Bezpečnost internetového bankovnictví, bankomaty

Filip Marada, *filipmarada@gmail.com*

KM FJFI

15. května 2014

Obsah prezentace

Bezpečnost internetového bankovnictví

- Zabezpečení správy účtu
- Komunikace pomocí protokolu TLS

Používané úrovně zabezpečení

Zabezpečení prostřednictvím hesla

- Ověření přihlášení a transakcí prostřednictvím SMS zprávy
- Riziko: fyzický útok

Certifikátu v souboru nebo v čipové kartě

- Využití soukromého a veřejného klíče, certifikát externí
- Riziko: nízké

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

Ověření identity banky

- TLS certifikát
- Autorita vydávající certifikát
- Ověření webovým prohlížečem

- Ověření identity klienta
- Autorizace plateb
- Šifrování dat

- Ověření identity banky

Ověření identity klienta

- Uživatelské ID a heslo
- Certifikát
- PIN
- Jednorázový SMS kód

- Autorizace plateb
- Šifrování dat

- Ověření identity banky
- Ověření identity klienta

Autorizace plateb

- Certifikát
- Jednorázový SMS kód

- Šifrování dat

- Ověření identity banky
- Ověření identity klienta
- Autorizace plateb

Šifrování dat - Protokol TLS

- Protokol TLS (Transport Layer Security) pro komunikaci po síti zabezpečeně
- Vužívá šifer AES, 3DES, RC4,...
- Dále hash a MAC
- Certifikáty založeny na X.509

Protokol TLS

- TLS 1.0 = SSL 3.1.

Protokol TLS

- TLS 1.0 = SSL 3.1.
- TLS zabezpečená přihlašovací stránka
  - Data zašifrována před odesláním na server (https)

Protokol TLS

Průběh komunikace

- Klient a webserver si vymění své veřejné klíče pro asymetrické šifrování

Šifry

Protokol TLS

Průběh komunikace

- Klient a webserver si vymění své veřejné klíče pro asymetrické šifrování
- Asymetrickou šifrou si vymění klíč pro symetrickou komunikaci

Šifry

- RSA -pomalé

Protokol TLS

Průběh komunikace

- Klient a webserver si vymění své veřejné klíče pro asymetrické šifrování
- Asymetrickou šifrou si vymění klíč pro symetrickou komunikaci
- Výměna informací symetrickou šifrou

Šifry

- RSA -pomalé
- AES - rychlé

Protokol TLS

Průběh komunikace

- Klient a webserver si vymění své veřejné klíče pro asymetrické šifrování
- Asymetrickou šifrou si vymění klíč pro symetrickou komunikaci
- Výměna informací symetrickou šifrou
- Generování nového klíče pro symetrické šifrování

Šifry

- RSA -pomalé
- AES - rychlé

Protokol TLS

AES

- Bloková šifra (128 bit)

Protokol TLS

AES

- Bloková šifra (128 bit)
- Symetrický klíč (128, 196 nebo 256 bitů)

Protokol TLS

AES

- Bloková šifra (128 bit)
- Symetrický klíč (128, 196 nebo 256 bitů)
- Zatím bezpečný

Certifikát

```
Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting c
            OU=Certification Services Division,
            CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    Validity
        Not Before: Jul  9 16:04:02 1998 GMT
        Not After : Jul  9 16:04:02 1999 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
             OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@fr
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                e8:35:1c:9e:27:52:7e:41:8f
            Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
    92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
    ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
    d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
    0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
    5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
    8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
    68:9f
```

- Version: verze certifikátu
- Serial Number: sériové číslo certifikátu
- Signature Algorithm: označení algoritmu (ID)
- Issuer: vydavatel
- Validity: platnost
  - Not Before: nepoužívat před datem
  - Not After: nepoužívat po datu
- Subject: vlastník veřejného klíče
- Subject Public Key Info: informace o veřejném klíči vlastníka
  - Public Key Algorithm: algoritmus pro veřejný klíč
  - veřejný klíč (data)
- Issuer Unique Identifier: unikátní identifikátor vydavatele (volitelný)
- Subject Unique Identifier: unikátní identifikátor vlastníka (volitelný)
- X509v3 extensions: rozšíření (volitelné)
  - atd.
- Signature Algorithm: algoritmus pro certifikát (elektronický podpis)
- certifikát (elektronický podpis)

Možná rizika

- Phishing - sociální inženýrství: často jsou uživatelé prostřednictví podvodného emailu přesměrováni na kopii webu banky - tam zadají své přihlašovací údaje
- Man in the middle - nepoužívat veřejné hotspoty
- Keyloggery
- Bezdrátové klávesnice
- Cross site scripting

Bankomaty

Výběr z bankomatu

- Identifikace karty pomocí čipu - data přenesena zabezpečeným kanálem bance
- Zabezpečení použitím PINu
- Hardware Security Module - zašifruje 64 příchozích bitů pomocí 56-bit DES klíče, transformace na 16 bitů - srovnáno s 16-bit PVV

Bankomaty

Skimovací zařízení

- Zjistí PIN kód při běžném použití bankomatu (foto)
- Ve vstupu pro kartu - přečte data z magnetických platebních karet - uloží nebo posílá (např.: sms)
- Falešná klávasnice
- Mikrokamery
- Falešný bankomat

Bankomaty

Skimovací zařízení

Bankomaty

Skimovací zařízení

Bankomaty