DUM č. 17 v sadě

36. Inf-12 Počítačové sítě

Autor: Lukáš Rýdlo

Datum: 06.05.2014

Ročník: 3AV, 3AF

Anotace DUMu: bezpečnost sítí - digitální podpis, asymetrická kryptografie, certifikáty

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Počítačové sítě
Bezpečnost – digitální podpis

Zabezpečení dig. podpisem

- některé služby vyžadují rozpoznat uživatele
  - **autentizace** = identifikace osoby
  - **autorizace** =přidělení oprávnění provést činnost
  - př.: HTTPS protokol ověřuje identitu serveru, někdy chceme ověřit odesílatele e-mailu, ověření uživatele SSH
- občas je potřeba přenášená data šifrovat
  - je nutné najít způsob, jak distribuovat klíč k dešifrování, aby zprávu nemohl číst nikdo jiný než adresát

řešení: **Asymetrická kryptografie**

Certifikační autorita

Asymetrická kryprografie

- Pracujeme se dvěma klíči (hesly), které k sobě patří.
- Jeden klíč zašifrovává, druhý rozšifrovává (a naopak).
- **Privátní klíč** si hlídá vlastník a nikomu ho nikdy nedá.
- **Veřejný klíč** dá vlastník volně k dispozici komukoliv.
- Princip činnosti (šifrování dat):
  - Alice a Bob si chtějí poslat tajnou zprávu.
  - Oba si vytvoří privátní a k nim příslušné veřejné klíče.
  - Bob napíše zprávu a zašifruje ji veřejným klíčem Alice.
  - Alice obdrží zprávu a rozšifruje ji svým privátním klíčem, který nikdo jiný nevlastní a proto nikdo jiný zprávu nerozšifruje.

Jakým klíčem bude Alice šifrovat odpověď?

Digitální podpis

- využívá také privátní a veřejný klíč, ale opačně
- Jak se podepíše e-mail
  - je potřeba klient, který to umí
  - autor napíše zprávu, spočítá se speciální číslo (hash), které slouží jako stručný identifikátor obsahu
  - hash se spolu se jménem a příp. dalšími daty zašifruje pomocí privátního klíče
  - kdokoliv zprávu obdrží, může veřejným klíčem hash a jméno rozšifrovat
  - spočítá se hash znovu a pokud sedí, nebyla zpráva pozměněna
  - zbývá zjistit, zda je podpis pravý (tj, zda jsem uvedl své jméno)

Certifikační autorita…

Certifikační autorita

- důvěryhodná organizace, která vydává privátní a veřejné klíče pouze ověřeným osobám
- zavazuje se k zodpovědnosti za zkontrolování totožnosti toho, komu klíče vydala
- součástí klíče je elektronický podpis certifikační autority
- v programech jsou certifikáty autorit uložené, uživatel ale může importovat další

Rizika

- uživatel nesmí za žádnou cenu ztratit/zapůjčit privátní klíč
- klíče musí být dostatečně složité, aby nebyly uhodnutelné
  - dnes princip součinu velkých prvočísel, rozklad na prvočísla by trval příliš dlouho (hádání), ale pronásobení je rychlé (šifrování)
  - doufáme, že opravdu nikdo nedokáže součiny rozkládat rychle
- nikdy nesmíme ukládat neověřené certifikáty
  - při přístupu na web přes HTTPS se někdy prohlížeč ptá, zda chceme vstoupit na stránku s neznámým certifikátem…
- na cizích počítačích mohou být uložené různé falešné certifikáty (opatrně v kavárnách apod.)

Zdroje

- http://interval.cz/clanky/jak-funguje-digitalni-podpis/
- http://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita
- http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis