a tzv. telefonní kód. V ostatních případech ještě navíc tzv. connect ID. Tyto citlivé informace lze získat jen přímo na pobočce banky.

Bank of China (*Hong Kong*) umožňuje kromě jména a hesla využít také certifikátů uložených na USB tokenu nebo čipové kartě, používá i jednorázová hesla zasílaná pomocí SMS. Souběžná přihlášení z více počítačů nejsou povolena.

Canara Bank India – autentizační údaje jsou pouze uživatelské jméno, heslo a TAN. Podobně je na tom také *Standard Bank Group South Africa* a *Stockland Australia*, uživatelské heslo lze zadat také pomocí virtuální grafické klávesnice (stejně jako je tomu u Servisu24 České spořitelny).

Bank of Baroda India nabízí svým zákazníkům mobile banking a internet banking. Autentizačními údaji jsou opět pouze uživatelské jméno a heslo. V případě mobile bankingu je možno účet ovládat pouze z jediného (zaregistrovaného) telefonního čísla.

3.6 Útoky na platební transakce z pohledu uživatelů

V této části se zaměříme na některé typy útoků, jejichž úspěch či neúspěch do značné míry závisí i na samotných uživatelích (na chování, obezřetnosti či manipulaci se systémem).

3.6.1 Nejčastější typy útoků

Phishing je druh podvodu, při kterém je od uživatele získána důvěrná informace. 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 je stále častěji využívány i VoIP (*Voice over IP*) systémy. V prvním případě je uživatel vyzván k navštívení stránek např. své banky, aby změnil přihlašovací informace ke svému účtu. Ona stránka je ve skutečnosti podvržena útočníkem, je ale obvykle věrnou kopií originální stránky např. dané banky. Ve druhém případě je využíváno sociální inženýrství přes telefon, ve kterém je uživatel vyzván k návštěvě stránek, které opět mohou téměř k nerozeznání 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, kdy se bude vydávat za oklamaného uživatele.

Mnohem sofistikovanějším útokem je pak *pharming*, který, namísto sociálního inženýrství, staví na manipulaci s DNS (Domain Name System) záznamy, a je tak v principu vlastně obdobou DNS spoofingu. Cílem útočníka je automatické přesměrování na své 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 – takový prostředník 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 prohlížečem Internet Explorer je psaní i šíření spywaru snazší, stačí se zaměřit na chyby v těchto programech. Viz „útok hackerů na KB" v roce 2006, kdy trojský kůň pravděpodobně posloužil ke krádeži desítky přístupových certifikátů a hesel k elektronickému bankovnictví a následně krádeži peněz z postižených účtů; či nové trojské koně „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 *libanonské smyčky* spočívá ve vhodném umístění části pásky videokazety do štěrbiny pro vkládání platební karty do 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 blokací karty.

Skimming je útok, jehož cílem je *zkopírovat magnetický proužek platební karty*. Ke zkopírování magnetického proužku může dojít buď ve snímači ovládajícím vstup do prostoru bankomatu nebo ve snímači umístěném přímo na bankomatu samotném (viz obrázek). 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.

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

3.6.2 Experiment zabývající se autorizacemi bezhotovostních plateb

V letech 2005 a 2006 proběhl na Fakultě informatiky Masarykovy univerzity (FI MU) experiment zaměřený na bezpečnost plateb kartami v „kamenných" obchodech za fyzické přítomnosti karty a jejího držitele. Celý experiment byl rozdělen do dvou částí, kdy první z nich proběhla na jaře 2005 v knihkupectví P. Marečka na FI MU (obr. 10) a druhá část v roce 2006 v jednom z brněnských supermarketů. Cílem experimentu bylo zjistit:

Obr. 10: Prostředí knihkupectví P. Marečka

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

První fáze experimentu

Této fáze se zúčastnilo 32 studentů bakalářského a magisterského programu (nakupujících), 7 studentů doktorského programu (někteří z nich pozorovali studenty při zadávání PINů, ostatní v knihkupectví vytvářeli dojem náhodných zákazníků) a 3 koordinátoři experimentu (posílání studentů do knihkupectví, měření času potřebného k provedení transakce a zaznamenávání nahlášených pozorování).

