PV157 – Autentizace a řízení přístupu

Zdeněk Říha

Konzultační hodiny
FI MU: B415

St 17:00 – 18:00

Vašek Matyáš

část semestru mimo CZ
Microsoft Research Cambridge

Email: zriha / matyas @fi.muni.cz

Průběh kurzu

- Přednášky v D2 St 18:00 – 19:30
- Doplňkové čtení
  - *http://www.fi.muni.cz/usr/matyas/lecture/pv157.html*
- Písemná práce v polovině semestru!!! (30 %)
- Závěrečná zkouška písemná (70 %)
- Možnost pokračování v práci formou bakalářské práce

Hodnocení

A: 90 % (bodů) a více,
B: 80 % a více, ale méně než 90 %,
C: 70 % a více, ale méně než 80 %
D: 60 % a více, ale méně než 70 %
E: 50 % a více, ale méně než 60 %
F = neprospěl(a), za méně než 50 %.

- Kolokvium nebo zápočet alespoň 50 %.

Užitečné předchozí znalosti

- Informační bezpečnost – PV080, PV017
  - Není nutné, je užitečné
  - PV157 volně navazuje na PV080, resp. PV017/018
- Úvod do kryptografie
- Digitální podpis
- Internet a bezpečnost, ochrana soukromí
- Biometriky

Témata kurzu – I

1. Úvod, pojmy
2. Autentizace dat/zpráv
3. Autentizační protokoly
4. Autentizace mezi počítači
5. Autentizace uživatelů tajnými informacemi
6. Autentizace uživatelů tokeny

Témata kurzu – II

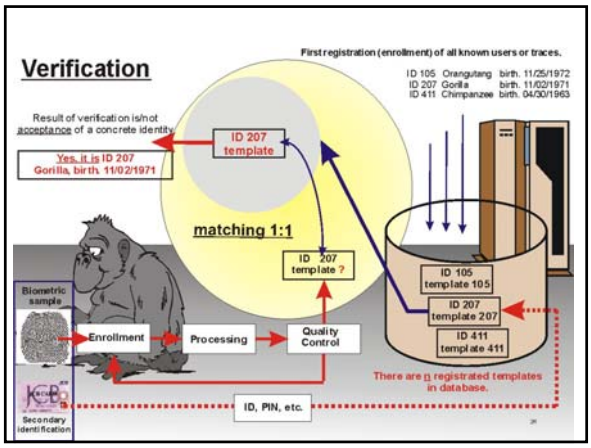
7. Úvod do biometrik
8. Biometrické autentizační metody
9. Problémy a využití biometrik
10. Úvod do řízení přístupu
11. Řízení přístupu – trendy, víceúrovňové systémy (MLS), tyto a další modely
12. PKI, prostředky pro autentizaci

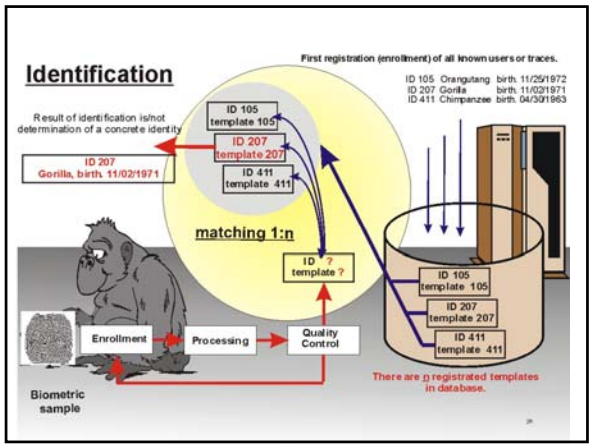
3 zásadní pojmy

- ***Autentizace*** – proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky).
- ***Autorizace*** – udělení určitých práv a určení povolených aktivit.
- ***Identifikace*** – rozpoznání určité entity (systémem) v dané množině entit.

Autentizace a identifikace uživatele

- *Autentizace (verifikace)* – subjekt předkládá tvrzení o své identitě – 1:1
- *Identifikace* (*vyhledání*) – subjekt identitu nepředkládá. Systém prochází všechny (relevantní) záznamy v databázi, aby našel patřičnou shodu a identitu subjektu sám rozpoznal – 1:n
- Následující ilustrace od Romana Raka...





