Útoky na platební systémy

Jan Krhovják, Marek Kumpošt, Václav Matyáš, FI MU

V předchozích příspěvcích jsme se seznámili se základními mechanizmy autentizace/autorizace a s jejich bezpečným nasazením v reálných (zejména bankovních) systémech. Mnohdy jsme se však zmiňovali, že korektní implementace či začlenění těchto mechanizmů do systému není až tak jednoduchá a přímočará, a že jakákoliv (byť jen nepatrná) chyba může vést k různým útokům a zneužití systému. V tomto příspěvku se tedy zaměříme právě na existující nedostatky současně používaných metod.

1 Analýza a identifikace nedostatků současných metod

Jak již bylo naznačeno v předchozích článcích, existuje celá řada bezpečnostních problémů, které se týkají jak používaného hardwaru a jeho softwarového vybavení, tak i používaných komunikačních protokolů. Je proto snaha celou situaci s bezpečností takovýchto zařízení držet na vysoké úrovni, což mají za úkol některé existující normy a standardy (FIPS 140-1, 140-2, právě vyvíjená 140-3, případně pak také např. Common Criteria). Tím se však ani zdaleka neřeší všechna rizika.

Při běžném používání čipové karty nebo kryptografického tokenu je totiž v cestě celá řada autorit a institucí, kterým je třeba bezvýhradně věřit. Od počátečního výrobce, jemuž je nutné důvěřovat, že se nedopustil žádných chyb (ať už záměrných nebo náhodných) v návrhu, přes autora aplikace, která na takových kartách poběží a bude zpracovávat důvěrné informace, dále pak přes inicializaci dat na tokenu až konečně k fázi předpersonalizace a personalizace. Teprve v tento okamžik se karta s jejím obsahem dostává ke koncovému uživateli a další bezpečnost závisí na tom, jakým způsobem s ní bude on zacházet.

Většina bezpečnostních procesů a metod se v současné době zabývá zejména zajištěním co nejmenšího rizika při průchodu kryptografického zařízení výše uvedeným řetězcem autorit a samotnému používání karty pak není věnována pozornost na potřebné úrovni. Přitom z pohledu uživatele je právě fáze vlastního provozu karty tím nejdůležitějším bodem, kdy většinou ručí za veškeré operace s jeho tokenem provedené.

Při práci s počítačem a v něm uloženým kryptografickým materiálem si uživatelé zvykají na ukládání privátních klíčů v bezpečných úložištích, ať už jde o (speciální) USB tokeny, čipové karty nebo o využívání nově nastupující technologie *trusted computing* [4] a souvisejících služeb.

V bankovním sektoru je situace jiná. Z historického hlediska je možné rozlišovat dvě různé možnosti autorizace finančních transakcí pomocí platebních karet. Jedna, založená na klasických ručně psaných podpisech, bývala výhradně určena při platbách u obchodníků; druhá, za použití PINu, zase při výběrech hotovosti z bankomatů. Během tohoto období si uživatelé zvykli používat různá bezpečnostní měřítka při autorizaci – bankomat byl a stále bývá považován za bezpečné prostředí, zatímco u obchodníka se při autorizaci podpisem očekávalo, že případné zfalšování podpisu půjde vždy dodatečně prokázat.

Postupem času, zejména s nástupem EMV čipových karet [5], se však začala situace měnit. A to nejen v České republice, ale i po celé Evropě. Autorizace plateb se i u obchodníků začíná provádět čím dál častěji pouze za pomoci platební karty a odpovídajícího uživatelova PINu, což s sebou přináší další problematický bod, kterým je prokazování neoprávněných transakcí a zodpovědnosti bank za sporné platby. U podpisů totiž bylo možné nechat znalecky ověřit zfalšovaný podpis a často pak prokázat, že uživatel platební karty neprovedl autorizaci vlastnoručně. Vyzrazení nebo ukradení PINu a jeho následné zneužití někým jiným než právoplatným vlastníkem karty je však zpětně jen velmi obtížně prokazatelné.