Popišme nejdříve průběh první fáze experimentu, tj. pozorování zadávaných PINů. Pro tuto fázi jsme zvolili dva PINpady – jeden bez tzv. bezpečnostního krytu a druhý s masivním krytem (viz obr. 11). Studenty jsme rozdělili do dvou skupin (17 z nich použilo PINpad s masivním krytem a zbylých 15 potom PINpad bez krytu). Výsledky jsou vyhodnoceny pro každou skupinu zvlášť, aby byl patrný rozdíl v úspěšnosti odpozorování PINů a vliv ochranného krytu kláves.

Obr. 11: PINpady s krytem a bez krytu

Každý student dostal platební kartu – v této části experimentu se jednalo o nefunkční čipové karty a terminály nebyly nijak zapojeny. Po příchodu do knihkupectví si student vybral knihu a poté provedl simulovanou platbu kartou. Na tomto místě je potřeba zdůraznit, že studentům byl pravý smysl experimentu utajen, abychom zajistili jejich přirozené chování. Skutečná podstata experimentu byla odhalena až po skončení první fáze.

Co se týče pozorovatelů při zadávání PINu, nejednalo se o žádné trénované „profíky". Pozorovatelé byli zejména doktorandi a nácvik s maketou PINpadu trval maximálně 2 hodiny pro každou fázi experimentu.

Výsledky, které jsme získali v první fázi jsou následující (nejprve uvádíme výsledky pro *PINpad s krytem*):

- z celkově nahlášených 39 čtyřmístných PINů (tj. 156 číslic) bylo úspěšně odpozorováno 75 číslic (48 %);
- pozorovatelům se podařilo úspěšně odpozorovat 6 ze 17 zadaných PINů (35,5 %);
- v pěti případech byl PIN odpozorován přesně (tj. na zadání PINu stačí jeden pokus); v posledním případě by tři pokusy stačily na uhodnutí správného PINu.

Výsledky pro druhý (tj. *bez krytu*) PINpad:

- z celkově nahlášených 45 čtyřmístných PINů (tj. 184 číslic) bylo úspěšně odpozorováno 129 číslic (70,1 %);
- pozorovatelům se podařilo úspěšně odpozorovat 12 z 15 zadaných PINů (80 %);
- pouze ve dvou případech by na zadání správného PINu bylo potřeba více pokusů (maximálně 3); ostatní PINy byly odpozorovány zcela přesně (!).

V druhé části první fáze experimentu dostalo 15 studentů kartu, kterou sami podepsali svým vlastním podpisem a 17 studentů dostalo již podepsané karty. Úkolem druhé skupiny bylo naučit se (v čase 20–30 minut) co nejlépe tento podpis napodobit a pokusit se s kartou provést úspěšnou autorizaci. V knihkupectví byl k dispozici skutečný obchodník, který prováděl ověření a věděl, že se někteří studenti budou snažit napodobit cizí podpis. Na tomto místě je vhodné podotknout (vzhledem k pozdějším výsledkům s podpisy), že tento obchodník má zkušenosti z práce v luxusním klenotnictví, kde se za zboží platí mnohem vyšší částky než v běžných obchodech, a proto byla kontrola podpisů velice důkladná. Tuto skutečnost vnímáme jako největší příčinu značných rozdílů zjištěných v obou fázích experimentu (v knihkupectví na FI a v supermarketu).

Výsledky z podpisové části experimentu:

- Obchodník odhalil 12 ze 17 falešných podpisů – pouze 5 z nich akceptoval jako korektní (tj. 29,4% úspěšnost úspěšné autorizace cizím podpisem);
- z 12 odhalených studentů bylo 8 odhaleno po prvním podpisu (25 %) a 4 poté, co je obchodník požádal o opakované podepsání (12,5 %);
- celkem bylo úspěšně ověřeno 20 studentů (15 těch, co podepisovali sami sebe a 5 falešných) – z nich 16 (50 %) po prvním podepsání a 4 (12,5 %) po druhém podepsání.