Autentizace dat/zpráv

- Problematika digitálního podpisu
  - Ochrana soukromého klíče
  - Veřejný klíč – certifikát, CA
- Hašování – hašovací funkce, jejich principy a typické použití
- Autentizační kódy (MAC) atd.
- Slabé mechanismy – CRC ap.
- Praktické nasazení autentizace dat/zpráv

Autentizační protokoly

- Kryptografický protokol
- Cíle a metody kryptografických protokolů
- Autentizace jedné strany a oboustranná
- Spojení autentizace a jiných cílů kryptografických protokolů
- Standardy ISO/IEC – základní úroveň
- Protokoly vyšší úrovně (SSL, IPv6 ap.) a autentizace

Autentizace mezi počítači

- Netriviální problém – nelze použít biometriky a obvykle ani tokeny
- Autentizace podle síťových adres (MAC, IP adresy)
- Protokol výzva-odpověď – ověření znalosti tajné informace – kryptografie
- Např. protokoly ssh, SSL

Autentizace uživatelů tajnými informacemi

- „Něco, co uživatel zná“ (a ostatní ne ☺)
- Hesla
  - Druhy hesel a jejich použití
  - Správná práce s hesly
- PINy
- Výhody a nevýhody těchto autentizačních metod

Autentizace uživatelů tokeny

- Token – „něco, co uživatel má“ (a ostatní ne)
- Inteligentní token
  - Základní druhy
  - Jejich princip a použití
- Čipové karty – využití, parametry, bezpečnost
- Výhody a nevýhody těchto autentizačních metod

Úvod do biometrik

- „Něco, co uživatel je“ (a ostatní ne)
- Měřitelné biologické charakteristiky člověka-uživatele
- Fyzické – parametry orgánů
- Chování (behaviorální) – parametry činnosti
- Míra tolerance – prahová hodnota
- Nesprávné odmítnutí/přijetí

Biometrické autentizační metody

- Otisk prstu 
- Vzor oční duhovky 
- Vzor oční sítnice 
- Srovnání obličeje 
- Geometrie ruky 
- Verifikace hlasu
- Dynamika podpisu 
- Dynamika psaní na klávesnici

Využití biometrik

- Problémy biometrik – bezpečnost
- Otázky praktického použití
  - Současná omezení a použitelnost
  - Vhodné použití
  - Nevhodné použití
- Vztah biometrik a kryptografie

Řízení přístupu I.

- Úvod do řízení přístupu
- Mechanismy pro systémy řízení přístupu
- Volitelné řízení přístupu – Discretionary Access Control (DAC)
- DAC systémy v praxi

Řízení přístupu II

- Povinné řízení přístupu – Mandatory Access Control (MAC)
- Víceúrovňové systémy – Multilevel Systems (MLS)
- Role-Based Access Control (RBAC) a další nové modely a trendy

PKI

- Public-key infrastructure
  - Principy, použití
  - PKI není jen CA
  - PKI je prostředek, ne cíl
  - Výhody a nevýhody
- Na jednu z aplikací se podíváme v detailu na některé z posledních přednášek kurzu

Kryptologie

- Fyzická ochrana – cena!
- ***Kryptografie*** – ochrana významu (informační hodnotu) dat i „na dálku“
- ***Kryptoanalýza*** – zjišťování slabin kryptografických algoritmů a parametrů
- ***Kryptologie*** – kryptografie & kryptoanalýza
- ***Steganografie*** – utajení samotné existence dat
- ***Vodotisk (watermarking)*** – překryv se steganografií, metody vložení (ochranných) informací do dat

Kde kryptografie pomáhá

- Důvěrnost dat
- Integrita dat
- Autenticita dat (integrita a ověření původu)
- Nepopiratelnost
- Autentizace a autorizace uživatelů/strojů
  - Dostupnost
  - Prokazatelná zodpovědnost
  - Řízení přístupu

...

