Bezpečnost vzdáleného přístupu

Jan Kubr

Vzdálené připojení - protokoly

- IPsec
- PPTP, P2TP
- SSL, TSL

IPsec I

- RFC 4301-4309
- IPv6, IPv4
- autentizace – Authentication Header (AH)
- šifrování – Encapsulating Security Payload (ESP)
- transportní režim
  - vložení bezpečnostních hlaviček
- tunelující režim
  - zabalení datagramu do datagramu s bezpečnostními hlavičkami

IPsec II

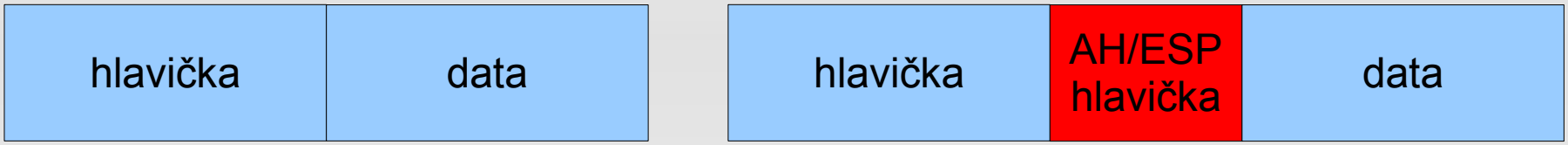
- bezpečnostní asociace (SA)
  - bezpečnostní protokol (AH, ESP)
  - algoritmus
  - klíče …
  - jednosměrné
- databáze bezpečnostních politik (SPD)
  - zahodit, zpracovat (bez IPsec), použít IPsec
  - manuální konfigurace
  - Internet Security Association and Key Management Protocol (ISAKMP)

IPsec III

- výměna klíčů
  - Internet Key Exchange (IKE)
  - Diffie-Hellman
- problém autentizace
  - Public Key Infrastructure (PKI)
- NAT Traversal (NAT-T)

IPsec – režimy provozu

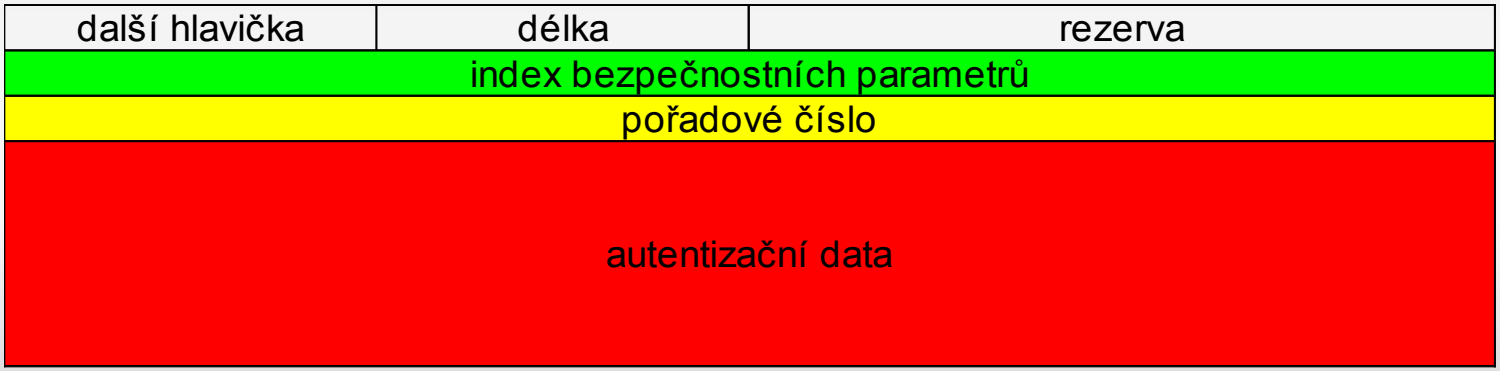
transportní režim



tunelující režim

Authentication Header

- slouží pro autentizaci dat
- umožňuje ochranu proti opakování
- SHA1, null, (MD5)
- postup
  - vložení AH hlavičky
  - vyplnění položek (autentizační data vynuluje)
  - výpočet autentizačních dat (dočasná úprava dat)

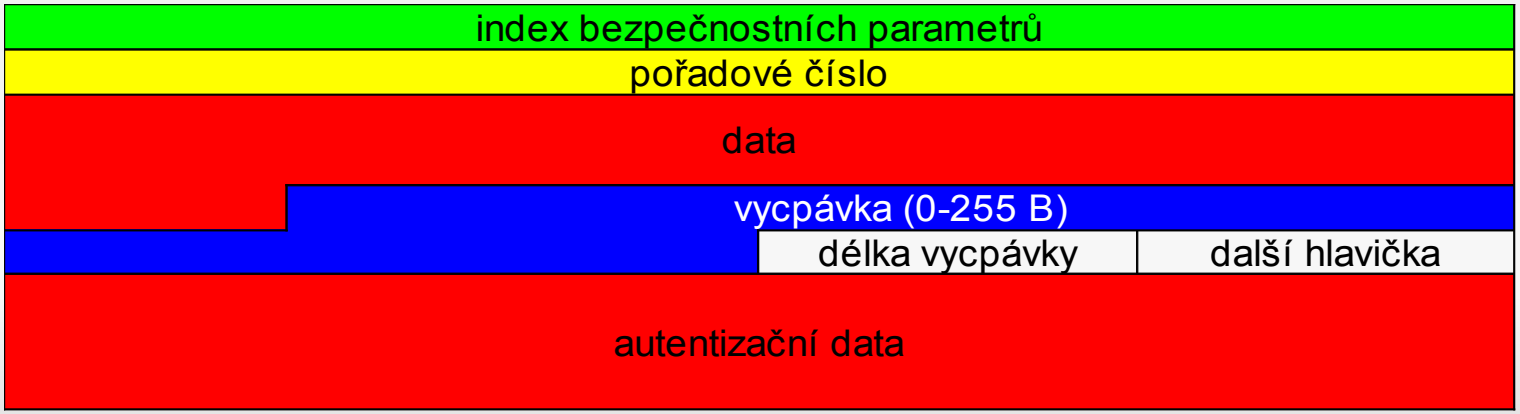


Encapsulating Security Payload I

- slouží pro šifrování obsahu (i služby AH)
- data a další hlavičky jsou obsah ESP hlavičky
- 3DES, null, (AES), ((DES))

Encapsulating Security Payload II

- postup
  - umístění ESP hlavičky, vycpávky, šifrování
  - vytvoření pořadového čísla
  - vytvoření autentizačních dat (je-li požadována autentizace a kontrola integrity)
  - fragmentace až po šifrování



IPsec - vlastnosti

- Point-to-Point spoje
- standard
- složitý na konfiguraci
- složitý na implementaci
- IKE – UDP 500
- NAT-T – UDP 4500
- ESP – IP id 50

Point-to-Point tunneling protocol

- není IETF standard
- autentizace MSCHAPv2, EAP-TLS
- šifrování Microsoft Point-to-Point Encryption
  - klíč odvozen z hesla
  - RSA RC4
- TCP 1723 – řízení
- Generic Routing Encapsulation (IP id 47) – data

Layer 2 tunneling protocol

- L2TP, L2TP/IPsec
- RFC 2661
- šifrování IPsec
  - DES, 3DES, AES
- UDP 1701 – vpn
- UDP 500 – IKE pro IPsec
- IP id 50 – ESP zapouzdření IPsec

Secure Sockets Layer (SSL) Transport Layer Security (TLS)

- původně pro http
  - imap. pop, smtp ...
- výměna klíčů
  - Diffie-Hellman, RSA, DSA, SRP, PSK
- šifrování
  - RC4, 3DES, AES, Camellia
- otisk
  - MD5, SHA

Vzdálené připojení - požadavky

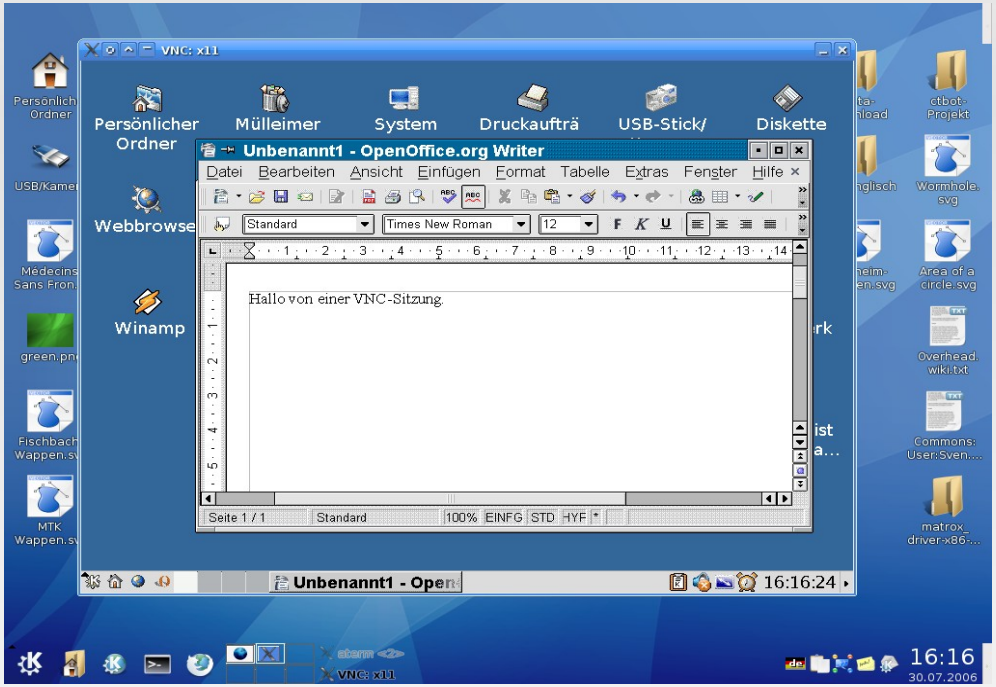
- přístup k www
- přístup k poště
- přístup k souborům
- přístup k aplikacím
- ...

Vzdálené připojení - aplikace

- vzdálený terminál
- ssl varianty aplikačních protokolů
- ssh
- vpn
  - pptp
  - ssl
  - IPsec

Vzdálený terminál

- VNC
  - TCP 5900-5906
  - ssh, vpn
- RDP
  - TCP 3389
  - RC4 (128b), TLS
- X Window
  - ssh
- ICA, NX



Vzdálený terminál – vlastnosti

- není přímý přístup k souborům
- jediný kanál k jedinému serveru
- společné prostředí a aplikace
- složité nastavení na různých platformách
- nízká výkonnost

Aplikace s ssl

- fungující standard
- podpora https aplikací
- ssl tunel
- omezené množství aplikací s ssl

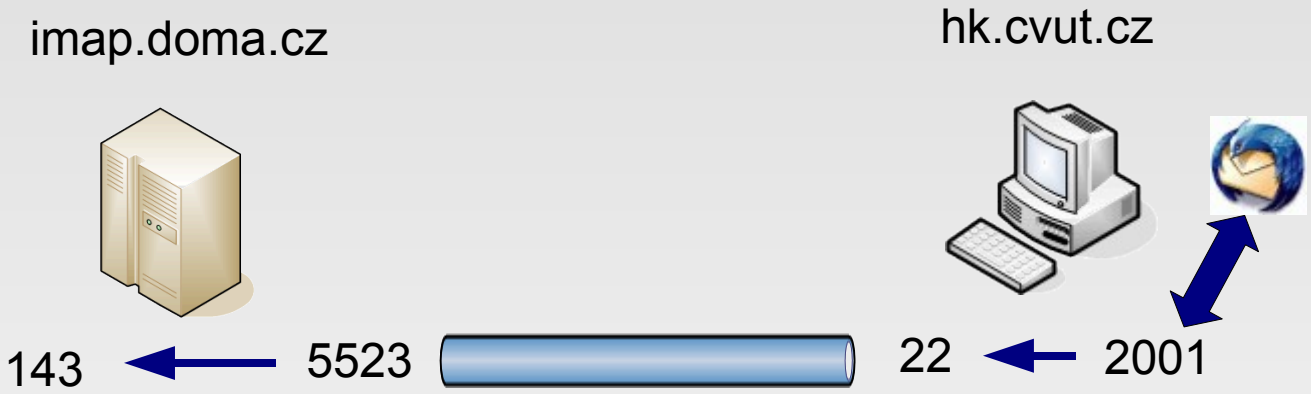
Secure Shell (ssh)

- terminálový přístup
- přenos souborů
- port forwarding
- X11 forwarding
- podpora vpn
- lze použít jen pro tunelování TCP

ssh tunel I

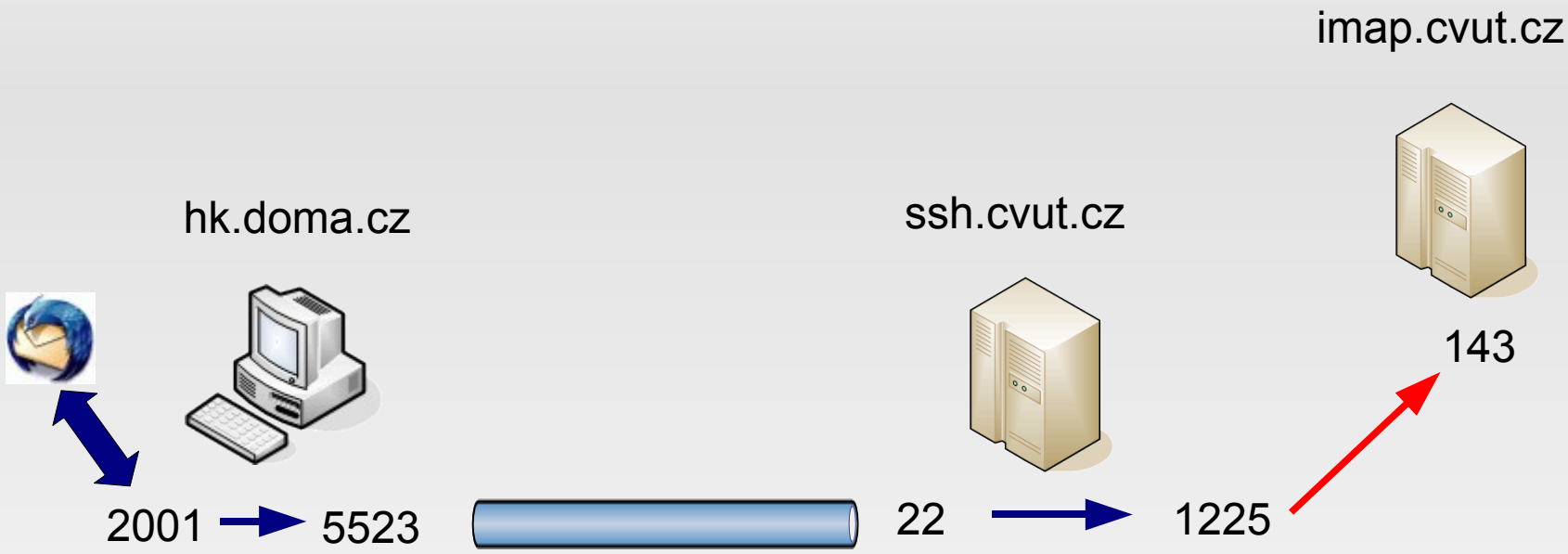
ssh -L2001:localhost:143 imap.cvut.cz
ssh -L2001:imap.cvut.cz:143 imap.cvut.cz

ssh tunel II



ssh -R2001:localhost:143 hk.cvut.cz

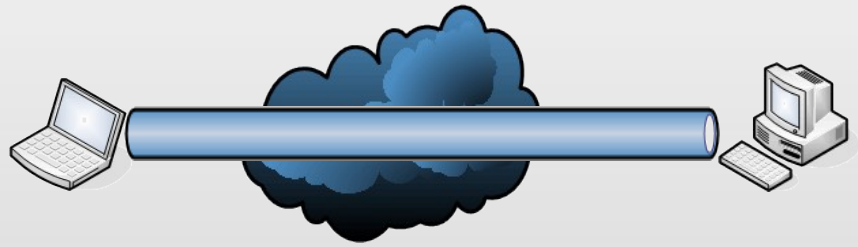
ssh tunel III

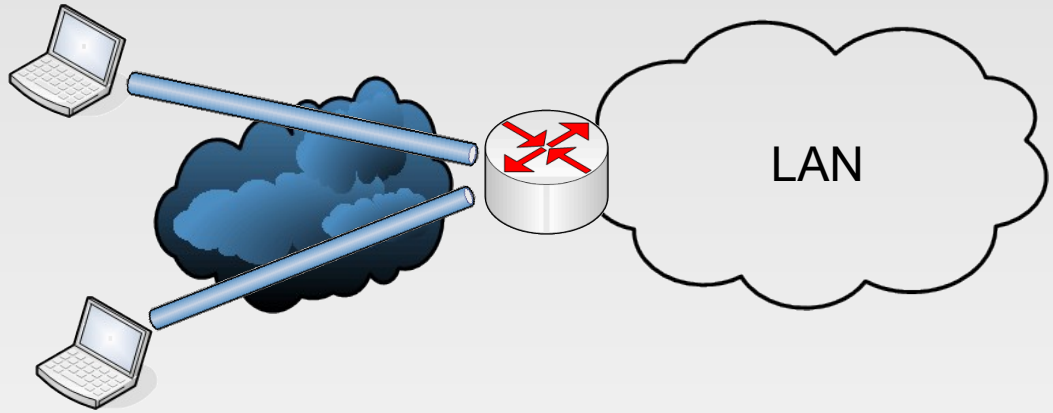


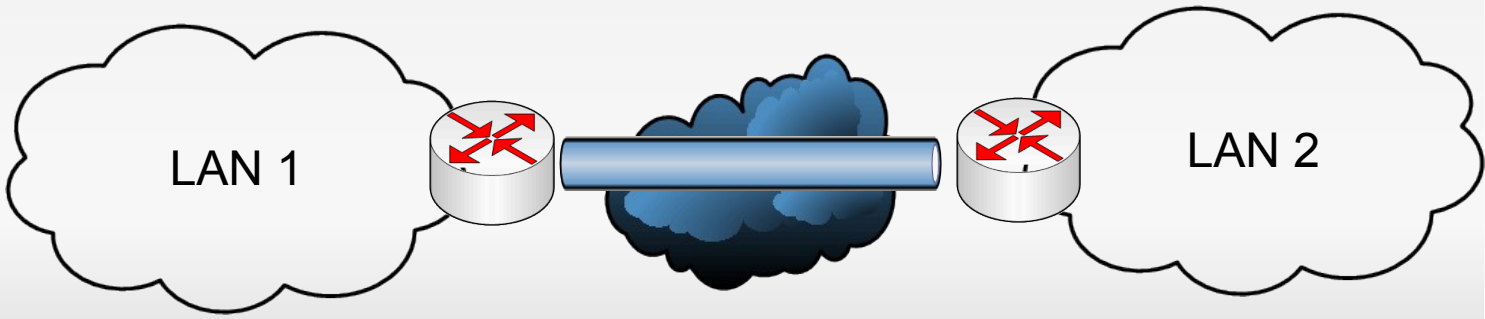
ssh -L2001:imap.cvut.cz:143 .ssh.cvut.cz

Virtual Private Network (vpn)

- způsob spojení
  - klient – klient
  - klient – brána
  - brána – brána
- protokol
  - PPTP
  - L2TP
  - SSL
  - SSH
  - IPsec







vpn - vlastnosti

- transparentní spojení
- nižší zatížení oproti vzdálenému terminálu
- složité nastavení klientů
- rozdílné prostředí
- lokálně instalované aplikace
- složitá implementace IDS

Vzdálený přístup bezpečnostní rizika

- chybné nastavení tunelu
  - X11 ssh tunneling
- kompromitování klienta
  - útok zevnitř sítě
  - nová brána do Internetu
  - nastavení osobního paketového filtru
- složitý dohled sítě
  - IDS ...

A mnoho dalšího ...

Literatura

- http://www.rfc-editor.org
- http://crypto-world.info
- Pavel Satrapa, IPv6, Cesnet, 2002
- Wenbo Mao, Modern Cryptography, Prentice Hall, 2004
- Barrett, Silverman, SSH, O'Reilly, 2003
- Northucutt, Network Perimeter Security, New Riders, 2003