA ověřování je velmi bezpečné, ale nákladnější oproti SDA.



Obr. 12. Offline autentizace dat u EMV pomocí DDA [10]

3.9.4.2 Verifikace držitele karty

Verifikace uživatele může být realizována několika způsoby, jako jsou:

- Ruční podpis.
- PIN.
- Kombinace verifikačních metod.

Čipová karta obsahuje seznam autentizačních a verifikačních metod uspořádaný podle bezpečnosti shora dolů. Tento seznam se porovnává s metodami, které podporuje konkrétní terminál a vybere se první shodná metoda. Úroveň bezpečnosti je tedy závislá na terminálu.

Ve specifikaci EMV je obsažena specifikace podpory offline autentizace uživatelů a to buď zašifrovanými, nebo nezašifrovanými PINy.

Při šifrování se pro přenos využívá asymetrického algoritmu RSA. V tomto případě musí karta obsahovat další pár šifrovacích klíčů určených výhradně pro zabezpečení přenosu zadaného PINu. Tyto klíče musí být ověřeny Certifikační autoritou.

Zadaný PIN je porovnáván s PINem uloženým na kartě. Základní prvky bezpečnosti jsou následující:

- Utajení soukromého klíče.
- Utajení vzorového PINu.
- Fyzické zabezpečení PINpadu.

Fyzické zabezpečení PINpadu, případně celého terminálu je nutné z důvodu možnosti zkopírování PINu před procesem zašifrování. Toto je nutné zejména v případech, kdy se PIN odesílá z terminálu v nezašifrované podobě.

3.9.4.3 Automatická analýza rizik při transakci

Účelem automatické analýzy rizik je minimalizace možností podvodů a ochrana všech zúčastněných subjektů. Tato analýza probíhá po úspěšné autentizaci držitele karty je rozdělena do těchto tří bodů:

- Analýza rizik terminálu.
- Analýza rizik akcí terminálu.
- Analýza rizik akcí karty.

Výsledkem analýzy je buď přijetí offline transakce, zamítnutí offline transakce nebo nutnost online autorizace transakce.

Analýza rizik terminálu umožňuje například kontrolu povoleného horního limitu transakce, náhodný výběr transakcí k online realizaci, omezení počtu po sobě jdoucích offline transakcí apod.

Analýza rizik akcí terminálu má v případě zamítnutí offline transakce vždy větší váhu, než pozitivní rozhodnutí z analýzy rizik akcí karty. Naopak umožní-li analýza realizaci offline transakce, ale analýza rizik karty ji zamítne, nebude tato provedena a může následovat online autorizace.

3.9.4.4 Online autorizace transakce

Je-li vyžadována online autorizace transakce, využívá se symetrické kryptografie v podobě algoritmu 3DES. V tomto případě musí být na kartě uložen tajný klíč. Tento klíč je sdílené tajemství s vydavatelem karty, neboli bankou, která kartu vydala držiteli. Dále se při transakci vytváří dočasný klíč odvozený právě od tajného klíče. Tento dočasný klíč slouží pro vytvoření Message Authentication Code (MAC) dat dané transakce. Při zasílání dat do banky je přiložen i MAC, který je následně porovnán s MAC vytvořeným ze sdíleného tajného klíče uloženého v bance. Jsou-li oba MAC stejné, je ověřena pravost karty. Následná komunikace pro zjištění zůstatku na účtu svázaného s danou kartou probíhá analogicky.

3.9.5 Nedostatky bezpečnosti čipových karet a standardu EMV

Standard EMV obsahuje širokou škálu bezpečnostních mechanizmů a byl vyvíjen k maximální bezpečnosti. Bohužel ne všechny obsažené mechanizmy jsou povinné, a proto každý systém, byť založený na stejném standardu, má vlastní úroveň bezpečnosti v závislosti na konkrétním řešení.

V praxi není samotná bezpečnost na prvním místě a je nutné volit vyvážený poměr mezi cenou, výkonem a bezpečnostní. Někdy také není nutné zavádět všechny mechanizmy, kdy například u sítě terminálů s podporou pouze online autorizace transakce, u nichž je implementováno ověření pravosti karty vyplívající ze symetrické kryptografie, je autentizace dat SDA dostačující.

Jako první byla implementována podpora standardu EMV v Anglii, kde byl extrémní počet podvodů s platebními kartami, který v roce 2000 dosahoval 75% všech těchto podvodů v Evropě.

Největší slabinou bezpečnosti je fakt, že v Anglii je většinou implementována pouze statická autentizace dat SDA, bez podpory online autorizace transakce. [10]

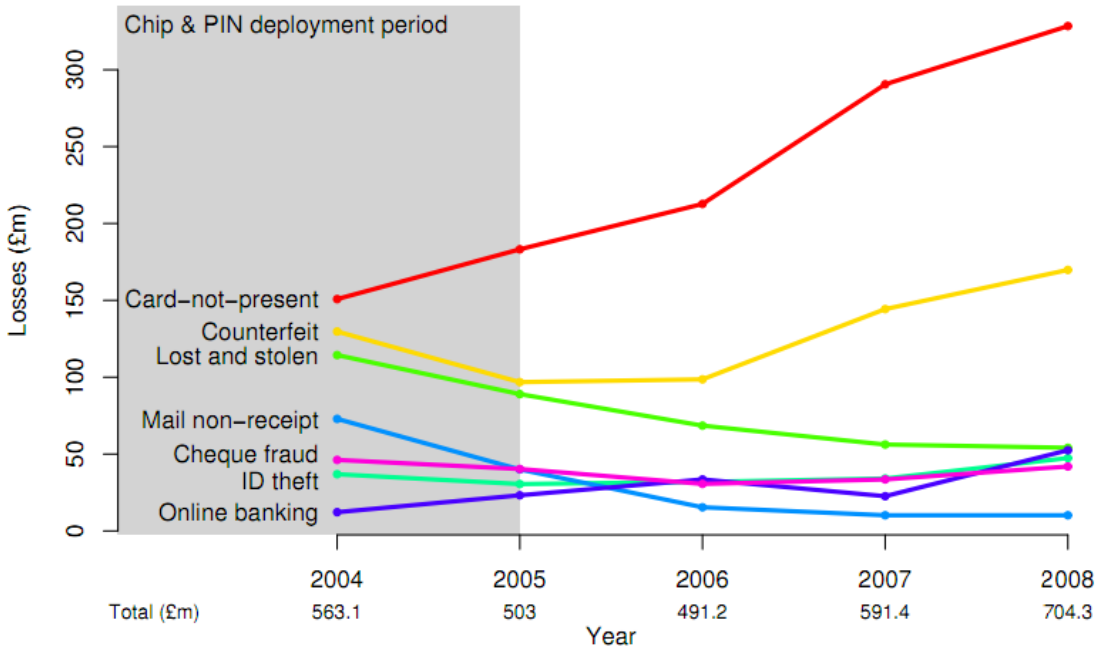
3.9.6 Prolomení zabezpečení čipových karet

Bezpečnost čipových karet v Anglii je velmi medializovaná, protože se na jejich testování zaměřil tým z University of Cambridge, který později uveřejnil úspěšné zneužití takto chráněných karet.

V roce 2006 byl uveřejněn útok, který díky použití technologie SDA odposlouchával data mezi kartou a terminálem a z takto získaných dat byly vytvořeny kopie karty s magnetickým proužkem. [41]

Čipové karty s SDA technologií lze ovšem zneužít jen když terminál nepodporuje online autorizaci transakcí, protože jinak útočník nezná tajný symetrický 3DES klíč sdílený mezi kartou a bankou. Většina zemí již používá DDA a v Anglii začal přechod z SDA na DDA v roce 2008.

Jak je vidět na obrázku (Obr. 13), objem podvodů realizovaný kartami „na dálku“ se i přes implementaci EMV a čipových karet nesnižuje (2004 - 2008).



Obr. 13 Statistika podvodů s kartami vydanými ve Velké Británii 2004 – 2008 [35]

Posledním dokumentem University of Cambridge popisující bezpečnostní nedostatek čipových karet je dokument „*Chip and PIN is Broken*“, který byl prezentován na IEEE Symposium on Security & Privacy v USA v květnu roku 2010. [35] Některé poznatky si dále uvedeme.

Princip zneužití spočíval ve využití chyby protokolu, která umožňuje útočníkovy provést platbu, aniž by věděl PIN karty a zůstal neodhalený i v případě, že obchodníkův terminál má online propojení s bankou. V dokumentu jsou také popsány rozdíly mezi různými

zeměmi, kdy například karty v Belgii a Estonsku funguji na stejném principu a lze je tedy stejně zneužít, zatímco ve Švýcarsku a Německu seznam autentizačních metod specifikuje přísnější autentizační metody, takže na ně není možné tento útok použít. Nicméně protože anglické terminály většinou nepodporují online ověření PINu, může zde být zneužita i karta z těchto zemí.

Princip útoku

Základní chyba v protokolu umožňující tento útok je, že krok ověřování PINu (offline), není nikdy explicitně zaznamenán. Data, která karta generuje – Issuer Application Data (IAD) jsou sice odesílána bance, ale banka neví, která metoda ověření uživatele byla použita, a proto toto nelze použít jako prevenci útoků. Proto zařízení pro útok MITM, které může zachytit a modifikovat komunikaci mezi kartou a terminálem může oklamat terminál, aby věřil, že ověření PINu proběhlo úspěšně odesláním 0x9000, což je zástupná hodnota pro zprávu, že ověření PINem proběhlo v pořádku, bez vlastního odeslání PINu do karty. Nějaký PIN musí být zadán, ale útok umožní, aby byl akceptován jakýkoliv PIN.

Karta poté „uvěří“, že terminál nepodporoval ověření PINem a buď přeskočí ověření držitele karty, nebo iniciuje ověření pomocí podpisu. Protože zadaný PIN nebyl nikdy odeslán do karty, počitadlo pokusů pro zadání PINu se nezmění a je stále na hodnotě 3. Ani terminál, ani karta si tohoto nevšimnou, protože hodnota, která detekuje správnost ověření, je změněna pouze při neúspěšném pokusu. Terminál věří, že zadání PINu proběhlo v pořádku, takže generuje nulový bajt a karta „věří“, že nebyl zadán žádný, takže také generuje nulový bajt.

Popis útoku

Zařízení pro útok MITM je spojeno s terminálem skrze falešnou kartu. K této kartě jsou připevněny tenké kontakty, které ji propojují s rozhraním čipu. Tato je spojena s rozhraním Field Programmable Gate Array (FPGA), což je universální programovatelný čip obsahující velké množství hradel. FPGA kartu řídí a překládá tok dat mezi kartou a rozhraním laptopu. FPGA je přes sériovou linku propojeno s laptopem, na který je dále zapojena čtečka čipových karet. Do této čtečky je vložena originální karta. Skript napsaný v programovacím jazyce Python přenáší transakci, zatímco čeká na ověřovací příkaz od terminálu. Tento příkaz potom nepošle kartě a odpoví terminálu 0x9000, což znamená, že

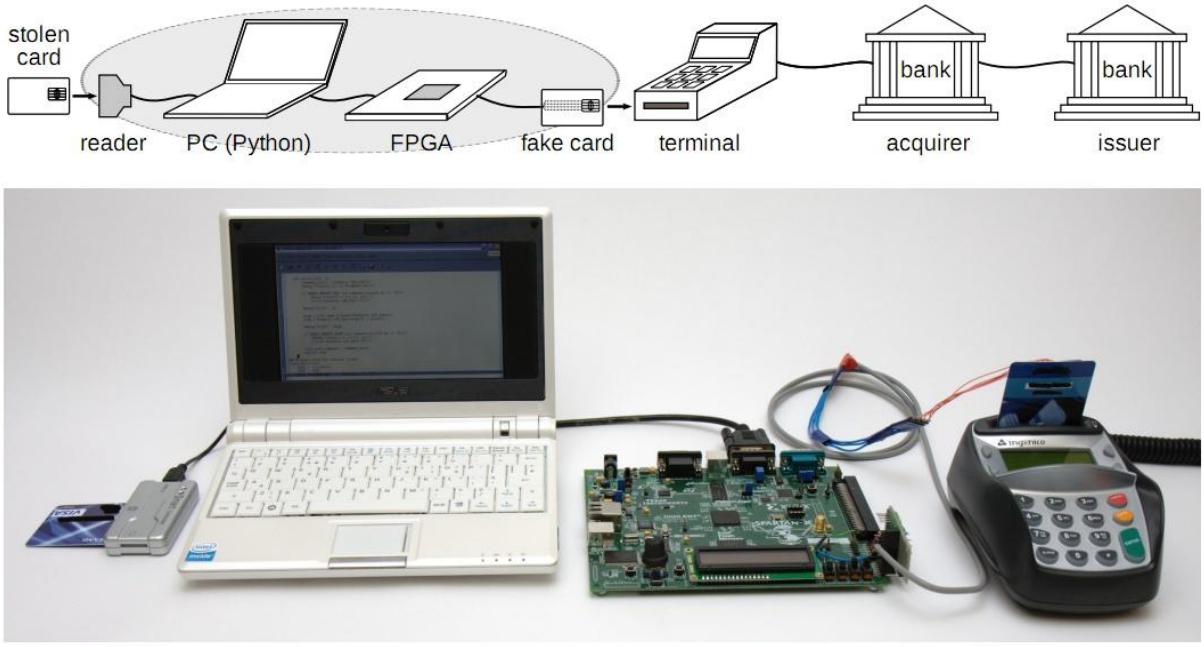
ověření PINu proběhlo v pořádku, jak jsme si řekli již výše. Část kódu, který toto řeší, je zobrazena na obrázku (Obr. 14).

```
if VERIFY_PRE and command[0:4] == "0020":
    debug("Spoofing VERIFY response")
    return binascii.a2b_hex("9000")
```

Obr. 14 Pozměněný kód komunikace mezi čipovou kartou a terminálem [35]

Samotný útok byl proveden tak, že zařízení FPGA, laptop a čtečka karet s originální kartou byly ukryty v batohu a ke kabelu, který byl vedený přes rukáv útočníka, byla připevněna falešná karta, která se vložila do terminálu. Tím, že obchodník má tendenci nedívat se na zákazníka při zadávání PINu, byl útok o to jednodušší z pohledu fyzického odhalení.

Jednotlivé komponenty zařízení použitého k tomuto útoku, jsou znázorněny na obrázku (Obr. 15).



Obr. 15. Komponenty použité k útoku na čipovou kartu [35]

Ochrana proti obdobným útokům

Chyby v jádře protokolu je náročné opravit. Přechod z SDA na DDA zřejmě nebude mít efekt, protože obě tyto metody se provádí před ověřením držitele karty PINem.

Možným řešením je analýza IAD dat z karty terminálem, protože obsahuje výsledek ověření PINem. Z pohledu útočníka se ovšem toto dá teoreticky překonat, protože MITM může manipulovat s IAD daty, která jsou generována kartou. Náročné na implementaci je to ale z důvodu, že IAD byl zamýšlený pouze pro vydavatele karet, neboli banky a existuje několik různých formátů.

Takové řešení bude vyžadovat dohodu mezi bankami a prodejci, což bude pomalé a zdlouhavé. [35]

Jiným účinným řešení je analýza dvou datových objektů vzniklých při transakci a jejich porovnání. Jeden z nich je CVR (Card Verification Results), kde je vidět, že karta žádnou kontrolu PINu neprovedla. Druhý je CVM Results (Cardholder Verification Method Results) terminálu, kde je uložena informace o použité metodě a výsledku verifikace držitele (v tomto případě úspěšné provedení kontroly offline PIN). CVM Results nemůže útočník měnit (jde z terminálu rovnou do banky), CVR je sice přenášeno z karty do terminálu a pak do banky, hodnota je ovšem chráněna kryptogramem generovaným kartou (zabezpečení dat transakce unikátním 3DES klíčem). Bohužel, přenos CVM Results z terminálů do banky není zatím povinný, banky tedy nemají vždy dostatek spolehlivých informací, podle kterých situaci vyhodnotit. Dále je nutné online spojení s bankou pro ověření těchto dat. Při zúčtovaní na konci dne by banka ovšem měla alespoň dostatek informací pro zjištění, zda se jednalo o tento typ útoku, což by bylo výhodné pro držitele použité karty. [36]

Dalším řešením je zavedení terminálů, pouze s podporou online verifikace PINu. V tomto případě probíhá ověření PINu online, bez účasti karty.

Závěrečné posouzení EMV

Standard EMV je oproti předchozím letům velký posun v bezhotovostních platbách zajišťující vyšší úroveň bezpečnosti a interoperability mezi systémy. I přes mnohé bezpečnostní problémy spočívající v samotné specifikaci, v realizaci jednotlivých

platebních systémů, či implementaci funkcí v terminálech, je toto krok, který výrazně snižuje možnost kopírování karet.

Jelikož většina terminálů v Evropě využívá nebo brzy začne využívat online spojení s bankou a dynamickou autentizaci dat karty, je zřejmě nejslabším místem systému samotný terminál. I když by terminály měli splňovat poměrně přísné nároky na fyzickou bezpečnost, je velice těžké toto v praxi garantovat. Pro zákazníka je nemožné rozlišovat mezi nesčetnými typy terminálů, a proto nemůže poznat, zda se jedná o řádný terminál, nebo lehce pozměněný, který může umožňovat kopírovat PINy, či umožňuje přesměrování EMV protokolu. Tento problém je téměř neřešitelný a vždy bude záležet na poctivosti daného obchodníka.

3.10 Problematika bezpečnosti terminálů při platbě u obchodníka

Bezpečnosti platebních terminálů se věnuje málo pozornosti, i když riziko není zanedbatelné a podvody realizované touto cestou jsou na realizaci jedny z nejjednodušších.

Jelikož obchodník vlastní terminál, může si jej i nelegálně upravit. Následně může terminál kopírovat vložené karty nebo snímat zadávané PINy.

Kvůli existenci mnoha typů terminálu, není v silách zákazníka modifikovaný terminál rozpoznat.

3.11 Experiment bezpečnosti zadávání PINu a podpisu při platbě kartou u obchodníka

Experiment, který byl prováděn v letech 2005 a 2006 na Fakultě informatiky Masarykovy univerzity, měl odpovědět na dvě základní otázky [37]:

- Jak náročné je zfalšovat vlastnoruční podpis držitele karty?
- Jak náročné je odpozorovat PIN zadávaný zákazníkem do PINpadu při platbě?

