INFORMAČNÍ BEZPEČNOST

INFORMAČNÍ BEZPEČNOST

TECHNICKÝ POHLED

Shrnutí bezpečnostních mechanismů

Základní atributy chráněných informací

1. **Důvěrnost** - ochrana před neoprávněným čtením (šifrovací mechanismy, autorizovaný přístupu k datům).
2. **Dostupnost** - zajištění adekvátního přístupu a ochrana před jeho neoprávněným zamezením (fungování informačního systému, bezpečnostní mechanismy, komunikační kanálu).
3. **Celistvost** - ochrana před neoprávněnými úpravami nebo zničením (pečetě, digitální podpis).

Další podstatné atributy

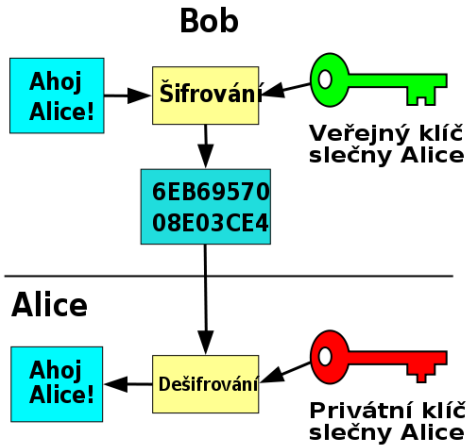
1. **Autentizace -** ověření, že subjekt je tím, za koho se vydává (heslo, biometrických prostředků, čipové karty či tzv. tokeny).
2. **Autorizace -** omezení dostupnosti operací, jakými jsou například čtení nebo zápis informací, jen pro oprávněné uživatele
3. **Nepopiratelnost** – vyloučení možnosti popřít dřívější provedení nějaké operace

Počítačová kryptografie

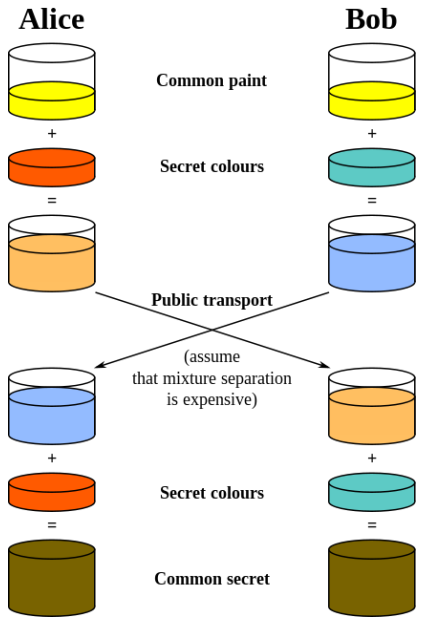
Nástupem počítačů se prudce mění způsob kryptografie a kryptoanalýzy:

- Šifra může být tvořena tisíci složitých algebraických operací.
- Silná kryptografie X slabá kryptografie.

Algoritmy: šifrování



- Kryptografické algoritmy s **privátním klíčem:** symetrická kryptografie (3DES, RC4, AES).
  - Symetrické šifry (neboli šifry tajného klíče) používají pro šifrován i dešifrování jediný klíč.
  - Zásadním aspektem tohoto algoritmu je tzv. problém distribuce klíčů.



- Kryptografické algoritmy s **veřejným klíčem:** asymetrická kryptografie (Diffie-Helman, DSA, RSA).
  - Kryptografie veřejného klíče pro šifrování a dešifrování používají odlišné klíče.
  - Obě strany komunikace mají svůj vlastní klíč, přičemž jeden je veřejný a druhý soukromý.

Algoritmy: hash (otisk)

- Hašovací funkce se začínají objevovat v polovině padesátých let, na poli výpočetní techniky se využívají později.

