Projekt 2 - Nejčastější chyby

Ing. Dominik Breitenbacher

ibreiten@fit.vutbr.cz

BRNO UNIVERSITY OF TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

Projekt 2 - Nejčastější chyby

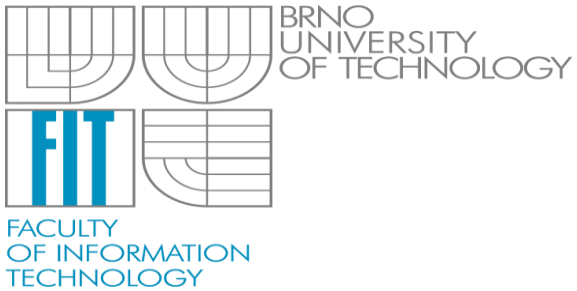
- Překlepy a interpunkce
- Estetika
- Kvalita obrázků
- Zdrojové kódy v textu
- Text nebyl rozdělen na kapitoly
- Slangové výrazy

Projekt 2 - Pozitiva

- Většina si naprogramovala nějakou faktorizační metodu
- V některých pracích se pracovalo s více než dvěma znaky při šifrování a dešifrování
- Také někteří volili větší prvočísla
- Osvěžil jsem si množství programovacích jazyků
  - VBA
  - Pascal
  - Delphi
  - C#
  - Python
  - ...

Úvod do Certifikátu a Certifikačních Autorit

Ing. Dominik Breitenbacher
ibreiten@fit.vutbr.cz
Mgr. Radim Janča
ijanca@fit.vutbr.cz



Proč PKI a certifikáty?

- K čemu asymetrická kryptografie?
  - Dodání identity (za předpokladu utajení privátního klíče)

- Jak zajistit jednoznačnou vazbu mezi osobou(subjektem) a jejím privátním/veřejným klíčem?
  - Zaslání emailem – bez autentizace nepoužitelné
  - Vytavení na server – bez autentizace nepoužitelné - spoofing
  - Osobní předání – použitelné v malé skupině
  - Předání třetí stranou – praktické ve velkých skupinách, třetí strana musí být důvěryhodná

- Jednotný způsob jak ukládat klíče a zajistit pravost
- Obsah certifikátu:
  - Verze certifikátu (x.509v1-3)
  - Sériové číslo certifikátu
  - Algoritmus podpisu (asymetrická šifra + hashovací funkce)
  - Vydavatel
  - Platnost – od\do
  - subjekt vlastník veřejného klíče
    - Algoritmus
    - Veřejný klíč
  - Elektronický podpis (podpis certifikátu vydávající CA)

Formáty certifikátů

- .DER – DER zakódovaný certifikát
- .PEM –DER certifikát zakódovaný pomocí base64, uzavřený mezi řádky "-----BEGIN CERTIFICATE-----" a "-----END CERTIFICATE-----"
- .P12 – PKCS #12, může obsahovat certifikát(y), veřejné i soukromé klíče (chráněno heslem)
- .crt – přípona ve windows, typicky obsahuje certifikát formátu PKCS #12

PKCS – Public Key Cryptography Standards

- PKCS #1 – RSA Cryptography
  - Šifrování a podpis algoritmem RSA
- PKCS #7 – Cryptography Message Syntax
  - Syntaxe zašifrované a podepsané zprávy
- PKCS #10 – Certification Request Syntax
  - Formát zpráv zasílaných certifikační autoritě s žádosti o certifikát pro veřejný klíč.
- PKCS #12 – Personal Information Exchange Syntax
  - Definuje formát souborů běžně použitých pro ukládání soukromých klíčů s odpovídajícími certifikáty veřejných klíčů, chráněných šifrováním založeným na hesle (symetrické šifrování).

- Organizace zajišťující vydávání a distribuci certifikátů
  - Svým privátním klíčem podepisuje vydávané certifikáty
- Udržuje CRL (Certificate Revocation List) / OCSP (Online Certificate Status Protocol)
- Součástí CA je tzv. Registrační Autorita
  - Stará se o přijímání žádostí o certifikát
  - Ověřuje žádosti (identitu žadatele)
- Od důkladnosti ověření RA a zabezpečení CA včetně vnitřních politik organizace se odvíjí její důvěryhodnost
  - Některé CA mohou požadovat pouze ověření identity přes internet – nízká důvěryhodnost certifikátu, ale i cena
  - Komplexní ověření žadatele – vyšší důvěryhodnost za vyšší cenu

Míra důvěryhodnosti

- Pouze jedinečnost vlastníka
  - lze získat i anonymně
  - typicky pouze pro testovací účely
- Identita vlastníka
  - vyžadujeme kontrolu identity třetí stranou
  - nevyžaduje se osobní kontakt
  - většinou notářské ověření
  - není příliš důvěryhodné
- Vlastník osobně navštívil CA
  - reálně se rozpadá na několik podtříd
  - musí být kontrola dokladu totožnosti
- Třída 3 + kontrola dalších informací v certifikátu
  - např. vlastník musí prokázat, že je jednatelem banky
  - kromě toho, že prokáže svoji totožnost

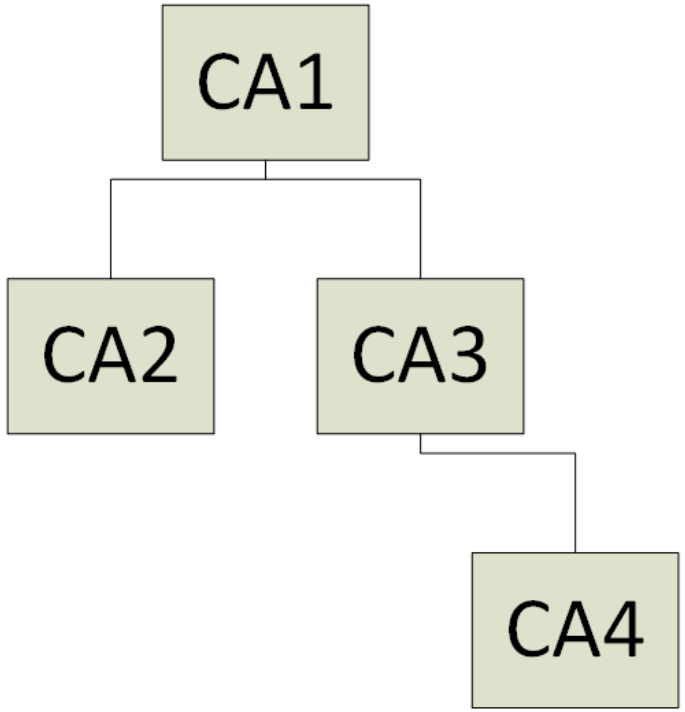
CRL – Certificate Revoke List

- Byl prozrazen soukromý klíč uživatele
- Změnil se zaměstnavatel uživatele (příslušnost uživatele), čímž je neplatné jméno obsažené v certifikátu
- Uživatel již nemá být certifikovanou CA
- Soukromý klíč CA byl kompromitován
- Uživatel porušil bezpečnostní pravidla CA

Stromová struktura CA

- Historie - předpoklad jedné CA distribuující pravomoci
- Realita – celá řada nezávislých CA

- Hierarchie CA
  - Geografického hledisko
  - Rozložení zátěže
  - Rozložení rizik



Příklad žádosti o certifikát

```
Certificate Request:
Data:
    Version: 0 (0x0)
    Subject:  C=CZ, ST=Czech Republic, L=Brno, O=VUT,
CN=JohnDoe/emailAddress=JohnDoe@vutbr.cz
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
            00:cb:76:51:6e:62:8d:0a:31:50:44:94:2d:37:12:
                3d:00:1f:da:7e:54:4b:ab:fb:a9:09:48:b8:d0:7e:
…
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
     1d:1f:05:5b:a5:8b:4b:a1:fe:48:61:a7:2f:c7:44:b9:c9:af:
     fd:97:c9:b9:41:95:b4:f5:cd:ce:f9:20:5b:a1:a4:5b:2c:27:
…
```

Příklad certifikátu

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            c2:29:ca:54:c8:c9:ee:41
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CZ, ST=Czech Republic, O=VUT, OU=testCA, CN=Moje testovaci CA/emailAddress=ijanca@fit.vutbr.cz
        Validity
            Not Before: Oct  6 18:01:01 2014 GMT
            Not After : Oct  6 18:01:01 2015 GMT
        Subject: C=CZ, ST=Czech Republic, L=Brno, O=VUT, CN=John Doe/emailAddress=JohnDoe@vutbr.cs
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:cb:76:51:6e:62:8d:0a:31:50:44:94:2d:37:12: …
            Exponent: 65537 (0x10001)

    Signature Algorithm: sha1WithRSAEncryption
        65:30:5f:f5:3e:24:d1:12:72:f2:ca:a5:0f:c2:ed:2c:2c:46: …
```

Děkuji za pozornost