Při pokusu o zfalšování podpisu u platby kartou dostali figuranti karty, na kterých byl uveden originální podpis držitele a měli 20 minut na nacvičení podpisu. Poté se ve vybraném supermarketu pokusil zaplatit kartou a platbu autorizovat podpisem. Experiment byl ukončen po 17 úspěšných pokusech ze sedmnácti. Na tomto příkladu je velmi dobře vidět, že bezpečnost zajištěná pouze pomocí podpisu držitele karty je velmi nízká. Studie

také uvádí, že při platbě kartou například v klenotnictví byl personál ostražitější a podpis kontroloval důkladněji.

Odpozorování PINů, které také probíhalo v supermarketu, bylo založeno na několika pozorovacích týmech, které měly za úkol zjistit hodnoty PINů při zadávání do PINpadu. Výsledky jsou následující:

- Z 26 tipů na 4místný pin bylo správně odpozorováno 42% zadávaných číslic.
- Správné odhadnutí celého PINu do třech pokusů se povedlo ve 20 % případů.
- Nejlepší tým dokázal správně odpozorovat 68% zadaných číslic.
- Většina PINů (3/4) byly odpozorovány na PINpadu bez ochranného krytu.

Z tohoto experimentu vyplývá, že podpis při platbě kartou je velice slabá bezpečností metoda. Tato metoda je již naštěstí na ústupu. Nejrozšířenější metoda autentizace držitele karty pomocí PINu je sice bezpečnější, ovšem jak ukazují výsledky experimentu riziko odpozorování PINu je vysoké. Tomuto napomáhají zejména zákazníci, kteří nejsou při zadávání PINu dostatečně ostražití. U obchodníků je vhodné zavést PINpady s ochraným krytem, který podle pokusu značně komplikuje odpozorování PINu.

Při ztrátě karty je její náhodné zneužití v terminálech malé, ale při cílené krádeži s předchozím odpozorováním PINu, které pro „profesionála“ není větší problém, je riziko již značné.

4 INTERNETOVÉ, TELEFONICKÉ, GSM, WAP BANKOVNICTVÍ

V této kapitole popíšu nejoblíbenější způsoby osobního bankovnictví a rozeberu u nich bezpečnostní prvky.

4.1 Internetové bankovnictví a jeho bezpečnost

Při používání internetového bankovnictví probíhá komunikace mezi bankou a klientem pomocí internetu. Internetové bankovnictví je velmi rozšířené a oblíbené a to jak ze strany klientu, tak ze strany bank.

Bankám snižuje náklady na platební operace. Klientovy zase dává možnost spravovat svůj účet online, čímž získává flexibilitu a přístup odkudkoliv, kde má k dispozici webový prohlížeč. S tímto se ovšem váží i bezpečnostní rizika.

4.1.1 Rozdělení hrozeb

Bezpečnost internetového bankovnictví můžeme rozdělit do těchto skupin [38]:

- Identifikace banky a bezpečná komunikace.
- Autentizace uživatele a autorizace transakcí.
- Bezpečnost přístupového počítače.
- Ostatní bezpečnostní opatření.

I když je bezpečnost systému nejčastěji konstruována na útok zvenčí je dobré si uvědomit, že nebezpečí hrozí i zevnitř. „*Provoz a rozvoj systémů bank je dohledován regulátorem, tj. ČNB. V této souvislosti je nutné zmínit hrozbu, jakou je selhání administrátora a zneužití jeho pravomocí. Proti této hrozbě jsou systémy chráněny organizačními opatřeními (např. zásady čtyř očí), specializovanými hardwarovými prvky (HSM) a využitím elektronického podpisu zpracovávaných dat (např. platebních příkazů) pro pozdější prokazování zodpovědnosti.“* [39]

4.1.2 Identifikace banky a bezpečná komunikace

Identifikace je nejčastěji realizována pomocí certifikátů vydaných obecně uznávanými CA jako například VeriSign. Tyto certifikáty jsou standardně obsaženy u všech masově rozšířených webových prohlížečů, a proto probíhá identifikace bezproblémově. Certifikáty vydávané národními certifikačními autoritami by měly pracovat obdobně, ale z důvodu

integrace v mezinárodních prohlížečích nejsou v reálu aplikovatelné. Bezpečná komunikace se realizuje za pomoci standardního protokolu SSL (TLS) vyplívajícího z HTTPS.

4.1.3 Falšování certifikátů zneužitím MD5 hash

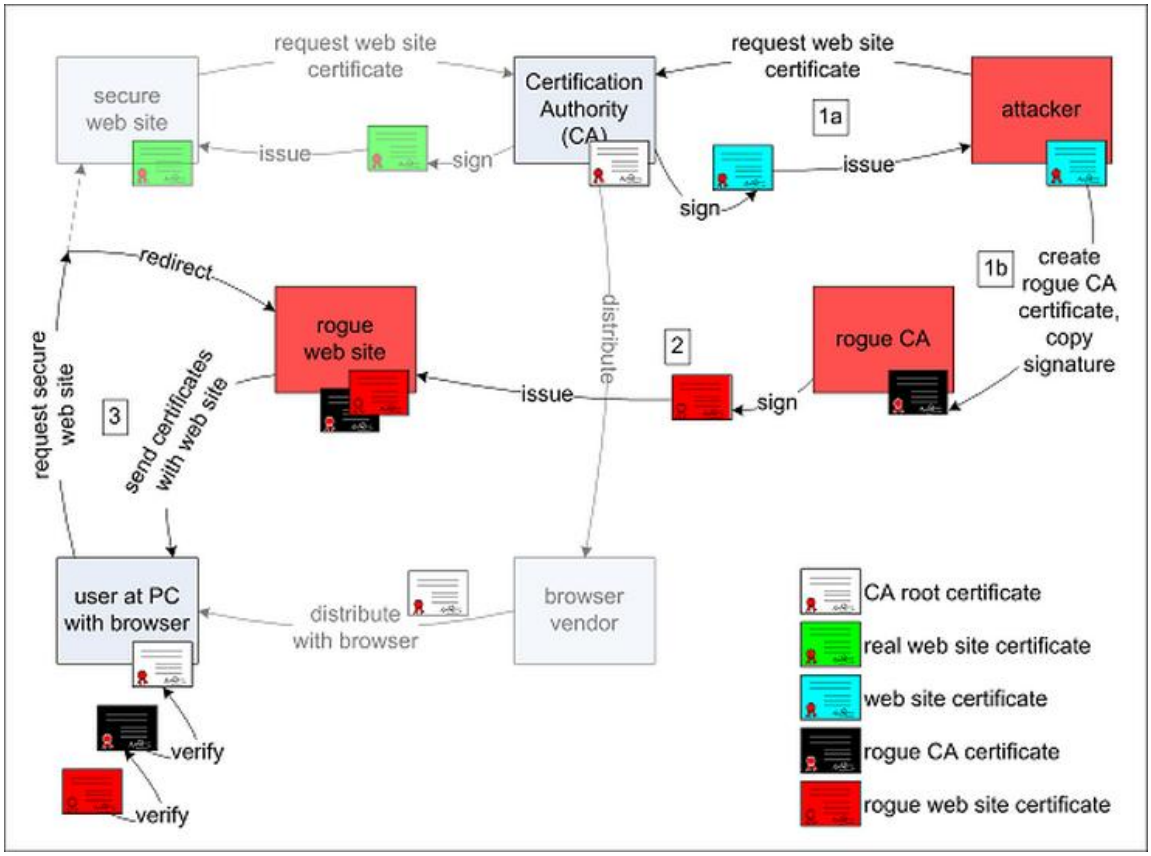
V roce 2009 byl uveřejněn článek [40], který popisuje jak tým inženýrů z USA a několika evropských universit vytvořil falešný certifikát autority VeriSign. Takto vytvořený certifikát, může být dále použitý pro phishing, kde může podepsat falešné stránky útočníka vydávající se například za stránku internetového bankovnictví. Některé poznatky z článku si uvedeme dále.

Projekt se zaměřil na kryptografii, SSL protokol a certifikační autority, které používají hashovací funkci MD5. Při přístupu na zabezpečené stránky (HTTPS), například internetového bankovnictví, vznikne zabezpečené spojení mezi uživatelem a serverem banky, kdy ověření pravosti banky, je realizováno pomocí certifikátu. Tyto certifikáty používají hash kódy, jejichž součástí je otisk informaci do kdy má daný certifikát platnost apod.

Tento projekt byl založen na tom, že certifikáty webových serverů se neověřují online u vydávající certifikační autority, ale pomocí kořenového certifikátu přeinstalovaného v počítači. Díky tomu se pomocí reverzního inženýrství analyzoval hash kód vygenerovaný algoritmem MD5 a z toho se dále vytvořil nový certifikát identický s původním.

Konkrétně se útočilo na certifikát RapidSSL od firmy VeriSign. „Superpočítač“ složený z 200 herních konzol PlayStation 3, který porovnával tisíce různých certifikátů od této CA a hledal rozdíly v dynamice změny znaků v hash kódu apod. Funkce MD5 byla v průběhu tohoto experimentu, zpracována více než 2^{51} krát a výpočet trval několik desítek hodin.

Konkrétní popis zneužití takto vytvořeného falešného certifikátu je zobrazen na obrázku (Obr. 16).



Obr. 16. Princip zneužití falešného certifikátu [5]

1a – Útočníkovy je vydán legitimní certifikát od CA (modrý),

1b – vytvoří se podvržený certifikát CA, který nese stejný podpis jako webový certifikát, a proto vypadá jako originál vydaný CA.

2 – Certifikát webových stránek nesoucí originální identitu, ale jiný veřejný klíč je vytvořen a podepsán podvrženou CA (rouge CA). Dále je vytvořena kopie originálních webových stránek, které se umístí na jiný server s falešným webovým certifikátem.

3 – Jakmile chce uživatel navštívit zabezpečenou stránku je nasměrován na podvodné stránky (DNS útok, sociální inženýrství…). Tyto stránky se ovšem prezentují falešným certifikátem (červený) spolu s podvrženým certifikátem CA (černý). Tyto se začnou „stromově“ ověřovat až k certifikátu uloženému v prohlížeči, který tyto stránky ověří za pravé, právě díky okopírování původního certifikátu (modrý).

Firma VeriSign po oznámení o vytvoření falešného certifikátu přešla z algoritmu MD5 na SHA-1, který nebyl doposud prolomen, ale obsahuje podobný typ nedostatků jako MD5 a jeho prolomení je jen otázkou času. [42]

Ovšem jak Robert Graham na svém blogu ERRATA SECURITY uvádí, ne všechny certifikáty MD5 jsou tímto způsobem zranitelné. „*Ty z nich, které využívají přiřazení náhodného sériového čísla certifikátu, jsou proti tomuto útoku odolné. Tento útok funguje pouze tehdy, když je obsah, který bude hashován předvídatelný. Nicméně certifikáty obsahují dvě pole, která jsou vybrány CA. Jedno je „sériové číslo“ a druhé je „období platnosti“ certifikátu.*“ [43]

Při tomto útoku bylo útočeno právě na RapidSSL, protože při každém vydaném certifikátu inkrementoval sériové číslo právě o hodnotu jedna. Tímto, spolu se znalostí data platnosti certifikátu, mohli „útočníci“ vyrobit padělaný certifikát.

4.1.4 Autentizace uživatele a autorizace transakcí

Uživatel, který se přihlašuje přes PC k internetovému bankovnictví, musí být autentizován některým (v závislosti na konkrétní bance) z následujících systémů [10][14][38]:

- Uživatelské jméno a heslo.
- Certifikát (čipová karta, USB token).
- Autentizační kalkulátor PINu.
- Autorizační SMS kód.
- Autorizační SMS kód v šifrované pomocí SIM-TOOLKIT.
- Jednorázové transakční autorizační kódy - TAN kódy.
- Souřadnicová identifikace.
- Personalizovaný login.

Uživatelské jméno a heslo je základní metodou pro ověření identity klienta. Při použití této metody je nezbytné dodržovat požadavky na silné heslo, jako je minimální počet znaků, kombinace několika soustav znaků a tím minimalizovat možnost útoku hrubou silou nebo slovníkovými útoky, které lze dále omezit aplikací maximálního počtu nesprávných pokusů o přihlášení po kterých dojde k dočasné blokaci účtu. V dnešní době se tato metoda autentizace užívá jen pro neaktivní operace s účtem (prohlížení). V případě aktivních (tvorba příkazů) se kombinuje s dalšími metodami.

Certifikát vydávaný bankou klientovi má omezenou časovou platnost a slouží k ověření autentizační žádosti od klienta. Tento certifikát by měl být bezpečně uložen na externím

paměťovém zařízení jako flash disk, či CD. Certifikát lze uložit také bezpečně na následující zařízení:

- Čipová karta.
- Optická karta.
- USB token.

Tato zařízení jsou bezpečná, protože certifikát dané zařízení neopouští a to provádí požadované kryptografické operace s citlivými klíči samo.

V případě karet je k provedení bankovní operace potřeba speciální čtečka karet, která bývá připojena přes USB (možno také PCMCIA nebo ExpressCard u notebooků). U USB tokenu, který obsahuje bezpečně uložený podpisový certifikát je použití stejné jako u klasického USB flash disku.

Autentizační kalkulátor PINu je zařízení, které generuje jednorázový PIN. Podle způsobu generování je můžeme dále dělit:

- Vygenerování kódu za časovou periodu (30, 60,… sekund).
- Vygenerování kódu ihned po otevření.
- Vygenerování kódu po zadání přístupového PINu.
- Vygenerování kódu po zadání přístupového PINu a dalších dat o platbě.

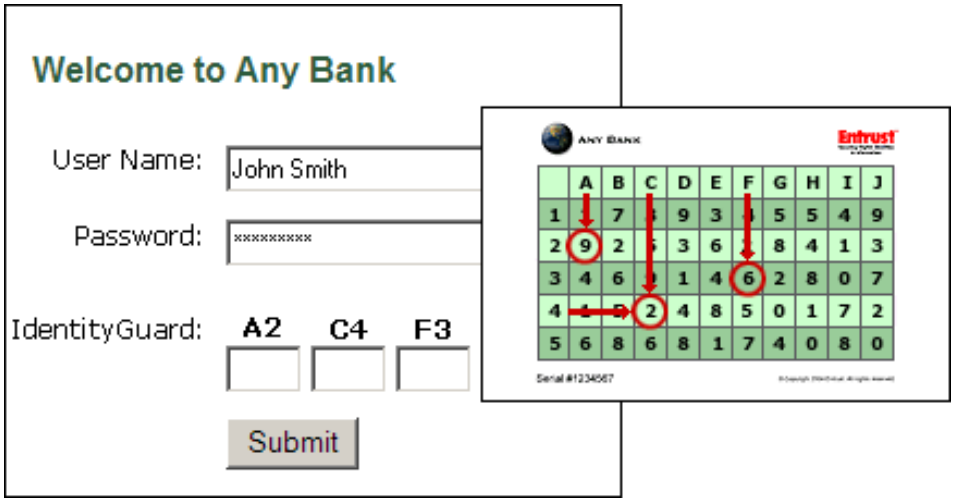
Autorizační SMS kód je zaslán na registrované číslo mobilního telefon. Tento kód je nutno přepsat do určeného pole v internetovém bankovnictví, čímž je transakce autorizována. Tento kód může být odeslán zašifrovaně. V GSM sítích se pro šifrování používá symetrický algoritmus A5 a jeho variace. Problém je, že data jsou zašifrovaná pouze mezi telefonem a základnovou stanicí z čehož vyplývá, že operátor má přístup k nezašifrovaným datům. Navíc není šifrování v rámci sítě povinné, a proto je výhodnější využít jinou bezpečnou metodu.

Autorizační SMS kód v šifrované podobě pomocí SIM-TOOLKIT. Uživatel obdrží od banky na svůj mobilní telefon zašifrovanou autorizační SMS, kterou je nutné přepsat do určeného pole v internetovém bankovnictví. Pro přečtení šifrované SMS je nutné mít SIM kartu podporující SIM Toolkit. SIM karta vyžaduje zadání BPIN, což je PIN, který

obdržíte od banky. Pro pozdější změnu BPINu slouží BPUK. Šifrování probíhá sdíleným symetrickým klíčem mezi bankou a SIM kartou.

Jednorázové transakční autorizační kódy - TAN kódy – zákazníkovy je předán (na pobočce, poštou) seznam několika (např. 100) čísel, kterými později autorizuje odesílané transakce. Tato čísla jsou zpravidla 6-ti místná a každé lze použít právě jednou.

Souřadnicová autentizace je řešení poměrně bezpečné a málo nákladné. Uživatel obdrží kartičku s předtištěnou tabulkou obsahující čísla odpovídající konkrétním souřadnicím. Při přihlášení, či autorizaci transakce je požádán kromě jména a hesla o několik čísel z náhodně vybrané kombinace souřadnic v tabulce, jak je vidět na obrázku (Obr. 17). Tato kartička má určitou časovou platnost a poté je ji třeba vyměnit za novou.



Obr. 17. Ukázka souřadnicové autentizace [44]

Tato další vrstva autentizace je také odolná proti útokům jako je phishing, malware apod., protože i při úspěšném útoku odhalí útočník jen malou část znaků autentizační karty.

Tento princip je analogií na jednodušší metodu sekundárního hesla, kde se využívá zadání několika znaků z náhodně vybraných pozic při autentizaci, či autorizaci.

Personalizovaný Login slouží jako ochrana před útoky typu phishing jako jsou podvržené přihlašovací formuláře. Ochrana spočívá v tom, že při procesu přihlašování se na stránkách zobrazí obrázek, či text, který si uživatel dříve zvolil, čímž pozná, že se nejedná o podvrženou stránku a může zadat své heslo. Toto opatření je ovšem účinné pouze v případě, že je spojení chráněno pomocí SSL (HTTPS). Jestliže není, může útočník

pomoci MITM útoku přesměrovávat data z autentických stránek a tím i obrázky a text z personalizovaného loginu.

4.1.5 Bezpečnost přístupového počítače

Přístupové PC by mělo být bezpečné, a proto je v první řadě důležité nepřihlašovat se do důležitých aplikací z internetových kaváren, či cizích PC, kde si nejsme jistí, jaké programy může obsahovat. Na svém PC bychom měli zajistit ochranu proti malware, což je souhrnný název pro škodlivé počítačové programy typu [45]:

- Viry.
- Trojské koně.
- Spyware.
- Advare.

Že se jedná o reálné nebezpečí, dokládá i útok z roku 2006, kdy trojský kůň sloužil ke krádeži desítky přístupových certifikátů a hesel k elektronickému bankovnictví a následné krádeži peněz z těchto účtů. Z roku 2008 zase pochází útok trojského koně „Sinowal“, který zobrazoval podvržené stránky internetového bankovnictví České spořitelny.

„Sinowal tiše číhal na uživatelově počítači, dokud se uživatel nechtěl připojit k serveru karetní společnosti nebo do on-line bankovnictví. Potom uživatele přesměroval na podvodně vytvořenou stránku, zaznamenal údaje zadávané do formulářů a odeslal je na server podvodníků. Rozšíření podvodného programu je celosvětové, ovšem s výjimkou Ruska. RSA z toho vyvozuje, že právě odtud zřejmě podvodníci pochází. (Což má být údajně běžná metoda, jak se vyhnout postihu místními orgány; navíc v případě mezinárodních urgencí policie údajně postupuje liknavěji, pokud podvodníci nejsou aktivní i přímo v dané zemi.)“ [46]

Druhy rizik pro internetové bankovnictví a doporučená obrana

Každý uživatel může používat jiný operační systém pro PC, ke kterému se vztahují jiná specifika. My se budeme zabývat nejrozšířenějším systémem Windows.

„Operační systém Windows se historickým vývojem dostal do situace, kdy většina domácích uživatelů pracuje s právy privilegovaného účtu. Toto vede k tomu, že případný škodlivý kód má po spuštění v moci celý počítač, pak může instalovat ovladače na nejnižší

úrovni, obcházet bezpečnostní mechanismy operačního systému apod. Na takto kompromitovaném počítači je možno zcela transparentně vést útok tzv. man-in-the-middle, tedy modifikace komunikačního kanálu mezi bankou a klientem na všech myslitelných úrovních.“ [39]

Jestli-že se tyto škodlivé programy dostanou do PC, mohou způsobit velkou škodu. Jako relevantní hrozby pro internetové bankovnictví uveďme například:

- Odposlech citlivých údajů.
- Útoky typu MIDM.
- Manipulace s DNS.
- Zkopírování uloženého certifikátu.

Proti těmto hrozbám je vhodné se chránit podle následujících bodů:

- Používat počítač, nad kterým máte plnou kontrolu jen vy a můžete ovlivnit bezpečnostní nastavení.
- Používat aktualizovaný operační systém.
- Používat vždy aktualizovaný antivirový software od renomovaných firem.
- Používat firewall.
- Používat aktualizovaný internetový prohlížeč.
- Věnovat pozornost bezpečnostním upozorněním systému.
- Hesla zadávat přes virtuální klávesnice.
- Navštěvovat pouze známé a důvěryhodné stránky internetu.
- Nestahovat neznámý software z internetu.
- Neklikat na reklamní banery slibující výhry, tapety, či cokoli zdarma.
- Nenavštěvovat stránky s erotickým obsahem.
- Neotvírat e-mailové zprávy od neznámých adresátů nebo zprávy s podezřelým názvem či obsahem.
- Nikdy nereagovat na e-mail, který po vás požaduje sdělení vašich osobních údajů, hesla, nebo PINu.
- Vždy kontrolovat správnost adresy zadaných stránek banky a připojení přes SSL (HTTPS).
- Nezapisovat PINy do souborů uložených v PC.
- Aktivovat ochranu heslem při přihlášení do systému.

4.1.6 Ostatní bezpečnostní opatření

Mezi ostatní bezpečnostní opatření můžeme zařadit postupy, které nemají přímý vliv na jednotlivé prvky systémů, ale doplňují bezpečnost u internetového bankovnictví jako celek. Patří sem zejména:

- Peněžní limit pro transakce.
- Časový limit pro odhlášení z internetového bankovnictví.
- Časový limit autorizačního kódu v SMS.
- Upozornění o provedené transakci na účtu klienta pomocí SMS.
- Zákaz uložení hesla pro internetové bankovnictví v prohlížeči.
- Virtuální klávesnice zabraňující odposlechu.

4.2 Telefonické bankovnictví a jeho bezpečnost

Telefonické bankovnictví je služba, která pro spojení s bankou a ovládáním účtu klienta využívá klasické telefonní linky, nebo mobilní telefony. Po zavolání na speciální číslo určené bankou pro telefonické bankovnictví komunikuje klient buď s živým operátorem nebo s automatem IVR (Interactive Voice Response). S kým bude klient komunikovat, záleží na jeho požadovaných akcích. Jsou-li pasivní (zůstatek na účtu), komunikuje obvykle s IVR a pro aktivní operace (zadávání příkazu k úhradě) komunikuje obvykle s živým operátorem. [10]

4.2.1 Autentizace uživatele

Před vstupem do systému telefonického bankovnictví musí být ověřena klientova identita. Toto se realizuje několika způsoby:

- Uživatelské jméno + heslo.
- Uživatelské jméno + jednorázové heslo.
- Selektivní ověření identifikačních údajů uživatele.

Při hovoru může poměrně jednoduše dojít k odposlechnutí přihlašovacích údajů, a proto je vhodné používat jednorázová hesla, či ověření náhodně vybraných identifikačních údajů uživatele.

4.3 GSM bankovnictví a jeho bezpečnost

Základními prvky GSM bankovnictví je SIM karta s bankovními funkcemi – SIM toolkit a mobilní telefon s její podporou. Na této SIM kartě je uložena bankovní aplikace, která zprostředkovává komunikaci mezi bankou a klientem. [47]

4.3.1 Autentizace uživatele

Přístup do aplikace je chráněn bankovním PINem – BPIN. Komunikace je šifrovaná klíčem, který se nachází v chráněné oblasti SIM karty. Každý účet může být ovládán právě jedním telefonem s GSM bankovnictvím, což zvyšuje bezpečnost aplikace.

4.4 WAP bankovnictví a jeho bezpečnost

Pro využívaní WAP bankovnictví, musí mobilní telefon podporovat technologii WAP a mít aktivovány datové přenosy. Pro přístup do bankovnictví se uživatel připojí na stránky příslušné banky přes WAPovou bránu. Tato brána zabezpečuje komunikaci mezi GSM a internetem.

Zabezpečení spojení je realizováno technologií WTLS, která je odvozena od SSL s ohledem na nízkou šířku přenosového pásma u mobilních zařízení. [48]

4.4.1 Bezpečnostní protokol WTLS

Hlavní rozdíly mezi SSL a WTLS jsou následující [49]:

- **Komprimovaná struktura dat**, která je zajištěna pomocí: redukování velikosti paketů, odstraňování redundancí, zkracování kryptografických prvků.
- **Nový certifikační formát**, který v zásadě dodržuje kryptografický standard X. 509 pro PKI, ale používá menší datové struktury.
- **Paketově orientovaná konstrukce**, která na rozdíl od konstrukce SSL navržené pro datový proud, je vhodná pro paketově založenou síť.

5 ELEKTRONICKÉ PENĚŽENKY

5.1 Popis

Elektronická peněženka (EP) je určena k bezpečným platbám obvykle menších částek nejčastěji na internetu. Funkce je podobná jako bankovní účet, ale platby probíhají online, čímž jsou rychlejší. Platby pomocí EP jsou také levnější a to proto, že se většinou nevyužívá infrastruktury bank.

Peněžní prostředky jsou u elektronických peněženek buď složeny přímo u provozovatele systému, nebo jsou v případě složitějších systému alokovány z bankovního účtu zákazníka.

Pro EP v české republice byl přelomový rok 2002, kdy začal platit zákon č. 124/2002 Sb. [50], který stanovil, že platební systémy včetně EP můžou provozovat jen subjekty s bankovní licencí. Tímto se zvýšila kvalita, ale také zaniklo mnoho projektů. [51]

5.2 Bezpečnost

Hlavní výhodou v oblasti bezpečnosti je to, že platby se realizují přes prostředníka, kterým je v tomto případě poskytovatel dané EP. I při nedovolené manipulace útočníka s účtem napadeného není obvykle možné vyčerpat více prostředků, než kolik je na kartě, či účtu uloženo a pachatel navíc nezíská citlivé údaje o postiženém.

Pro bezpečnou komunikaci, autentizaci a autorizaci transakcí se používají obdobné technologie jako u elektronického bankovnictví. Podrobně si bezpečnost u jednotlivých zástupců rozebereme v praktické části.

EP lze platit skrze platební bránu na kterou Vás přesměrují přímo stránky prodejce. Účet EP můžete ovládat také přes webové rozhraní a například u PayPal i pomocí SMS zpráv. PayPal je také jeden z mála systémů, který se napojuje přímo na kartu (účet s ní spojený) zákazníka a přesune požadovanou částku přímo z bankovního účtu. [52]

5.3 Rozdělení

5.3.1 Předplacená karta

Platební karta elektronické peněženky je debetní kartou. Obvykle je realizovaná jako čipová karta. Tyto karty bývají provozovány zpravidla v uzavřených systémech. Informace

o zůstatku na kartě jsou uchovávány v čipu, čímž je karta schopna provádět platby v offline režimu. Díky tomu je její provoz levný.

Platby mohou být autorizovány pomocí PINu, který čip ověří a transakci buď autorizuje, či zamítne.

Systém může podporovat i platby bez autorizace pinem pro zařízení, které toto nepodporují. To mohou být např. automaty, turnikety atd. Obvykle bývá pro tyto platby určený limit.

Při krádeži karty může být u jednoduchých systémů zůstatek karty odčerpán (neautorizovanou platbou) nebo, v případě transakčních systémů, zrekonstruován a převeden na novou kartu. Z tohoto důvodů musí být systém kryptograficky chráněn proti neautorizované modifikaci. [10]

5.3.2 Bankovní elektronická peněženka

Jedná se o debetní elektronickou kartu svázanou s bankovním účtem. Je provozována na základě transakčního sytému, kde jsou všechny transakce evidovány. [10]

5.3.3 Internetová elektronická peněženka

Jedná se o typický příklad EP. Uživatel si založí účet u poskytovatele a následně si na něj převede peníze. Tímto účtem lze poté platit u podporovaných prodejců rychleji než klasickými metodami a bez rizika zneužití údajů z platebních karet. [53]

5.3.4 Bankovní platební tlačítko

Bankovní platební tlačítko (BPT) není typická EP, protože funkce je dostupná pouze zákazníkům dané banky. Nicméně jde o pohodlný způsob jak zaplatit za zboží pomoci přístupu do omezené formy internetového bankovnictví, kam dané tlačítko uživatele přesměruje a před-vyplní příkaz k úhradě.

V případě, že daný prodejce BPT dané banky podporuje, proběhne platba okamžitě.

Myslím si, že jejich bezpečnost, která do velké míry souvisí se zabezpečením internetového bankovnictví a jednoduchost použití pro zákazníka, bude mít za následek další rozšiřování podpory této platební metody.

6 TRENDY V ELEKTRONICKÝCH TRANSAKCÍCH A JEJICH BEZPEČNOST

6.1 Adaptivní autentizace

6.1.1 Popis

Jedná se o metodu více faktorové autentizace založenou na rizikové analýze. Pro přihlášení se využívá klasické přihlašovací jméno a heslo bez dalších požadavků na uživatele.

Systém dále vyhodnocuje rizikovost dané autentizace na základě několika faktorů a jejich kombinace. Tento systém používá již více než 200miliónů uživatelů. [54]

6.1.2 Faktory pro vyhodnocování rizikovosti autentizace

Hlavními faktory pro vyhodnocování jsou:

- IP adresa uživatele.
- Země, ze které probíhá přihlášení.
- MAC adresa uživatele.
- Čas přihlášení.
- Dřívější informace o přihlášení apod.

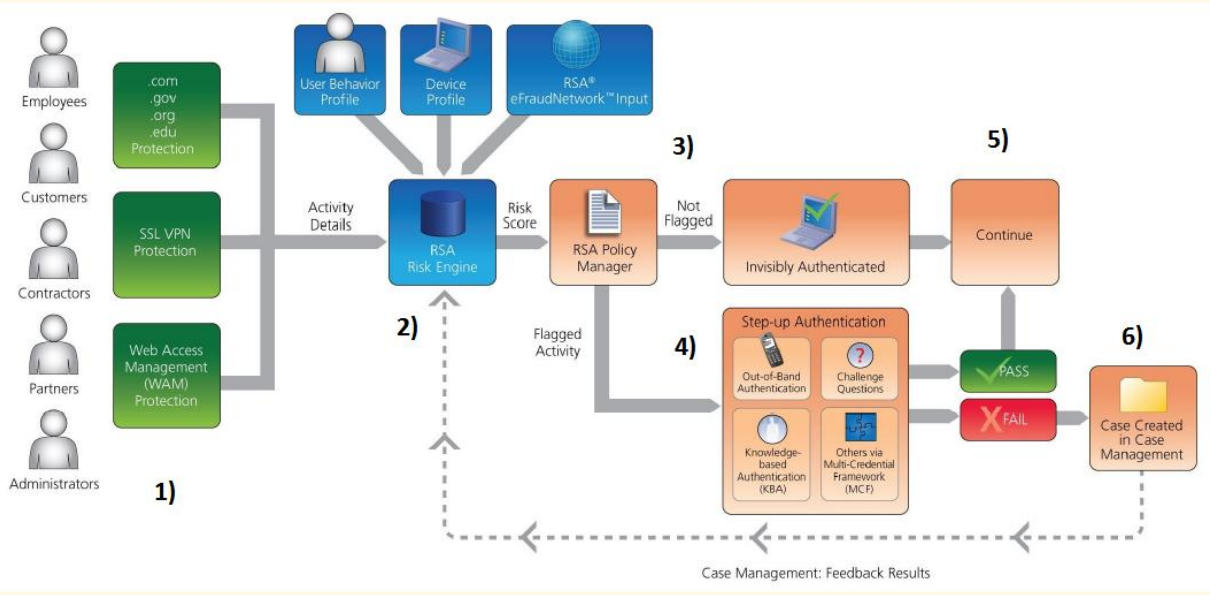
Jestliže jsou tyto faktory standardní, uživateli stačí pro přihlášení pouze již zmíněné jméno a heslo. V případě, že systém vyhodnotí autentizaci jako rizikovou, bude uživatel požádán o dodatečnou autentizaci nebo, v případě vysokého rizika, může systém omezit přístup k danému účtu.

6.1.3 Typy dodatečných způsobů autentizace

Dodatečné způsoby autentizace mohou být:

- Jednorázové hesla, SMS kód.
- Osobní otázky na uživatele.
- Hovor vedený operátorem s uživatelem.

Schéma typického autentizačního postupu s popisem je zobrazen na obrázku (Obr. 18).



Obr. 18. Schéma funkce adaptivní autentizace [54]

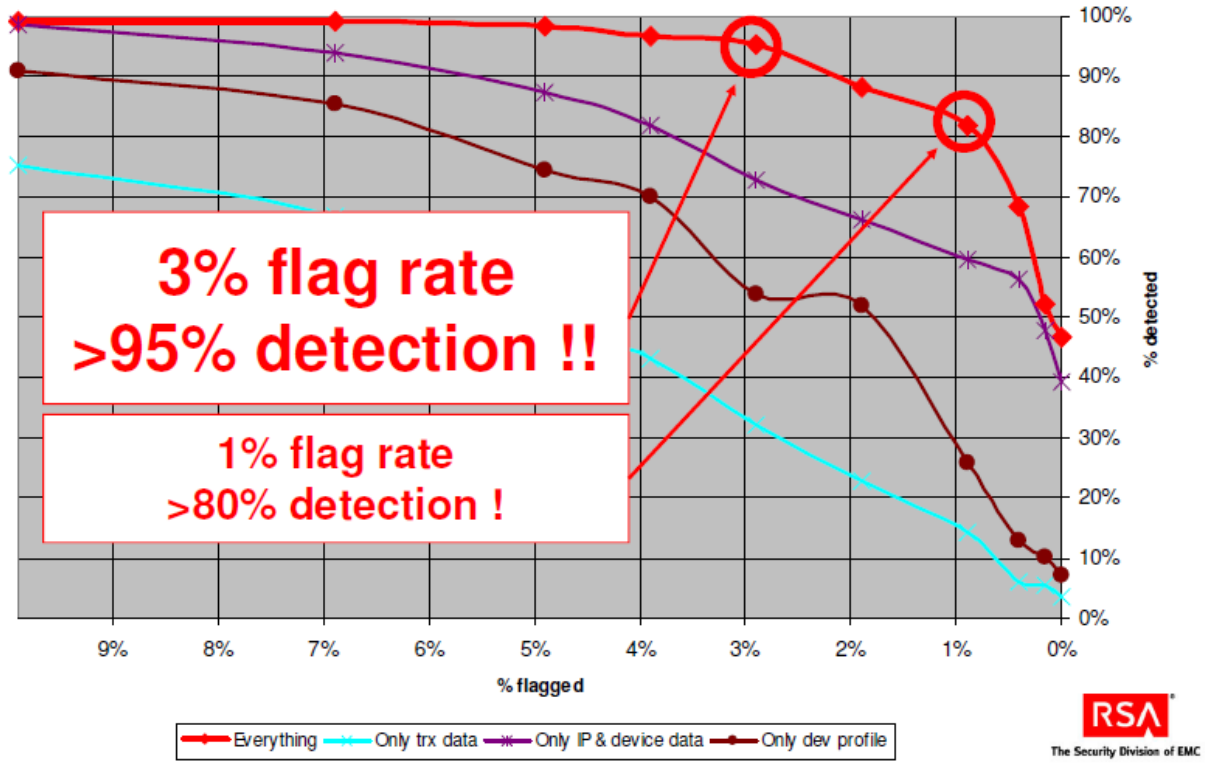
1) Uživatel přistupuje přes konkrétní aplikaci k systému svým jménem a heslem.
2) Iniciuje se rozhodovací centrum, které obsahuje informace o uživatelských profilech.
3) Systém vyhodnotí přihlášení jako standardní a uživatel je autentizován.
4) Systém označí přihlášení jako rizikové a přistoupí k další úrovní autentizace.
5) Po úspěšné autentizaci může uživatel pracovat dále se systémem.
6) Při neúspěšné autentizaci jsou data zaznamenána a zaslána zpět rozhodovacímu centru pro rozšíření databáze profilů.

