Napadnutelná místa v komunikaci

Beret

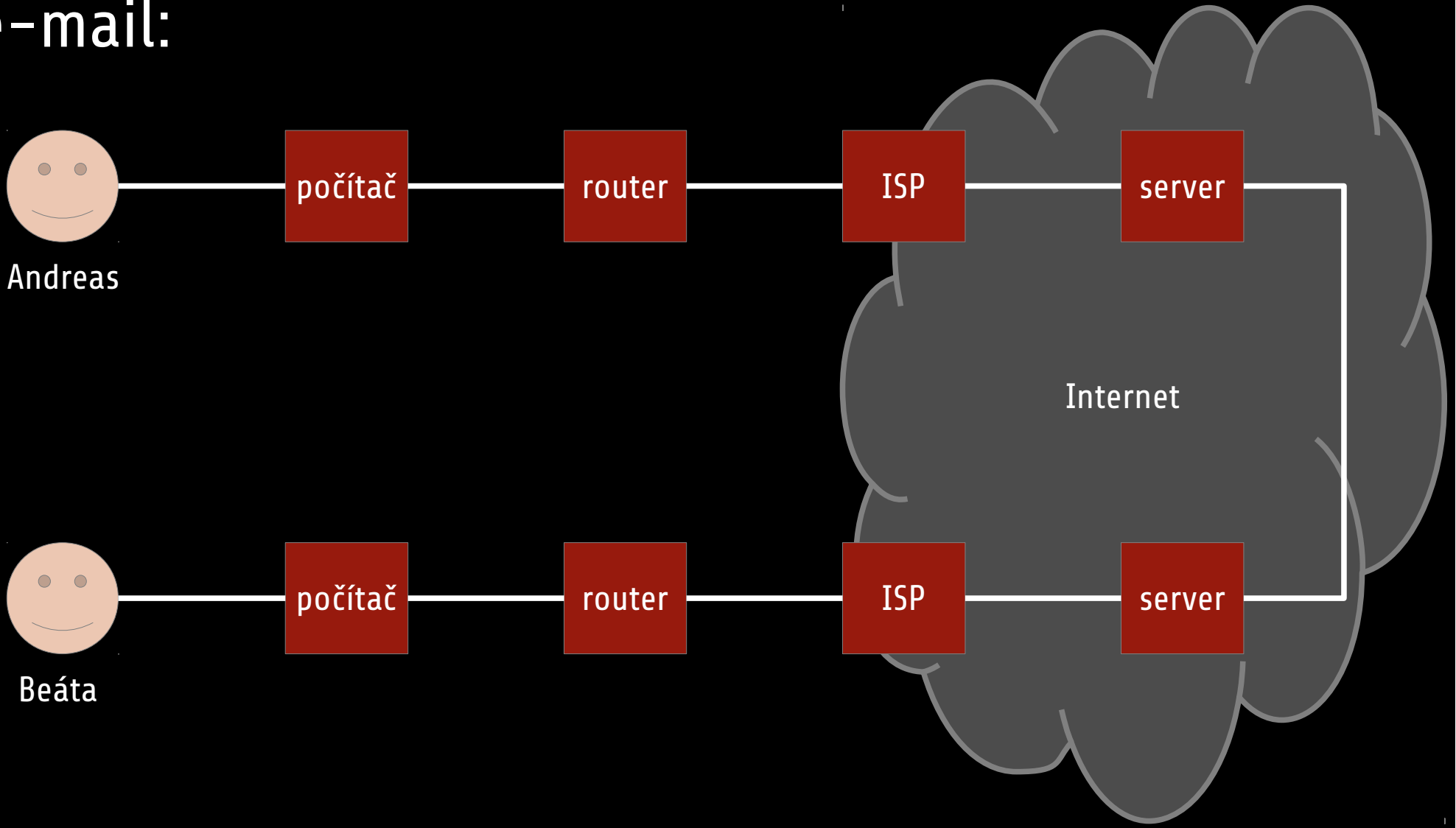
CryptoParty 11.02.2013

Obsah prezentace

1. Příklad komunikace: e-mail
2. Napadnutelná místa
3. Typy narušitelů
4. Metody ochrany
   - obecně
   - šifrování komunikace – klient-server, end-to-end
   - VPN, anonymizace
   - off-line ochrana dat

