# IPsec na Linuxu

Pavel Šimerda
pavlix@pavlix.net

39. konference EurOpen.CZ

http://data.pavlix.net/europen39/

# Cíle IPsec

- Zabezpečení IP vrstvy (IP security → IPsec)
- Autentizace strojů a uživatelů
- Integrita přenášených dat
- Utajení přenášených dat
- Odolnost proti útokům
- Transparentnost, otevřenost

# Předmětem přednášky jsou...

- Praktické ukázky (funguje to!)
- Vybrané případy užití
- Příklady konfigurace
- Datové toky na síti

# Předmětem přednášky naopak není...

- Kryptografie
- Bezpečnost protokolů
- Efektivita protokolů
- Srovnání s alternativami

# IPsec – Sada standardů

- IPsec je ekosystém, stavebnice
- Jednotlivé standardy se vyvíjejí a nahrazují
- Je v tom zmatek!

# IPsec – Co nás bude zajímat

- Bezpečnostní asociace
- Bezpečnostní politiky
- ESP – protokol pro šifrovanou komunikaci
- Transportní a tunelová varianta
- ISAKMP/IKE/IKEv2 – protokoly pro sestavení bezpečnostních asociací
- IPv4 NAT-T – mechanismus pro překonávání IP maškarády

# Ochutnávka: Manuální konfigurace šifrovaného kanálu

# Úkol: Šifrovaný kanál

Test jednosměrného zabezpečeného kanálu z uzlu a.example.net do uzlu b.example.net.

- Bezpečnostní politika
- Bezpečnostní asociace
- Transportní varianta protokolu ESP

# Transportní varianta ESP

- Pořadí hlaviček: IPv4/IPv6—ESP—ICMP/UDP/TCP
- ESP zajišťuje autenticitu, integritu i utajení
- Není šifrována zdrojová ani cílová IP adresa

# Příprava

## a.example.net

```
ip address add 2001:db8::a/64 dev eth0
ip address add 198.51.100.1/24 dev eth0
```

## b.example.net

```
ip address add 2001:db8::b/64 dev eth0
ip address add 198.51.100.2/24 dev eth0
```

Varování (zrušeného) ministerstva informatiky:
Nastavení neplatných IPv6 adres vám způsobí nedostupnost některých internetových služeb.

# Řešení (iproute)

## a.example.net, b.example.net

```
ip xfrm state add \
    src 2001:db8::a dst 2001:db8::b proto esp spi 1 \
    enc 'cbc(aes)' 0x3ed0af408cf5dcbf5d5d9a5fa806b224
```

## a.example.net

```
ip xfrm policy add dir out \
    src 2001:db8::a dst 2001:db8::b \
    tmpl proto esp
```

## b.example.net

```
ip xfrm policy add dir in \
    src 2001:db8::a dst 2001:db8::b \
    tmpl proto esp
```

# Řešení (ipsec-tools)

## a.example.net, b.example.net

```
#!/sbin/setkey -f
add 2001:db8::a 2001:db8::b esp 0x1
    -E rijndael-cbc 0x3ed0af408cf5dcbf5d5d9a5fa806b224;
```

## a.example.net

```
#!/sbin/setkey -f
spdadd 2001:db8::a 2001:db8::b any
    -P out ipsec esp/transport//require;
```

## b.example.net

```
#!/sbin/setkey -f
spdadd 2001:db8::a 2001:db8::b any
    -P in ipsec esp/transport//require;
```

## Bezpečnostní asociace (a.example.net)

```
# ip xfrm state show src 2001:db8::a dst 2001:db8::b
src 2001:db8::a dst 2001:db8::b
        proto esp spi 0x00000000 reqid 0 mode transport
        replay-window 0
        enc cbc(aes) 0x3ed0af408cf5dcbf5d5d9a5fa806b224
        sel src ::/0 dst ::/0
```

## Bezpečnostní asociace (a.example.net)

```
# ip xfrm policy show src 2001:db8::a dst 2001:db8::b
src 2001:db8::a/128 dst 2001:db8::b/128
        dir out priority 0 ptype main
        tmpl src :: dst ::
                proto esp reqid 0 mode transport
```

# Tcpdump a ICMP ping

## a.example.net

```
# ping6 2001:db8::b
PING 2001:db8::b(2001:db8::b) 56 data bytes
64 bytes from 2001:db8::b: icmp_seq=1 ttl=255 time=0.630 ms
64 bytes from 2001:db8::b: icmp_seq=2 ttl=255 time=0.504 ms
64 bytes from 2001:db8::b: icmp_seq=3 ttl=255 time=0.541 ms
```

## b.example.com

```
# tcpdump -i eth0 -n esp or icmp6
IP6 2001:db8::a > 2001:db8::b: ESP(spi=0x00000001,seq=0x1), length 104
IP6 2001:db8::b > 2001:db8::a: ICMP6, echo reply, seq 1, length 64
IP6 2001:db8::a > 2001:db8::b: ESP(spi=0x00000001,seq=0x2), length 104
IP6 2001:db8::b > 2001:db8::a: ICMP6, echo reply, seq 2, length 64
IP6 2001:db8::a > 2001:db8::b: ESP(spi=0x00000001,seq=0x3), length 104
IP6 2001:db8::b > 2001:db8::a: ICMP6, echo reply, seq 3, length 64
```

# Úklid

## a.example.net, b.example.net

```
ip xfrm policy flush
ip xfrm state flush
```

# Domlouvání klíčů: ISAKMP, IKE, IKEv2

# Úkol: Automatický šifrovaný kanál

- Protokol pro domlouvání klíčů
- Démon, který se o domlouvání stará
- Autentizace koncových bodů
- Konfigurace transportních kanálů
- Navazování asociací podle potřeby (on demand)