6.1.4 Výhody adaptivní autentizace

Nyní si uvedeme několik výhod adaptivní autentizace oproti klasickým způsobům autentizace:

- Nevyžaduje zkušenosti od uživatele.
- Není potřeba řešit distribuci HW, SW.
- Nemusíme se zabývat managementem životního cyklu (tokeny, certifikáty).
- Není náchylná na online útoky.
- Snadná integrace s protokoly SSL apod.

Na závěr je třeba říci, že úspěšnost systému, je přímo úměrná „přísnosti“, s jakou posuzuje jednotlivé pokusy o přístup. S 3% „označených“ přihlášení (které systém považuje za rizikové), systém detekoval 95% ze všech neoprávněných pokusů o přihlášení. Dokonce i s 1% „označených“ přihlášení (což znamená, že systém byl méně „přísný“ a označil za rizikové pouze 1% přihlašovacích pokusů) byl systém stále schopný detekovat 80% ze všech neoprávněných pokusů o přihlášení. Míru „přísnosti“ je nutné určovat s ohledem na typ systému a pohodlí uživatele. Graf detekce je zobrazen na obrázku (Obr. 19).



Obr. 19. Míra detekce adaptivní autentizace [54]

6.2 Super tokeny

Super tokeny reagují na riziko nedůvěryhodného prostředí, ve kterém může být token používán. Při práci s tokenem a na něm uloženými daty musí uživatel zadat přístupový PIN, který může být útočníkem „odposlechnut“, například pomocí programů typu keylogger, které zaznamenávají data zadaná přes klávesnici. [10]

Jedním z řešení je implementace biometrické vrstvy ochrany v podobě například čtečky otisků prstů na daný token, pomocí kterého probíhá autentizace uživatele. Tímto se minimalizuje riziko zneužití i v případě ztráty tokenu.

Obr. 20. Token s čtečkou otisků prstů [55]

6.3 Super čipové karty

Na Veletrhu platebních a identifikačních karet Cartes v Paříži v prosinci 2010, byly prezentovány karty s rozšířenou bezpečností. Jde o následující karty [56]:

- Embosovaná karta s displejem.
- Elektronická karta s displejem a klávesnicí.

6.3.1 Platební karta s displejem

Zvyšuje úroveň bezpečnosti, protože může generovat jednorázové autentizační kódy, které můžou sloužit buď pro přístup do internetového bankovnictví, nebo potvrzovat platby na internetu. Při podpoře této technologie všemi účastníky transakce, nehrozí její zneužití bez fyzické přítomnosti, jako u klasických karet.

Nevýhodou je, že při ztrátě či krádeži karty, má útočník stejné možnosti jako majitel a může se pokusit přihlásit do Internetového bankovnictví (je-li takto nastaveno). Tyto karty můžou nahradit některé autentizační tokeny.

6.3.2 Karta s displejem a klávesnicí

Tato karta je ještě bezpečnější, protože před vygenerováním autentizačního kódu musíte zadat PIN.

Obr. 21. Super čipové karty s displejem a klávesnicí [56]

Při kombinaci těchto karet s bezdotykovou technologií vzniká konkurence pro NFC technologii (popsaná dále), protože karty budou umožňovat jak rychlou platbu nízkých částek, tak bezpečné zadávání PINu do karty při větších částkách. Toto by v současných podmínkách bylo špatně realizovatelné z důvodu nedůvěryhodnosti terminálů, do kterých by se měl zadávat PIN externě (automat na kávu, cigarety).

Zamezit dalšímu rozvoji může vysoká výrobní cena právě těchto karet, kterou by nesla banka, potažmo zákazník.

6.4 Bezkontaktní čipové karty a jejich bezpečnost

Bezkontaktní platby jsou umožňovány pomocí platebních karet, či tokenů, které využívají princů RFID technologii pro přenos dat. Vestavěný čip a anténa, umožňuje zákazníkovy zaplatit pouhým přiblížením ke kompatibilnímu platebnímu terminálu na několik centimetrů.

Existují dvě základní dělení používaných systému a jejich karet a to [57]:

- Bankovní bezkontaktní karty (kompatibilní se standardem EMV).
- Ostatní bezkontaktní karty.

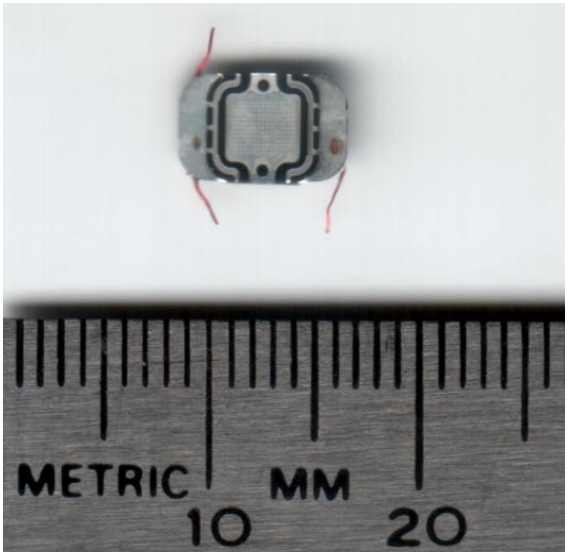
6.4.1 Bankovní bezkontaktní karty

Tato technologie využívá pro přenos technologii indukce a rádiových vln podobně jako RFID zařízení, ale tyto karty obsahují také mikroprocesor a paměť pro provádění kryptografických operací pro zvýšení bezpečnosti. Mají programovatelné funkce a musí komunikovat na mnohem menší vzdálenosti než zařízení RFID. [58]

Na obrázku (Obr. 22) je zobrazen znak pro bezkontaktní platby.

Obr. 22. Znak pro bezkontaktní platby [59]

Karty jsou vydávány bankami a jsou kompatibilní se standardem EMV. V ČR budou první karty Visa s touto technologií vydány Českou spořitelnou na podzim tohoto roku (2011). [58]



Obr. 23. RFID čip technologie PayPass od MasterCard [60]

Protože transakce nejsou ověřovány PINem ani podpisem, jsou platby omezeny pouze do určité výše. Typické limity jsou [58]:

- USA – 25USD,
- UK – 15GBP,
- EU – 20EUR.

Dále je po určitém počtu bezkontaktních plateb v řadě, požadován PIN, pro ověření držitele karty.

Nejrozšířenější projekty jsou [60]:

- Visa PayWave,
- MasterCard PayPass.

Obr. 24. Platba bezkontaktní kartou PayWave [61]

Tyto systémy dvou největších karetních organizací jsou vzájemně kompatibilní.

Tento typ systému umožňuje offline transakce, které jsou založené na limitu uloženém v aplikaci na daném zařízení (karta, token).

První bankovní bezkontaktní karty byly v UK vydány v roce 2008. V červnu 2010 bylo v oběhu necelých 10 miliónů karet, umožňující bezkontaktní platbu. Toto reprezentuje asi 7% všech karet v UK. Celosvětově je vydáno přes 320 milionů bezkontaktních bankovních karet.

Některé výzkumy ukazují, že zákazníci mají tendenci utrácet více, díky snadnosti provedení transakce. Data z MasterCard v Kanadě ukazují, že zákazníci vybaveni bezkontaktními platebními kartami utrácí asi o 25% více, než zákazníci s klasickými kartami. [60]

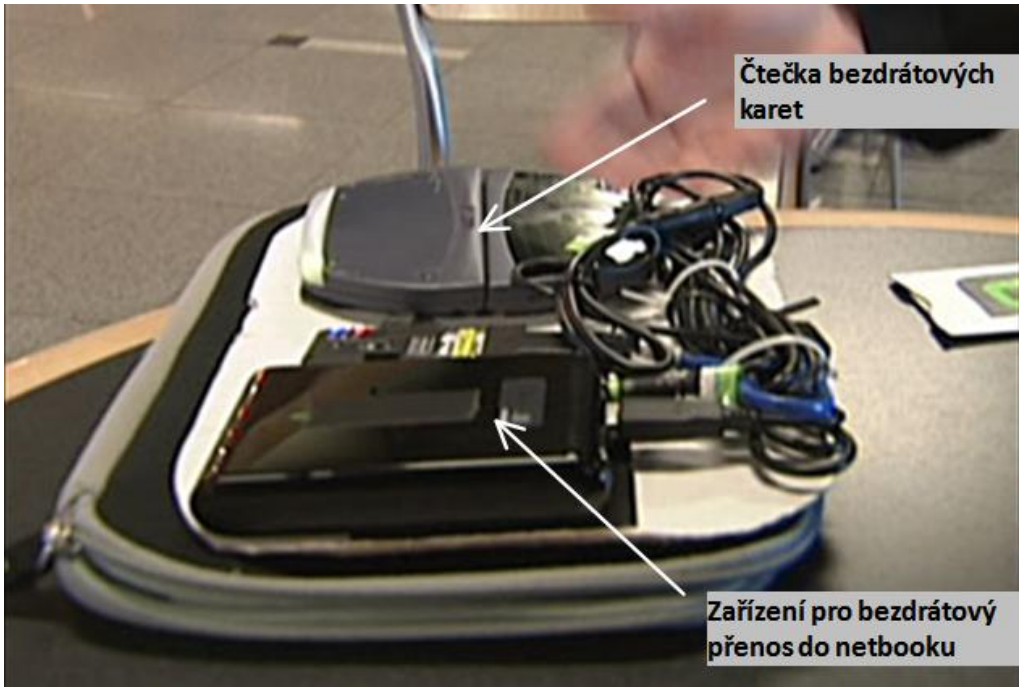
Bezpečnost

Bezpečnostní opatření se liší podle implementace každého vydavatele těchto karet, ale obecně se dají shrnout následovně [57]:

- ***Šifrování transakce přenosu*** – každá karta má zabudovaný tajný klíč, kterým se pomocí šifrovacích algoritmů generují unikátní ověřovací číslo karty, neboli Unique Card Verification Value (UCVV), které exkluzivně identifikuje každou transakci. Žádné dvě karty neobsahují stejný klíč a klíč se také nikdy nepřenáší.
- ***Autentizace*** – Vydavatel karty ověřuje, zda má transakce platné číslo UCVV před autorizací transakce. Díky tomuto má vydavatel možnost odhalit pokus o použití kódu transakce více než jednou.
- ***Anonymita*** – bezkontaktní transakce nevyžaduje díky UCVV používání osobních údajů při platbě.
- ***Kontrola*** – uživatel má plnou kontrolu nad kartou při platbě, čímž je zamezeno zkopírování údajů z karty.
- ***Bezkontaktní terminály*** – u bezkontaktního terminálu je situace stejná jako u běžných terminálů a uživatel musí více méně spoléhat na důvěryhodnost obchodníka.

Prolomení bezpečností bezkontaktních karet

Navzdory výše uvedenému byla v prosinci 2010 v USA vysílána reportáž o krádeži identit z bezdotykových karet [62]. V této reportáži Walt Augustinowicz ze společnosti Identity Stronghold, která se zabývá výrobou elektromagneticky odolných krytů karet, načítá data z karet náhodných kolemjdoucích. Využívá k tomu čtečku bezdrátových karet a notebook se softwarem. Vybavení je zobrazeno na obrázku (Obr. 25).



Obr. 25. Vybavení pro kopírování dat z bezdotykových karet [63]

Pomoci tohoto zařízení se po přiblížení ke kartě oběti načtou tyto údaje:

- Typ karty.
- Číslo karty.
- Exspiraci karty.

Tyto údaje mohou být například zneužity v online obchodech, které nevyžadují kontrolní číslo karty. Tedy hlavně v USA, Asii.

Tento útok ukazuje, že ne všechny instituce používají šifrovaného přenosu z karty do terminálu.

Více k tématu je možné nalez na internetu pod heslem „ Electronic Pickpocketing“.

Ochranou ze strany bank je zavádění šifrovaného přenosu. Banky navíc refundují všechny škody vzniklé zneužitím bezkontaktních karet. Zákazník se i přes to může chránit krytem karty, který zabraňuje průchodu elektromagnetického záření.

6.4.2 Ostatní bezkontaktní čipové karty

Dalším typem bezkontaktních karet jsou nebankovní karty. Nejrozšířenějším standardem karet v US a EU jsou karty MIFARE od firmy Philips. Tyto karty se používají zejména při platbách v hromadné dopravě, nebo řízení fyzického přístupu do objektů.[64] [65]

Technologie karet

Jedná se o kartu s integrovaným obvodem, který může zpracovávat a ukládat data. Tato karta komunikuje s platebním terminálem přes radiové vlny.

Komunikace využívá frekvenci 13,56 MHz a je definována čtyřdílným standardem ISO/IEC 14443. Pro komunikaci karty s terminálem se používá indukční technologie RFID, takže nepotřebuje vlastní napájení.

Karty jsou aktivovány, jen když jsou v elektromagnetickém poli kompatibilním s ISO14443A. Rychlost přenosu je mezi 106 – 848 Kbit/s. Tyto karty jsou pro snadnost použití velmi často užívány pro placení v hromadné dopravě. Masově jsou nasazeny například v:

- Taiwan – EasyCard – MIFARE technologie,
- Hong Kong – Octopus card,
- Japonské dráhy – Suica Card,
- Londýn – Oyster card – MIFARE technologie,
- České dráhy – In-karta – MIFARE technologie.

Bezpečnost bezkontaktních karet MIFARE

Čipy MIFARE jsou vyráběny v několika variantách v závislosti na jejich vlastnostech. [65]

Nejnižší varianty čipů (MIFARE Ultralight, MIFARE Classic) používají pouze proprietární protokol a šifrování. Na transportní vrstvě využívají také proprietárního řešení Mifare.

Vyšší varianty čipů mají HW podporu šifrování v podobě DES a 3DES (MIFARE Ultralight C) či algoritmus AES s délkou klíče 128bitů. Pro transportní vrstvu je integrována podpora standardizovaného transportního protokolu dle ISO-14443-4. Nejvyšší varianty podporují strukturu PKI či podporují otevřené operační systémy jako je Java Card OpenPlatform.

Funkce proprietárního algoritmu Mifare u karet Standard byla zjištěna a prolomena. Tyto karty se již nevyrábějí, ale stále se používají. Útok provedli vědci z Institute for Computing and Information Sciences z Radboud University v Holandsku v roce 2008 [67].

Vědci za pomoci mikroskopu pořídili snímky jednotlivých vrstev čipu a pomoci speciálního software odhalili proprietární algoritmus Mifare. Dále byla analyzována komunikace mezi kartou a terminálem a popsány šifrovací a autentizační postupy tohoto algoritmu.

Prolomení bezpečnosti karet Oyster card pro dopravu v Londýně

V roce 2008 byla prolomena bezpečnost systému Oyster card, který je založený na bezkontaktních kartách MIFARE Classic. Tento systém slouží pro dopravu v Londýně.

Útočníci skenovali terminál pro příjem bezkontaktních karet, aby získali jeho šifrovací klíč. Poté využili bezdrátovou anténu připojenou k počítači. V londýnském metru anténu aktivovali a postižené karty odesílaly zpět své záznamy. S těmito záznamy mohli útočníci karty naklonovat.

Tento útok byl aplikován na základě prolomení proprietálního šifrování popsaného výše. Toto zabezpečení bylo principielně slabé a hlavní bezpečnost zajišťovalo utajení jeho funkce. Za toto byla firma později kritizována [68].

České dráhy – In-karta

Tato bezkontaktní čipová karta funguje na standardu MIFARE DESFire. Umožňuje číst a zapisovat data. Lze ji využít jako elektronickou jízdenku, elektronickou peněženku, na evidenci docházky apod. [66]

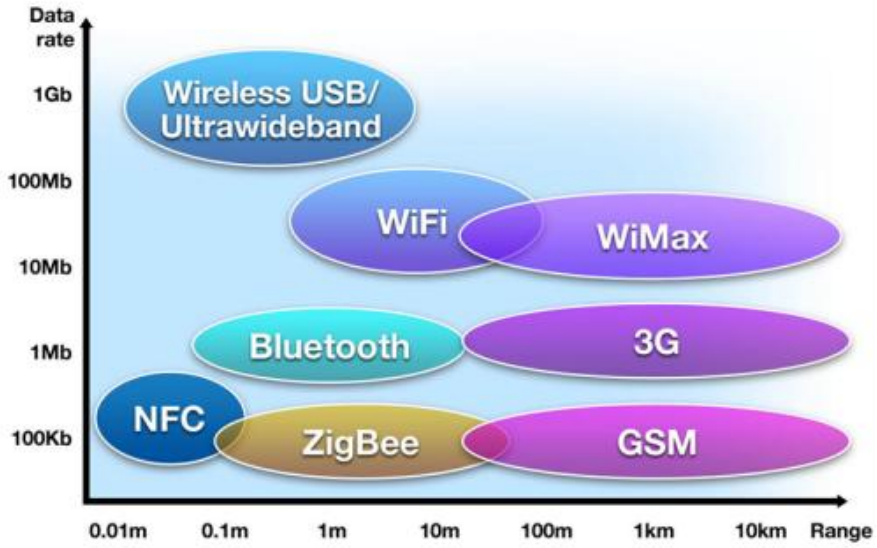
Používané řešení DESFire je kompatibilní s normou ISO/IEC 14443A-4. Toto řešení je oproti kartě Classic (na které jsem popisoval prolomení bezpečnosti) lépe zabezpečené. Karta již z výroby obsahuje svůj operační systém, který poskytuje jednoduchou adresářovou strukturu se soubory.