V tomto bodě se liší i přístup amerických a evropských bank k odpovědnosti za sporné platby. Zatímco banky v USA se v případě elektronického bankovnictví musí řídit tzv. „Regulation E", kdy za všechny platby ručí banky a v případě pochybností je jejich povinností prokázat, že se uživatel dopustil podvodu, v evropském bankovnictví

je tomu přesně naopak. Veškeré platby, u kterých je pochybnost, jsou připsány na vrub vlastníkovi a ten pak musí prokazovat, že je neprovedl on. Odpovědnost je pak na straně uživatele (typicky, neprokáže-li jinak), nebo obchodníka (byla-li platba autorizována prokazatelně falešným podpisem).

Je tedy v nejvyšším zájmu uživatele kryptografického tokenu ochránit se před jeho zneužitím, identifikovat možné zdroje potenciálních rizik při prováděných operacích a efektivně jim předejít. To samozřejmě vyžaduje alespoň základní povědomí uživatele o existujících rizicích a útocích, které jsou pro daný systém relevantní. V následujících částech se proto také změříme na některé typy útoků, které do značné míry závisí i na samotných uživatelích (jejich chování, obezřetnosti či manipulaci se systémem).

2 Útoky z pohledu uživatelů

Podívejme se tedy nejprve na nejběžnější útoky se kterými se může uživatel (resp. zákazník banky) v dnešní době při realizaci (bezhotovostních) plateb či transakcí setkat.

Asi nejrozšířenějším druhem podvodu, při kterém je od uživatele získána důvěrná informace, je *phishing*. Útok probíhá tak, že uživateli je doručena zpráva, která ho jménem důvěryhodné instituce žádá o osobní informace. Toto je obvykle provedeno e-mailovou zprávou, ale v poslední době jsou stále častěji využívány systémy umožňující přenos digitalizovaného hlasu (VoIP – Voice over Internet Protocol). V prvním případě je uživatel vyzván k navštívení stránek např. své banky, aby změnil přihlašovací informace ke svému účtu – daná stránka je ovšem stránka vytvořená útočníkem, která je obvykle obtížně rozeznatelná od originálních stránek. Ve druhém případě je využíváno sociální inženýrství přes telefon, ve kterém je uživatel vyzván k návštěvě stránek, které mohou nápadně připomínat stránky organizace, jejíchž služeb využívá. Uživatel v domnění, že komunikuje s důvěryhodnou institucí, předává např. autentizačnímu formuláři své identifikační údaje. Útočník tak získá citlivé údaje, které později velmi pravděpodobně zneužije pro neoprávněný přístup.

Novějším a mnohem důmyslnějším útokem je pak *pharming*. Ten staví – namísto na sociálním inženýrství – na manipulaci DNS záznamů a je tak v principu vlastně obdobou DNS spoofingu. Cílem útočníka je automatické přesměrování uživatele na vlastní stránky, které mohou být replikou stránek bankovních institucí a sloužit tak např. k získávání přihlašovacích údajů zákazníka. V horším případě pak mohou sloužit také jako jakýsi prostředník mezi uživatelem a skutečným systémem internetového bankovnictví – ten pak například korektně přeposílá pouze autorizační údaje, zatímco informace vztahující se k samotné transakci (číslo účtu, velikost převáděné částky) již mohou být zmanipulovány útočníkem.

Spyware je druh programu, který je spuštěn takovým způsobem, že o něm uživatel nemá tušení. Úkolem spywaru je sbírat informace o činnosti uživatelů. Do počítače se dostává např. v podobě trojského koně – škodlivého kódu přibaleného k jinému programu. Díky rozšířenosti operačního systémů Windows s webovým prohlížečem Internet Explorere je snazší psát i šířit spyware, stačí se zaměřit na chyby v těchto programech. Příkladem budiž „útok hackerů na Komerční banku" v roce 2006, kdy trojský kůň pravděpodobně posloužil ke krádeži desítky přístupových certifikátů a hesel k elektronickému bankovnictví a následně ke krádeži peněz z postižených účtů. Novějším příkladem jsou trojské koně typu „Sinowal" zobrazující podvržené stránky internetbankingu SERVIS 24 (Česká spořitelna). Problémem spywaru je, že je velice obtížné předcházet jeho „získání" a je třeba pravidelně kontrolovat stav počítače; pozitivní zprávou je relativně snadné odstranění spywaru z počítače.

Útok pomocí tzv. *libanonské smyčky* (viz obrázek 1) spočívá ve vhodném umístění části nařízнuté pásky videokazety do štěrbiny pro vkládání platební karty v bankomatu. Pokud je karta vložena, zadrží ji páska tak, že ji bankomat není schopen dále zasunout ani vysunout. K oběti se přiblíží útočník a poradí jí opětovné vložení PINu, který odpozoruje. Jakmile oběť odejde problém reklamovat, vytáhne útočník kartu z bankomatu a s pomocí zjištěného PINu z karty

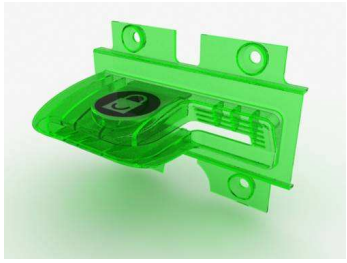
odcizí požadované peníze ještě před zablokováním karty.

Obrázek 1: Libanonská smyčka.

Skimming je útok, jehož cílem je zkopírovat magnetický proužek platební karty. Ke zkopírování magnetického proužku může dojít buď ve čtečce umístěné u vstupu do prostoru bankomatu nebo ve čtečce umístěné přímo na bankomatu samotném (viz obrázek 2). Útočník např. umístí na bankomat repliku klávesnice (resp. PINpadu), která v sobě zaznamená zadané PINy. Replika klávesnice je na bankomatech doplněna speciálním „nástavcem" na štěrbinu, do které se vkládají platební karty a která je nerozeznatelná od součástí bankomatu. Útočník po získání informací velmi jednoduše vyrobí kopie platebních karet, které může použít k výběru hotovosti v bankomatech. K odpozorování PINu pak lze kromě výše zmíněné falešné klávesnice využít například i poblíž nainstalované kamery.

Obrázek 2: Kryt s falešnou čtečkou.

V současné době právě kvůli tomuto typu útoků mnohé české banky instalují ochranná zařízení (FDI – Fraudulent Device Inhibitor) pro štěrbinu na vkládání karty do bankomatu (viz obr. 3). Pro neinformované zákazníky však takto vyvstává problém rozhodnout, zdali se jedná o zařízení banky či zařízení útočníka.



Obrázek 3: Ochranný nádstavec.

Alternativně také může útočník PIN odpozorovat přímo při jeho zadávání v libovolném místě prodeje a poté platební kartu zcizit (obtížností odpozorování se zabýval experiment popsaný v další části).

3 Experiment zabývající se autorizacemi bezhotovostních plateb

V letech 2005–2006 proběhl na Fakultě informatiky MU (FI MU) experiment zaměřený na bezpečnost plateb kartami v „kamenných" obchodech za fyzické přítomnosti karty a jejího držitele. Cílem experimentu bylo zjistit:

1. Jak obtížné je odpozorovat PIN, který zadává zákazník v obchodě při platbě platební kartou.
2. Jak snadno lze napodobit cizí podpis při autorizaci platby podpisem.

Celý experiment byl rozdělen do dvou fází, kdy první z nich proběhla na jaře 2005 v knihkupectví P. Marečka na FI MU a druhá část ve skutečném supermarketu v Brně v březnu 2006. Detailní popis průběhu experimentu lze nalézt v [1].

3.1 Výsledky experimentu

Co se týče autorizace pomocí PINu, tak zde je zřejmé, že solidní kryt klávesnice velmi přispívá k bezpečnosti při zadávání PINu s ohledem na možného pozorovatele, který není přímo vedle zákazníka, který PIN zadává. Nicméně zatím je stále poměrně velké procento terminálů vybaveno PINpadem bez ochranného krytu nebo neúčinným krytem (viz obr 4).

Co se týče korektně odpozorovaných číslic PINu, tak porovnání úspěšnosti v obou fázích je 60 % a 42 %, což není veliký rozdíl. Co se týče celých

Obrázek 4: Srovnání krytů PINpadů.

