# Oblíbené omyly v bezpečnosti

Pavel Růžička
<ruza@ruza.eu>

Brmlab
hackerspace Prague
Lightning talks

3. listopadu 2011

# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX

# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX
- Všichni sekuriťáci vás budou vždycky strašit "co by kdyby"

# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX
- Všichni sekuriťáci vás budou vždycky strašit "co by kdyby"
  - .. a nikdy s tím nepřestanou.

# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX
- Všichni sekuriťáci vás budou vždycky strašit "co by kdyby"
  - .. a nikdy s tím nepřestanou.
    - A pokud přestanou tak asi nejsou až tak dobří bezpečáci.

# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX
- Všichni sekuriťáci vás budou vždycky strašit "co by kdyby"
  - .. a nikdy s tím nepřestanou.
    - A pokud přestanou tak asi nejsou až tak dobří bezpečáci.
- Respektujte je, většinou vědí o čem mluví!

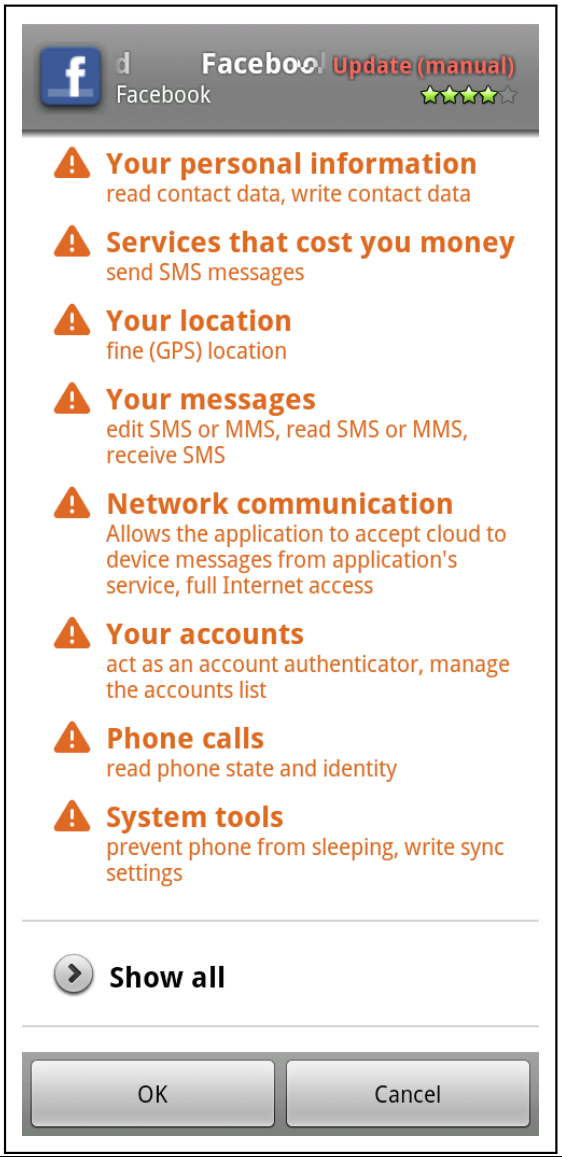
# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX
- Všichni sekuriťáci vás budou vždycky strašit "co by kdyby"
  - .. a nikdy s tím nepřestanou.
    - A pokud přestanou tak asi nejsou až tak dobří bezpečáci.
- Respektujte je, většinou vědí o čem mluví!
  - .. ale berte na vědomí že potřebují váš strach aby si u vás vydělali.

# Bezpečáci a pojišťováci

- Moje první prezentace v  LaTeX
- Všichni sekuriťáci vás budou vždycky strašit "co by kdyby"
  - .. a nikdy s tím nepřestanou.
    - A pokud přestanou tak asi nejsou až tak dobří bezpečáci.
- Respektujte je, většinou vědí o čem mluví!
  - .. ale berte na vědomí že potřebují váš strach aby si u vás vydělali.

# Nečekejte soukromí kde nikdy nebylo a zřejmě ani nebude




TOTO není vtip!