- Zjednodušeně řečeno, je to funkce, která vytváří z libovolně dlouhé zprávy (souboru) digitální otisk (hash) s pevně definovanou délkou (128, 160, 256 bitů)

- Hašovací funkce je výpočetně efektivní funkce, která transformuje posloupnosti binárních symbolů libovolné délky na binární posloupnosti určité konstantní délky, nazývané hash (hodnota, otisk).“(PŘIBYL, 2004)

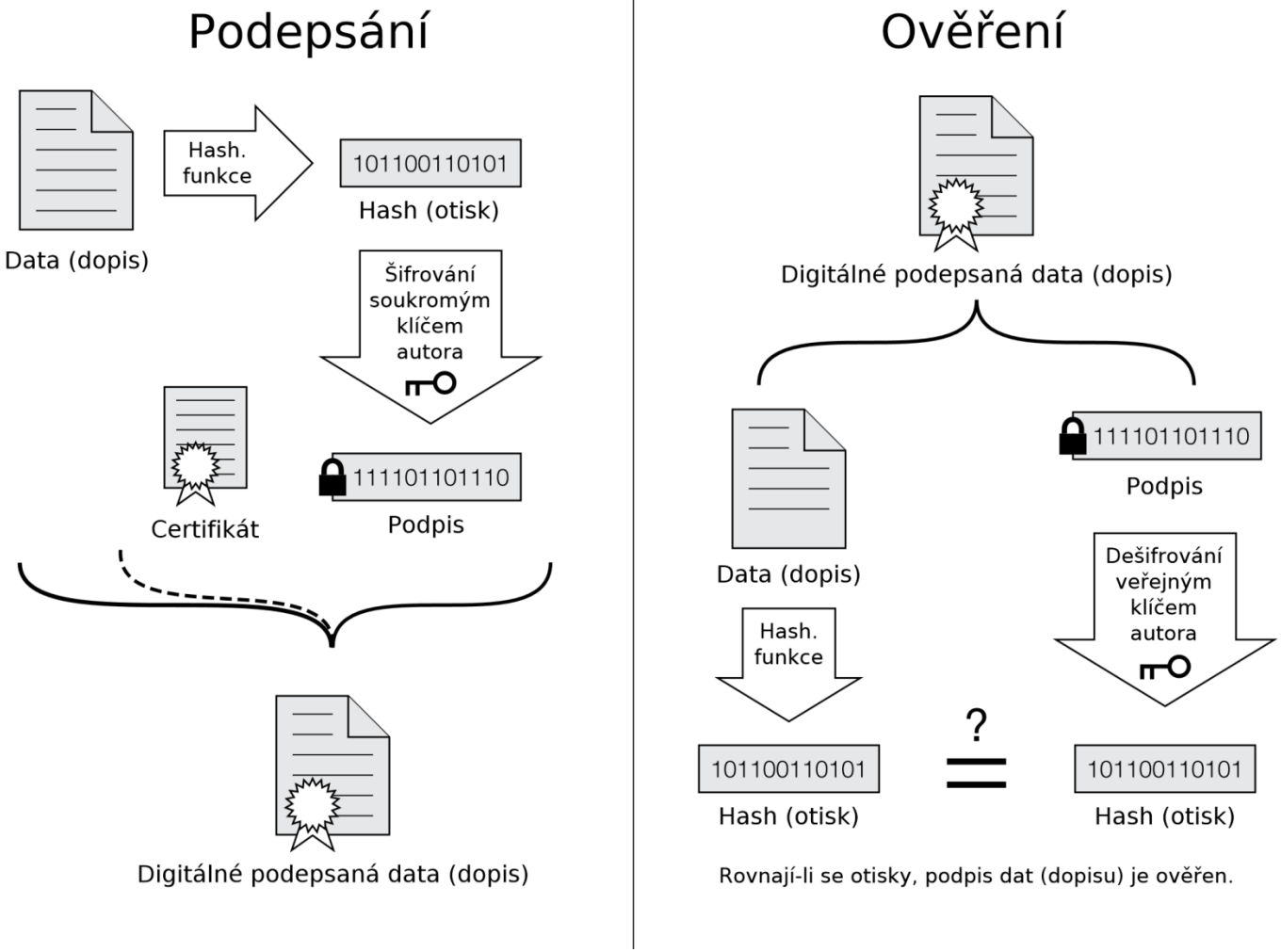
Algoritmy: hash (otisk)

