

Prevence

Radomír Orkáč
VŠB-TUO, CIT 872
20. 5. 2009, Praha

radomir.orkac@vsb.cz



Informační bezpečnost

- = cílená ochrana před ztrátou, zničením, zneužitím nebo odcizením dat
- Bezpečnostní cíle se soustřeďují na zajištění:
 - důvěrnosti – ochrana informací před zneužitím
 - integrity – ochrana dat proti nežádoucí úpravě
 - dostupnosti – dostupnost dat pro uživatele
 - Bezpečnostní funkce jsou prostředky k dosažení bezpečnostních cílů:
 - administrativní, fyzické, technické, logické
 - preventivní, průběžné, detekční, opravné

Bezpečnostní incident

= narušení informační bezpečnosti

- Z pohledu cíle
 - pasivní – únik informací (odposlech)
 - aktivní – modifikace, narušení dostupnosti, integrity
- Z pohledu škod
 - ztráta dobrého jména, finanční škoda, ostuda, ...
- Z pohledu zavinění
 - nedbalostní, neznalostní, nevědomostní, úmyslné

Prevence

- Prevence
 - opatření, která mají předcházet bezpečnostním incidentům
 - minimalizace možných rizik
 - zlepšení ochrany a obnovy dat
- Preventivní opatření
 - směrnice, nařízení, předpisy
 - připojení počítačů k síti
 - zacházení s dokumenty
 - jednotná autentizace uživatelů
 - logování přístupů a aktivity uživatelů

Prevence

- logy zabezpečit a archivovat
- zálohování a archivace (pravidelné prověřování)
- spolehlivě a nenávratně mazat nepotřebná data
- data šifrovat
- zakázat anonymní účty (vždy vyžadovat heslo)
- přidělování odpovídajících přístupových práv
- pravidelná údržba systému (aktualizace, kontrola nepotřebných služeb)
- **školení uživatelů a správců**
- ...

Autentizace a autorizace

Autentizace = ověření totožnosti partnera

- základní metody - **znalost** (heslo, PIN), **vlastnictví** (identifikační karta, čip), **fyzická charakteristika** (otisk prstu)
- např. omezí skupinu lidí, kteří mohou zneužít nalezenou chybu nebo využívat vytvořené návody

Autorizace = udělení oprávnění, ověření rolí

- kontrola přístupu k jednotlivým částem aplikace podle uživatelského účtu, role

Autentizace a autorizace

Autentizace a autorizace zahrnuje:

- zajištění odolnosti proti pokusům o náhodné uhodnutí údajů
- ochranu integrity a důvěrnosti autentizačních dat
- upozornění na právní důsledky zneužití systému
- zobrazení informací o posledním přihlášení
- definování postupů pro správu uživatelských účtů
- definování důvodů, které mohou vést k uzamčení sezení uživatele

Uživatel a heslo

- Nevhodná volba
 - jména, rodná čísla, adresa, názvy, běžné znaky
- Mnemotechnické pomůcky
 - Dvakrát do stejné řeky nevstoupíš! 2XdsrN!
- Prolomitelnost (100 hesel za sekundu)
 - znaky 0..9; délka 4→2min; délka 8→11dní
 - znaky a..Z,0..9; délka 4→2dní; délka 8→70 000 let
- Správci hesel (Revelation PM, Password Safe)
- Pozor na papírové štítky!!!

Heslo k účtům u Seznam.cz

- <http://openid.cz/server/>
 - „Seznam.cz spouští OpenID - jen další důkaz, že OpenID se stane hlavním způsobem přihlašování na Internetu!”
- Ověřeno u následujících poskytovatelů
 - seznam.cz, gmail.com, centrum.cz, volny.cz
- Odeslat na openid@email.cz
předmět: **heslo1234**
\$auth=radomir.orkac@seznam.cz
\$email=petr.novak@seznam.cz

Kryptografie

- Kryptografie z pohledu prevence
 - utajení a zachování integrity přenášených dat
 - identifikace a autenticita odesílatele zprávy
- Symetrická šifra
 - pro šifrování i dešifrování se používá shodný klíč
 - klíč se musí dostat ke všem stranám
 - nenáročné na výpočetní výkon
- Asymetrická šifra
 - veřejný klíč pro šifrování
 - soukromý klíč pro dešifrování