# nobody není jen tak nikdo

```
nekdo@nekde:~$ grep nobody /etc/passwd
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

Pozor na sdílení práv

dnsmasq - A lightweight DHCP and caching DNS server.
dříve i nfs, apache a další.

# Známější nesmysly

- naučili jsme se utahovat šrouby, tak to tak děláme dál

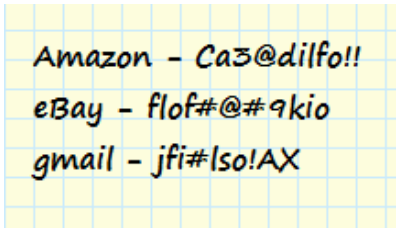
  přísná bezpečnostní politika

# Známější nesmysly

- naučili jsme se utahovat šrouby, tak to tak děláme dál
  - příliš přísná bezpečnostní politika

# Známější nesmysly

- naučili jsme se utahovat šrouby, tak to tak děláme dál
  - příliš přísná bezpečnostní politika
  - => hesla na papírcích



# Nebezpečí bezpečnostních otázek

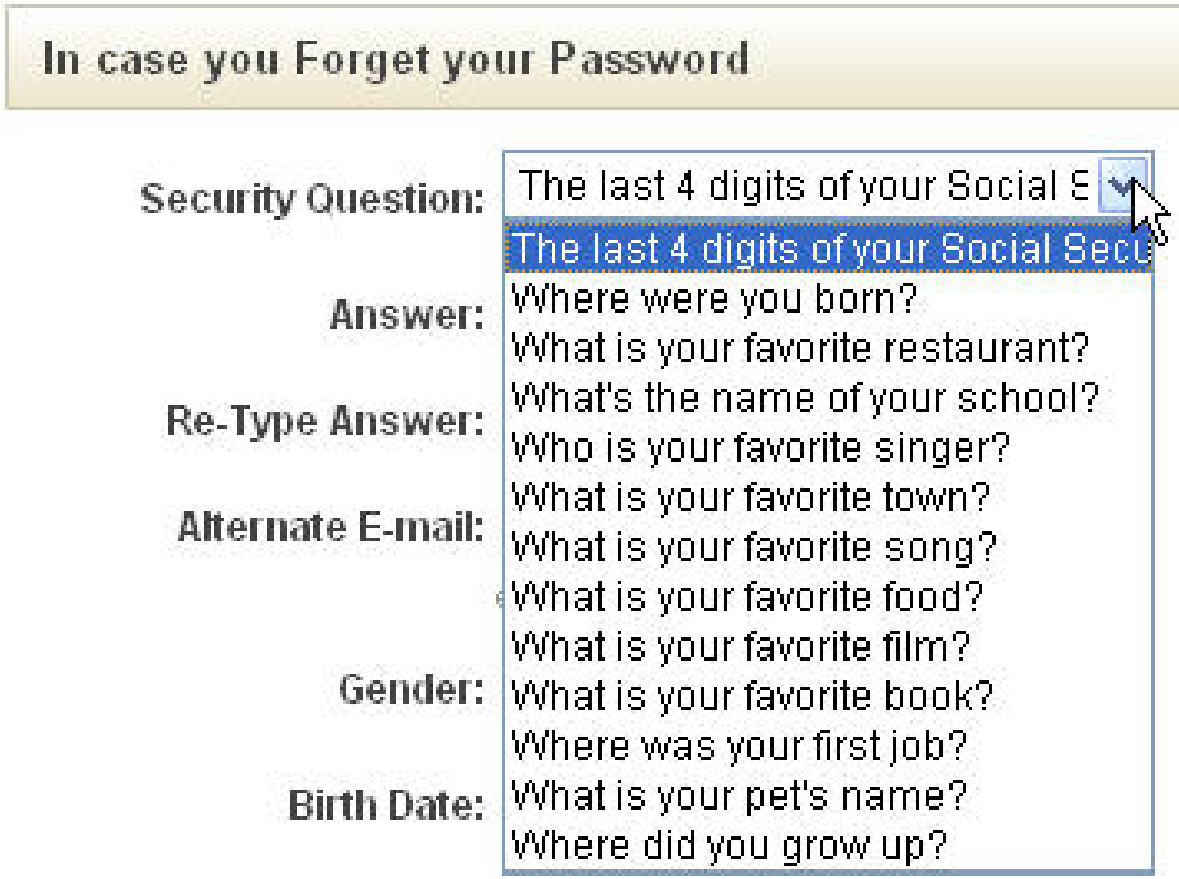
HESLO: ohafah3-9fjJFNAP32'FN3A-0RJ32-RJm32M3A-20RJ32A


Odpověď na bezpečnostní otázku: Azor

brmlab hackerspace prague

# Nebezpečí bezpečnostních otázek

HESLO: ohafah3-9fjJFNAP32'FN3A-0RJ32-RJm32M3A-20RJ32A




Odpověď na bezpečnostní otázku: Azor

brmlab hackerspace prague

# Biometrie

- princip variability mezi jednotlivci

# Biometrie

- princip variability mezi jednotlivci
- každé sejmutí dat musí korelovat nepřesnosti
- při silnější shodě předloženého vzorku s uloženým vzorem by měla být nižší pravděpodobnost obejití autentizace

# Biometrie

- princip variability mezi jednotlivci
- každé sejmutí dat musí korelovat nepřesnosti
- při silnější shodě předloženého vzorku s uloženým vzorem by měla být nižší pravděpodobnost obejití autentizace
- absolutní shoda by ale měla být vyhodnocena jako replay attack

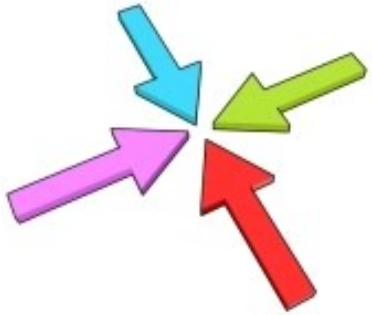
# Končí éra IP filtrů?

# Končí éra IP filtrů?

# Končí éra IP filtrů?


# Končí éra IP filtrů?


# Končí éra IP filtrů?

# "a teď potřebujeme pracovat na tomhle"

# Mnohem větší tlak na autentizační mechanismy

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM
- dedikované linky

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM
- dedikované linky
- dedikované servery

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM
- dedikované linky
- dedikované servery

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM
- dedikované linky
- dedikované servery

- většina komunikace přes Internet