- Hašovací funkce musí vyhovovat následujícím požadavkům:
  - musí být jednosměrná, tedy nesmí být možné z hodnotu hash odvodit původní zprávu,
  - musí být nekolizní, není tedy možné odvodit dvě různé výchozí zprávy pro tutéž hodnotu hash.
- Příkladem využití hašovací funkce je uložení hesla do systému pro možnost následné autentizace pomocí tohoto hesla,
  - samotné tajné heslo nemusí být nikde ukládáno.
- Standardem jsou hash algoritmy: MD5, SHA1-3

Algoritmy: digitální podpis

- Autentizační systém pro ověřování pravosti elektronických dat, využívá algoritmy asymetrické kryptografie.
- Elektronický podpis má následující vlastnosti:
  - Je spojen s jedním konkrétním elektronickým dokumentem (tj. potvrzuje pravost a autenticitu tohoto dokumentu) a nemůže být použit pro podepsání jiného dokumentu.
  - Může být vytvořen pouze tím, kdo zná jisté tajemství – soukromý klíč.
  - Je nemožné vytvořit jiný dokument, sebeméně odlišný od původního dokumentu, pro který by byl původní elektronický podpis stále platný.
  - Jakmile je jednou elektronický podpis v dokumentu vytvořen, kdokoli si může ověřit pravost tohoto podpisu.

Algoritmy: digitální podpis



Implementace: Secure Sockets Layer

Secure Sockets Layer, SSL (vrstva bezpečných socketů)

- Je to protokol vložený mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran.
- Pro bezpečnou komunikaci s internetovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP.
- Po vytvoření SSL spojení (session) je komunikace mezi serverem a klientem šifrovaná a tedy zabezpečená.

root@star.killesberg.org: /root

```
Jan 25 15:08:20 star smb: nmbd shutdown succeeded
Jan 25 15:08:21 star smb: smbd startup succeeded
Jan 25 15:08:21 star smb: nmbd startup succeeded

==> /var/log/maillog <==
Jan 25 14:59:05 star postfix/cleanup[2767]: 90A6EBA893: message-id=<200201251356
19.GH17045@charite.de>
Jan 25 14:59:05 star postfix/qmgr[1278]: 90A6EBA893: from=<owner-postfix-users@p
ostfix.org>, size=4082, nrcpt=1 (queue active)
Jan 25 14:59:05 star postfix/local[2769]: 90A6EBA893: to=<fbijlsma@localhost.kil
lesberg.org>, relay=local, delay=0, status=sent ("|/usr/bin/procmail")
Jan 25 14:59:13 star postfix/smtpd[2766]: disconnect from localhost[127.0.0.1]
Jan 25 15:01:18 star postfix/smtpd[2786]: connect from localhost[127.0.0.1]
Jan 25 15:01:18 star postfix/smtpd[2786]: 5D0E3BA893: client=localhost[127.0.0.1
]
Jan 25 15:01:18 star postfix/cleanup[2787]: 5D0E3BA893: message-id=<MBBBIIABCNEJ
EFGKDAEJMEBBCAAA.dkanter@rushu.rush.edu>
Jan 25 15:01:18 star postfix/qmgr[1278]: 5D0E3BA893: from=<owner-postfix-users@p
ostfix.org>, size=4167, nrcpt=1 (queue active)
Jan 25 15:01:18 star postfix/local[2788]: 5D0E3BA893: to=<fbijlsma@localhost.kil
lesberg.org>, relay=local, delay=0, status=sent ("|/usr/bin/procmail")
Jan 25 15:01:27 star postfix/smtpd[2786]: disconnect from localhost[127.0.0.1]

[root@star /root]#
```