Kryptografie

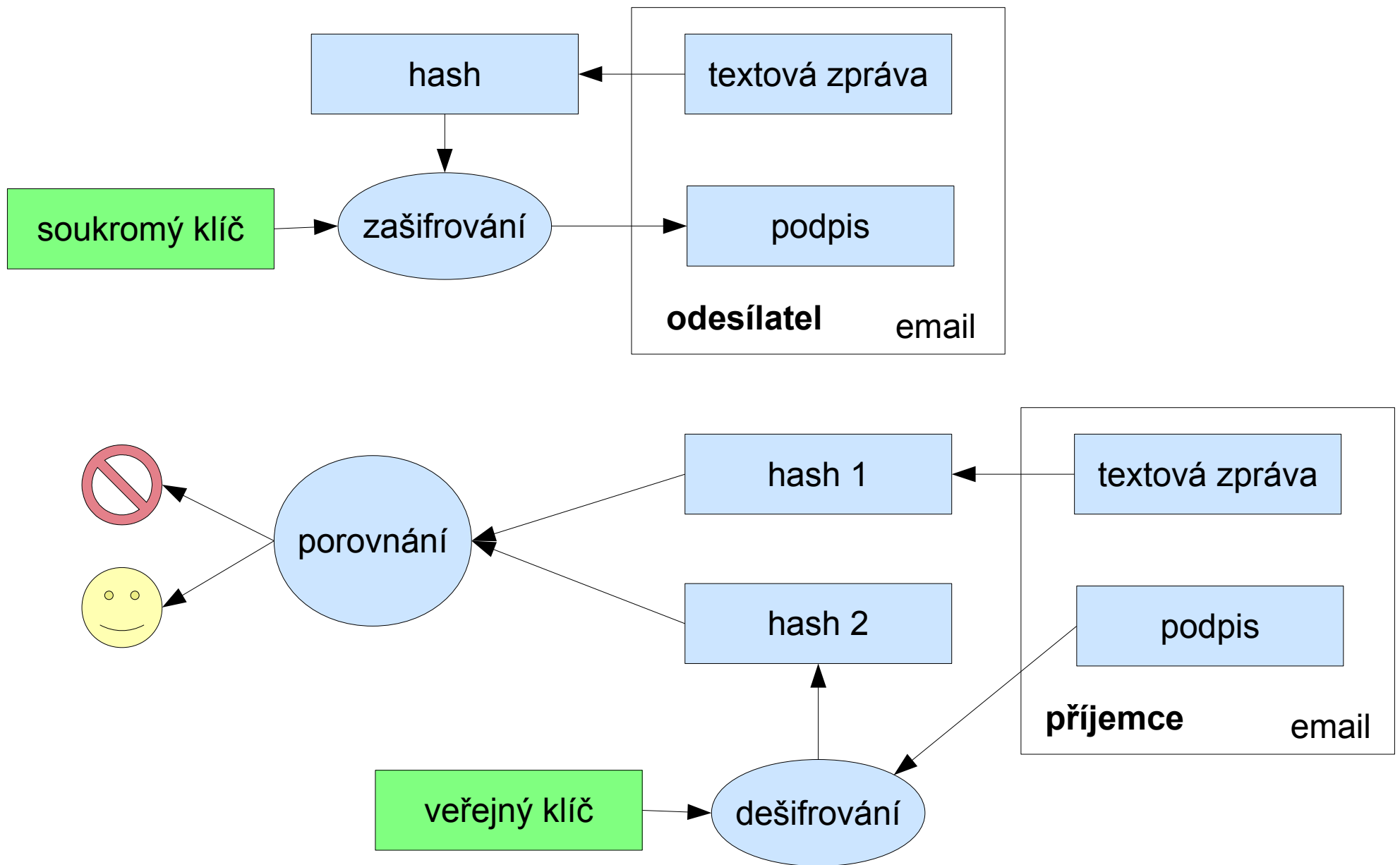
- problém distribuce klíče je vyřešen
- ověření pravosti

- PKI (Public Key Infrastructure) – systém standardů a doporučení pro bezpečnou komunikaci v Internetovém prostředí
- Certifikační autorita – vydává certifikáty k použití ostatním zúčastněným
- Certifikát – identifikace a veřejný klíč uživatele, identifikace CA, platnost certifikátu a další ...
- Veřejný a soukromý klíč, CRL

Elektronický podpis

- Elektronický podpis (prostý)
 - elektronické identifikační údaje odesílatele připojené k elektronickému dokumentu, které zaručují identifikaci
 - ekvivalent vlastnoručního podpisu
- Zaručený elektronický podpis
 - pomocí kryptografických metod zajišťuje garanci původu a pravost obsahu (nebyl změněn)
 - ekvivalent úředně ověřeného vlastnoručního podpisu