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM
- dedikované linky
- dedikované servery

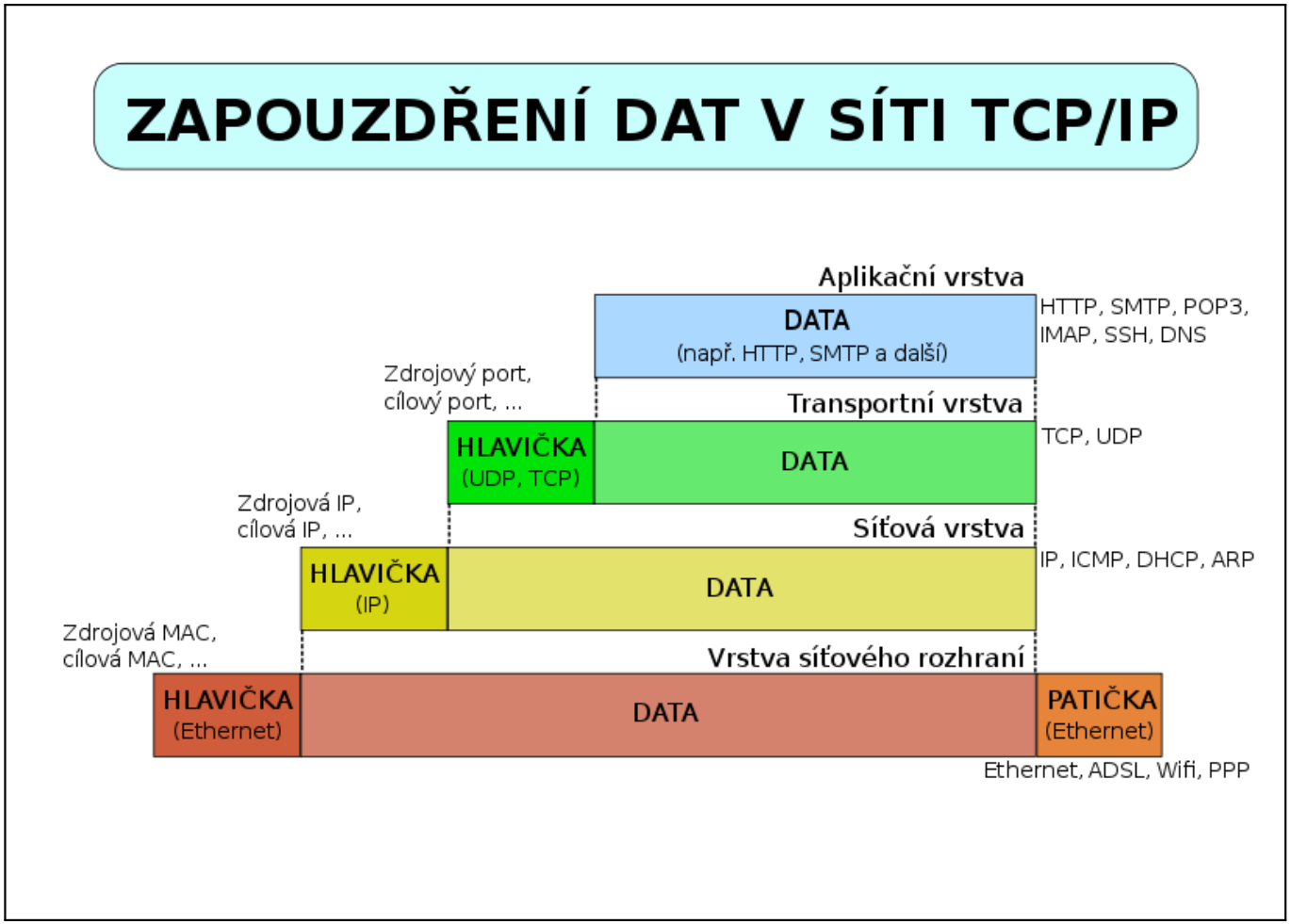
- většina komunikace přes Internet
- virtuály sdílející hw (s kým?)

# Mnohem větší tlak na autentizační mechanismy

- žádné ATM
- dedikované linky
- dedikované servery

- většina komunikace přes Internet
- virtuály sdílející hw (s kým?)
- cloudy (kde?)

# Končí éra IP filtrů?



# a taky kvůli IPv6 (IPocalypse)

# IPv6 - rozhovor

"IPv6 konektivita mě nemusí zajímat, to nemám."

# IPv6 - rozhovor

"IPv6 konektivita mě nemusí zajímat, to nemám."

"Má!" autokonfigurace, link-local adresy

# IPv6 - rozhovor

"IPv6 konektivita mě nemusí zajímat, to nemám."

"Má!" autokonfigurace, link-local adresy

"Ale ten hacker určitě nemá moji IPv6 adresu,
tu já ani nepřečtu natož aby si ji někdo pamatoval."

# IPv6 - rozhovor

"IPv6 konektivita mě nemusí zajímat, to nemám."

"Má!" autokonfigurace, link-local adresy

"Ale ten hacker určitě nemá moji IPv6 adresu,
tu já ani nepřečtu natož aby si ji někdo pamatoval."

"Má ji!" On se na ni totiž zeptá ;)

# Separátní routovací pravidla pro IPv4 a IPv6