Implementace - Secure Shell

SSH neboli Secure Shell

- Klient/server protokol v síti TCP/IP, který umožňuje bezpečnou komunikaci mezi dvěma počítači pomocí šifrování přenášených dat.
- Pokrývá tři základní oblasti bezpečné komunikace:
  - autentizaci obou účastníků komunikace,
  - šifrování přenášených dat,
  - integritu dat.
- SSH je používán pro vzdálenou práci, např. správu serverů.
- Bezpečný přenos souborů pomocí SFTP nebo SCP.

Implementace - PKI

- PKI neboli Public Key Infrastructure je prostředí, které umožňuje ochranu informačních systémů, elektronické komunikace.

- Zahrnuje veškerý software, technologie a služby, které umožňují využití šifrování s veřejným a privátním klíčem.

- PKI zahrnuje celou řadu různých prvků, např.:
  - digitální certifikáty,
  - klíče,
  - asymetrickou kryptografii,
  - certifikační autority,
  - nástroje pro správu, obnovu a rušení certifikátů.

Vládou ovládaná kryptografie

- Problematika šifrování je řešena na vládní úrovni.
- Národní bezpečnostní agentura – **National Security Agency**, má právo odposlouchávat jakoukoliv komunikaci související s USA, brzdí rozšiřování kryptografických informací, povoluje vývoz jen oslabených šifer.
- Odposlech telefonních hovorů, e-mailů a další komunikace bez povolení soudu.
- **Aktivity**: ECHELON, TEMPORA, PRISM

Zásadní rozpor :

Lidé požadují právo a možnost chránit svá data tím nejlepším šifrovacím systémem.

X

Vláda, tajné služby se snaží použití kryptografie omezit, protože potenciálně umožňuje ilegální a nekontrolovatelné aktivity.

INFORMAČNÍ BEZPEČNOST

UŽIVATELSKÝ POHLED

Obecný pohled

- Základní lidská potřeba
- Paretovo pravidlo – snaha : problém = 20 : 80
- 3 pravidla:
  - 100% bezpečí neexistuje
  - nejvíc problémů si způsobí každý sám
  - prevence je vždy úspěšnější než represe

Útoky s využitím sociálního inženýrství

- útočníci snaží působením na psychiku **manipulovat uživatelem** tak, aby žádané informace sám prozradil
- podvod, jehož cílem je **přesvědčit uživatele**, aby **udělal** něco, **co ho poškodí**
- působí na psychiku
  - zvědavost
  - strach o peníze
  - strach obecně
  - soucit
- tomuto útoku nezabrání technické prostředky, nejlepší ochranou je zdravý rozum a důsledné ověřování

Problém digitální stopy

- na internetu je mnoho informací spojitelných s určitou osobou

- označujeme je jako **digitální stopu**
  - využitelné pro cílenou reklamu, personalizace služeb,
  - vyšetřování porušení legislativy v elektronickém prostředí

  - informace ukládané **bez zásahu uživatele**
    - IP adresa, verze operačního systému či jiného vybavení,
    - čas strávený na určité webové stránce (cookies)
    - vyhledávané výrazy a další

  - informace **vědomě zanechané**
    - úřední údaje
    - sociální sítě
    - emaily, sms, historie chatu ..

Útoky na osobní informace

- Většina útoků stále častěji vede s cílem získat OI.
- V komerční oblasti bývá kvalitní technické zajištění,
  - o to častěji se vedou útoky na zaměstnance.
- Pro uživatele největší ohrožení přes jeho soukromí.
- Člověk je vždy nejslabší článek zabezpečení.

O co jde útočníkům především?