PINů, v první fázi se podařilo korektně odpozorovat celkem 18 ze 32 PINů (56,25 %) a ve druhé fázi pouze 4 z 20ti zadaných PINů (20 %).

Velký rozdíl jsme pozorovali v podpisové části, kde v druhé fázi experimentu nebyl odhalen jediný (!) zákazník falšující podpis někoho jiného, zatímco v první fázi experimentu bylo odhaleno 70 % falešných podpisů. Částečně si to vysvětlujeme tím, že obchodník v první fázi experimentu měl zkušenosti s prací v klenotnictví, kde se platí obecně řádově vyšší částky než v běžném supermarketu a podpisům se proto věnuje vyšší pozornost. Naše domněnka, že možná v supermarketu provádějí důkladnější kontrolu až v okamžiku, kdy částka za nákup přesáhne určitou hodnotu, se bohužel nepotvrdila. Celkově lze tedy říci, že při ztrátě karty stačí tomu, kdo ji nalezne, cca 20 minut na nacvičení podpisu a má téměř stoprocentní šanci, že v běžném supermarketu nebude odhalen. Jedinou ochranou jsou v tomto případě kamerové systémy v supermarketech

3.2 Shrnutí

Z výsledků experimentu je zřejmé, že autorizace podpisem, která v současné době převládá ve většině obchodů, není příliš bezpečná a v případě ztráty karty může velmi rychle dojít k jejímu zneužití. Ovšem zlepšení úrovně důslednosti ověření podpisu alespoň při platbě vyšších částek může nejen zabránit přímým ztrátám obchodníků, ale také částečně ochránit majitele inkriminovaných účtů.

Co se týče autorizace PINem, tak zde je situace v případě ztráty výrazně lepší, ovšem v případě cílené krádeže jen minimálně. V případě falšování podpisu stačí útočníkovi pouze karta – v případě autorizace PINem musí útočník nejprve úspěšně odpozorovat PIN a pak získat platební kartu. To je jen o něco málo složitější – ovšem se zpochybněním transakce to bude právě naopak! Při zvážení obtížnosti reklamace transakce se správně zadaným PINem je tedy na místě otázka, zda z pohledu nezapomětlivého držitele karty (tzn. zohledňujícího především otázku krádeže) není karta pro platby s autorizací PINem méně výhodná.

V každém případě lze jen doporučit volbu takové platební karty, u které lze okamžitě provést zablokování při zjištění její ztráty. Případně pak karty takové, kterou je možno dočasně blokovat nezávislým způsobem, např. kanálem GSM bankovnictví.

4 Bezpečnost PIN-mailerů

Položme si však nyní otázku, zdali je odpozorování PINu jediná možnost jak může útočník k PINu přijít. Mnohé banky své zákazníky nabádají, aby si svůj PIN po přečtení zapamatovali, obálku s PINem zničili a hlavně PIN nikdy a nikde nezapisovali. Útočníkovi tak již nezbývá mnoho možností, kde jinde PIN získat; a protože PIN je po vygenerování vytištěn tzv. *PIN-mailerem* přímo do zapečetěné obálky, tak by k němu neměli mít přístup ani bankovní pracovníci ani nikdo na cestě mezi bankou a zákazníkem. Zdali je však PIN v obálkách skutečně bezpečně ukryt před potenciálním útočníkem, to bylo předmětem našeho dalšího experimentu.

Jedním z kroků při zakládání účtů a vydávání platebních karet (nezbytných pro druhou fázi předcházejícího experimentu) bylo i získání obálek s odpovídajícími PINy. Protože část platebních karet vyžadovala při bezhotovostních transakcích autorizaci PINem, byli jsme také nuceni část těchto obálek otevřít. Inspirováni článkem [2] z roku 2005, který popisuje nedostatečnou bezpečnost PIN-mailerů využívajících laserového tisku, rozhodli jsme se ověřit situaci u České spořitelny, u níž jsme si v rámci výše zmiňovaného experimentu nechali založit účty a vydat karty. Přečtení PINů z prvních šesti uzavřených obálek

však bylo (i s běžně dostupnými zdroji světla) natolik snadné, že jsme se po dalších úvahách rozhodli zhodnotit situaci i v dalších třech českých bankách.

