Autorizace finančních transakcí PINem nebo podpisem?

Vašek Matyáš, Dan Cvrček,
Jan Krhovják, Marek Kumpošt
Masarykova univerzita, Brno

Autentizace finančních transakcí

- Chip&PIN vs. podpis
  - Věříme ve zvýšení ceny nutné pro výrobu padělků
  - Nebyli jsme si jisti, zda eliminuje *příležitostné* zloděje
    - Zloděj (nebo malá skupina zlodějů) ukradne karty a následně padělá podpis nebo odpozoruje PIN a ukradne karty
- Hlavní otázky
  - Je pro zloděje jednodušší zneužít karty s technologií Chip&PIN nebo ty, co vyžadují podpis držitele?
  - Různé pohledy různých subjekty
  - Cílem bylo experimentálně ověřit naše domněnky

Vlastní experiment

- Dvě fáze
- První fáze „nanečisto“
  - Byla provedena v částečně realistických podmínkách v univerzitní knihovně (Masarykova univerzita, FI)
    - věk nakupujících mezi 18 až 26 lety – studenti
    - čas pro nacvičení podpisu – 30 minut
    - čas pro nacvičení pozorování PINu – 2 hodiny
- Druhá fáze
  - Byla provedena v reálném obchodě
    - velký supermarket v Brně
    - podmínky experimentu byly stanoveny na základě zkušeností z první fáze

Příprava první fáze experimentu

- Několik místností
  - Místo pro simulované nákupy – knihkupectví
  - Místnost A pro lidi, kteří půjdou nakupovat
  - Místnost B pro lidi, kteří provedli nákup

- Celkem se zúčastnilo cca 40 lidí
  - 32 zákazníků
  - 4 útočníci-pozorovatelé PINů
  - 3 okolostojící
  - 3 koordinátoři experimentu
  - majitel knihkupectví
  - obchodník, který běžně pracuje s plat. kartami

Normální chování nakupujících?

- Zákazníci nevěděli skutečnou podstatu experimentu => bylo jim řečeno, že testujeme uživatelskou přívětivost bezhotovostních plateb…
- Každý účastník vyplnil dotazník týkající se „zástěrky“
  - Otázky zjišťující se časů potřebných pro autorizaci podpisem, resp. PINem…
  - …uživatelská přívětivost, zkušenosti
- Část týkající se falšování podpisu byla účastníkům sdělena po části s PINy
- Účastníkům bylo řečeno, že budou vyplňovat další dotazníky po experimentu, skutečnost ale byla jiná…

Vyhodnocení dotazníků

- Vedlejší efekt – 32 vyplněných dotazníků
- 25 z 32 účastníků využívají karty s magnetickým proužkem
- ½ účastníků někdy použila kartu s čipem

- Celková spokojenost (1 – nejlepší, 5 – nejhorší)
  - Karty s mag. proužkem/podpis – 3,4
  - Smart karty/PIN – 2,5

- Maximální čas pro dokončení transakce (možnosti 10, 20, … 50 sec.)
  - 21 s

- Celková úspěšnost transakcí
  - 89 % bez problémů, 7,5 % drobné problémy, 2 % velké problémy, < 2 % neúspěšné

První kolo - PINy

- Dva PINpady =>
  - Dvě skupiny zákazníků (17/15)
  - První PINpad byl s masivním ochranným krytem
- Průběh nákupu
  1. Zákazník přišel do obchodu (kde byly jiní „zákazníci“, pozorovatelé a „křoví“), vybral si a zaplatil zboží
  2. Zákazník odešel z obchodu
  3. Pozorovatelé nahlásili své tipy (každé číslici mohli přiřadit váhu 0-2)
  4. Koordinátor měřil čas (kvůli „zástěrce“)
  5. Do obchodu přišel další zákazník
- Otázka nedůvěryhodných obchodníků
  - Poměrně snadné, např. CCTV namířených na PINpady
  - V obou fázích experimentu bylo toto jen ad hoc posuzováno

Druhé kolo – podpisy

- Dvě skupiny zákazníků
  - 15 zákazníků si kartu podepsalo svým podpisem
  - 17 zákazníků dostalo podepsanou kartu
    - V místnosti B měli 20-30 minut na nácvik
- Průběh – obchodník je zvyklý přijímat karty
  - V místnosti B zákazník dostal kartu se svým/cizím podpisem
  - Obchodník ověřil podpis – identifikoval podvodníky
  - Obchodník věděl, že se zákazníci budou podvádět, ale nevěděl kolik z nich to bude
- Poznámka: Zákazníci i koordinátoři se shodli, že ověřování podpisů bylo příliš důkladné – což bohužel není v běžných obchodech pravidlem

Výsledky prvního kola – PINpad1

- Pozorovatelé uspěli v 6 ze 17 PINů (35,3 %)
  - Vzájemná spolupráce pozorovatelů
  - 5 ze 6 PINů zcela přesně (83,3 %)
    - 3 PINy odpozorovány 2 pozorovateli
    - 2 PINy odpozorovány 1 pozorovatelem
    - 1 PIN zrekonstruován společně
- Z celkových 39 nahlášených pozorování – (tj. 156 číslic)
  - 75 číslic bylo pozorováno úspěšně (48 %)

