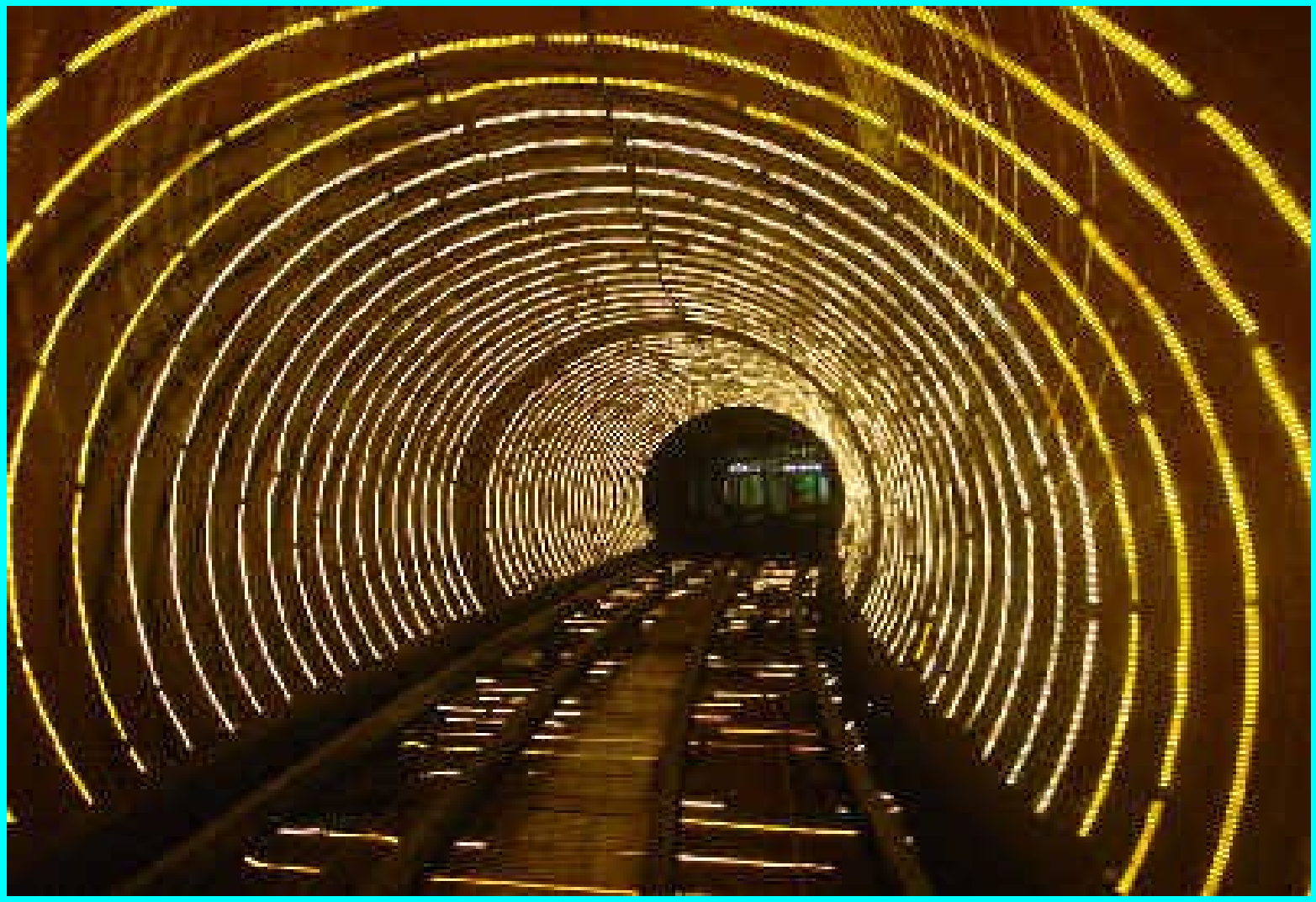
Tunelování



Jiří Jánský SUT SH 27.10.2009

Průchodnost

- máme síť s omezením služeb
- zjistíme otevřené porty – nmap
- přes otevřené porty vytvoříme spojení do našeho počítače v internetu
- openvpn (udp), ssh tunel (tcp)

- pokud jsou všechny porty uzavřené, můžeme se pokusit zabalit provoz do icmp, dns nebo http(s)

SSH tunel

- ssh -L <locport>:<remotehost>:<remoteport>
  - přitáhne remoteport z remotehost na locport
- ssh -R <remoteport>:<localhost>:<localport>
  - dotlačí localport z localhost na remoteport
- ssh -N -w any root@sut-intel.sh.cvut.cz
  - vytvori p2p tunel pomoci virtualních rozhraní tun
  - PermitTunnel Yes do /etc/ssh/sshd_config

Ping Tunnel

- „For those times when everything else is blocked.“
- implementace jako přesměrování portů

- server: ptunnel -v 4
- client: ptunnel -p sut-intel.sh.cvut.cz -lp 81 -da sut-intel.sh.cvut.cz -dp 80 -v 4

- max 62kBps (1052 znaku v 1080 ip paketu)

ICMTX

- IP-over-ICMP
- implementace pomoci tun devices

- server: icmptx -s sut-intel
- client: icmptx -c sut-intel

- nestabilní při rychlostech nad 1MBps

NSTX

- Komunikace pomocí DNS dotazů a odpovědí přes lokální DNS server (při otevřeném UDP 53 je lepší použít přímý tunel)
- delegujem poddoménu na náš počítač
  sut.oskar.aa.am IN NS sut-intel.sh.cvut.cz
- místo nameserveru spustíme tunelovací program
- komunikujem
- Strahov 320kBps - overload 2.5x (max 255 znaku u 400 ip paketu)
- další iodyne, OzymanDNS

NSTX - použití

apt-get install nstx

server:

nstxd sut.oskar.aa.am

ifconfig tun0 up 10.0.0.1 netmask 255.255.255.0

client:

nstxcd sut.oskar.aa.am 147.32.127.241

ifconfig tun0 up 10.0.0.2 netmask 255.255.255.0

Reference

- OpenVPN od Ondřeje Caletky na

  http://avc.sh.cvut.cz
- SSH tun tunnel

  http://www.debian-administration.org/articles/539
- Ping Tunnel

  http://www.cs.uit.no/~daniels/PingTunnel/
- ICMPTX (IP-over-ICMP) HOWTO

  http://thomer.com/icmptx/
- NSTX (IP-over-DNS) HOWTO
  http://thomer.com/howtos/nstx.html

Dotazy ???

Děkuji za pozornost.

HTTP(S) od Oskara