Bezpečnost internetového bankovnictví, bankomaty, platební karty

Jiří Šleis

Fakulta jaderná a fyzikálně inženýrská, ČVUT Praha

13.5.2013

OBSAH

INTERNETOVÉ BANKOVNICTVÍ

Zabezpečení internetového bankovnictví:

- Ověření identity banky.
- Ověření identity klienta.
- Autorizace plateb.
- Šifrování dat.

INTERNETOVÉ BANKOVNICTVÍ

Zabezpečení internetového bankovnictví:

- Ověření identity banky.

Identifikace banky

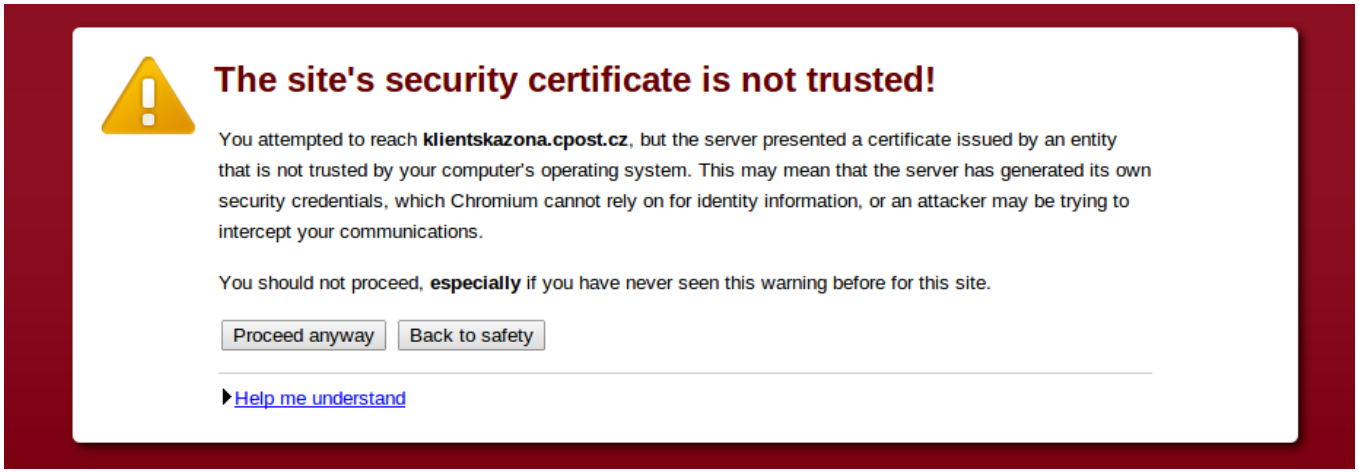
  - SSL certifikát,
  - vydán certifikační autoritou,
  - ověřuje webový prohlížeč.

- Ověření identity klienta.
- Autorizace plateb.
- Šifrování dat.

INTERNETOVÉ BANKOVNICTVÍ

Zabezpečení internetového bankovnictví:

- Ověření identity banky.



- Ověření identity klienta.
- Autorizace plateb.
- Šifrování dat.

INTERNETOVÉ BANKOVNICTVÍ

Zabezpečení internetového bankovnictví:

- Ověření identity banky.
- Ověření identity klienta.

Způsoby autentizace

- Uživatelské jméno a heslo,
- certifikát,
- čipová karta,
- SMS kód,
- PIN kalkulátor.

- Autorizace plateb.
- Šifrování dat.

INTERNETOVÉ BANKOVNICTVÍ

Zabezpečení internetového bankovnictví:

- Ověření identity banky.
- Ověření identity klienta.
- Autorizace plateb.

Kromě základní autentizace klienta

- Certifikát,
- čipová karta,
- SMS kód,
- PIN kalkulátor,
- denní limity transakcí.

- Šifrování dat.

INTERNETOVÉ BANKOVNICTVÍ

Zabezpečení internetového bankovnictví:

- Ověření identity banky.
- Ověření identity klienta.
- Autorizace plateb.
- Šifrování dat.