Před vlastním popisem provádění a výsledků našich testů ještě připomeňme, že koncem roku 2006 došlo k napadení několika účtů v internetovém bankovnictví Komerční banky. To vedlo u většiny ostatních bank k revizím stávajících bezpečnostních opatření, které mnohdy zahrnovaly např. zákaz zasílání platebních karet poštou. Z několika vhodných kandidátů jsme proto záměrně zvolili banky, které ještě umožňovaly zaslání karty nebo obálky s PINem (ideálně však obojího) poštou. Pokud byla u těchto bank v ceně standardního účtu nabízena také aktivace Telebankingu či Internet-bankingu, provedli jsme ji rovněž, čímž jsme obvykle získali další obálky s PINy či hesly.

Naším cílem nebylo poukázat na slabiny konkrétních PIN-mailerů – jejich typy jsme neznali a ani jsme po nich nepátrali. Tímto se již zabývali autoři [2], a jejich závěry byly výrobcům PIN-mailerů a postiženým britským bankám známy ještě půl roku před zveřejněním (v listopadu 2004). Naším záměrem bylo spíše ukázat, jakou mají útočníci (mezi které řadíme i pracovníky na pobočkách bank) šanci s běžně dostupnými prostředky nepozorovaně zcizit citlivé údaje – a zda se tedy téměř po třech letech od zveřejnění problému s PIN-mailery a po půl roce od napadení několika účtů přes internetové bankovnictví (a následné revizi bezpečnostních opatření mnoha bank) situace nějak zlepšila.

4.1 Provedení a výsledky

Celkem jsme testovali PIN-mailery používané čtyřmi českými bankami: Česká spořitelna, eBanka, GE Money Bank, HVB Bank. Z první banky jsme měli k dispozici pět obálek s PINy k platebním kartám a z ostatních tří bank jsme měli vždy po dvou obálkách. U druhé a třetí banky jsme měli také po dvou obálkách s přihlašovacími údaji pro Internet-banking a u čtvrté banky po dvou obálkách s přihlašovacími údaji pro Tele-banking. K prosvěcování obálek jsme použili běžně dostupných zdrojů světla – největší úspěchy jsme zaznamenali s klasickou kapesní svítilnou a s LED diodami. K prvnímu úspěšnému prosvícení obálky (a následnému úspěšnému přečtení PINu) dokonce posloužila běžná optická počítačová myš (!).

Banka 1 – Česká spořitelna

K dispozici jsme měli pět obálek (všechny zaslány poštou) s PINy k platebním kartám, k jejichž vytvoření byl použit PIN-mailer využívající laserového tisku. Prosvěcovaní a zjišťování PINů zde patřilo k nejsnazším, obálky obsahovaly pouze jeden list papíru s vytištěným PINem. Celkově (včetně obálky) bylo tedy nutno prosvítit tři listy papíru (s černým krytím vždy pouze z jedné strany) a správně přečíst PIN. Celý úkol nám výrazně usnadnilo, že jsme již z předchozí analýzy (otvírání prvních šest obálek) věděli, kde je PIN umístěn – tj. že se nachází v oblasti obdélníkového červeného razítka. Úspěšnost útoku byla 100%, všech pět PINů bylo přečteno bez jediné chyby. K prosvěcování se nejvíce osvědčily LED diody – byla použita klasická optická počítačová myš (červené světlo) nebo čelovka (bílé světlo) obsahující tři takové diody. Se znalostí umístění PINu bylo jeho přečtení v tomto případě natolik snadné, že to do dvou minut (a opět se 100% úspěšností) zvládli i dva naprostí začátečníci. S trochou tréninku k jeho přečtení dokonce nebyla nutná ani absolutní tma – stačilo pouze dostatečné přítmí, např. v pootevřené zásuvce stolu.

Banka 2 – eBanka

Zde jsme testovali čtyři obálky – dvě s PINem ke kartám a dvě s přihlašovacími údaji pro Internet-banking. První dvě obálky byly zaslány poštou, druhé dvě obálky bylo nutno převzít na pobočce a otevřít je. Ve všech čtyřech případech byl použit průklepový tisk na samostatný prostřední list. U prvního typu obálek byly dokonce čtyři vrstvy černého krytí, u druhého typu pak opět pouze tři vrstvy.