Karty existují ve dvou variantách. Starší se šifrováním 3DES a 4Kbyte paměti a novější se šifrováním AES, které obsahují kryptografický akcelerátor. Nové karty mají certifikovaný HW a SW na úrovni Common Criteria EAL 4+ ze stupnice 1 – 7. [65]

6.5 Využití NFC technologie pro rychle platby

6.5.1 Popis

Technologie Near Field Communication (NFC) je určena pro komunikaci mezi elektronickými zařízeními na krátkou vzdálenost cca do 20cm. Jedná se o rozšíření standardu ISO/IEC 14443, který definuje komunikaci pro bezkontaktní čipové karty RFID. NFC tedy pracuje na frekvenci 13,56 MHz. Zařazení NFC z pohledu rychlosti přenosu a dosahu je zobrazeno na obrázku (Obr. 26). [69]



Obr. 26. Srovnání technologie NFC z pohledu přenosové rychlosti a dosahu [69]

Výhodou NFC je její kompatibilita s infrastrukturou bezdotykových karet. NFC rozšiřuje možností RFID pomocí sdílení informací mezi zařízeními. Přenosová rychlost 424 kbit/s je oproti 2,1 Mbit/s u Bluetooth V2.1 sice nízká, ale inicializace přenosu trvá méně než 0,1 sekundy na rozdíl od 6 sekund potřebných u zmíněného Bluetooth. NFC není schopný zároveň přijímat a vysílat signál. Porovnání dalších parametrů je zobrazeno v (Tab. 6). [70]

Tab. 6. Porovnání NFC s Bluetooth

Technologie	**NFC**	**Bluetooth V2.1**	**Bluetooth V4.0 (nízká spotřeba)**
Kompatibilita s pasivním RFID	ano (ISO 18000-3)	ne (pouze aktivně)	ne (pouze aktivně)
Tvůrce standardu	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Standard	ISO 13157	IEEE 802.15.1	IEEE 802.15.1
Typ sítě	Point-to-point P2P	WPAN	WPAN
Kryptografie	ne s RFID	možná	možná
Dosah	< 0,2 m	~10 m (třída 2)	~1 m (třída 3)
Frekvence	13,56 MHz	2,4-2,5 GHz	2,4-2,5 GHz
Rychlost přenosu	424 kbit/s	2,1 Mbit/s	~200 kbit/s
Čas pro sestavení přenosu	< 0,1 s	< 6 s	< 1 s
Spotřeba energie	< 15 mA (čtení)	závislé na třídě	< 15 mA (střed)

Tato technologie je primárně určena pro použití v mobilních telefonech.

Možné využití NFC v telefonech [71]:

- Platby za dopravu.
- Platby prostřednictvím platební karty.
- Přístupové zařízení.
- Přihlašování k PC.
- Získávání informací z RFID informačních tokenů (nálepky na památkách).
- Sdílení informací mezi uživateli.

6.5.2 Výhody

- Integrace do mobilního telefonu přináší možnost vyžívat displej a klávesnici – různé aplikace.
- Integrace NFC do čipu SIM karty poskytne obdobné zabezpečení jako SIM Toolkit.
- Široká variace uplatnění.

6.5.3 Bezpečnostní rizika

Samotná technologie NFC neposkytuje žádné zabezpečení komunikace. Její bezpečnost je často prezentována nízkým dosahem přenosu a tím pádem fyzickému zamezení útoků.

Nicméně data můžou být kompromitována i na delší vzdálenosti pomocí výkonných antén. NFC je proto náchylná na odposlouchávání a modifikaci přenášených dat (MITM). Tímto způsobem se do telefonů může dostat škodlivý kód v podobě spyware, malware apod., čímž následně může nakazit další telefony, s kterými přijde do interakce.

Z tohoto vyplývá, že správně napsaný operační systém, který kontroluje tok informací mezi aplikacemi a aplikace antivirů v prostředí mobilních telefonů bude mít zásadní vliv na bezpečnost. [72]

Rizika se týkají několika úrovní [73]:

- Hardwarová bezpečnost s oporou ve standardech (ISO/IEC apod.).
- Kryptografické prostředky ze strany zařízení.
- Kvalitně napsaný kód operačních systém.
- Podpora bezpečnosti ze strany poskytovatelů infrastruktury.
- Informovanost uživatelů o možném zneužití a jejich proaktivní chování.

Rizika technologie NFC a možnosti zvýšení její bezpečnosti jsou podrobně rozebrané již v dokumentu z roku 2006 od Ernst Haselsteiner and Klemens Breitfuß [73].

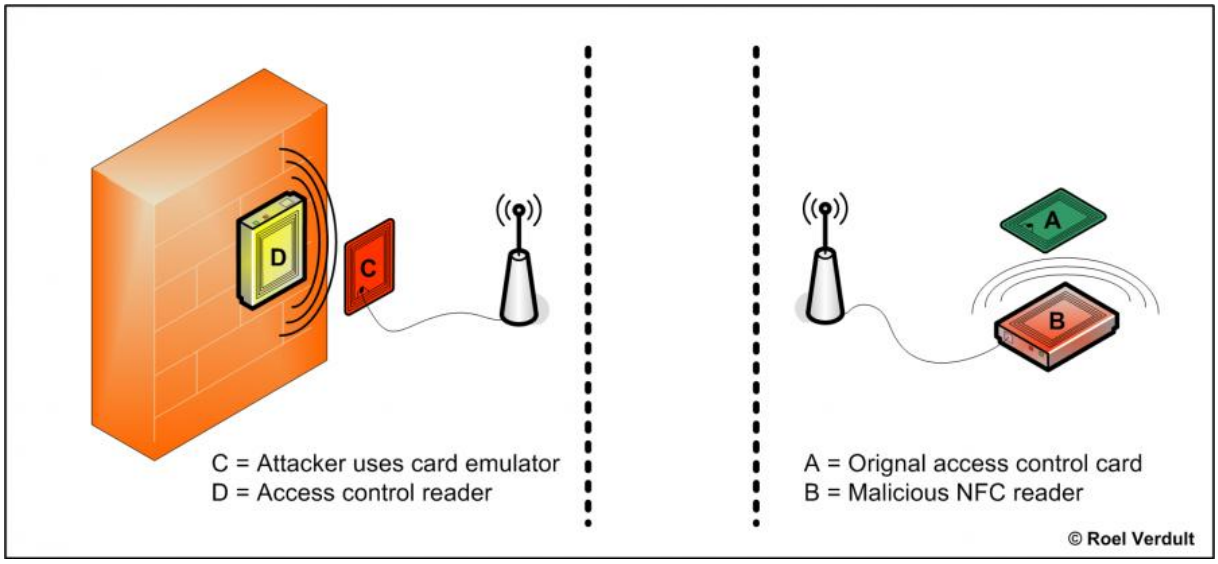
Bohužel tyto techniky nejsou zahrnuty ve standardech, a proto je technologie náchylná ke zneužití. [70]

Bezpečnostní opatření

Pro snížení rizik je možné aplikovat bezpečnostní opatření ze strany aplikací [72]:

- Používání protokolů typu SSL pro navázání bezpečného komunikačního kanálu.
- Aplikace kryptografických a autentizačních protokolů do mobilních telefonů.
- Zabezpečení telefonů pomocí přístupových hesel ze strany zákazníků.
- Používání antivirů.
- Zabezpečení systému ze strany poskytovatelů proti napadení škodlivým kódem.

Jsou také zdokumentované případy [74], přesměrování protokolu (podobně jako jsem popisoval u čipových karet), kdy útočník přikládá ke čtecímu zařízení svůj NFC emulátor a požadavek čtečky předává bezdrátově na jiný NFC čip, přes upravenou čtečku podvodníka. Princip je zobrazen na obrázku (Obr. 27). Principielně je toto možné použít i u plateb.



Obr. 27. Přesměrování protokolu NFC čipu [74]

6.5.4 Technologie NFC v České republice

Podle tiskové zprávy [88], je nevětším připravovaným testovacím projektem nasazení NFC plateb u nás projekt Telefoniky O2, KB a Citibank v supermarketech Globus v Praze a v Plzni, za podpory Visa Europe. Projekt zahrnuje 200 zákazníků vybavených NFC telefonem Samsung S5230 s přeinstalovanou aplikací O2 wallet. Projekt má být spuštěn v polovině roku 2011 a potrvá do konce roku.

6.5.5 Souhrn

Technologie NFC má velký potenciál, ale jako každá nová technologie musí projít úpravami, které jsou nezbytné pro zvýšení bezpečnosti. NFC má z uživatelského hlediska velké výhody oproti podobně fungujícím bezkontaktním kartám (i s displejem a klávesnicí) v podobě telefonu, který značně rozšiřuje její využití pomocí nejrůznějších aplikací.

Podle mého názoru by byla implementace čipů NFC do SIM karet ideálním řešením, jak z pohledu bezpečnosti, kde by mohla navázat na SIM Toolkit, tak z pohledu univerzálnosti a nezávislosti na mobilním telefonu (za předpokladu podpory softwaru).

II. PRAKTICKÁ ČÁST

7 ROZBOR MOŽNOSTÍ ELEKTRONICKÝCH PENĚŽENEK A ANALÝZA JEJICH BEZPEČNOSTI

V praktické části popíšu technické možnosti vybraných zástupců elektronických peněženek (EP) a porovnám úroveň zabezpečení pro následující oblasti:

- Bezpečnost přenosu dat.
- Bezpečnost autentizace uživatele.
- Bezpečnost autorizace transakcí.

7.1 Analýza bankovních elektronických peněženek

7.1.1 MaxKarta

MaxKarta spadá mezi bankovní elektronické peněženky a v ČR ji jako jediná provozuje ČSOB.

Popis a vlastnosti

MaxKarta je v současnosti největším projektem tohoto typu ve střední a východní Evropě. V ČR je přes 8000 terminálů přijímajících MaxKartu.

Bezpečnost

MaxKarta obsahuje jak kontaktní čip, tak magnetický proužek Maestro, takže ji lze využívat jako klasickou platební kartu. S tímto jsou spojena obdobná rizika jako u klasických karet.

7.2 Analýza internetových elektronických peněženek

7.2.1 PayPal

Popis a vlastnosti

PayPal jako elektronická peněženka byl založen v roce 2000 v USA, ale značné expanze dosáhl v roce 2002, kdy jej koupila firma eBay (za cca 30 miliard Kč). PayPal je používán jako hlavní platební brána pro eBay i Skype. V roce 2008 koupila společnost eBay

izraelskou bezpečnostní firmu Fraud Sciences (za cca 3 miliardy Kč), aby dosáhla větší ochrany svých zákazníků před zneužitím jejich údajů a zvýšila zabezpečení jejich plateb. K tomuto rozhodnutí firmu vedl i útoku hackerů na eBay koncem roku 2007, kdy byly ukradeny osobní údaje několika tisíc zákazníků a následně zveřejněny na eBay fóru.

Dnes (I/2011) PayPal nabízí několik úrovní ochrany, ať už jde šifrování spojení, rozšířenou bezpečnost přihlašování, limity převodů, či program ochrany zákazníků.

PayPal je díky více než 100 milionům účtů a implementací v desítkách tisíc eshopech největším elektronickým platebním systémem na světě. [52]

PayPal má licenci na provoz v USA, ale aby mohl poskytovat služby i v Evropě má zřízenou pobočku v Lucembursku, kde je pod dohledem kontrolního finančního úřadu CSSF. [75]

Dobíjení PayPal účtu - propojení s platební kartou

PayPal umožňuje jak dobíjení peněženky z účtu jako většina poskytovatelů, tak možnost napojení platební karty na účet. Napojit lze jakoukoliv bankovní kartu s podporou elektronických plateb. Výhodou pro uživatele je komfort, protože nemusí sledovat zůstatky na účtu.

Účet na PayPal lze také přímo napojit na platební kartu (bankovní účet), takže poté není potřeba převádět peníze, ale platba se vždy odečete přímo z bankovního účtu.

Ověření karty probíhá tak, že po zadání údajů na stránce PayPal je následně stržena částka zhruba 50,-Kč z účtu spojeného s platební kartou. Po následném zadání čísla transakce, která je viditelná na výpisu z účtu je karta přiřazena k účtu PayPal. Zkušební částku je poté možno použít k platbě.

Toto komfortní řešení na první pohled představuje zvýšené nebezpečí odčerpání prostředků z bankovního účtu při zjištění přihlašovacích údajů. PayPal proto zvyšuje zabezpečení několika extra prvky jako autentizační kalkulátor pro přihlášení, software pro rozeznání phishingu, či limity pro neověřené uživatele PayPal. Tyto metody budou popsány dále.

Zhodnocení bezpečnosti

PayPal se podle společnosti Avira stal v roce 2009 nejčastějším cílem phishingu s počtem více než 32000 objevených útoků [76].

Bezpečnostní oddělení PayPal monitoruje probíhající transakce a podezřelé blokuje. Jestliže se například k účtu přihlásí uživatel z jiné země, než kde je účet registrován, je účet preventivně zablokován. Stejně tak větší finanční transakce můžou být zablokovány do podání dokladů o platbě nebo vysvětlení. Tento systém funguje na principu dříve popisované Adaptivní autentizace.

Paypal má několik úrovní blokace účtu od zákazu odesílání plateb až po zablokování prostředků na účtu. [77]

Tento postup funguje dobře jako prevence, ale blokace účtu klientů, která je ve velké části případů bezdůvodná snižuje komfort užívání služby.

Paypal také nedovoluje z důvodu ochrany před „praním špinavých peněz“ převádět peníze z PayPal účtu na bankovní účet vedený pod jiným jménem.

Maximální možná částka pro převod z Paypalu je nyní (I/2011) 240 000,-Kč.

Při změně adresy emailu je potřeba znovu vložit heslo a na původní email je odesláno upozornění, takže nehrozí změna v případě, že vlastník účtu zůstane přihlášen například v internetové kavárně.

Šifrování

Stránka je ověřena certifikační autoritou VeriSign, spojení je zabezpečeno 128 bitovým šifrováním a šifrovacím standardem 3DES_EDE_CBC. Toto zabezpečení je použito i při zadávání informací o platební kartě.

Rozšířená bezpečnost autentizace

PayPal nabízí pro zvýšení bezpečnosti produkt „PayPal Security Key“. Jedná se autentizační kalkulátor generující unikátní šesti-číselný kód každých 30 sekund. Tento kód se vkládá spolu s přihlašovacím jménem a heslem při přihlášení. Poté tento kód expiruje a nemůže být znovu využit.

PayPal Security Key je možné objednat přímo ze stránek PayPal za jednorázový poplatek $5.00 USD

V případě ztráty tohoto klíče se budete stále moci přihlásit do svého účtu, a to pomocí zadání rozšířených informací. Může to být číslo karty, bankovního účtu atp. V tomto případě budete také požádáni o vytvoření nového hesla k účtu.

Pro Českou republiku zatím není PayPal Security Key dostupný. [52]

Limity transakcí

Transakce odesílání a přijímání prostředků skrze PayPal jsou limitovány podle úrovně ověření účtu. Toto opatření má zabraňovat „praní špinavých peněz“ a zneužití osobních údajů. Existují tři možnosti:

- Unverified,
- Verified,
- Unlimited.

Unverified, neboli neověřený je účet, který získáte po registraci a nemusíte nijak prokazovat totožnost.

Verified, neboli ověřený je účet, který získáte po ověření, že učet (při dobíjení PayPal), nebo karta (při propojení platební karty s PayPal) patří opravdu Vám. Toto se ověřuje zadáním kódu transakce z výpisu k účtu na stránkách PayPal.

Unlimited, neboli bez omezení je učet dostupný až po rozšířené verifikaci, která je požadována v momentě, kdy obrat účtu přesáhne určitou hranici. U rozšířené verifikace jsou požadované naskenované doklady. Jeden s fotkou jako je občanský průkaz nebo pas a další s adresou jako je účet za kabelovou televizi apod.

Limity pro neověřený, ověřený a neomezený účet jsou zobrazeny v tabulce (Tab. 7) [52]

Tab. 7. Limity transakcí u PayPal účtu

Limity transakcí	Unverified (EUR)	Verified (EUR)	Unlimited (EUR)
odchozí / měsíc	-	-	-
odchozí / rok	500	-	-
příchozí / měsíc	100	-	-
příchozí / rok	1000	2500	-

Program ochrany zákazníků

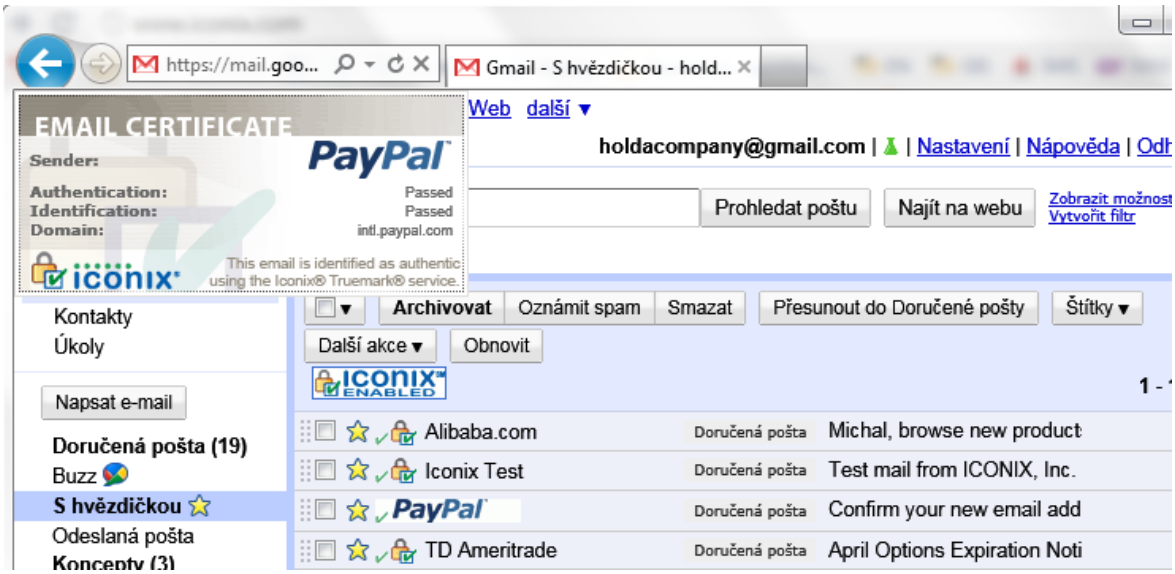
Jestliže zboží, které je placeno přes PayPal nedorazí, nabízí PayPal možnost „otevřít spor“ v době do 45dnů od zaplacení. Poté běží lhůta 20 dnů na vyřešení sporu s prodejcem. Jestliže se spor nevyřeší, nebo prodejce neodpovídá, můžete vznést nárok na navrácení platby. Poté PayPal posoudí nárok a je-li uznán, vrátí celou částku na původní účet.

Toto funguje poměrně spolehlivě o čemž vypovídají dvě mé zkušenosti, kdy v prvním případě mi byla vrácena celá částka bez zbytečných průtahů a v druhém případě asi polovina částky, z důvodu vyčerpání jistiny.

Ochrana proti phishingu

PayPal spolupracuje s firmou ICONIX, která poskytuje program rozpoznávající pravou poštu od phishingu. Ze stránek PayPal jste přesměrování na stránky ICONIX, kde si můžete stáhnout program pro Microsoft Outlook, nebo některého z dalších poskytovatelů emailové pošty jako Gmail, MSN Hotmail, Yahoo! Mail…

ICONIX obsahuje ověření pro více než 1500 společností (hlavně amerických). Integrace v Gmail s ověřením od ICONIX je zobrazena na obrázku (Obr. 28).



Obr. 28. Ochrana proti phishingu ICONIX v Gmailu

Testování pravosti zprávy je založeno na standartu Domain Keys Identified Mail (DKIM), díky kterému je možné ověřit pravost původce zprávy z hlavičky emailu. [78]

DKIM využívá elektronický podpis s veřejným a soukromým klíčem. Vytvoří se hash z těla zprávy a na odchozím SMTP serveru, který může být buď firemní, nebo poskytovatele internetového připojení je spolu s doménou odesilatele podepsán soukromým klíčem. Tento podpis je uložen v hlavičce DKIM-Signature spolu s ostatními informacemi nutnými ke svému ověření.

Pro distribuci veřejných klíčů se využívá Domain Name System (DNS), s tím, že se předpokládá bezpečnost DNS záznamů, které mohou být měněny pouze vlastníkem domény.

Server přijímající tuto podepsanou zprávu si vyžádá soukromý klíč z DNS a pomocí něj ověří elektronický podpis a tím pravost zprávy.

Na rozdíl od standardů pro zabezpečení elektronické pošty S/MIME, která funguje na principu šifrování a podepsání zprávy uživatelem se v případě DKIM používá podpisu a identifikace emailu přímo na poštovním serveru, což nevyžaduje žádnou činnost ze strany uživatele.

7.2.2 PayU

Popis a vlastnosti

Platební systém PayU který provozuje společnost Aukro s.r.o. zastřešuje několik platebních systémů. PayU jako platební agregátor podporuje následující platební metody:

- GE Money Bank,
- Volksbank,
- Fio banka,
- Mojeplatba (KB),
- mPeníze (mBank),
- ePlatby (Raiffeisen),
- Visa, MasterCard.

První čtyři platební metody podporuje PayU v kooperaci s platebním portálem PayMyway, který umožňuje rychlé platby z těchto čtyř bank.

Toto řešení obvykle funguje přesměrování platby na internetové bankovnictví každé jednotlivé banky. Toto bývá realizováno ve zjednodušené podobě s možností pouze potvrzení, či zamítnutí aktuální transakce. Bezpečnost jednotlivých metod se odvíjí od zabezpečení jejich internetového bankovnictví.

Nyní si popíšeme bezpečnost čtyř platebních metod sjednocených pod PayMyway.

GE Money Bank (PayU)

platba probíhá přesměrováním do zjednodušené verze internetového bankovnictví. Zde se přihlásíte pomocí ID (číslo účtu) a hesla. Po úspěšném přihlášení se objeví před-vyplněný příkaz k úhradě a po potvrzení přijde na registrované mobilní číslo SMS s kódem pro danou transakci. Po zadání kódu a odeslání transakce je tato v reálném čase připsána na obchodníkův účet.

Slabinu v zabezpečení vidím ve shodnosti přihlašovacího ID s číslem účtu. Naopak SMS zpráva, která obsahuje kromě kódu také celý popis transakce, zvyšuje bezpečnost a je stále pohodlná pro uživatele.

Volksbank platba (PayU)

probíhá také přes přesměrování do zjednodušené verze internetového bankovnictví. Zde jsou dvě možnosti autentizace:

- Certifikát (1024bitů) + heslo.
- Přihlašovací jméno + PIN + Token kód.

Přihlášení promocí certifikátu probíhá přes digitální certifikát o délce 1024 bitů, který je šifrován vlastním heslem uživatele. Při tomto druhu přihlášení jsou transakce omezeny částkou 20 000,-Kč.

Přihlášení pomocí tokenu (Obr. 29) je rozšířenou formou a přidává další vrstvu bezpečnosti. Token je generátor jednorázových autentizačních klíčů, tzv. token kódů.

Token kód má omezenou časovou platnost, každou minutu je generován nový. Token je vyráběn firmou RSA a generuje 6 místný kód. Tento kód je spolu se 4 místným pinem zadán pro potvrzení transakce. Při tomto druhu ověření není limit 20 000,-Kč aplikován. Token se vydává za jednorázový poplatek 250,-Kč.

Obr. 29. Autentizační kalkulátor RSA [79]

Fio banka (PayU)

Platba probíhá opět přes přesměrování do zjednodušené verze internetového bankovnictví. Zde stačí pro přihlášení uživatelské jméno a heslo. Transakci je dále nutno potvrdit kódem, který je odeslán SMS zprávou.

Další druhy plateb budou popsány samostatně dále v tomto oddílu.

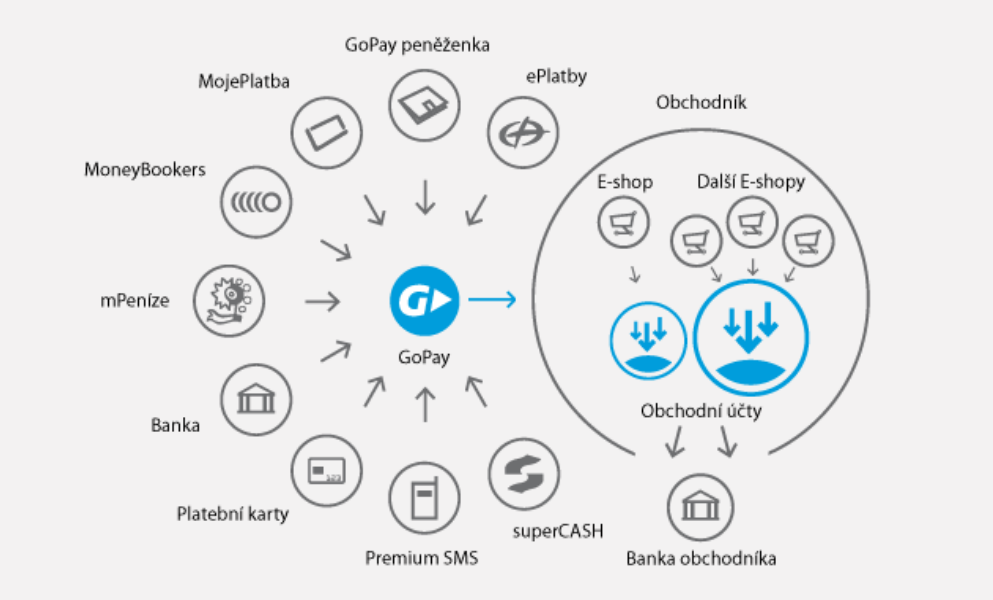
7.2.3 GoPay

Popis a vlastnosti

Bezpečnost tohoto sytému je řešena anonymitou uživatele, kde k registraci a využívání služeb této elektronické peněženky stačí email, heslo a přezdívka uživatele. Tímto lze ovšem využívat pouze platby malého rozsahu, pro které platí ze zákona následující [80]:

- maximální zůstatek na GoPay peněžence nepřesáhne v přepočtu 150 EUR,
- maximální objem příchozích plateb za kalendářní rok nepřesáhne v přepočtu 2.500 EUR,
- maximální objem odeslaných bankovních plateb za kalendářní rok nepřesáhne v přepočtu 1.000 EUR.

Systém integruje několik nejpoužívanějších platebních metod (Obr. 30). Při placení v eshopu s podporou GoPay, si zákazník může vybrat z několika metod plateb.



Obr. 30. Integrace platebních metod pod systém GoPay [81]

Bezpečnost

Stránka s výběrem metod je zabezpečena pomocí protokolu TLS 1.0 a šifrovacího standartu AES_256_CBC. Pro výměnu klíčů se využívá DHE_RSA a kontrola otisku zprávy je realizována pomocí SH1.

Při registraci, která probíhá na zabezpečených stránkách (viz výše) si zvolíte přihlašovací přezdívku a heslo, následně vám přijde na email aktivační odkaz se zvolenou přezdívkou, ale bez hesla, což eliminuje nebezpečí přístupu k účtu útočníkem při získání přístupu k emailu.

Při vkládání hesla je požadováno minimálně 8 znaků, které musí obsahovat alespoň jedno číslo, nebo zvláštní znak.

Přihlašování probíhá zadáním přezdívky vybrané u registrace a hesla.

Stránky mají také ochranu proti útokům pomocí „slovníkových útoků“ po několika neúspěšných pokusech o přihlášení je účet zablokován a uživateli odeslán následující email:

„Dobrý den, opakovaně jsme zaznamenali chybné přihlášení k vaší GoPay peněžence.

Z bezpečnostních důvodů byl přístup k vaší GoPay peněžence na 1 hodinu zablokován.

Pokud se tak stalo bez vašeho vědomí, kontaktujte nás neprodleně na emailové adrese: fraud@gopay.cz“ [82]

Toto se spolu s požadavky na poměrně bezpečné heslo jeví jako dobrá ochrana před neautorizovaným přihlášením.

Lepší úroveň ochrany by mohl nabídnout systém upozorňování o blokaci formou SMS, kvůli lepší dostupnosti informace.

GoPay by měl také od 1. 5. 11 podporovat rozesílání emailů s potvrzením objednávky a platby, což opět zvýši kontrolu nad účtem a tím jeho bezpečnost. GoPay také uvažuje o zavedení upozornění na mobilní telefony, bohužel až v budoucnu. [83]

Přesměrování plateb

Bezpečnost při platbách skrze partnerské systémy záleží na každém jednotlivém poskytovateli.

Problém může vzniknout při přesměrování na vybranou platební metodu.

Při volbě „platba kartou“ je uživatel přesměrován na platební bránu Moneybookers, která sice podporuje stejné šifrování stránky, ale transakce není realizována přes 3D SECURE.

Platba pomocí superCASH je realizovaná vygenerováním čárového kódu, který umožní hotovostní platbu prostřednictvím terminálů společnosti SAZKA, a.s. a České Pošty.

Platby přes ePlatby, Mojeplatba, mPeníze, Moneybookers probíhají přesměrováním na stránky provozovatelů, jejichž bezpečnostní opatření jsou popsána jednotlivě dále v této kapitole.

7.2.4 Moneybookers

Popis a vlastnosti

Moneybookers je platebním systémem s elektronickou peněženkou. Je možné ji využít pro platby online, nebo převody prostředků mezi uživateli Moneybookers po celém světě. Moneybookers má okolo 17 miliónů zákazníků. Tento systém je konkurentem pro PayPal hlavně mimo Ameriku. Společnost má sídlo ve Velké Británii a bankovní účty ve více než 30 zemích světa. Tímto je autorizován a regulován Financial Services Authority (FSA) Velké Britanie.

Platební servis Moneybookers využívá přes 80000 obchodníků. [84]

Bezpečnost

internetové stránky jsou při přihlašování k účtu ověřeny certifikační autoritou VeriSign. Používá se šifrovací algoritmus CAMELLIA_256_CBC a 256 bitové šifrování. Pro výměnu klíčů se využívá DHE_RSA a kontrola otisku zprávy je realizována pomocí algoritmu SH1.

Moneybookers podporují oznámení o změně zůstatku na účtu na mobilní telefon. Cena je 0,13,-EUR za zprávu.

Moneybookers také podporují Escrow platby. Tyto platby umožňují při nákupu zboží uložit své peníze za zboží u prostředníka (Moneybookers), kdy po přijetí zboží jsou dále předány prodejci.

Limity transakcí

Limity transakcí jsou určeny podle stupně ověření. Hned po založení účtu je bez ověření zákazníka dostupný limit 1 000,-EUR (nebo ekvivalent v dané měně). Po verifikaci jména

pomocí platební karty, nebo účtu se limit zvýší na 5 000EUR a po verifikaci adresy pomocí dopisu a v něm vloženého kódu, se limit zvýší na 10 000EUR. Tyto limity jsou v souladu s mezinárodními předpisy proti „praní špinavých peněz“.

7.2.5 PaySec (ČSOB, Poštovní spořitelna)

Popis a vlastnosti

Systém funguje jako předplacená, online elektronická peněženka. Patří mezi nejoblíbenější a pro platby ji akceptuje asi 450 internetových obchodů v ČR. Platby probíhají v uzavřeném prostředí systému PaySec. Dobíjení probíhá mezi bankou zákazníka a systémem PaySec. Dobíjet je možné přes převod na účet, nebo pomocí karty. Kartou se platí zabezpečeně pomocí 3D SECURE.

Bezpečnost

V začátcích (VI/2008) měl systém problém s nezabezpečenou změnou čísla pro potvrzení transakce. Ten byl ovšem na základě upozornění odstraněn [85]. Dále se objevila slabina v podobě Cross Site Scripting, který spočívá v podstrčení jascriptového kódu útočníka stránce, která obsahuje bezpečnostní chyby ve scriptech, jako jsou neošetřené stupy. Zejména se využívá pole pro vyhledávání do kterého je možné vložit vlastní kód typu <SCRIPT>. Tímto způsobem se dají získat citlivé údaje návštěvníků, cookies, ale i obcházení bezpečnostních prvků a aplikaci phishingu. [86]

Nyní už jsou tyto problémy odstraněny a bezpečnost platebního systému PaySec můžeme shrnout v těchto bodech:

- Platby probíhají přes prostředníka.
- Nabíjení pomocí IB, nebo kartou – 3D SECURE.
- Platby autorizované pomocí SMS.
- Komunikace zabezpečena pomocí SSL – 128bitů.
- Identita PaySec ověřena certifikační autoritou.
- Změna čísla pro SMS potvrzení má časovou prodlevu a upozornění na staré číslo.

7.3 Analýza bankovních platebních tlačítek

7.3.1 mPeníze (mBank)

Popis a vlastnosti

Tato služba bankovního tlačítka je dostupná pro zákazníky mBank, kteří u ní mají účet. Místa kde je možné platit přes mBank jsou označeny logem mPeníze. Komerčním partnerem je Seznam a obchody s možností platit pomocí mPeníze jsou označeny v porovnávači Zboží.cz.

Bezpečnost

Při platbě u obchodníka přes mPeníze, neposkytuje zákazník žádné osobní údaje, protože je přesměrován do zjednodušené verze svého internetového bankovnictví. Zde se přihlásí a potvrdí platbu (jiné operace s účtem nejsou dostupné). Tímto se automaticky vyplní formulář pro platbu. Tento musíte nakonec autorizovat kódem transakce, který přijde v SMS na přednastavené číslo mobilního telefonu.

Přihlašovací stránka je ověřena certifikační autoritou VeriSign, spojení je zabezpečeno 128 bitovým šifrováním a šifrovacím standardem 3DES_EDE_CBC.

Platba je velice jednoduchá a rychlá. Výhodou je, že při přihlašování do zjednodušené verze internetového bankovnictví, nejsou jiné operace s účtem dostupné, což zvyšuje bezpečnost. Na druhou stranu, jelikož se nejedná o platbu kartou, nejsou zde nastaveny limitu pro platbu. Dále je velkou výhodou nutnost potvrzení platby přes kód v mobilním telefonu. Tuto možnost většinou elektronické peněženky nepodporují.

Hlavní nevýhoda (jako u všech BPT) je svázání s běžným účtem u mBank a podpora pouze 202 obchodů [87] a z tohoto plynoucí omezení.

7.3.2 Mojeplatba (Komereční Banka)

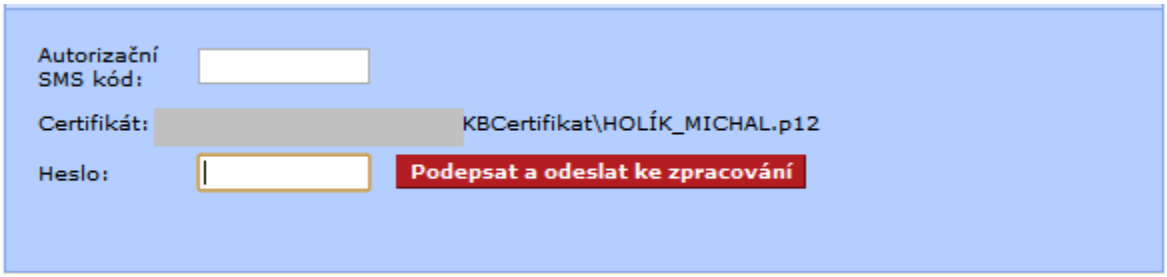
Popis a vlastnosti

Tato služba je dostupná pro zákazníky Komereční Banky(KB) a funguje podobně jako mBank. Jedná se o platební tlačítko u partnerských obchodníků, které zrychlí platbu. Při

volbě Mojeplatba je uživatel přesměrován do internetového bankovnictví KB na předem vyplněný platební příkaz.

Bezpečnost

Přihlášení do IB probíhá přes osobní certifikát a heslo. Transakce je dále autorizována pomocí SMS kódu a je nutné znovu zpřístupnit certifikát a zadat heslo (Obr. 31). Lze provést pouze transakci, která na službu Mojeplatba přesměrovala. Po potvrzení následuje zpětně přesměrování s potvrzením, či zrušením transakce.



Obr. 31. Autorizace transakce u Mojeplatba

Nevýhoda je obdobně jako u mBank omezení pouze pro zákazníky KB, což ovšem vyplývá z povahy služby.

7.3.3 ePlatby (Raiffeisenbank)

Popis a vlastnosti

ePlatby je platební metoda pro zákazníky Raiffeisen BANK, pomocí které jste obdobně jako u předchozích typů přesměrování do zjednodušené verze internetového bankovnictví. Zde je před-vyplněný platební příkaz a žádné další akce s účtem nejsou dovoleny. ePlatby jsou nejpopulárnějším systémem pro platbu tohoto druhu a podporuje ji zhruba tisícovka internetových obchodů.