El. podpis a pošta



Elektronický podpis a pošta

- Proč podepisovat své zprávy?
 - příjemce bude mít jistotu, že email pochází od Vás
 - příjemce bude mít jistotu, že obsah nebyl změněn
 - odlišnost od nevyžádané pošty
 - zvýšení úspěšnosti doručení
 - minimalizace možnosti zneužití Vaší adresy

```
$ telnet smtp.abcdserver.cz 25
EHLO microsoft.com
MAIL FROM: radomir.orkac@microsoft.com
RCPT TO: prijemce@abcdefmail.cz
DATA
Subject: predmet
.
QUIT
```

Ochrana elektronické pošty

- Šifrování
 - vždy, když není žádoucí, aby Vaše zpráva byla čitelná (mimo příjemce)
 - pomocí veřejného klíče příjemce se data zašifrují a pomocí soukromého klíče příjemce se rozšifrují
 - GnuPG - Thunderbird + Enigmail
- Zabezpečené připojení
 - pokud možno nepoužívat smtp, pop3, imap, http
 - imaps: 993, pop3s: 995, smtps: 465, https: 443

Šifrování

- Co je šifrování?
 - algoritmus pro změnu zdrojových dat do podoby, ze které lze převést data zpět pouze se znalostí speciálního šifrovacího klíče
- Proč šifrovat?
 - ochrana soukromí a obchodního tajemství
 - ochrana pouhým heslem je nedostatečná
 - může dojít ke ztrátě usb klíčenky či notebooku
 - krádež zálohovaných či archivovaných dat
 - data přístupná více lidem (online úložiště, správce)

Šifrování

- Co se šifruje?
 - komunikace a přenos dat po síti (Internet)
 - celé disky, oddíly (včetně systémových), klíčenky
 - domovské adresáře
 - jednotlivé soubory (dokumenty, fotky, ..)
 - zálohy, archívy

Truecrypt

- Virtuální disk uložen v souboru
- Šifrování celých disků/oddílů
- Šifrování systémových oddílů (Windows)
- Podporuje cestovní režim (Windows*)
- Umožňuje vyvážení skrytých oddílů
- Velikost instalačního souboru cca 3 MB.
- Windows Vista/XP, GNU/Linux a Mac OS X
- Domovské stránky: <http://www.truecrypt.org/>

Zálohování

- Příčina ztráty dat
 - selhání systému
 - poškození fyzikálními a přírodními vlivy
 - poškození vlivem lidského faktoru
 - úmyslné zničení dat
- Určení aktiv, která budou zálohována
 - ideální je zálohovat celé disky/oddíly
 - data programů, které používáme pro svoji činnost (programy ekonomické, evidenční,..)
 - dokumenty, obrázky, videa

Zálohování

- konfigurace, nastavení, logy
- instalační soubory/média
- kontakty, hesla
- Jak často zálohovat
 - záloha by měla být prováděna tak často, jak rychle se mění zálohovaná data
 - stará data mohou být bezcenná
- Typ zálohy – úplná, přírůstková, rozdílová
- Ochrana dat – šifrování, úschova, přírodní jevy

Zálohování

- Úložiště
 - CD/DVD, HDD, síťový disk, online úložiště
 - cena, spolehlivost, životnost
- Plán obnovy
 - kde nalezneme zálohy a přístupová hesla
 - kdo, co a jak se bude obnovovat
- Linux/Unix
 - rsync, tar, Bacula, Amanda, Clonezilla
- Windows
 - Cobian Backup, Acronis True Image, Norton Ghost

Archivace

- Přesun dat, která již nejsou aktivně využívána
 - dokumenty
 - fotky
 - staré verze www stránek
 - účetnické záznamy
- Šetření zdrojů a prostředků
- Neměnnost
- Bezpečná úschova dat

Sociální inženýrství

- Termín pro metodu, která je využívána útočníky k získávání důležitých informací od uživatelů „bez jejich vědomí”
- Albert Einstein

„Pouze dvě věci jsou nekonečné – vesmír a lidská hloupost. Ačkoliv tím prvním si nejsem jist.”
- Médium
 - **telefon** a Internet (e-mail, IM)
- Zneužívání vlastností lidí
 - důvěřivost, neznalost, ochota pomoci druhým, obava, nepodezíravost, naivita, hloupost

Sociální inženýrství

- Příklady zneužití
 - ...mám nový bankovní účet, pošlu Vám mail...
 - keylogger na odložené usb klíčenice
 - ...máte napadený počítač, navštivte tyto stránky a zjistěte mi prosím adresu serveru...

- Obrana
 - vzdělávání/školení
 - jasně stanovená pravidla a postupy
 - (zpětné) ověřování totožnosti
 - zdravý rozum

Prostor pro případné dotazy

Děkuji za pozornost.