Tři dimenze kryptografie

- Druhy použitých operací
  - Substituce
  - Permutace
  - …
- Druh a parametry klíčů
  - Symetrické = konvenční = sdílené
  - Asymetrické = veřejné & soukromé
  - Bez klíčů (hašovací funkce, RND)
- Způsob zpracování dat
  - Po blocích
  - V souvislém proudu

Kryptografie – Kerckhoffův princip

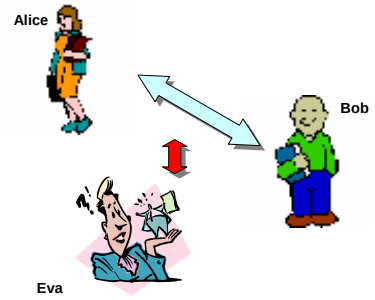
- Algoritmus – postup – je všem znám a všemi ověřitelný (jako bezpečný)
- Klíč – tajná informace – musí být chráněna před nepovolanými osobami

Co je hašování (hashování)

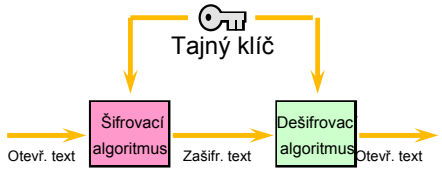
- "Otisk dat"
  - Malý a jedinečný reprezentant jakkoliv velkých dat
- 01:A0:7D:2B:76:52:67:05
- EC:43:6F:B3:68:CE:20:E7

- Hašovací funkce
  - jednosměrnost, bezkoliznost
  - SHA-1 (160 bit), SHA-x
  - MD5 (128 bit)

Obvyklá označení činitelů

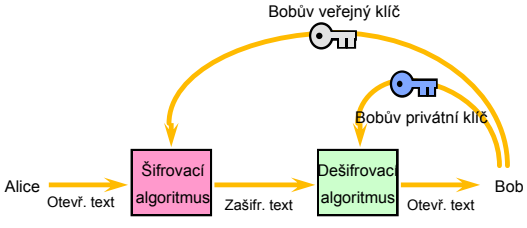


Zjednodušený model konvenčního šifrování



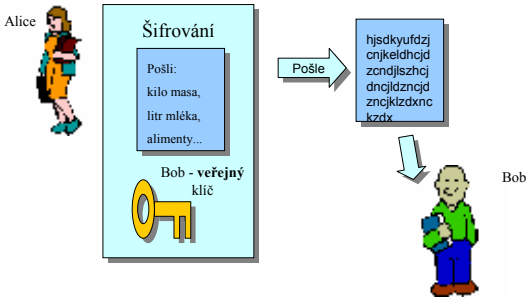
Převzato z: *Network and Internetwork Security* (Stallings)

Zjednodušený model šifrování veřejným klíčem

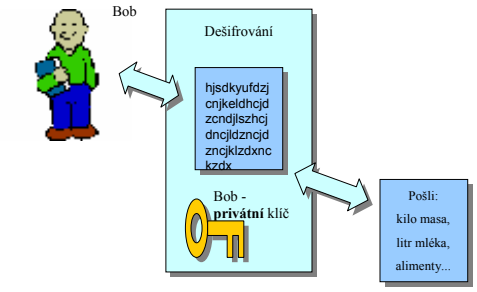


Převzato z: *Network and Internetwork Security* (Stallings)

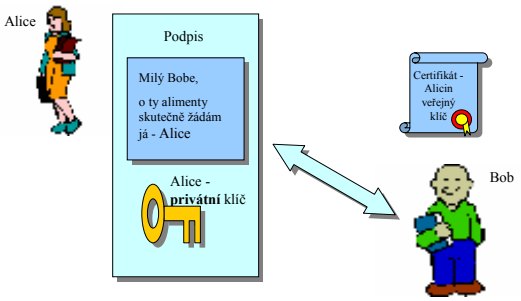
Šifrování veřejným klíčem



Dešifrování zprávy od Alice



Co je digitální podpis?



Otázky?

Vítány!!!

Příští přednáška 6. 10. 18:00

matyas@fi.muni.cz
zriha@fi.muni.cz