Bezpečnost

Pro potvrzení platby je zapotřebí přihlásit se pomocí autentizačního kódu, který dochází buďto SMS zprávou, vygenerováním z autentizačního tokenu, anebo zpřístupněním

platného certifikátu od Raiffeisenbank. Po potvrzení autentizace je zapotřebí certifikace, tedy znovu odeslat SMS, vygenerovat kód nebo podepsat certifikátem.

7.4 Závěrečné srovnání bezpečnostních opatření

V této části si v tabulkách porovnáme přístup k bezpečnosti u elektronických peněženek a platebních tlačítek, a to na úrovních bezpečnosti přenosu dat, autentizace a autorizace transakce.

7.4.1 Bezpečnost přenosu dat pro elektronické peněženky

Všechny analyzované EP mají svoji autentičnost ověřenou CA a podporují šifrování přenosu.

Pro šifrování spojení se využívají standardní symetrické šifry. Výměna klíčů se ve všech případech realizuje pomocí asymetrického algoritmu RSA. hashovací algoritmus je u všech případů použitý SHA-1.

Tab. 8. Srovnání bezpečnosti přenosu dat pro elektronické peněženky

Služba	**PayPal**	**PayU**	**GoPay**	**Moneybookers**	**PaySec**
Ověřeno úřadem	VeriSign	Thawe	Equifax	VeriSign	GlobalSign
Šifrované spojení se serverem	112 bitů	128bitů	256 bitů	256 bitů	128 bitů
Protokol připojení	TLS 1.0	TLS 1.0	TLS 1.0	TLS 1.0	TLS 1.0
Šifrovací standard	3DES	RC4_128	AES	CAMELLIA	RC4_128
Ověřování zpráv	SHA1	SHA1	SHA1	SHA1	SHA1
Výměna klíčů	RSA	RSA	DHE_RSA	DHE_RSA	RSA
Komprimace	NE	NE	ANO	NE	NE
Znovuzískání TLS ze serveru	NE	NE	NE	NE	NE

7.4.2 Bezpečnost přenosu dat pro platební tlačítka

Všechny analyzované BPT mají svoji autentičnost ověřenou CA a podporují šifrování přenosu. Pro šifrování spojení se využívají standardní symetrické šifry. Výměna klíčů se ve všech případech realizuje pomocí asymetrického algoritmu RSA. Hashovací algoritmus je u všech případů použitý SHA-1.

Tab. 9. Srovnání bezpečnosti přenosu dat pro platební tlačítka

Služba	mPeníze	Mojeplatba	ePlatby	Volksbank
Ověřeno úřadem	VeriSign	VeriSign	VeriSign	VeriSign
Šifrované spojení se serverem	112 bitů	128bitů	256 bitů	256 bitů
Protokol připojení	TLS 1.0	TLS 1.0	TLS 1.0	TLS 1.0
Šifrovací standard	3DES	RC4_128	AES	AES
Ověřování zpráv	SHA1	SHA1	SHA1	SHA1
Výměna klíčů	RSA	RSA	DHE_RSA	DHE_RSA
Komprimace	NE	NE	NE	NE
Znovuzískání TLS ze serveru	NE	NE	NE	NE

7.4.3 Bezpečnost autentizace uživatele pro elektronické peněženky

I přes využívání adaptivní autentizace u PayPal, nepovažuji bezpečnost autentizace za dostatečnou. Hlavním důvodem je možná provázanost PayPal s platební kartou a nemožnost využití bezpečnostního tokenu v ČR.

U ostatních EP je nedostatkem pouze základní možnost autentizace pomocí jména a hesla a v případě Moneybookers navíc shodného přihlašovacího jména s emailem, což zvyšuje pravděpodobnost úspěšného útoku například hrubou silou.

Tab. 10. Srovnání úrovně autentizace uživatele pro elektronické peněženky

Služba	PayPal	GoPay	Moneybookers	PaySec
Šifrování přístupových stránek	ano	ano	ano	ano
Přihlašovací jméno	ano	ano	ano (email)	ano
Heslo	ano	ano	ano	ano
Zablokování po 3 neúspěšných přihlášeních	ano	ano	ano	ano
Autentizační certifikát	ne	ne	ne	ne
Autentizační SMS	ne	ne	ne	ne
Bezpečnostní token	ano (ne v ČR)	ne	ne	ne
Adaptivní autentizace	ano	ne	ne	ne

7.4.4 Bezpečnost autentizace uživatele pro platební tlačítka

V případě BPT je autentizace uživatele u jednotlivých bank řešena obdobně jako v případě internetového bankovnictví.

Zajímavé řešení provozuje Volksbank, kde je možnost přihlášení pomocí přihlašovacího jména, hesla a vygenerovaného kódu z bezpečnostního tokenu.

Zajímavá je také možnost u ePlatby, kde je možné si nechat poslat autentizační kód na mobil, pomocí zadání klientského čísla na stránkách banky. Toto číslo je zasláno pomocí SIM Toolkit technologie, takže je ještě chráněno BPINem.

Tab. 11. Srovnání úrovně autentizace uživatele pro platební tlačítka

Služba	**mPeníze**	**Mojeplatba**	**ePlatby**	**Volksbank**
Šifrování přístupových stránek	ano	ano	ano	ano
Přihlašovací jméno	ano	ne	ano	ano
Heslo	ano	ano	ano	ano
Zablokování po 3 neúspěšných přihlášeních	ano	ano	ano	ano
Autentizační certifikát	ne	ano	ano	ano
Autentizační SMS	ne	ne	ano	ne
Bezpečnostní token	ne	ne	ne	ano
Adaptivní autentizace	ne	ne	ne	ne

7.4.5 Bezpečnost autorizace transakce pro elektronické peněženky

Z této tabulky vyplývá z mého pohledu velká bezpečnostní slabina EP, kdy většina z nich nepodporuje rozšířené ověření autorizace transakce. Výjimkou je PaySec, který je společným projektem bank ČSOB a České spořitelny, které do ní implementovaly vlastnost, která je u elektronického bankovnictví již standardem. Slabou náhražkou v podobě upozornění na email podporuje například GoPay, či PayPal.

Tab. 12. Srovnání úrovně autorizace transakce pro elektronické peněženky

Služba	**PayPal**	**GoPay**	**Moneybookers**	**PaySec**
Autorizační SMS kód	ne	ne	ne	ano
Certifikát	ne	ne	ne	ne
Čipová karta	ne	ne	ne	ne
Bezpečnostní token	ne	ne	ne	ne
Upozornění na email	ano	ano	ano	ano

7.4.6 Bezpečnost autorizace transakce pro platební tlačítka

V případě autorizace transakce u BPT je situace podobná jako u internetového bankovnictví. Dnes velmi rozšířený způsob autorizace pomocí SMS nepodporuje Volksbank, která jej nahrazuje zadáním PINu + kódu z bezpečnostního tokenu.

Tab. 13. Srovnání úrovně autorizace transakce pro platební tlačítka

Služba	mPeníze	Mojeplatba	ePlatby	Volksbank
Autorizační SMS kód	ano	ano	ano	ne
Certifikát	ne	ano	ano	ano
Čipová karta	ne	ano	ne	ne
Bezpečnostní token	ne	ne	ne	ano
Heslo	ne	ano	ne	ano

7.4.7 Souhrn výsledků

Z pohledu bezpečné komunikace jsou všechny analyzované služby na dobré úrovni, protože používají jak certifikaci svých stránek, tak šifrovanou komunikaci s uživatelem.

Autentizace uživatele je u EP na nižší úrovni, než u BPT, a to zejména kvůli absenci osobních certifikátů a bezpečnostních tokenů. Kladně naopak hodnotím kontrolu pokusů o přihlášení s následným zablokováním účtu, při překročení daného limitu. U BPT je situace obdobná jako u jejich klasického IB. Jako velmi silnou kombinaci hodnotím Přihlašovací jméno + PIN + Token kód u Volksbank.

Autorizace transakcí je z mého pohledu velmi důležitá, ale u EP ji umožňuje pouze PaySec, a to pomocí SMS. U BPT je autorizace transakcí realizována většinou obdobně jako při autentizaci uživatele nebo jako u mPeníze pomocí SMS kódu.

Při pohledu na kompletní bezpečnost bych jako nejslabší službu mezi EPT z analyzovaných zástupců vybral mPeníze, z důvodu podpory nejméně dodatečných metod jak autentizace uživatele, tak autorizace transakce.

Nejslabší zástupce z EP se může podle tabulky zdát PayPal, ale z důvodu nasazení adaptivního systému autentizace a programu na ochranu zákazníka to nemusí být pravda. V reálných podmínkách vždy záleží na konkrétním typu útoku.

ZÁVĚR

V oblasti platebních karet a bezpečnostních tokenů se musíme zaměřit na všechny úrovně zabezpečení. Útoky na fyzickou bezpečnost čipových karet, či kryptoprocesorů invazivními metodami jsou nebezpečné a účinné, ale pro útočníky také velice náročné, jak po stránce vybavení, tak vynaloženého úsilí, nicméně pomocí technik neinvazivních, jako je například odběrová, či časová analýza může útočník dosáhnout podobných výsledku s mnohem menším úsilím. Je proto důležité, aplikovat na tato zařízení ochrany v podobě generátorů šumu, náhodného časování instrukcí, úpravy vyzařovacích charakteristik a podobně, i za cenu jejich vyšší spotřeby, či nižší rychlosti.

Útoky na logické úrovni často využívají toho, že standardy jako EMV obsahují sice velmi precizní bezpečnostní postupy, ale z důvodu zachování interporability a kompatibility často pouze ve formě doporučení. Útok provedený Universitou Cambridge na čipové karty v Anglii využil nedostatku možnosti offline autentizace a toho, že data generovaná terminálem a kartou nejsou povinně odesílána do banky pro analýzu. Poté použili útok typu MITM mezi kartou a terminálem. Software poslal terminálu data, že byl PIN zadán a kartě, že terminál přeskočil autentizaci. Těmto útokům se dá zabránit zavedením online verifikace PINu, či analýzou generovaných dat terminálem a kartou. Pro ověření pravosti karty je důležité nahradit metodu statické autentizace SDA za dynamické ověření DDA, které zamezuje možnosti kopírování dat při přenosu.

Provozní bezpečnost, do které spadá zacházení se zařízením koncovým uživatelem, se jeví jako nejsnadněji aplikovatelná. Přesto útoky na ni generují velmi vysoké ztráty. Zásadním problémem je informovanost uživatele o možných hrozbách a dodržování bezpečnostních zásad. Spadají sem útoky typu sociálního inženýrství, Skimmingu, odpozorování PINu, či podstrčení Malwaru na PC. Největším problémem je, že řada uživatelů upřednostňuje pohodlí před bezpečím. Řešením je opatrnost při zacházení s kartou, používání technologie 3D Secure a bezpečného PC při online platbách a sledování aktuálních rizik.

V oblasti internetového bankovnictví existuje několik klíčových úrovní pro zajištění bezpečnosti. Základem je ověřitelnost identity banky pomocí certifikační autority a šifrování přenosu dat pomocí TLS protokolu. Z důvodu možnosti generování falešných certifikátů, kvůli nedostatku hasnovacího algoritmu MD5, se dnes využívá nejčastěji SHA-

1. Bezpečnější SHA-2 není masově nasazen z důvodu špatné kompatibility na systémech Windows XP a starších.

Velmi důležitá je silná autentizace uživatele, která by měla zahrnovat kromě jmen a hesel uživatelské certifikáty, autentizační kalkulátory, či SMS kódy. Tato rozšíření můžou zabránit zneužití i při odposlechnutí citlivých údajů, a to z důvodu jednorázového použití.

Poslední úrovní je bezpečnost přístupového PC, která by měla být zajištěna aktualizovaným softwarovým vybavením, používáním antiviru, firewall a proaktivním přístupem uživatele.

Oblast internetových peněženek se skládá z obdobných úrovní zabezpečení jako IB, ale jelikož se jimi realizují obvykle malé platby, nedosahuje stejných kvalit. Hlavní nedostatek je obecná absence rozšiřujících bezpečnostních prvků pro autentizaci uživatele, či autorizaci transakce. Z testovaných EP měl pouze PaySec rozšířenou autorizaci transakce v podobě SMS kódu. Největší EP na Světě – PayPal je dostupná i v ČR, ale bez možnosti využití autentizačního kalkulátoru, který je dostupný v jiných zemích a s nízkou podporou prodejců v ČR, tak zůstává jeho výhodou a zároveň slabinou pouze provázanost s bankovním účtem uživatele a poměrně tvrdá politika kontroly přístupů na základě Adaptivní autentizace.

Je zřejmé, že technologické trendy v podobě NFC budou mít bezpečnostní rizika na základě použité technologie RFID, kde se faktickou absenci zabezpečení tohoto standardu budou výrobci snažit vylepšit aplikací softwarového šifrování. Jako ideální se jeví kombinace NFC čipu aplikovaného do SIM karty s podporou technologie GSM Toolkit, která může poskytnout základ pro zabezpečení a nabídne nezávislost na konkrétním mobilním telefonu.

Další trend v podobě bezdotykových karet přijde do ČR v druhé polovině roku, ale již z popsaných útoků v USA, kdy ke krádeži čísla, typu a expirace karty stačila čtečka karet a netbook se software, dává tušit problémům, které nevyřeší pouze často prezentovaný „bezpečný“ krátký dosah karet. Jednoduché řešení se nabízí v používání krytu karty s rušením elektromagnetického záření. Z pohledu bank je to šifrování přenosu dat mezi kartou a terminálem.

ZÁVĚR V ANGLIČTINĚ

In the area of payment cards and security tokens is necessary to explore all security levels. Attacks on the physical security of smart cards, or crypto chip by invasive methods are dangerous and effective, but for attackers also very challenging, in terms of equipment and effort, but using non-invasive techniques such as sampling analysis or time analysis, an attacker can achieve similar results with much less effort. It is therefore important to apply protection in following forms: a noise generator, random timing of instructions, adjustments in radiation characteristics etc. Even at the cost of higher consumption or lower speed rates.

Attacks on a logical level often uses, that standards such as EMV contains precise security procedure but which are often only in form of recommendations. The attack carried out by Cambridge University on smart cards in England took advantage of lack of offline authentication and non analyzing data from card and terminal by banks. It used attack MITM between card and terminal to deception terminal that the PIN was entered correctly and the card that the authentication was skipped. These types of attacks can by avoided by introducing the online PIN verification or analyzing data from terminal and card by bank. To verify the authenticity of card is important to replace the static method of authentication SDA by dynamic verification DDA which avoid the copying of data during transmission.

Operational safety, which includes the treatment of end-user with device seems easy to apply. But attacks to it generates the biggest looses. Problem is in education of users about the threats and compliance with security policy. These areas include social engineering attacks, Skimming, derived PIN codes, or planted malware on PC. The solution is to use caution when handling with the smart card, using 3D Secure technology and secure PC for online payments and monitoring of actual threads.

In the area of internet banking, there are several key levels for ensure safety. It is based on the verifiability of identity of the bank by the certificate authority and encryption of data using TLS protocol. Because of the possibility of generating false certificates due to lack of MD5 hash in algorithm is now used mostly SHA-1. Safer SHA-2 is not used widely due to poor compatibility with Windows XP and older.

Very important is the strong user authentication, which should include, in addition to user names and passwords, certificates, authentication calculators or SMS codes. These extensions can prevent abuse because each code is used one time.

Last level is security of access PC which should be provided by updated software equipment, using antivirus, firewall and by proactive user behavior.

The area of internet wallets is composed of similar levels of security but because it usually realizes smaller payments the security is not in the same quality. Main disadvantage is general lack in extended security features to authenticate users, or authorize transactions. Only one internet wallet named PaySec had the extended authorization of payment by SMS code. The largest internet wallet PayPal is also available in the Czech but without the security authentication token and low vendor support it has only few advantages.

It is obvious that technological trends as NFC will have to deal with security risks based on RFID technology. There is lack of security which can be improved by application software encryption. The ideal solution can by implementation of NFC chip to SIM cards with technology GSM Toolkit which can provide a basis for security and offers independence at a particular cell phone.

Trend in form of contactless cards is coming to Czech in second half of the year, but attacks realized in USA where numbers, types and expirations of credit cards was stolen only by contactless card reader and laptop with software sensing another problems which cannot be solved only by short range of cards. A simple solution would be to use the card cover which interference with electromagnetic radiation. Otherwise banks should apply data transfer encryption between cards and terminals.

SEZNAM POUŽITÉ LITERATURY

[1] Česko. Zákon č. 284/2009 Sb., o platebním styku. In *Sbírka zákonů, Česká republika*. 2009, částka 89, s. 4174-4210.

[2] *Internetprovsechny.cz* [online]. 2010 [cit. 2011-05-14]. Mobilní komerce a elektronické platby. Dostupné z WWW: <http://www.internetprovsechny.cz/mobilni-komerce-a-elektronicke-platby/>.

[3] Symetrická kryptografie. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-23]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Symetrick%C3%A1_kryptografie>.

[4] Asymetrická kryptografie. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-23]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie>.

[5] *Technische Universiteit Eindhoven* [online]. 2008 [cit. 2011-04-21]. MD5 considered harmful today. Dostupné z WWW: <http://www.win.tue.nl/hashclash/rogue-ca/>.

[6] X.509. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/X.509>.

[7] Transport Layer Security. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Transport_Layer_Security>.

[8] Hash function. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-23]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Hash_function>.

[9] Pharming. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-23]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Pharming>.

[10] MATYÁŠ, Václav ; KRHOVJÁK , Jan. *Autorizace elektronických transakcí a autorizace dat i uživatelů*. Brno : Masarykova univerzita, 2008. 125 s. ISBN 978-80-210-4556-9.

[11] *Hardwaresecurity* [online]. 2010 [cit. 2011-04-21]. Why use a payment HSM?. Dostupné z WWW: <http://www.hardwaresecurity.info/why-use-a-payment-hsm/>.

[12] Hardware security module. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Hardware_security_module>.

[13] MARTINÁSEK, Zdeněk. *Útoky postranními kanály na čipové karty* [online]. Brno : Vysoké učení technické v Brně, 2010. 87 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikacních technologií. Dostupné z WWW: <http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=28101>.