- **Tradiční OI:**
  - Kontaktní údaje
  - Informace o majetku, dovolené
  - Rodné číslo, čísla dokladů, kódy platebních karet, jméno matky za svobodna, informace o blízkých osobách apod.

- **Elektronické OI:**
  - E-mailová adresa
  - Heslo k různým aplikacím

Ohrožnení dětí – přístup k internetu

Neomezený a nechráněný přístup k internetu mají dvě třetiny školních dětí v Česku,

- ¾ školních dětí má svůj notebook,
- více než ¼ má tablet,
- v 8. a 9. třídě přes 90 % dětí připojuje před mobilní telefon.

Ohrožení dětí

Statistiky EU Kids Online:

- 17 % se cítilo na internetu poškozeno,
- 21 % obdrželo sexuální zprávy,
- 8 % kyberšikana (26 % online i offline dohromady),
- 46 % kontakt online s cizím člověkem, 15 % následně setkání,

  11 % z nich (1 % ze všech dotázaných) se špatnou zkušeností.

Nahlášená oznámení:

- 36 % nahlášeno rodičům, 28 % kamarádům a 24 % učiteli,
- 60 % sexuální zprávy, 77 % šikana, 53 % sexuální obrázky.

Ohrožení dětí

Kyberšikana

- zneužití IT k ponižování, pomluvám, pronásledování, záznamům šikany či násilí
- dlouhodobé působení na oběť, strach v mnoha formách
- viz. Ghyslain Raza, Ryan Patric Halligan, Anna Halman, Megan Meier

Grooming

- útočník chce získat důvěru oběti => schůzka pro sexuální zneužití
- cílem nalezení v reálném světě (i foto, video)
- oběti obvykle 9-16 let

Sexting (sex + texting)

- 2 % dětí 9-16 let se v posledním roce setkalo s požadavkem zaslání intimní fotografie či videa
- v podstatě šíření dětské pornografie
- viz. Jessica Logan

České obecné preventivní programy

- Saferinternet CZ a Bezpečně online (primárně děti)
- e-Bezpečí (hl. pedagogové)
- Bezpečný internet.cz – kurzy různým skupinám, ne moc systémové, ale kvalitní díky zaštítění významnými firmami
- Průvodce bezpečným chováním na internetu od Google
- Český Microsoft Security Center

Zahraniční obecné preventivní programy

- inSafe – hl. materiály jednotlivých uzlů
- i-SAFE – velmi bohatý zdroj, virtuální akademie
- Microsoft Security Center
- On Guard
- Internet Safety Project

Literatura

DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. vyd. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

POŽAR, J. *Informační bezpečnost*. Plzeň : Vydavatelstvi a nakladatelstvi Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.

PŘIBYL, J. *Informační bezpečnost a utajování zpráv*. 1. vyd. Praha : Vydavatelstvi ČVUT, 2004. 239 s. ISBN 80-01-02863-1.

VLČEK, K. *Teorie informací, kódování a kryptografie*. 1. vyd. Ostrava : Vysoka škola baňska - Technicka univerzita Ostrava, 1999. 182 s. ISBN 80-7078-614-0.

What is Diffie-Hellman?. *RSA Security* [online]. c 2004 [cit. 2006-04-10]. Dostupny z WWW: <http://www.rsasecurity.com/rsalabs/node.asp?id=2248>.

ZELENKA, J., et al. *Ochrana dat : Kryptologie*. 1. vyd. Hradec Kralove : Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.

KLIMA, V. Co se stalo s hašovacimi funkcemi? aneb přehled udalosti z posledni doby, čast 2. *Crypto-World: informační sešit GCUCMP*, 4/2005 [online]. Dostupny z WWW < http://crypto-world.info/casop7/crypto04_05.pdf>.

BOROVIČKA, V. P. *Přísně tajné šifry*. Vyd. 1. Praha: Naše vojsko, 1982. 315 s. Fakta a svědectví; sv. 82.