V tomto případě nevedlo prosvěcování obálek s PINy k platebním kartám k žádným výsledkům, avšak u přihlašovacích údajů pro Internet-banking jsme již zaznamenali částečný úspěch. Ze čtyř vytištěných PINů (každá obálka obsahovala dva) se nám podařilo jeden PIN přečíst úplně a další s jedinou chybou. U zbylých dvou PINů

jsme si byli vědomi, že jsme vždy jednu číslici nepřečetli, ale ze zbylých šesti jsme tři přečetli správně.

Důvodem úspěšného přečtení těchto PINů bylo použití modrého podkladu, na němž byly PINy vytištěny. Je však třeba poznamenat, že prosvěcování a úspěšné přečtení PINu již vyžadovalo značné soustředění a také poměrně velkou tmu.

Banka 3 – GE Money Bank

K analýze jsme opět měli čtyři obálky – dvě s PINem ke kartám (zaslány nedoporučeně poštou) a dvě s přihlašovacími údaji pro Internet-banking (vyzvednuty na pobočce). V prvních dvou případech byl použit opět průklepový tisk na samostatný prostřední list a na obálce byly čtyři vrstvy černého krytí. Námi prováděnými technikami nebylo možno PIN zjistit.

U druhého typu obálek byl použit laserový tisk a pouze dvě ochranné vrstvy černého krytí. Přístupové heslo k Internet-bankingu bylo vytištěno přímo na vnitřní straně obálky a navíc ještě výrazně větším písmem. Jeho přečtení proto při prosvícení obálky nečinilo žádné problémy. Díky výše popsaným technikám (technologie tisku, umístění PINu, velikost fontu) bylo jeho přečtení ještě snazší než přečtení PINu z obálek České spořitelny.

Banka 4 – HVB Bank

I v tomto případě jsme k testování měli čtyři obálky – dvě s PINem ke platebním kartám (zaslány poštou) a dvě s přihlašovacími údaji pro Tele-banking (vyzvednuty na pobočce). V prvních dvou případech byl použit laserový tisk. Kromě standardních dvou vrstev černého krytí byla na prostředním listu použita speciální černá odnímatelná krycí vrstva nalepená na průhledné fólii. PIN byl vytištěn z druhé strany průhledné fólie a pravděpodobně měl být čitelný pouze po odstranění odnímatelné krycí vrstvy. To se však po otevření obálky nepotvrdilo – PIN šel přečíst i bez odstranění černé fólie. Zjišťování hodnoty PINu prosvěcováním uzavřené obálky bylo v tomto případě poměrně obtížné, ale i přesto se nám podařilo jeden PIN určit přesně a u druhého jsme nedokázali přečíst jen první číslici.

U druhého typu obálek byl použit průklepový tisk s dvěma vrstvami černého krytí. Kromě zjištění, že bylo vytištěno sedm řádků textu a určení pozice a délky PINu se však bez znalosti obsahu obálky nedalo nic s jistotou přečíst. Po otevření obálky se ukázalo, že prvním řádkem textu byl skutečně šestimístný PIN a zbylých šest řádků překvapivě odpovídalo jeho číslicím zapsaným slovy. To však umožňuje útočníkovi ke zjištění/upřesnění hodnot číslic PINu využít také znalost délky jejich slovního zápisu (jak jsme již uvedli výše, tu lze při použití průklepového tisku snadno určit). Navíc celý PIN lze, s výjimkou číslic dvě a devět (které je možné snadno odlišit na základě jejich délky), jednoznačně určit pouze na základě prvního písmene slovního zápisu. Toto počáteční písmeno je navíc vždy velké a dá se proto částečně rozpoznat. S pomocí znalosti délky slovního popisu je možné proces rozpoznání prvního písmene značně ulehčit.

I přes všechna výše uvedená tvrzení se při experimentu ukázalo, že přesné určení všech číslic PINu zůstává poměrně obtížné. Redundance v podobě slovního zápisu číslic PINu však rozhodně není z bezpečnostního hlediska příliš žádoucí.