Z výsledků první fáze experimentu jsme usuzovali, že vzhledem k podmínkám, které jsme měli, je autorizace podpisem z pohledu zákazníka bezpečnější než autorizace zadáním PINu. Dále jsme zjistili, že dobrý ochranný kryt klávesnice pro zadávání PINů má

na úspěšnost odpozorování PINu vliv. Protože jsme si však byli vědomi přísnosti verifikace podpisu a také jsme chtěli získat ještě jednu nezávislou sérii výsledků, přikročili jsme po složitých přípravách ke druhé fázi experimentu.

Druhá fáze experimentu

Druhá fáze experimentu se odehrála v jednom brněnském supermarketu; šlo o to, abychom dosáhli reálných podmínek jak pro zákazníky, tak i pro týmy pozorovatelů. Pro zajištění reálných podmínek bylo třeba zařídit velké množství věcí. Prvním krokem bylo zajištění skutečných platebních karet. Byly proto založeny účty v bance a k těmto účtům byly vystaveny platební karty. Při první návštěvě jsme při otestování, zda daný typ karty vyžaduje jeden ze dvou typů autorizace, zjistili fakt, že i při autorizaci zadáním PINu je nutné se podepsat – ale také to, že podpis je kontrolován jen zběžně.

Dále bylo potřeba zajistit dostatečné množství „zákazníků“. Požádali jsme proto naše rodinné příslušníky, známé a několik studentů, zda by se našeho experimentu zúčastnili – s tím, že jsme jim neuvedli pravý cíl experimentu. Místo toho jsme jim řekli, že se podílejí na testech bezpečnosti supermarketu, v žádném případě ale nevěděli, že budou při zadávání PINu pozorováni. Bylo nutné zajistit naprosté utajení skutečné podstaty experimentu – o té vědělo jen několik lidí z FI MU a vedení supermarketu (pokladní u přepážek ani ostraha v obchodě o probíhajícím experimentu nevěděli – vedení supermarketu skutečně chtělo prověřit mj. i své vlastní bezpečnostní procedury). V neposlední řadě jsme také podnikli náležité organizační a právní kroky pro ochranu „zákazníků“.

Druhé fáze experimentu se celkem zúčastnilo cca 50 lidí – 20 „zákazníků“, 15 pozorovatelů, další osoby, které instruovaly „zákazníky“, dohlížely na průběh experimentu atd. Velmi důležité bylo, aby z naší strany nedošlo k ohrožení ani omezení ostatních zákazníků, kteří nebyli zapojeni do experimentu.

„Zákazník“ byl po svém příchodu znovu informován, že probíhá testování bezpečnostních procedur v supermarketu a že se snažíme zjistit pohled zákazníků na bezhotovostní transakce pomocí platebních karet. Pro navození ještě lepšího dojmu byl „zákazníkům“ předložen stručný dotazník zjišťující jejich zkušenosti s online platbami. V okamžiku, kdy šel „zákazník“ nakupovat, byl „aktivován“ tým pozorovatelů, který zákazníka sledoval až k pokladně a pokusil se odpozorovat zadávaný PIN. V supermarketu operovaly celkem tři týmy pozorovatelů. Část PINpadů z druhé fáze experimentu také nedisponovala ochranným krytem (viz obr. 12).

Obr. 12: PINpad z druhé fáze experimentu (bez ochranného krytu)

Poté, co proběhla tato část experimentu, jsme provedli platby autorizované podpisem. Podpisy napodobovali zejména pozorovatelé a několik osob z předchozího kola, které se chtěly zúčastnit i této části. Každý dostal podepsanou platební kartu a měl cca 20 minut na nácvik podpisu. Následně dostal „zákazník" hotovost pro případ odmítnutí platby kartou a šel nakupovat. Nakonec ohlásil, zda byl podpis akceptován nebo nikoliv.

Výsledky první části experimentu – *platby kartami autorizované PINem*:

- celkem jsme od pozorovatelů měli nahlášeno 26 tipů na 4místný PIN (bylo nahlášeno 91 číslic), z čehož 38 číslic bylo odpozorováno správně (42 %);
- úspěšně (tj. na tři pokusy by se podařilo odhalit správný PIN) byly odpozorovány 4 PINy z celkových 20 (20 %);
- 3 ze 4 odpozorovaných PINů byly zadány na terminálu s ochranným krytem;
- další 3 odpozorované PINy byly uhodnutelné do 10 pokusů a další 3 potom do zhruba 200 pokusů. Ostatní pozorování by správný PIN odhalila po více než 1000 pokusech.