[14] MÁČE, Miroslav. *Platební styk - klasický a elektronický*. Praha : Grada Publishing, 2006. 220 s. ISBN 80-247-1725-5.

[15] *Pandatron.cz* [online]. 2008 [cit. 2011-04-28]. Karty s magnetickým pruhem. Dostupné z WWW: <http://pandatron.cz/?535&karty_s_magnetickym_pruhem>.

[16] *Prevencepodvodu.cz* [online]. 2009 [cit. 2011-04-23]. Technické členění podvodů. Dostupné z WWW: <http://www.prevencepodvodu.cz/podvodne-praktiky/technicke-cleneni-podvodu.php>.

[17] *Ihned.cz* [online]. 2011 [cit. 2011-04-24]. Zrušte karty s magnetickými proužky, žádají němečtí kriminalisté. Dostupné z WWW: <http://byznys.ihned.cz/osobni-finance/c1-49237660-zruste-karty-s-magnetem-zadaji-nemecti-kriminaliste>.

[18] *Mbank.cz* [online]. 2008 [cit. 2011-05-04]. CVV kód - vyjádření mBank. Dostupné z WWW: <http://www.mbank.cz/forum/read.html?f=1&i=38288&t=38153&cat=0> .

[19] *Financnik.cz* [online]. 2010 [cit. 2011-05-04]. Jak platit na internetu?. Dostupné z WWW: <http://www.financnik.cz/komodity/financnik/jak-platit-na-internetu.html>.

[20] 3-D Secure. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://en.wikipedia.org/wiki/3-D_Secure>.

[21] *Simplia.cz* [online]. 2010 [cit. 2011-04-28]. Eshopy. Dostupné z WWW: <http://www.simplia.cz/eshopy/>.

[22] *Csas.cz* [online]. 2010 [cit. 2011-04-28]. 3D SECURE. Dostupné z WWW: <http://www.csas.cz/banka/content/inet/internet/cs/karty_3dsecure.pdf>.

[23] *Mesec.cz* [online]. 2011 [cit. 2011-05-14]. Citibank spustila u svých karet podporu 3D Secure. Jak to funguje?. Dostupné z WWW: <http://www.mesec.cz/clanky/citibank-spustila-u-svych-karet-podporu-3d-secure/>.

[24] *Csas.cz* [online]. 2011 [cit. 2011-04-29]. Csas@csas.cz . Dostupné z WWW: <http://www.csas.cz>.

[25] *Pay MUZO Seznámení se systémem, vytváření objednávek* [online]. Praha : Global Payments Europe, a. s., 2008 [cit. 2011-05-2]. Dostupné z WWW: <http://www.assembla.com/spaces/cxLSicQC8r3yPqab7jnrAJ/documents/dUEp14Q9Gr3z3Gab7jnrAJ/download/cz_PayMuzo-Seznamenisesystemem.pdf>.

[26] *Mojebanka.cz* [online]. 2011 [cit. 2011-04-29]. mojebanka@kb.cz . Dostupné z WWW: <http://www.mojebanka.cz>.

[27] *CSOB.cz* [online]. 2011 [cit. 2011-04-29]. info@csob.cz . Dostupné z WWW: <http://www.csob.cz>.

[28] *Unicreditbank.cz* [online]. 2011 [cit. 2011-04-29]. INFORMACNI@unicreditgroup.cz . Dostupné z WWW: <http://www.unicreditbank.cz>.

[29] *Ihned.cz* [online]. 2011 [cit. 2011-05-03]. Limit pro bezkontaktní platby bude 500 korun. Dostupné z WWW: <http://m.ihned.cz/c4-10000125-51130960-700000_mamdetail-limit-pro-bezkontaktni-platby-bude-500-korun>.

[30] *Homel.vsb.cz* [online]. 2008 [cit. 2011-05-21]. Norma ISO 7816. Dostupné z WWW: <http://homel.vsb.cz/~nav79/cipkart/cpno7816.htm>.

[31] Federal Information Processing Standard. In *Wikipedia : the free encyclopedia*[online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-23]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Federal_Information_Processing_Standard> .

[32] *Gcn.com* [online]. 2007 [cit. 2011-05-06]. Smart cards play it safe . Dostupné z WWW: <http://gcn.com/Articles/2007/05/27/Smart-cards-play-it-safe.aspx?Page=2>.

[33] EMV. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-23]. Dostupné z WWW: <http://en.wikipedia.org/wiki/EMV>.

[34] *Nfcworld.wpcdn.com* [online]. 2010 [cit. 2011-05-07]. Worldwide EMV Deployment. Dostupné z WWW: <http://www.emvco.com/about_emvco.aspx?id=202>.

[35] MURDOCH, Steven. *Chip and PIN is Broken* [online]. Cambridge : University of Cambridge, 2010. 13 s. Oborová práce. University of Cambridge . Dostupné z WWW: <http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf>.

[36] *Penize.cz* [online]. 2010 [cit. 2011-05-09]. Čipové karty nejsou tak bezpečné, jak se předpokládalo. Dostupné z WWW:

<http://www.penize.cz/diskuze/72975-cipove-karty-nejsou-tak-bezpecne-jak-se-predpokladalo#comment_133087>.

[37] *Info.muni.cz* [online]. 2008 [cit. 2011-05-15]. Odpozorovat PIN platební karty není tak složité. Dostupné z WWW: <http://info.muni.cz/index.php?option=com_content&task=view&id=1073&Itemid=92>.

[38] *Anz.com* [online]. 2011 [cit. 2011-05-12]. Internet security threats. Dostupné z WWW: <http://www.anz.com/personal/ways-bank/internet-banking/protect-banking/security-threats/>.

[39] *Systemonline.cz* [online]. 2006 [cit. 2011-05-09]. Bezpečnost elektronické komunikace. Dostupné z WWW: <http://www.systemonline.cz/it-security/bezpecnost-elektronicke-komunikace.htm>.

[40] *Zive.cz* [online]. 2009 [cit. 2011-05-09]. Superpočítače způsobují kryptografům problémy. Dostupné z WWW: <http://www.zive.cz/clanky/superpocitace-zpusobuji-kryptografum-problemy/sc-3-a-145121/default.aspx>.

[41] ADIDA, Ben. *Phish and Chips* [online]. Cambridge : University of Cambridge, 2006. 10 s. Oborová práce. University of Cambridge . Dostupné z WWW: <http://www.cl.cam.ac.uk/~rja14/Papers/Phish-and-Chips.pdf>.

[42] *Iaik.tugraz.at* [online]. 2011 [cit. 2011-05-09]. SHA-1 Collision Search. Dostupné z WWW: <http://www.iaik.tugraz.at/content/research/krypto/sha1/>.

[43] *Erratasec.blogspot.com* [online]. 2008 [cit. 2011-05-21]. Not all MD5 certs are vulnerable. Dostupné z WWW: <http://erratasec.blogspot.com/2008/12/not-all-md5-certs-are-vulnerable.html>.

[44] *Entrust.com* [online]. 2011 [cit. 2011-05-10]. Internet Privacy and Security. Dostupné z WWW: <http://www.entrust.com/internet-privacy-security/>.

[45] Malware. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-24]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Malware>.

[46] *Securityworld.cz* [online]. 2008 [cit. 2011-05-10]. Trojský kůň Sinowal řádil úspěšně po celé tři roky . Dostupné z WWW: <http://securityworld.cz/securityworld/trojsky-kun-sinowal-radil-uspesne-po-cele-tri-roky-213>.

[47] *T-mobile.cz* [online]. 2011 [cit. 2011-05-12]. GSM Banking - Zaručení bezpečnosti. Dostupné z WWW: <http://www.t-mobile.cz/web/cz/residential/tarifysluzby/mobilniplatby/gsmbanking-zarucenibezpecnosti>.

[48] *Sfinance.cz* [online]. 2011 [cit. 2011-05-15]. GSM a WAP banking. Dostupné z WWW: <http://www.sfinance.cz/osobni-finance/informace/prime-bankovnictvi/gsm-banking-wap-banking/>.

[49] Wireless Transport Layer Security. In *Wikipedia : the free encyclopedia*[online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-22]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Wireless_Transport_Layer_Security>.

[50] Česko. ZÁKON č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech. In *Sbírka zákonů, Česká republika*. 2002, 55, s. -.

[51] *Penize.cz* [online]. 2003 [cit. 2011-05-18]. Elektronické peněženky nevěří na svou záchranu. Dostupné z WWW: <http://www.penize.cz/investice/15313-elektronicke-penezenky-neveri-na-svou-zachranu>.

[52] *Paypal.com* [online]. 2011 [cit. 2011-05-15]. Security. Dostupné z WWW: <www.paypal.com>.

[53] ZANDL, Patrick. *Lupa.cz* [online]. 2009 [cit. 2011-05-12]. GoPay nastupuje do online plateb na český Internet. Dostupné z WWW:

<http://www.lupa.cz/clanky/gopay-nastupuje-do-online-plateb-na-cesky-internet/>.

[54] *Aec.cz* [online]. 2010 [cit. 2011-05-11]. Security 2010 - konference. Dostupné z WWW: <http://www.aec.cz/cz/konference/security-2010/program>.

[55] *Az-pocitace.cz* [online]. 2011 [cit. 2011-05-12]. Pretec USB 2.0 i-disk Touch 1GB, s otiskem prstu. Dostupné z WWW: <http://www.az-pocitace.cz/z/21964702/pretec-usb-20-i-disk-touch-1gb-s-otiskem-prstu>.

[56] *Mesec.cz* [online]. 2011 [cit. 2011-05-12]. Novinky v platebních kartách v roce 2011. Dostupné z WWW: <http://www.mesec.cz/clanky/novinky-v-platebnich-kartach-v-roce-2011/>.

[57] *Smartcardalliance.org* [online]. 2011 [cit. 2011-05-13]. Contactless Payments Security. Dostupné z WWW: <http://www.smartcardalliance.org/pages/publications-contactless-payment-security-qa>.

[58] *Visa.cz* [online]. 2011 [cit. 2011-05-12]. Česká spořitelna umožní klientům platit kartami s bezkontaktní platební technologií. Dostupné z WWW: <http://www.visa.cz/>.

[59] *Krowne.wordpress.com* [online]. 2010 [cit. 2011-05-21]. Barclaycard and Barclays announce one millionth contactless transaction in UK. Dostupné z WWW: <http://krowne.wordpress.com/2010/11/09/barclaycard-and-barclays-announce-one-millionth-contactless-transaction-in-uk/>.

[60] Mastercard#PayPass. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Mastercard#PayPass>.

[61] *Vivotech.com* [online]. 2011 [cit. 2011-05-13]. Contactless POS terminal. Dostupné z WWW: <http://www.vivotech.com/products/vivo_pay/vivopay_5000.asp>.

[62] *Wreg.com* [online]. 2010 [cit. 2011-05-13]. Electronic Pickpocketing . Dostupné z WWW: <http://www.wreg.com/wreg-electronic-pickpocketing-story,0,6289527.story>.

[63] *Katu.com* [online]. 2010 [cit. 2011-05-13]. 'Magic wand' can pick your pocket of credit card info. Dostupné z WWW: <http://www.katu.com/news/121550239.html>.

[64] Contactless smart card. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-24]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Contactless_smart_card>.

[65] Mifare. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-24]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Mifare>.

[66] PALÁN, Michal . *Cdrail.cz* [online]. 2006 [cit. 2011-05-02]. Bezkontaktní čipové karty Českých drah . Dostupné z WWW: <http://www.cdrail.cz/VTS/CLANKY/vts21/2108.pdf>.

[67] KONING GANS, Gerhard. *A Practical Attack on the MIFARE Classic* [online]. Netherland : Radboud University, 2008. 15 s. Oborová práce. Radboud University Nijmegen. Dostupné z WWW: <http://www.proxmark.org/documents/mifare_weakness.pdf>.

[68] Oyster card. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Oyster_card>.

[69] *Nfc-forum.org* [online]. 2011 [cit. 2011-05-14]. NFC and Contactless Technologies. Dostupné z WWW: <http://www.nfc-forum.org/aboutnfc/nfc_and_contactless/>.

[70] Near Field Communication. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, [cit. 2011-05-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Near_Field_Communication>.

[71] *Nfc-forum.org* [online]. 2011 [cit. 2011-05-14]. NFC in Action. Dostupné z WWW: <http://www.nfc-forum.org/aboutnfc/nfc_in_action/>.

[72] *Cdt.org* [online]. 2011 [cit. 2011-05-14]. NFC Phones Raise Opportunities, Privacy And Security Issues. Dostupné z WWW: <http://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues>.

[73] HASELSTEINER, Ernst . *Security in Near Field Communication* [online]. Austria : Gratkorn, 2006. 11 s. Oborová práce. Gratkorn, Austria. Dostupné z WWW: <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf>.

[74] *Libnfc.org* [online]. 2010 [cit. 2011-05-15]. Trace: nfc-relay. Dostupné z WWW: <http://www.libnfc.org/documentation/examples/nfc-relay>.

[75] *Epenezenky.cz* [online]. 2008 [cit. 2011-05-13]. Jak funguje PayPal.com. Dostupné z WWW: <http://www.epenezenky.cz/paypal/jak-funguje-paypalcom>.

[76] *Root.cz* [online]. 2009 [cit. 2011-05-15]. Nejčastějším cílem phishingu je PayPal. Dostupné z WWW: <http://www.root.cz/zpravicky/nejcastejsim-cilem-phishingu-je-paypal/>.

[77] *Fandor.cz* [online]. 2008 [cit. 2011-05-15]. Jak vyřešit blokaci PayPal účtu. Dostupné z WWW: <http://www.fandor.cz/jak-vyresit-blokaci-paypal-uctu/comment-page-1/>.

[78] SATRAPA, Pavel. Lupa.cz [online]. 2007 [cit. 2011-05-14]. DKIM – dopisy ověřeného původu. Dostupné z WWW: <http://www.lupa.cz/clanky/dkimnbspndash-dopisy-overeneho-puvodu/>.

[79] *Volksbank.cz* [online]. 2011 [cit. 2011-05-17]. Vyzkoušejte nové zabezpečení!. Dostupné z WWW: <http://www.volksbank.cz/vb/jnp/cz/novinky/cz-novinky-090817_El_klic_nov.html>.

[80] *Gopay.cz* [online]. 2011 [cit. 2011-05-15]. Nejčastěji kladené dotazy. Dostupné z WWW: <https://www.gopay.cz/help/faq#18900>.

[81] *Gopay.cz* [online]. 2011 [cit. 2011-05-22]. Jak funguje GoPay obchodní účet. Dostupné z WWW: <https://www.gopay.cz/jak-funguje-gopay/obchodni-ucet>.

[82] *GoPay* [online]. 2011 [cit. 2011-05-05]. Dostupné z WWW: <https://www.gopay.cz/>.

[83] *GOPAY.cz* [online]. 2011 [cit. 2011-04-29]. podpora@gopay.cz. Dostupné z WWW: <http://www.gopay.cz>.

[84] *Moneybookers* [online]. 2011 [cit. 2011-05-01]. Dostupné z WWW: <http://www.moneybookers.com/app/>.

[85] *Lupa.cz* [online]. 2008 [cit. 2011-05-15]. Servis 24 bezpečnější, PaySec stále s nedostatkem (doplněno, opraveno). Dostupné z WWW: <http://www.lupa.cz/zpravicky/servis-24-bezpecnejsi-paysec-stale-s-nedostatkem/>.

[86] *Pooh.cz* [online]. 2003 [cit. 2011-05-16]. CROSS SITE SCRIPTING (XSS) - průvodce (nejenom) hackera. Dostupné z WWW: <http://www.pooh.cz/a.asp?id=2002598&db=>.

[87] *Mbank.cz* [online]. 2011 [cit. 2011-05-16]. MPeníze. Dostupné z WWW: <http://www.mbank.cz/osobni/mpenize/#tabs=2>.

[88] *Nearfieldcommunicationsworld.com* [online]. 2011 [cit. 2011-05-06]. Czech banks and supermarket to test NFC with Telefónica O2 . Dostupné z WWW: <http://www.nearfieldcommunicationsworld.com/2011/03/31/36771/czech-banks-and-supermarket-to-test-nfc-with-telefonica-o2/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	Triple Data Encryption Standard
ACS	Access Control Server
AES	Advanced Encryption Standard
AVV	Accountholder Authentication Value
BPIN	Bank Personal Identification Number
BPT	Bankovní Platební Tlačítka
CA	Certifikační Autorita
CAVV	Cardholder Authentication Verification
CD	Compact Disk
CPU	Central Processing Unit
CVM Result	Cardholder Verification Method Results
CVR	Card Verification Results
CVV	Card Verification Value
DDA	Dynamic Data Authentication
Diffie-Hellman	Název asymetrické šifry
DKIM	Domain Keys Identified Mail
DNS	Domain Name System
DPA	Differential Power Analysis
EEPROM	Electrically Erasable Programmable Read Only Memory
ElGamal	Název asymetrické šifry
EMV	Europay, MasterCard and VISA standard
EP	Elektronické peněženky
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FSA	Financial Services Authority
GSM	Global System for Mobile Communications
HASH	Algoritmus pro transformaci vstupních dat
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IAD	Issuer Application Data
IB	Internet Banking
ICC	Integrated Circuit Card
ID	Identity
IDEA	Název symetrické šifry
IEC	International Electrotechnical Commission
IP	Internet Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
IVR	Interactive Voice Response
MAC	Message Authentication Code

MD5	Algoritmus pro transformaci vstupních dat
MITM	Man In The Middle
MPI	Merchant Plug-In
NFC	Near Field Communication
PC	Personal Computer
PCMCIA	Personal Computer Memory Cards International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PVC	Polyvinylchlorid
RAM	Random Access Memory
RC2	Název symetrické šifry
RC4	Název symetrické šifry
RFID	Radio Frequency Identification
ROM	Read Only Memory
RSA	Název asymetrické šifry
S/MIME	Secure/Multipurpose Internet Mail Extensions
SDA	Static Data Authentication
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPA	Simple Power Analysis
SSL	Secure Sockets Layer
SW	Software
TAN kód	Transaction Authentication Number
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCAF	Universal Cardholder Authentification Field
UCVV	Unique Card Verification Value
URL	Uniform Resource Locator
USB	Universal Serial Bus
WAP	Wireless Application Protocol
WTLS	Wireless Transport Layer Security
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK