# Šifrování emailů

Michaela Sluková, Lenka Ščepánková

ČVUT FJFI

15.5.2014

# Úvod

- Jak?
  - → Zašifrovat email lze pomocí šifrování zprávy samotné či elektronickým podpisem emailových zpráv.
- Proč?
  - → Zprávu nepřečte někdo jiný a nemůže být změněna, zpráva chráněna jak při přenosu tak při útoku na emailovou schránku.
- Kdy?
  - → Šifrovat vždy!!
  - → ....nebo aspoň tehdy, posíláme-li:
    - RČ,
    - číslo bankovního účtu,
    - důvěrné info o zaměstnání, o podnikání apod.

# Rizika emailové komunikace

## Pasivní útoky

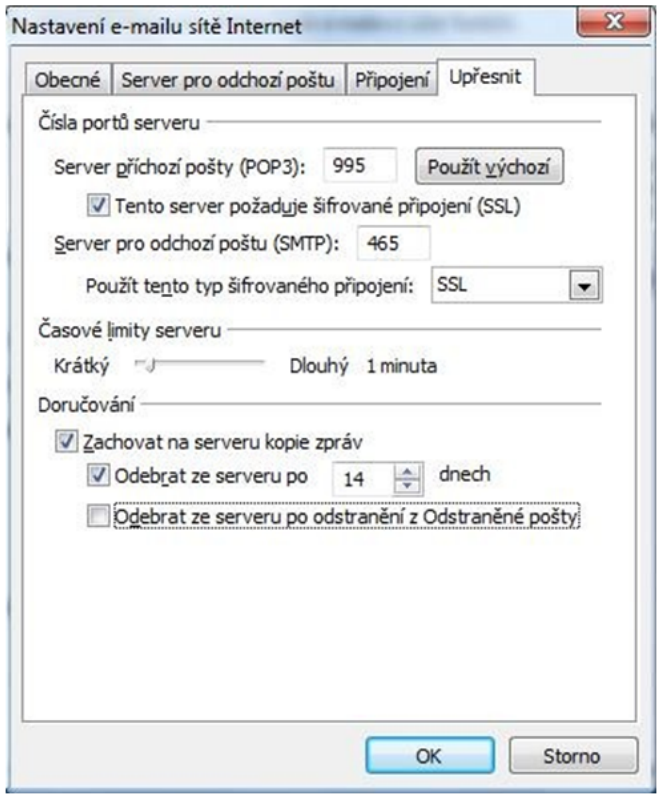
- zveřejnění obsahu zprávy
- traffic analysis - získávání informací podle frekvence komunikace a jiné

## Aktivní útoky

- změna obsahu zprávy - *man-in-the-middle-attack*
- převlek - posílaní zprávy ve jménu jiné osoby
- odmítnutí služby (*Denial of Service - DoS*) - přetížení mailového systému pomocí zahlcení zprávami

# Šifrování připojení k poskytovateli emailové schránky

- Pokud poskytovatel podporuje SSL/TLS, vždy používejme zabezpečené připojení přes adresu začínající na **https**.
- Zabezpečení SSL/TLS lze použít i u desktop. aplikací typu Microsoft Outlook (obtížnější nastavení).




*Pokud poskytovatel SSL/TLS nepodporuje, je rozumné u něj zůstat???*

# Šifrování emailové komunikace

- Vyžaduje spolupráci jak odesílatele, tak příjemce!!!

Možnosti šifrování:

- přímo v rámci e-mailové služby,
- pomocí staženého softwaru pro šifrování či doplňky doinstalované do aplikací (SafeGmail a Mailvelope - Chrome, Enigmail - Mozilla, Trend Micro Email Encryption Client - Microsoft Outlook)
- využití webových šifrovacích e-mailových služeb např. Sendinc, JumbleMe, Infoencrypt

*Musíme je však také považovat za důvěryhodné. . . Můžeme?*

# Šifrování pomocí softwaru/staženého doplňku

- Instalace certifikátu zabezpečení a poskytnout **veřejný klíč** (to samé platí pro příjemce!!).
- Zprávu může dešifrovat pouze příjemce, který má soukromý klíč odpovídající veřejnému klíči použitému při šifrování zprávy

$\Rightarrow$ *asymetrické šifry*

# Šifrovací protokoly

## OpenPGP - Pretty Good Privacy

- zdarma dostupný i komerční SW, také doplňky (Gpgwin či PGP Desktop Email).

## S/MIME - Secure/Multipurpose Internet Mail Extensions

- integrována do řady programů typu Microsoft Outlook,
- existují doplňky do prohlížečů (**Gmail S/MIME** pro Firefox),
- požádat si o bezpečnostní certifikát (např. firma Comodo)