Výsledky prvního kola – PINpad2

- Pozorovatelé uspěli v 12 z 15 PINů (80 %)
  - Vzájemná spolupráce pozorovatelů
  - 10 z 12 PINů zcela přesně (83,3 %)
    - 2 PINy odpozorovány 4 pozorovateli
    - 1 PIN odpozorován 3 pozorovateli
    - 4 PINy odpozorovány 2 pozorovateli
    - 3 PINy odpozorovány 1 pozorovatelem
    - 2 PINy zrekonstruovány
- Z celkových 46 nahlášených pozorování – (tj. 184 číslic)
  - 129 číslic bylo pozorováno úspěšně (70,1 %)

Výsledky druhého kola - podpisy

- Obchodník detekoval 12 ze 17 padělaných podpisů
  - 5 cizích podpisů bylo přijato (29,4 %)
- Z 12 detekovaných
  - 8 detekováno při prvním podepsání (25 %)
  - 4 detekování při druhém podepsání (12,5 %)
- Z 20 (15+5) přijatých podpisů
  - 16 přijato při prvním podpisu (50 %)
  - 4 přijaty při druhém podpisu (12,5 %)
- 8 zákazníků (25 %) bylo požádáno o zopakování podpisu
  - Verifikace podpisů byla velmi důkladná!!!
  - Jeden zákazník při druhém podpisu vzdal ☺
  - Průměrná doba verifikace – 36 s.

Příprava druhé fáze experimentu

- Skutečné platební karty
  - 5 pro první kolo – pozorování PINů
  - 6 pro druhé kolo – falšování podpisů
- Nutné právní kroky pro ochranu uživatelů karet
- Pouze několik lidí vědělo o experimentu
  - Tým z Fakulty informatiky
  - Vedoucí obchodu, bezpečnostní manager, obsluha kamerového systému
- Nikdo z pokladních ani ostraha v obchodě o experimentu nevěděla
- 20 lidí – zpravidla příbuzných se zúčastnilo jako „zákazníci“
- Celkem 15 lidí bylo „na druhé straně“…

Prostředí v obchodě

- Místnost pro instruování zákazníků
- Bylo nám umožněno použít libovolnou z určených pokladen (s ohledem na to, zda byla otevřena nebo ne)
- 1. kolo
  - Tři skupiny pozorovatelů, každá pracovala nezávisle a v daném čase vždy pouze jedna skupina
  - Dohled – pro případ, že by došlo k problémům a dohled na to, že je pozorován správný zákazník
- 2. kolo
  - Zákazníci si nacvičili cizí podpis a provedli nákup
  - Po nákupu nahlásili, zda ověření podpisu proběhlo úspěšně nebo nikoliv

Výsledky prvního kola – PINy

- 13 pozorování na krytém a 7 na nekrytém PINpadu
- Pozorovatelé uspěli ve 4 z 20 PINů (20 %)
  - Společná znalost
  - 3 PINy z krytého a jeden z nekrytého PINpadu
- 3 pozorování – správný PIN do 10 pokusů
- 3 pozorování – správný PIN do 222 pokusů
- Z celkových 26 nahlášení 4-místného PINu (91 nahlášených číslic)
  - 38 číslic bylo odpozorováno správně (42 %)

Výsledky prvního kola – PINy (2)

	první fáze	druhá fáze
PIN – ochranný kryt	6 ze 17 PINů (35%)	3 ze 13 PINů (23%)
PIN – bez krytu	12 z 15 PINů (80%)	1 ze 7 PINů (14%)
Počet správně odpozorovaných čísel	**60%**	**42%**
Správné odpozorované číslice podle pozorovatelů		25%, 27%, **68%**

- Jedna skupina byla vysoce aktivní a jejím členům se dařilo pozorovat zákazníky z výhodných pozic
  ➔ nejlepší výsledky

Pozorování PINů v reálných podmínkách

- Úspěšnost 68 % pro třetí tým (23 z 34)
  - Tento tým odpozoroval 4 PINy správně (na maximálně 3 pokusy)

- Nejlepší pozice pro pozorování je ve frontě přímo před a přímo za pozorovanou osobou
  - Pozice pozorovatelů za pokladnami (tito pozorovatelé předstírali činnost brigádníků) se ukázala jako nevýhodná (jejich pozorování nebylo při vyhodnocování bráno v úvahu)

Výsledky druhého kola - podpisy

- 10-30 minut pro nácvik podpisu
- 20 „zákazníků“ – většina z nich byly pozorovatelé z prvního kola
- Druhé kolo bylo zastaveno po 17 úspěšně ověřených podpisech
- V průběhu druhého kola nebyl nahlášen žádný problém při ověřování
- Nikdo nebyl požádán o zopakování podpisu
- Některé podpisy byly kontrolovány velmi zběžně nebo vůbec!
- V obchodě není stanovena hranice pro důkladnější kontrolu podpisu (např. když je částka > 1000 kč…)