Protokol TLS

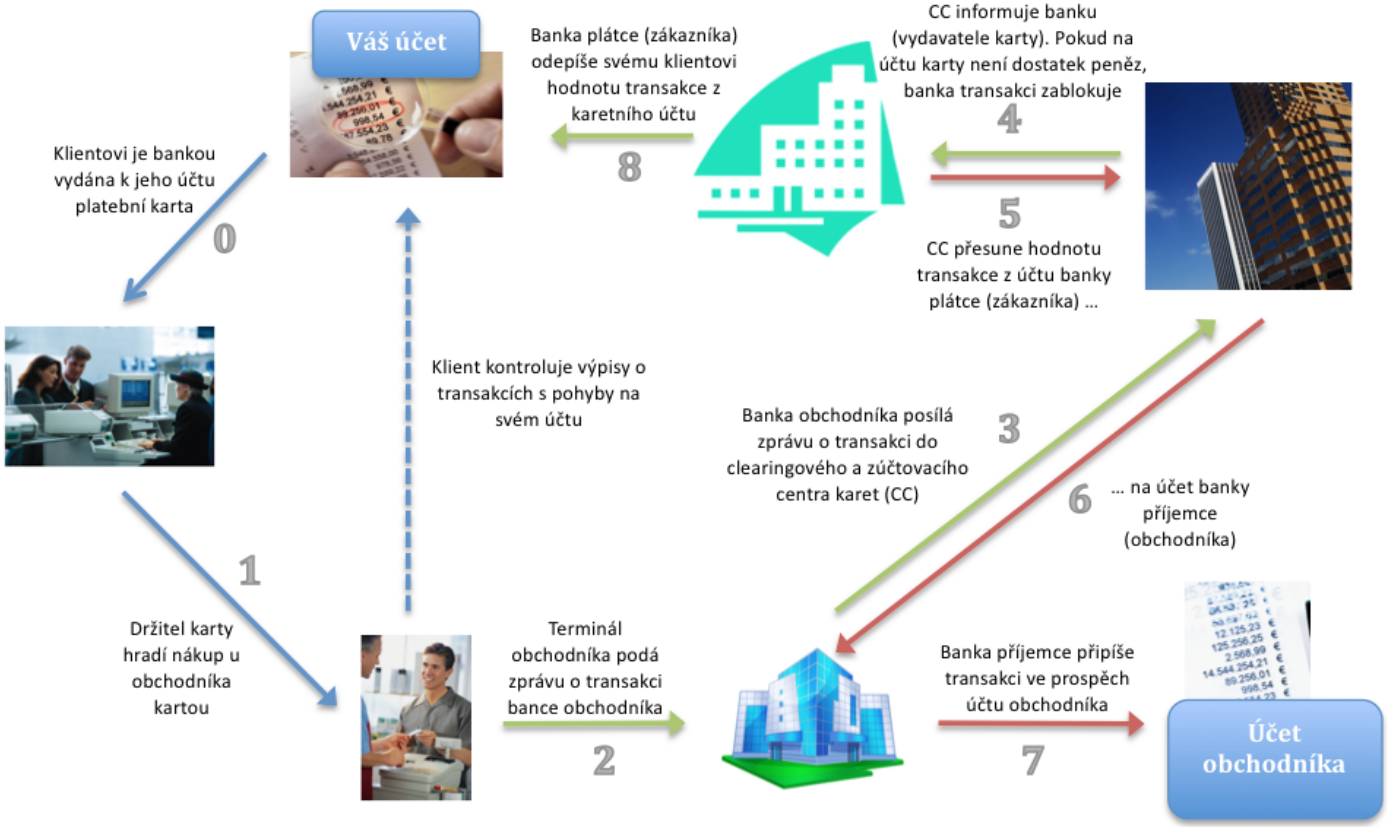
- užívání šifer AES, 3DES, RC4, . . .
- 128–256 bitové klíče,
- algoritmus RSA pro výměnu veřejných klíčů,
- hašovací funkce SHA-1 pro autentizaci.

INTERNETOVÉ BANKOVNICTVÍ

Možná nebezpečí:

- Přesměrování na podvržený server - phishing.
- Odposlech hesel - keylogger.
- Man in the middle.
- Hesla zálohovaná online.
- Proxy špionáž.