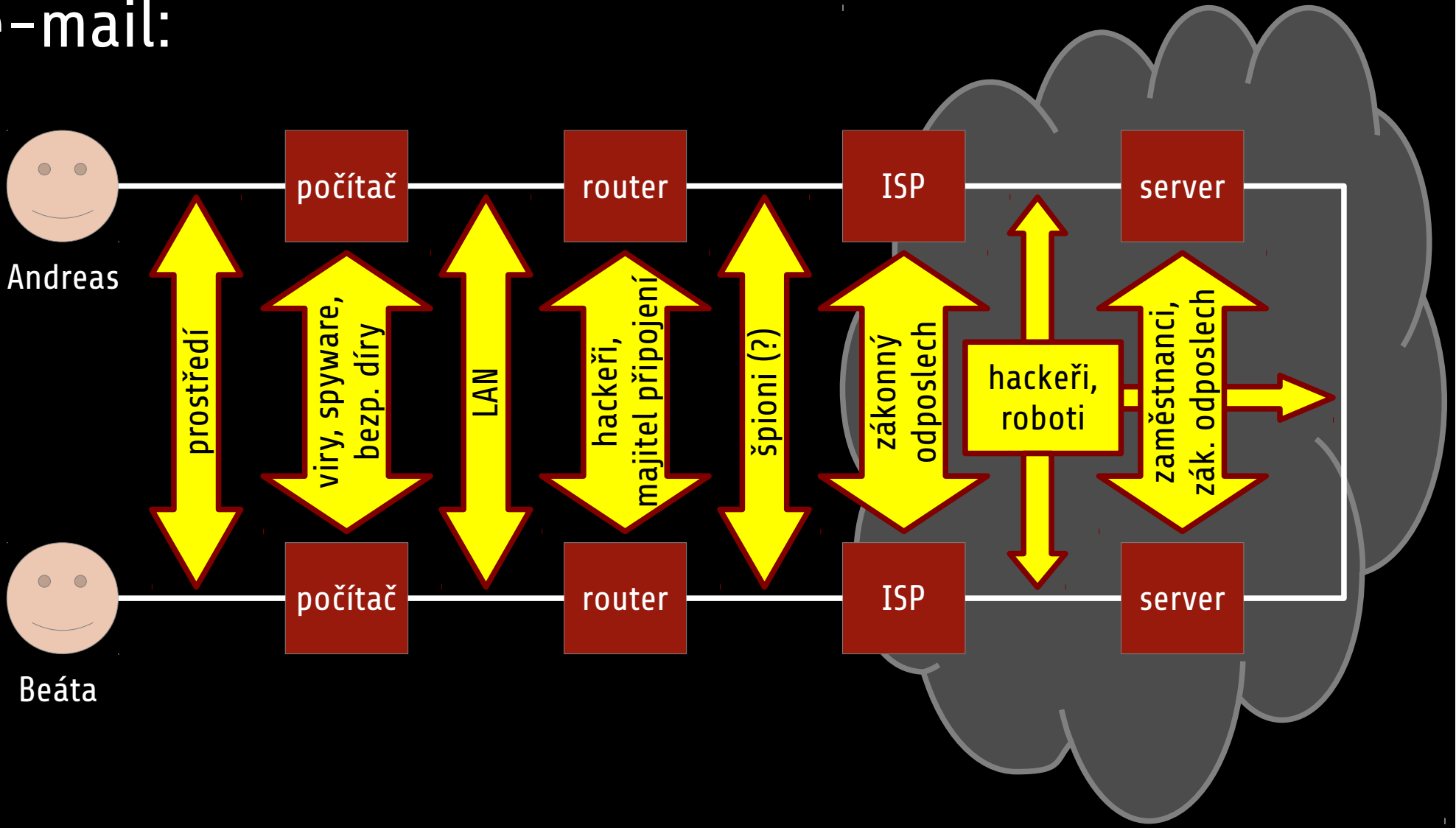
Příklad komunikace

- e-mail:



Napadnutelná místa

- e-mail:



Typy narušitelů

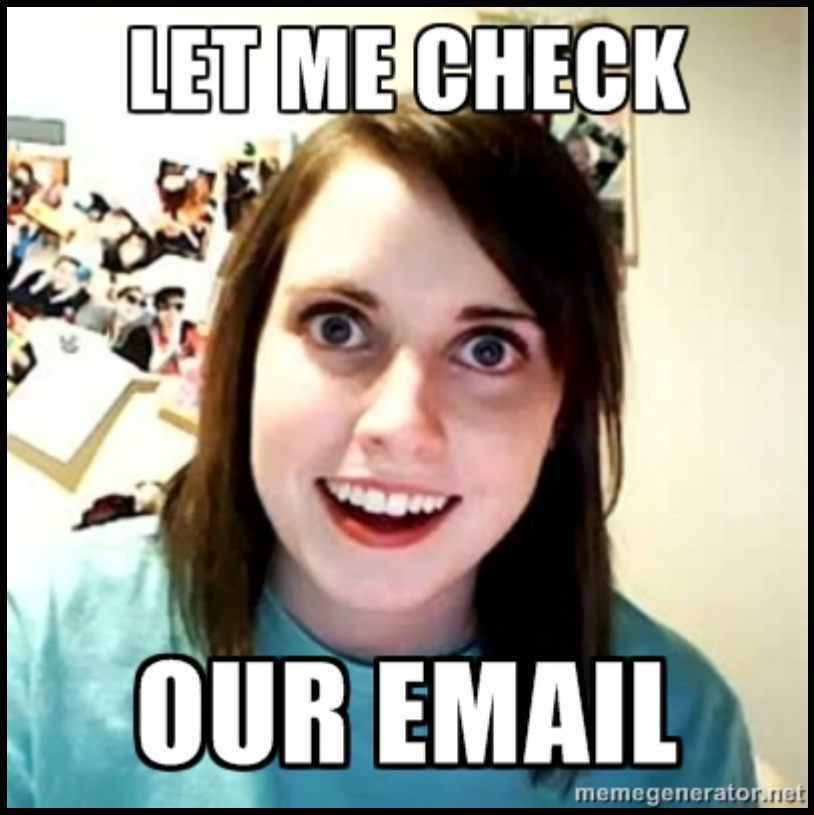
- kyberzločinci
  - získání dat: slabiny systému (nelegální)
  - využití: zábava, podvody, spam, krádež identity
- poskytovatelé
  - získání dat: uživatelé jim je svěřují
  - využití: cílená reklama
- zákonné složky
  - získání dat: soudní příkazy, odposlechy
  - využití: odhalování zločinu (včetně porušování copyrightu)

Metody ochrany – obecně

- bezpečnostní záplaty, firewall, antivirus, …
  - proti napadení systému
- šifrování
  - proti čtení informací
- podepisování
  - proti změně informací (zejména přesměrování toku)
- anonymizace
  - proti identifikaci odesílatele

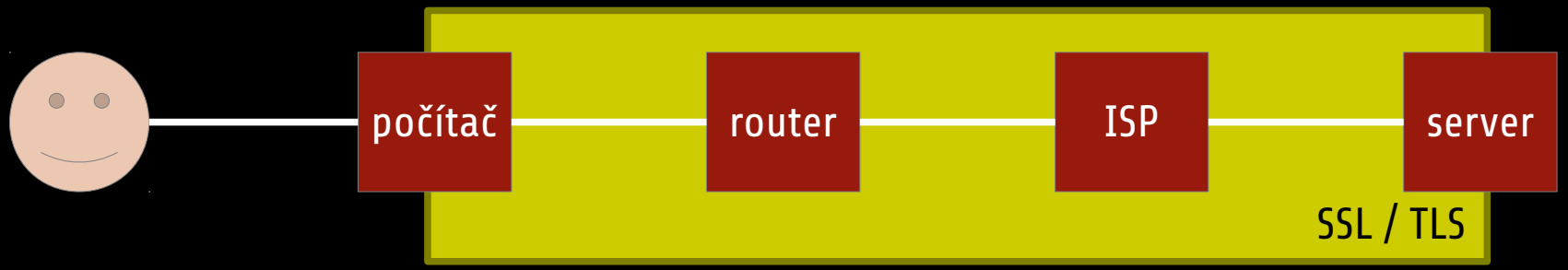
Metody ochrany

- pravidelné aktualizace, antivirus, antispyware, firewall, …
  - tomu se věnují jiní
- neudělejte si díru ve vlastním systému
  - spyware
  - osoby s přístupem k hardwaru
  - nešifrované informace (logy, uložené e-maily)



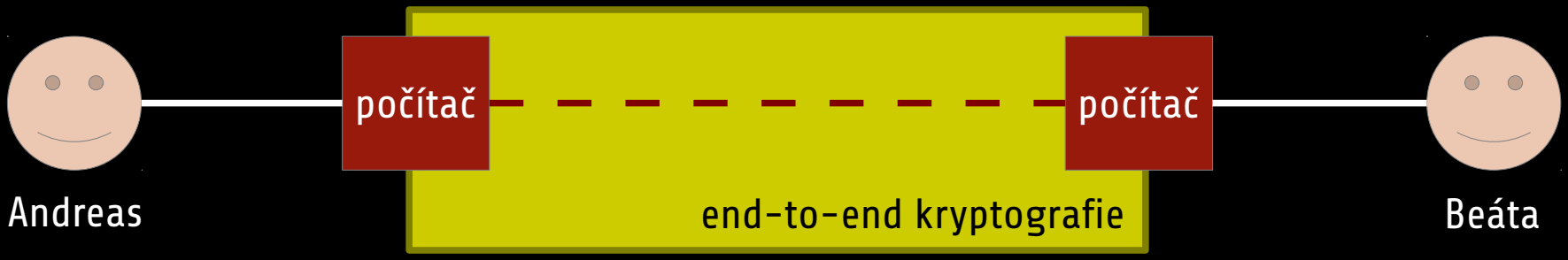
Metody ochrany

- zabezpečené spojení se serverem (SSL / TLS)
  - šifrování a podepisování
  - mezi klientem a serverem
  - univerzální použití
    (HTTPS, FTPS, POP3S, IMAPS, XMPP, ...)
  - lze napadnout pomocí:
    - hlouposti uživatele (ignoruje varování)
    - narušení certifikační autority



Metody ochrany

- end-to-end kryptografie (PGP, OTR, ...)
  - šifrování a podepisování
  - mezi klientem a klientem
  - pluginy do existujících služeb (Enigmail, Pidgin-OTR)
  - nutné ověřit uživatele,
    jinak hrozí Man-in-the-Middle Attack

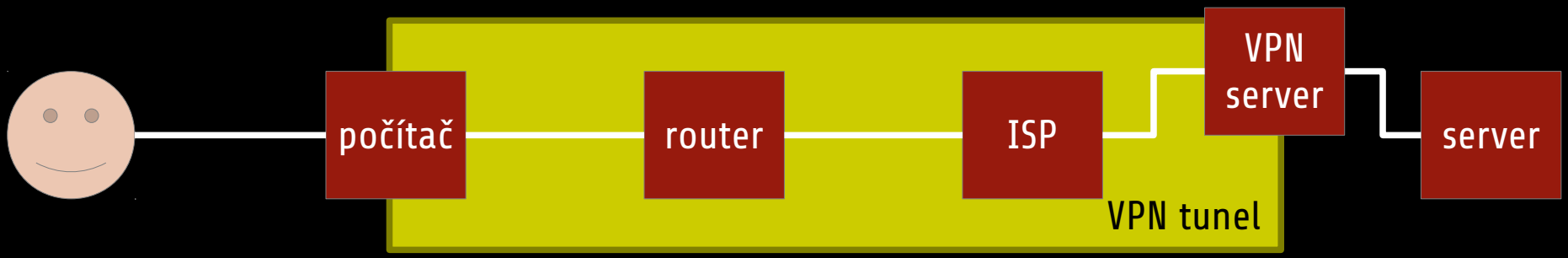


Metody ochrany

- pozn.: kombinace SSL / TLS a end-to-end
  - některá data chceme bezpečně odeslat serveru (heslo)
  - jiná data chceme bezpečně odeslat uživateli (zpráva)

Metody ochrany

- Virtual Private Network (VPN)
  - šifrování a podepisování
  - zabezpečený tunel od klienta k VPN serveru (tj. i skrz ISP)
  - získání bezpečí na nedůvěryhodných sítích (veřejná Wi-Fi)
  - využívají firmy s externími pracovníky
  - obvykle placené
  - pouze přesouvá napadnutelné místo jinam



Metody ochrany

- anonymizace (proxy, Tor)
  - obvykle změna IP adresy
  - „splynutí s davem“
  - je snadné se prozradit (přihlášení na Facebook, ID prohlížeče, styl psaní, end-to-end korelace)
  - nezaměňovat anonymitu se soukromím

Metody ochrany

- šifrování disku (TrueCrypt, dm-crypt, …)
  - chrání data, když je počítač vypnutý
  - odcizení, pohraniční kontrola, …
  - vyžaduje heslo při spuštění nebo probuzení počítače
- šifrování souborů
  - lze použít GnuPG, RAR, …
  - šifrované klíčenky (KeePass, součást Firefoxu, …)
    - fungují správně pouze s odemykacím heslem!

Metody ochrany

- steganografie (steghide)
  - popření existence tajných informací
  - skrytí v jiných datech (obrázky, hudba)

Závěr

Závěr

- komunikaci lze narušit na mnoha místech
- zabezpečený počítač je základ
- SSL a TLS chrání před zločinci – používat, kde to jde
- soukromé zprávy je vhodné chránit end-to-end
- VPN chrání v nejistých prostředích
- anonymita je křehká, Tor ji může poskytnout
- šifrování dat na disku je vhodné pro případ odcizení