Zajímavé je též vyhodnocení úspěšnosti v rámci týmu jako celku:

- první tým správně odpozoroval 25 % číslic (6 z 24 nahlášených),
- druhý tým správně odpozoroval 27 % číslic (9 ze 39 nahlášených),
- třetí tým správně odpozoroval 68 % (!) číslic (23 ze 34 nahlášených).

Není překvapivé, že právě třetí tým odhalil zmiňované 4 PINy. Jeden z jeho členů v sobě objevil nevídaný talent a dařilo se mu pozorovat „zákazníky" z natolik dobrých pozic, že nevzbudil žádné podezření.

Výsledky druhé části experimentu – *platby kartami autorizované podpisem*:

- tato část experimentu byla zastavena po 17 úspěšných nákupech z celkových 17 pokusů (100% úspěšnost!),
- žádný „zákazník" nezaznamenal problémy při placení, nikdo nebyl požádán o zopakování podpisu,
- někteří „zákazníci" si všimli, že pokladní kontrolují podpisy velmi zběžně nebo dokonce vůbec (!).

Shrnutí výsledků obou fází experimentu

Co se týče autorizace pomocí PINu, je zřejmé, že solidní kryt klávesnice velmi přispívá k bezpečnosti při zadávání PINu s ohledem na možného, mírně vzdáleného pozorovatele. Nicméně zatím je stále poměrně velké procento terminálů vybaveno PINpadem bez ochranného krytu nebo neúčinným krytem.

Co se týče korektně odpozorovaných číslic PINu, porovnání úspěšnosti v obou fázích je 60 % a 42 %, což není veliký rozdíl. Co se týče celých PINů, v první fázi se podařilo korektně odpozorovat celkem 18 ze 32 PINů (56,25 %) a ve druhé fázi pouze 4 z 20 zadaných PINů (20 %).

Velký rozdíl jsme pozorovali v podpisové části, kde v druhé fázi experimentu nebyl odhalen jediný (!) zákazník falšující cizí podpis, zatímco v první fázi experimentu bylo odhaleno 70 % falešných podpisů. Částečně si to vysvětlujeme tím, že obchodník v první fázi experimentu pracuje v klenotnictví, kde se platí i řádově vyšší částky než v běžném supermarketu. Naše domněnka, že v supermarketu možná provádějí důkladnější

kontrolu až v okamžiku, kdy částka za nákup přesáhne určitou hodnotu, se nepotvrdila. Celkově tedy lze říci, že při ztrátě karty stačí nálezci 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.

Závěry a dovětek

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, je zde 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 (tzn. zohledňujícího především otázku krádeže) klienta 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 nemilé skutečnosti, že karta už není tam, kde by být měla – a samozřejmě maximalizovat pravděpodobnost rychlého zjištění této skutečnosti. Případně pak volit karty takové, kterou je možno dočasně blokovat nezávislým způsobem, např. kanálem GSM bankovnictví.

3.6.3 Bezpečnost PIN-mailerů a další aspekty autentizace

PIN-mailer je zařízení určené k tisku dokumentů s citlivými informacemi, obvykle PINy. Jeho realizace, tj. způsob tisku a provedení obálky, by měla znemožnit zjištění obsažené informace bez poškození této obálky. Jak je tomu v praxi? V této části vycházíme z [KKM07].

Součástí přípravy experimentu popisovaného v předchozí části bylo i založení několika bankovních účtů a vydání potřebných platebních karet. S těmito kartami se pak prováděly jednotlivé nákupy zboží, kdy se ověřovala bezpečnost autorizace prováděných plateb.

Cíle testování

Jedním z kroků při zakládání účtů a vydávání platebních karet 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 [BMC05] z roku 2005, který popisuje nedostatečnou bezpečnost PIN-mailerů využívajících laserového tisku, rozhodli jsme se ověřit situaci u banky, u níž jsme