```
nekdo@nekde:~$ ip r
default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.22

nekdo@nekde:~$ ip -6 r
2001::/32 dev teredo  proto kernel  metric 256
fe80::/64 dev eth0  proto kernel  metric 256
fe80::/64 dev teredo  proto kernel  metric 256
default dev teredo  metric 1029
```

# Separátní routovací pravidla pro IPv4 a IPv6

```
nekdo@nekde:~$ ip r
default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.22

nekdo@nekde:~$ ip -6 r
2001::/32 dev teredo  proto kernel  metric 256
fe80::/64 dev eth0  proto kernel  metric 256
fe80::/64 dev teredo  proto kernel  metric 256
default dev teredo  metric 1029
```

# Tady jsou jen ti co už s námi mluvili

```
nekdo@nekde:~$ ip -6 neigh
2001:470:caee:1::1 dev eth0 lladdr 00:16:76:93:45:a3 router REACHABLE
fe80::216:76ff:fe93:25b1 dev eth0 lladdr 00:16:76:93:25:b1 router STALE
```

# IPv6 - zjištění lokálních sousedů multicastem

```
nekdo@nekde:~$ ping6 -I eth0 ff02::1
PING ff02::1(ff02::1) from fe80::216:76ff:fe93:45b3 eth0: 56 data bytes
64 bytes from fe80::216:76ff:fe93:55b3: icmp_seq=1 ttl=64 time=0.033 ms (sám sobě si)
64 bytes from fe80::2e0:81ff:fe34:e3e9: icmp_seq=1 ttl=64 time=0.182 ms (DUP!)
64 bytes from fe80::20f:b0ff:fe7a:825f: icmp_seq=1 ttl=64 time=0.190 ms (DUP!)
64 bytes from fe80::216:d3ff:fe33:ce97: icmp_seq=1 ttl=64 time=0.282 ms (DUP!)
64 bytes from fe80::216:cbff:fec2:967: icmp_seq=1 ttl=64 time=0.288 ms (DUP!)
64 bytes from fe80::20b:cdff:fe24:939e: icmp_seq=1 ttl=64 time=1.08 ms (DUP!)
64 bytes from fe80::211:d8ff:fecc:981a: icmp_seq=1 ttl=64 time=7.57 ms (DUP!)
64 bytes from fe80::1e6f:65ff:fea5:b68a: icmp_seq=1 ttl=64 time=7.57 ms (DUP!)
64 bytes from fe80::219:d2ff:fe07:f363: icmp_seq=1 ttl=64 time=33.1 ms (DUP!)
64 bytes from fe80::226:5eff:fef8:4b87: icmp_seq=1 ttl=64 time=33.7 ms (DUP!)
```

https://secure.wikimedia.org/wikipedia/en/wiki/Multicast_address#IPv6

# IPv6 - zjištění lokálních sousedů multicastem

```
nekdo@nekde:~$ ping6 ff02::1%eth0
PING ff02::1(ff02::1) from fe80::216:76ff:fe93:45b3 eth0: 56 data bytes
64 bytes from fe80::216:76ff:fe93:55b3: icmp_seq=1 ttl=64 time=0.033 ms (sám sobě si)
64 bytes from fe80::2e0:81ff:fe34:e3e9: icmp_seq=1 ttl=64 time=0.182 ms (DUP!)
64 bytes from fe80::20f:b0ff:fe7a:825f: icmp_seq=1 ttl=64 time=0.190 ms (DUP!)
64 bytes from fe80::216:d3ff:fe33:ce97: icmp_seq=1 ttl=64 time=0.282 ms (DUP!)
64 bytes from fe80::216:cbff:fec2:967: icmp_seq=1 ttl=64 time=0.288 ms (DUP!)
64 bytes from fe80::20b:cdff:fe24:939e: icmp_seq=1 ttl=64 time=1.08 ms (DUP!)
64 bytes from fe80::211:d8ff:fecc:981a: icmp_seq=1 ttl=64 time=7.57 ms (DUP!)
64 bytes from fe80::1e6f:65ff:fea5:b68a: icmp_seq=1 ttl=64 time=7.57 ms (DUP!)
64 bytes from fe80::219:d2ff:fe07:f363: icmp_seq=1 ttl=64 time=33.1 ms (DUP!)
64 bytes from fe80::226:5eff:fef8:4b87: icmp_seq=1 ttl=64 time=33.7 ms (DUP!)
```

https://secure.wikimedia.org/wikipedia/en/wiki/Multicast_address#IPv6

# A teď máme od všech nejbližších sousedů navštívenky ;)

