Bezpečnost internetového bankovnictví, bankomaty, platební karty

Úvod do kryptologie

Zdeněk Kabát

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

13. května 2010

PLATEBNÍ KARTY

Funkce platební karty dle zákona:

- Elektronický platební prostředek (nástroj pro přístup k účtu)
- Elektronický peněžní prostředek (nositel finanční hodnoty)

Tři kontrolní fáze při transakci:

- Ověření karty (její pravost jako taková)
- Ověření držitele (mám právo kartu používat)
- Autorizace transakce (požadovanou transakci lze provést)

OVĚŘENÍ KARTY

- Ověření bezpečnostních prvků přímo na kartě – možné jen u transakcí „tváří v tvář“
- Bezpečnostní kódy CVC/CVV (Card Verification Code / Card Verification Value):
  - CVx1: zakódován v magnetickém proužku – ověřuje, že data na proužku byla uložena vydávající bankou
  - CVx2: zadní strana karty vedle podpisu, používá se pro transakce bez přítomnosti karty (Internet, mail, fax, telefon)
  - např. obrana proti podvodným prodejcům (kopie magnetického proužku)
  - zákaz uchovávání kódů CVC/CVV (zákonem)
  - kódy generovány zašifrováním čísla karty, data platnosti a servisního kódu a převodem na 3- nebo 4-místné číslo

OVĚŘENÍ DRŽITELE

- Podpis – při některých transakcích na přepážce, u obchodníka
- PIN – autorizace u bankomatů a obchodníků
  - „Vynálezce“ Shephard-Barron, 1967 – 6-místné číslo, poté redukováno na 4 cifry kvůli manželce
  - Specifikace IBM 3624 – zašifrování čísla karty pomocí PGK (PIN Generation Key) $\Rightarrow$ „natural PIN“
  - Použití offsetu: uživatelský PIN $-$ natural PIN mod 10
  - Metoda VISA – PVV (PIN Verification Value): zašifrování 11 cifer čísla karty, hodnoty PVKI (PIN Validation Key Index) a uživatelského PINu pomocí PVK (PIN Validation Key)
  - VISA neověřuje přímo PIN, ale hodnotu PVV
  - Pravděpodobnost prolomení silou – cca 0,06%
- (Biometrická data – budoucnost)

AUTORIZACE TRANSAKCE A HROZBY

Autorizace transakce – provádí vydavatel karty

- Existence karty
- Platnost karty
- Transakční limity
- Finanční krytí transakce (kontrola zůstatku na účtu nebo úvěrového limitu)

Nejčastější hrozby podvodů

- Transakce ztracenou / odcizenou kartou
- Transakce padělanou kartou
- Transakce bez přítomnosti karty (s použitím dat z pravé karty, např. v e-commerce)

STANDARD PCI DSS

PCI DSS = Payment Card Industry Data Security Standard

- Celosvětový standard informační bezpečnosti
- Momentálně verze 1.2.1 ze sprna 2009
- Některé požadavky:
  - Instalace a udržování firewallu, bezpečnost hesel
  - Šifrované přenosy dat držitelů platebních karet
  - Omezení přístupu k datům jen na nutné minimum
  - Identifikace veškerých osob přistupujících k datům
  - Pravidelné testy bezpečnosti, antivirové testy atd.
- Bezdrátové sítě: požadavky změny SSID a defaultních hesel, použití protokolu WPA nebo WPA2 s ověřením 802.1X a šifrováním AES, archivace logů atd.

SYSTÉM 3-D SECURE

- 3-D Secure . . . protokol založený na XML sloužící k zabezpečení internetových transakcí platebními a kreditními kartami
- Online autentifikace založená na 3 doménách
  - Doména vlastníka (obchodník nebo banka, jíž platím)
  - Doména vydavatele (banka, která vydala kartu)
  - „Mezioperační“ doména (infrastruktura)
- Komunikace probíhá pomocí šifrovaného spojení SSL
- Zákazník je přesměrován na zabezpečené stránky vydávající banky – autorizace transakce např. pomocí čísla karty, data splatnosti a CVx2
- Obchodník nezíská žádné informace o platební kartě
- Útoky: např. sociální inženýrství, phishing

PROTOKOL SSL

Vrstva sloužící k šifrování a autentizaci komunikujících stran

- Klient pošle požadavek na SSL spojení s volbou šifrování:
  - Výměna klíčů: RSA, Diffie-Hellman, DSA, Fortezza
  - Symetrická šifra: RC2, RC4, IDEA, AES, DES, 3DES
  - Hašovací funkce: MD5, SHA
- Server potvrdí typ šifrování a zašle certifikát (obsahuje veřejný klíč a ověření autenticity serveru)
- Klient vygeneruje základ šifrovacího klíče, zašifruje veřejným klíčem serveru a pošle ho
- Server rozšifruje základ klíče a vygeneruje z něj hlavní šifrovací klíč, klient taktéž
- Klient a server potvrdí společný klíč a ustanoví zabezpečené spojení přes které dále komunikují

BANKOMATY

Zabezpečení bankomatů – pomocí PINu

- Data z čipu nebo magnetického proužku přenesena bezpečným kanálem bance
- Hardware Security Module – zašifruje 64 bitů příchozích dat pomocí 56-bit DES klíče $\Rightarrow$ 64 bitů zašifrovaných dat $\Rightarrow$ transformace na 16 bitů – srovnáno s 16-bit PVV

Úniky dat o kartě z bankomatů – hlavně „skimování“

- Bankomat je modifikován útočníkem: čtecí zařízení pro okopírování magnetického proužku a záznam PINu při zadávání uživatelem (kamera nebo falešná klávesnice)
- Součástí je paměťové médium pro záznam nebo přímé předávání dat na dálku
- Ochrana: např. rozvibrování karty nebo indikátor skimování

INTERNETOVÉ BANKOVNICTVÍ

Úrovně zabezpečení

(1) Zabezpečení pomocí hesla
- PIN, heslo
- Rizika: lidský faktor, nechráněné telefonní linky apod.

(2) Zabezpečení pomocí elektronického klíče
- Autentizační SMS kód pro přihlášení do IB, SMS kódy pro jednotlivé transakce
- Rizika: kopírovatelnost, fyzikální útoky

(3) Zabezpečení pomocí certifikátu
- Soukromý + veřejný klíč, kvalifikovaný certifikát (externí médium – USB disk, CD, lépe čipová karta)
- Rizika: minimální, jen při odcizení soukromého klíče

Komunikace pomocí protokolu SSL

Útoky: trojan, keylogger, phishing, hacking

ÚTOK: PHISHING

- Účel: získání osobních informací a jejich zneužití
- „Návnada“: e-mail – hrozící finanční ztráta, lákání na snadný zisk, potřeba ověřit majitele účtu, potřeba změn dat z bezpečnostních důvodů apod.
- Přesměrování na stránku, která je přesnou kopií přihlašovací stránky k IB (ale je to podrvh)
- Při zadání dat uživatelem získává útočník plný přístup
- Útočník často z exotických zemí – velmi náročné dohledání
- Ochrana: nepřecházet na IB z e-mailu, zadávat adresu pro IB ručně, autorizace transakce SMS kódem nebo certifikátem na čipové kartě, kontrola certifikátu

Děkuji za pozornost!