PLATEBNÍ KARTY



Obrázek: Průběh transakce platební kartou. Zdroj: `http://www.nenechsedojit.cz/platebni-karty`

PLATEBNÍ KARTY

Kontrolní fáze při transakcích:

- Ověření karty.
- Ověření zákazníka.
- Autorizace platby.

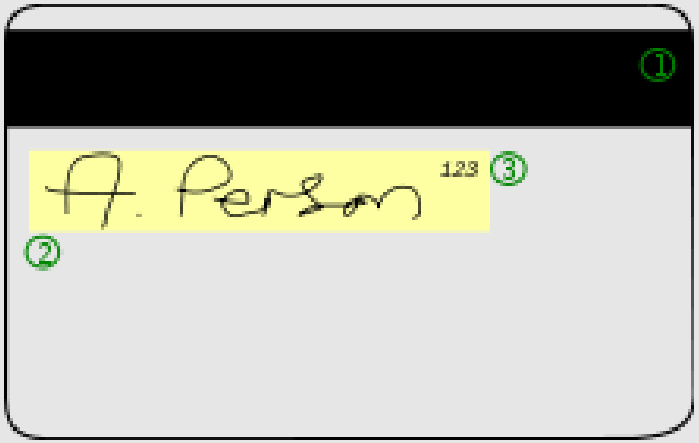
PLATEBNÍ KARTY

Kontrolní fáze při transakcích:

- Ověření karty.

Bezpečností prvky na kartě:

1. Magnetický proužek (zakódované informace).
2. Podpis majitele karty.
3. CVC2/CVV2 Card Verificaton Code (Value).



- Ověření zákazníka.
- Autorizace platby.

PLATEBNÍ KARTY

Kontrolní fáze při transakcích:

- Ověření karty.
- Ověření zákazníka.

V bance nebo u obchodníka:

  - Podpis majitele karty.
  - PIN/PVV (PIN Verification Value)

- Autorizace platby.

PLATEBNÍ KARTY

Kontrolní fáze při transakcích:

- Ověření karty.
- Ověření zákazníka.
- Autorizace platby.

Ověřování údajů:

- Existence karty.
- Platnost karty.
- Transakční limity.
- Zůstatek na účtu.

PLATEBNÍ KARTY

Platby na internetu - systém 3-D secure:

- Dodatečná bezpečnostní vrstva pro online transakce.
- Založen na XML, model 3 domén (obchodník, vydavatel karty, infrastruktura).
- **Obchodník nemá přístup k údajům o kartě**.
- Používání SSL spojení, přesměrování na webové stránky vydavatele karty.
- Možnost přidání dalších bezpečnostních prvků (heslo, autorizační SMS, . . .).

PLATEBNÍ KARTY

Možná nebezpečí:

- Odcizení karty + získání PIN.
- Znalost dat z karty - online transakce.
- Phishing.
- Padělání karty. ▸ Credit Card Skimming Operation

BANKOMATY

Výběr hotovosti z bankomatu:

- Dříve - identifikace karty z dat na magnetickém proužku.
- Dnes - použití bezpečnějších čipů.
- Bankomat vyžádá PIN.
- Šifrování PINu (algoritmus DES).
- Přenos zašifrovaných dat bance a zpět.

BANKOMATY

Možná nebezpečí.

- Okoukání PINu.
- Falešná klávesnice.
- Skimovací zařízení.
- Termokamera.
- Zalepení otvoru na kartu nebo hotovost.

Zdroje

- Jan Kuthan, Bezpečnost bank, část 1. - bankomaty. `http://goo.gl/jjlpG`, 2011.
- Kol.autorů, Wikipedia, the free encyklopedia. `en.wikipedia.org`, 2013.
- František Kučera, Je šifrování českých bank bezpečné, nebo je to jen iluze? `http://goo.gl/aUOq8`, 2010.
- Měšec.cz, Analýza zabezpečení internetového bankovnictví v České Republice. `http://goo.gl/1ymRt`, 2005.
- Kryptografie v praxi. `http://goo.gl/8MTXX`.

Děkuji za pozornost.