## TLS - Transport Layer Security

- vychází ze SSL
- pomáhá zabránit falšování e-mailových adres mezi servery

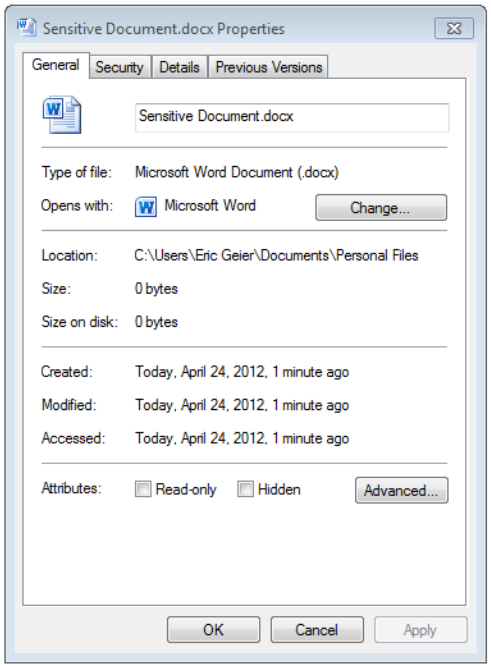
# Šifrováni uložených e-mailů

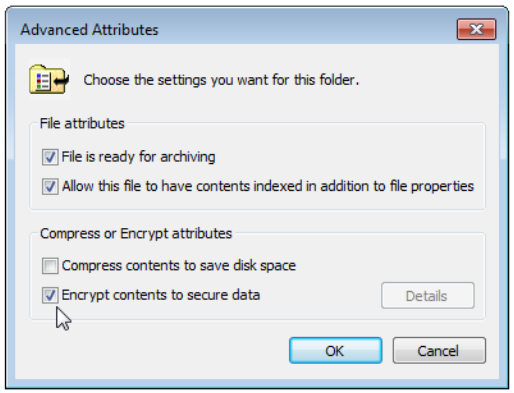
- hlavně u přenosných zařízení $\Rightarrow$ riziko odcizení!
- *Počítač s OS Windows:* zašifrování všech dat, nebo jen emailové schránky (nezávisí na programu pro poštu)
  - Windows Professional, Business, Ultimate $\Rightarrow$ přes funkci EFS (Encrypted File System)
- *Mobil/Tablet:* ideálně použít takový OS, který zajistí zašifrování veškerých dat PINu či hesla
  - Blackberry a iOS podporuje již několik let, Android až od verze 3.0, u starších lze využít e-mailové aplikace třetí strany TouchDown pro účty Exchange – již nabízí funkci šifrování).

# Encrypted File System

## Windows

*Vyhledat soubor s uloženými emaily → Pravé tl. → Vlastnosti → Obecné → Upřesnit → Šifrovat obsah a zabezpečit tak data.*



# Poskytovatelé

## Velké společnosti

- Google - Gmail
- Lavabit a Secret Circle - ukončili své služby kvůli odmítaní spolupráce s NSA, která by mohla požadovat přístup k datům
  - Lavabit - přes 400 000 uživatelů

## Menší poskytovatelé - často mimo USA

- Countermail (Švédsko) - placená služba (100 dolarů za 2 roky)
- Hushmail (Kanada) - PGP šifrování
- Mega - od Kima Dotcoma (Megaupload)

# OpenPGP

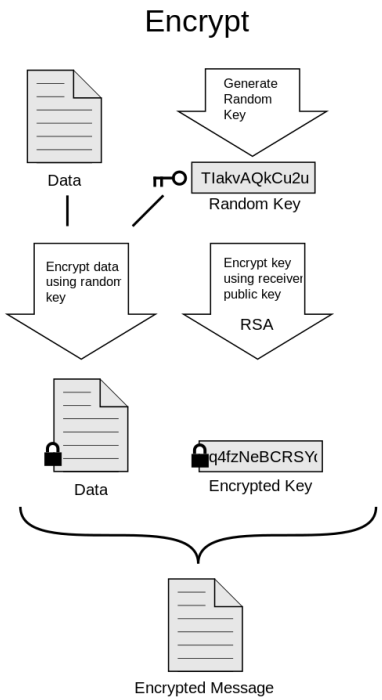
- nejpoužívanější program pro soukromé účely
- PGP znamená "Pretty Good Privacy"
- 1991 - Phil Zimmermann
- použití: email, datové soubory, rychlé zprávy (*Instant Messaging*)

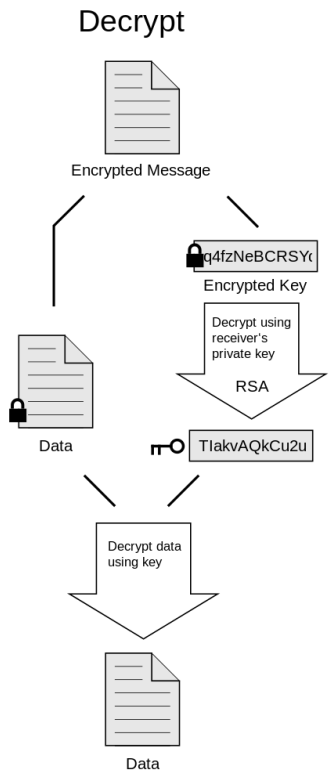
## Šifrování

- asymetrické šifrování RSA klíčem -
- čitelný text je zakódován a dále přenášen jako email nebo IM - příjemce dešifruje přes PGP
- existence *public key server* - distribuce veřejných klíčů mezi ostatní uživatele
- autenticita - využití digitálního podpisu

## programy využívající protokol OpenPGP

- GNU Privacy Guard (GnuPG či GPG)
  - svobodná alternativa k PGP
  - oblíbený v Linuxe
- ve Windows - Gpg4win



# Závěr

## Jak zašifrovat email

Budeme potřebovat :

- GNU Privacy Guard (GnuPG) ve formě GPGTools (OS X) nebo Gpg4win (Windows)
- Thunderbird (Win/OS X/Linux) nebo Postbox (Win/OS X) pro desktop emailové schránky
- Enigmail, OpenPGP doplněk pro Thunderbird a Postbox
- Mailvelope pro Chrome nebo Firefox a web mailový účet jako Gmail, Outlook, Yahoo nebo GMX.
- hlavně kamaráda, který také používá PGP a vyměníme si spolu veřejné klíče

# Zdroje


- http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html
- http://lifehacker.com/how-to-encrypt-your-email-and-keep-your-convers
- http://en.wikipedia.org/wiki/E-mail_privacy
- http://pcworld.cz/internet/tip-sifrujte-svou-e-mailovou-komunikaci-1-dil-4
- http://www.blog.sslmarket.cz/ssl/mejte-bezpecnost-svych-e-mailu-pod-kontrolou/