Shrnutí obou fází

- Ochranný kryt klávesnice je užitečný, nicméně
  - Většina PINpadů jej nemá
  - Slabé (málo efektivní) kryty v obchodech
  - Někteří zákazníci mohou mít problémy při použití PINpadu s masivním krytem
- Správně odpozorované číslice PINu (60 % a 42 %)
- Značný rozdíl při detekci falešných podpisů (70 % vs. 0 %) – prostor pro zlepšení
- Pozorovatelé a osoby falšující podpisy byly začátečníci – byla to jejich první práce tohoto druhu… ☺

Názory a spekulace

- Pečlivost kontroly podpisu je odlišná
  - V různých zemích
  - V různých obchodech (v téže zemi)
- „Profesionální“ zneužití karet je mnohem důležitější než náhodné zneužití
  - Platí dnes – co v budoucnosti?
- Dočasné opatření (?)
  - Použití jak PINu tak podpisu
  - Různé PINy pro různé typy transakcí (v závislosti na částce)

Závěr

- Technologie Chip&PIN nezlepší bezpečnost zákazníků oproti náhodným zlodějům
  - Problémové odmítnutí falešné transakce
  - Pojištění karty a ověření vlastnictví je velmi důležité
- **Dobrý** ochranný kryt PINpadu
  - Pokladny v obchodech nejsou nejvhodnějším místem pro zadávání PINů
- Ověření na základě podpisu (ve standardním obchodě) je zcela nedostačující (jinak např. v klenotnictví)
- Pozorování PINů je poměrně podceňovaná oblast
  - Podobně i v jiných podmínkách, např. kanceláře

P.S.: Posílání PINů poštou..

- Bezpečnost PINů zasílaných poštou
- Impulzem byla snadnost prosvícení u ČS
  - 100% úspěšnost s běžným zdrojem světla
- Šance útočníků nepozorovaně zjistit citlivé informace
- Česká spořitelna, eBanka, GE, HVB Bank
- Celkově 20 obálek (zaslané poštou, některé nedoporučeně)
- Zdroje světla: kapesní svítilna, LED, optická myš

Česká spořitelna

- PIN mailer využívající laserového tisku
- Prosvěcování bylo nejsnazší
- V obálkách jeden list papíru s PINem
- Prosvícení třech papírů + dvě černé krytí
- Nebyla nutná absolutní tma
- I začátečník dosáhl 100% úspěchu
- Starší obálky – průklepový tisk, bez úspěchu (PIN vytištěn velmi slabě)
- Průklepový tisk – nerovnosti na obálce -> umístění do další (vnější obálky)

eBanka a GE Money Bank

- PIN, přihlašovací údaje pro iBanking
- Průklepový tisk (až 4 vrstvy krytí)
- Horší výsledky (1 ze 4 PINů)

- PINy – průklepový tisk, bez úspěchu
- iBanking – laserový tisk
  - Heslo vytištěno výrazně větším písmem
  - Přečteno zcela bez problémů

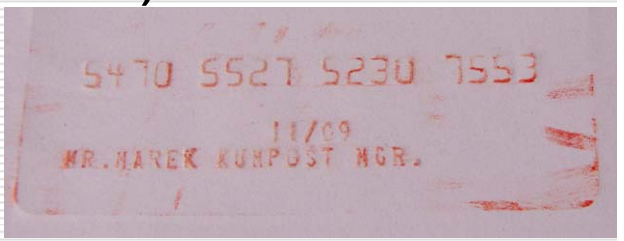
Heslo : Jsgdd7jX

HVB Bank

- PINy – laserový tisk, odnímatelná fólie
  - Jeden PIN (ze dvou) se podařilo přečíst
- Tele-Banking – průklepový tisk, dvě krytí
  - Určení pozice a délky PINu + 6 řádků textu
  - 6místný PIN + číslice zapsané slovně
  - Možnost zjištění PINu podle slovního zápisu nebo prvního (velkého) písmene
  - I tak je určení hodnoty PINu poměrně obtížné

Embosované karty a další pozorování

- Problém při posílání karet poštou (HVB)
  - Snadno lze získat informace z obálky
  - Vytvoření padělku karty



- Různé úrovně vyškolení personálu banky
  - GE – hodnota aktivačního kódu
  - HVB – změna limitů zasláním e-mailu
    - Žádné ověření e-mailové adresy
- ČS – autentizační SMS zprávy
  - Potvrzení převodu peněz, ale ne změn příjemců
- eBanka – social engineering např. při tel. hovoru

Závěr

- Banky nezareagovaly na publikované problémy PIN-mailerů
- Laserový tisk poskytuje menší ochranu
  - Dobré výsledky s ostrým světlem
  - Není nutná naprostá tma
- Průklepový
  - Dobré výsledky s kapesní svítilnou
  - Nutná naprostá tma
- Počet krycích vrstev nehrál významnou roli
- Redundantní informace o PINech ulehčují útoky
- Posílání embosovaných karet poštou zcela nevhodné
- Autentizační mechanizmy nutno aplikovat na veškeré operace

Děkuji za pozornost

Dotazy?