Dále zmiňme, že HVB banka umožňuje stále zaslání PINu i karty poštou – platební kartu je však nutno před prvním použitím aktivovat. Bohužel tato banka poštou zasílá i embosované karty a dává tak útočníkovi šanci získat (přežehlit) údaje vyryté na kartě. Stačí použít jen kousek papíru a obyčejnou tužku. Útok lze při použití klasické tuhy provést řádově během desítek sekund (a nezáleží ani, která strana karty je kopírována) a při použití hrany dřevěné tužky obarvené červenou barvou během jednotek sekund (zde již je třeba mít kartu správně otočenou embosovanou stranou nahoru). Zkopírované údaje pak mohou lehce posloužit k vytvoření padělku embosované karty. Zasílání platební karty poštou umožňuje také eBanka – nikoli však embosovaných. Nepovedlo se nám ji k tomu přinutit ani tím, že jsme zažádali o zaslání elektronické karty a později pak o změnu typu karty na embosovanou.

4.2 Shrnutí

Provedené útoky prosvěcováním patřily k těm zcela nejjednodušším – ostré světlo LED diod (např. použitá počítačová myš) se ukázalo vhodně k prosvěcování obálek tištěných laserovým tiskem, klasická kapesní svítilna se ukázala vhodnější k prosvěcování obálek tištěných průklepovým tiskem. Každý čtenář špionážní literatury jistě zná i účinnější postupy. Počet vrstev černého krytí u laserového tisku také nehrál nijak zásadní roli a útoky příliš neztížil. Použití speciálních technik, jakými je např. odnímatelná krycí vrstva, také nemělo žádný výrazný efekt. Přidání redundantních informací či barevného podkladu naopak některé útoky spíše usnadnilo. Stejně tak je pro útočníka příznivý i fakt, že všechny banky tisknou PIN vždy na stejné místo (což je dle našeho soudu pouze softwarový problém).

Během návštěvy bank jsme také zpozorovali další zdánlivě nenápadné a nevýznamné bezpečnostní problémy. Mnohé z nich – zmiňme například dodatečně neautorizovanou změnu seznamu příjemců plateb a vzorů platebních příkazů v systémech České spořitelny či eBanky – lze odhalit i s minimálním vhledem do problematiky; jejich popis lze nalézt v [3].

5 Závěr

Je známý fakt, že žádný systém není absolutně bezpečný, ale rozumné úrovně bezpečnosti lze vždycky nějakým (mnohdy ne příliš levným) způsobem dosáhnout. Bohužel banky často volí cestu kompromisů, tváří se, že právě ony absolutní bezpečnosti ve svých systémech dosáhly a skutečné bezpečnostní problémy a incidenty důsledně tají. Pokud se na veřejnost nedostane nějaká informace o bezpečnostních rizicích či útocích na jejich systémy, tak se banky předhánějí v informování klientů, že právě jejich banka již problém vyřešila (či právě řeší).

Nelze samozřejmě předpovědět, zda se přístup bank k bezpečnosti změní k lepšímu, ale dobrým signálem je, že mnozí klienti bank již bezpečnosti začínají přikládat vyšší váhu, a může u nich hrát dokonce roli při volbě banky.

Literatura

[1] Matyáš Václav, Kumpošt Marek, Krhovják Jan. *Platby kartou s použitím PINu.* Data Security Management (DSM), roč. 2006, č. 5, ISSN 1211–8737.

[2] Bond Mike, Murdoch Steven, Clulow Jolyon. *Laser-printed PIN Mailer Vulnerability Report.* 2005. Dostupné na: `http://www.cl.cam.ac.uk/~mkb23/research/PIN-Mailer.pdf`.

[3] Krhovják Jan, Kumpošt Marek, Matyáš Václav. *Jsou PINy zasílány bankami bezpečně?* Data Security Management (DSM), roč. 2007, č. 3, ISSN 1211–8737 *(přijato k otištění)*.

[4] *Trusted Computing Group*. Dostupné na: `http://www.trustedcomputinggroup.org/`.

[5] *EMVCo website.*. Dostupné na: `http://www.emvco.com/`. □