```
nekdo@nekde:~$ ip -6 neigh
fe80::1e6f:65ff:fed5:b68a dev eth0 lladdr 1c:6f:65:d5:b4:8a REACHABLE
2001:470:caee:1::1 dev eth0 lladdr 00:16:76:93:45:b3 router REACHABLE
fe80::216:cbff:fec1:964 dev eth0 lladdr 00:16:cb:c1:09:64 REACHABLE
fe80::224:1dff:fea6:3226 dev eth0 lladdr 00:24:1d:a6:32:26 REACHABLE
fe80::216:76ff:fe93:45b3 dev eth0 lladdr 00:16:76:93:45:b3 router REACHABLE
fe80::a00:27ff:fe3e:1df2 dev eth0 lladdr 08:00:27:3e:1d:f2 REACHABLE
fe80::219:d2ff:fe06:f263 dev eth0 lladdr 00:19:d2:06:f2:63 REACHABLE
fe80::a00:27ff:fe38:7c60 dev eth0 lladdr 08:00:27:38:7c:60 REACHABLE
fe80::2e0:81ff:fe36:e3e9 dev eth0 lladdr 00:e0:81:36:e3:e9 REACHABLE
fe80::20f:b0ff:fe7d:725f dev eth0 lladdr 00:0f:b0:7d:72:5f REACHABLE
```

# IPv6 - THC IPv6-attack toolkit

```
nekdo@nekde:~/thc-ipv6-1.8# ./alive6 eth0
Alive: 2001:470:caee:1:20d:cdff:fe27:939e
Alive: 2001:470:caee:1:20e:b0ff:fe7d:825f
Alive: 2001:470:caee:1:212:d8ff:fece:981a
Alive: 2001:470:caee:1:9e6f:65ff:fed5:b68a
Alive: 2001:470:caee:1:2f4:81ff:fe30:e3e9
Alive: 2001:470:caee:1:217:cbff:fec1:967
Found 6 systems alive
```

http://thc.org/thc-ipv6/

# IPv6 - THC IPv6-attack toolkit

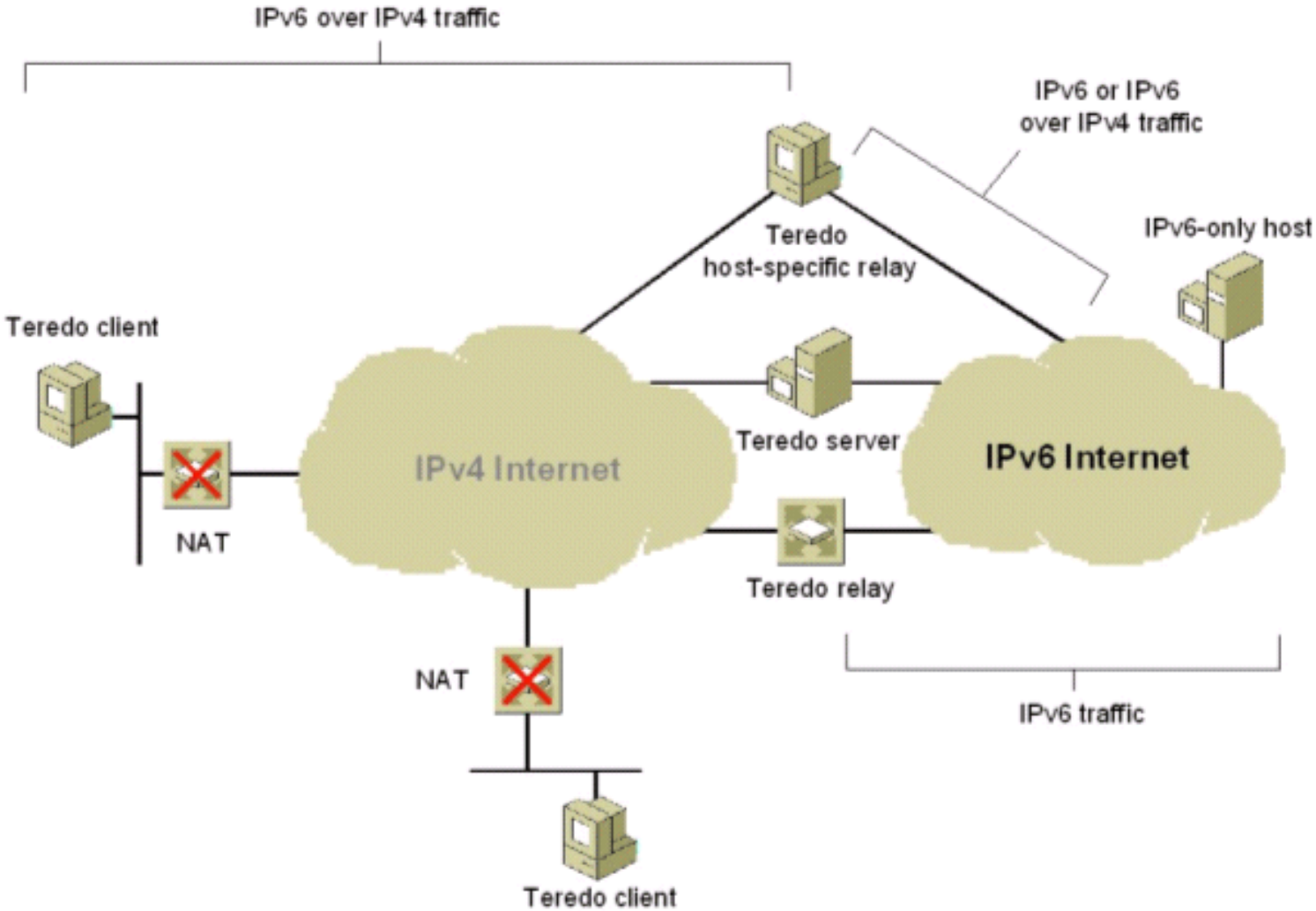
```
nekdo@nekde:~/thc-ipv6-1.8# ./alive6 eth0
Alive: 2001:470:caee:1:20d:cdff:fe27:939e
Alive: 2001:470:caee:1:20e:b0ff:fe7d:825f
Alive: 2001:470:caee:1:212:d8ff:fece:981a
Alive: 2001:470:caee:1:9e6f:65ff:fed5:b68a
Alive: 2001:470:caee:1:2f4:81ff:fe30:e3e9
Alive: 2001:470:caee:1:217:cbff:fec1:967
Found 6 systems alive
```

**http://thc.org/**thc-ipv6/

# Teredo (IPv6 over IPv4)

```
# apt-get install miredo

# /etc/miredo.conf
InterfaceName   teredo
# Pick a Teredo server:
#ServerAddress  teredo.ipv6.microsoft.com
#ServerAddress  teredo-debian.remlab.net
ServerAddress   teredo.nic.cz
# Some firewall/NAT setups require a specific UDP port num:
BindPort        3545
```


IPv6 over IPv4 traffic
IPv6 or IPv6
over IPv4 traffic
Teredo
host-specific relay
IPv6-only host
Teredo client
Teredo server
IPv4 Internet
IPv6 Internet
NAT
Teredo relay
NAT
IPv6 traffic
Teredo client

# Proč nás to všecko zajímá

```
root@omg:~# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy
ACCEPT)
target     prot opt source               destination
```

# Proč nás to všecko zajímá

```
root@omg:~# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy
ACCEPT)
target     prot opt source               destination
```

# Proto :)

```
root@omg:~# netstat -ntlp|grep :22
tcp   0   0 0.0.0.0:22   0.0.0.0:*   LISTEN    5452/sshd
tcp6  0   0 :::22             :::*   LISTEN    5452/sshd
```

.. a nejen proto

# Proto :)

```
root@omg:~# netstat -ntlp|grep :22
tcp   0   0 0.0.0.0:22   0.0.0.0:*   LISTEN    5452/sshd
tcp6  0   0 :::22             :::*    LISTEN    5452/sshd
```

.. a nejen proto

# Skenování na IPv6 - jaké cestičky vedou k sousedům

```
nmap -6 -PN ${HOST}%${IFACE}
```

# Skenování na IPv6 - jaké cestičky vedou k sousedům

```
#!/bin/bash
```

```
for HOST in ${IPV6_ADDRS}
  do
    nmap -6 -PN ${HOST}%${IFACE}
  done
```

# Skenování na IPv6 - jaké cestičky vedou k sousedům

```
#!/bin/bash

IFACE="eth0"
IPV6_ADDRS="$(ping6 -I ${IFACE} ff02::1 -c 2|grep icmp_seq=1\
 |awk 'print $4'|sed 's/:$//')"

for HOST in ${IPV6_ADDRS}
  do
    nmap -6 -PN ${HOST}%${IFACE}
  done
```

# IPv6 skill improving project

http://brmlab.cz/project/ipv6

# Nashle na psychiatrii