# Protokoly pro domlouvání symetrických klíčů

- ISAKMP – domlouvání bezpečnostních asociací
- IKE – autentizace a výměna klíčů
- IKEv2 – náhrada za ISAKMP/IKE a některé další protokoly

# Software pro domlouvání symetrických klíčů

- Racoon (pouze IKEv1, složitá konfigurace)
- Racoon2 (spíše experimentální, není v distribucích)
- Openswan (nedostatek dokumentace)
- Strongswan (složitější práce s klíči, není v některých distribucích))

# Příprava RSA klíčů (Openswan)

## a.example.net, b.example.net

```
certutil -N -d /etc/ipsec.d
ipsec newhostkey \
    --configdir /etc/ipsec.d \
    --output /etc/ipsec.secrets
```

# Zjištění veřejných klíčů (Openswan)

## a.example.net

```
# ipsec showhostkey --left
ipsec showhostkey nss directory showhostkey: /etc/ipsec.d
    # rsakey AQO1EFgL5
    leftrsasigkey=0sAQO1EFgL5Odxu8P...7DvKohvAwd
```

## b.example.net

```
# ipsec showhostkey --right
ipsec showhostkey nss directory showhostkey: /etc/ipsec.d
    # rsakey AQPGT6JIY
    rightrsasigkey=0sAQPGT6JIYP0o1bc...wZfx7bBGER
```

# Konfigurace IKEv2 (Openswan)

## /etc/ipsec.conf – a.example.net, b.example.net

```
include /etc/ipsec.d/*.conf
```

## /etc/ipsec.d/test.conf – a.example.net, b.example.net

```
conn test
    type=transport
    left=2001:db8::a
    leftid=@a.example.com
    leftrsasigkey=0sAQO1EFgL5Odxu8P...7DvKohvAwd
    right=2001:db8::b
    rightid=@b.example.com
    rightrsasigkey=0sAQPGT6JIYP0o1bc...wZfx7bBGER
    ikev2=yes
    auto=add
```

# Kontrola politik a asociací

## a.example.net

```
# ip xfrm policy show src 2001:db8::a/128 dst 2001:db8::b/128
src 2001:db8::a/128 dst 2001:db8::b/128
    dir out priority 17536 ptype main
    tmpl src :: dst ::
        proto esp reqid 0 mode transport
# ip xfrm policy show src 2001:db8::b/128 dst 2001:db8::a/128
# ip xfrm state show src 2001:db8::a/128 dst 2001:db8::b/128
# ip xfrm state show src 2001:db8::b/128 dst 2001:db8::a/128
```

# Tcpdump a ICMP ping

## a.example.net

```
# ping6 2001:db8::b
PING 2001:db8::b(2001:db8::b) 56 data bytes
64 bytes from 2001:db8::b: icmp_seq=2 ttl=255 time=0.630 ms
64 bytes from 2001:db8::b: icmp_seq=3 ttl=255 time=0.504 ms
64 bytes from 2001:db8::b: icmp_seq=4 ttl=255 time=0.541 ms
```

## b.example.net

```
IP6 2001:db8::a.isakmp > 2001:db8::b.isakmp: isakmp: parent_sa ikev2_init[I]
IP6 2001:db8::b.isakmp > 2001:db8::a.isakmp: isakmp: parent_sa ikev2_init[R]
IP6 2001:db8::a.isakmp > 2001:db8::b.isakmp: isakmp: child_sa  ikev2_auth[I]
IP6 2001:db8::b.isakmp > 2001:db8::a.isakmp: isakmp: child_sa  ikev2_auth[R]
IP6 2001:db8::a > 2001:db8::b: ESP(spi=0xefedc53b,seq=0x1), length 116
IP6 2001:db8::b > 2001:db8::a: ESP(spi=0x5de08dc4,seq=0x1), length 116
IP6 2001:db8::a > 2001:db8::b: ESP(spi=0xefedc53b,seq=0x2), length 116
IP6 2001:db8::b > 2001:db8::a: ESP(spi=0x5de08dc4,seq=0x2), length 116
IP6 2001:db8::a > 2001:db8::b: ESP(spi=0xefedc53b,seq=0x3), length 116
IP6 2001:db8::b > 2001:db8::a: ESP(spi=0x5de08dc4,seq=0x3), length 116
```

# Kontrola politik a asociací (po pingu)

## a.example.net

```
# ip xfrm policy show src 2001:db8::a/128 dst 2001:db8::b/128
src 2001:db8::a/128 dst 2001:db8::b/128
        dir out priority 17536 ptype main
        tmpl src :: dst ::
                proto esp reqid 16385 mode transport
# ip xfrm policy show src 2001:db8::b/128 dst 2001:db8::a/128
src 2001:db8::b/128 dst 2001:db8::a/128
        dir in priority 17536 ptype main
        tmpl src :: dst ::
                proto esp reqid 16385 mode transport
# ip xfrm state show src 2001:db8::a/128 dst 2001:db8::b/128
src 2001:db8::a dst 2001:db8::b
        proto esp spi 0x2e8e7150 reqid 16385 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x6813f555accc4e063e1285baa8d4817e0d2ef862 96
        enc cbc(aes) 0x877b4db55643cd084bbd19a1ba7aee7c
        sel src ::/0 dst ::/0
# ip xfrm state show src 2001:db8::b/128 dst 2001:db8::a/128
src 2001:db8::b dst 2001:db8::a
        proto esp spi 0xd04eb885 reqid 16385 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x0c63e8f1248773783fe01b35bf73e806622da48b 96
        enc cbc(aes) 0xad108620f282b968ead3b059fc39122d
        sel src ::/0 dst ::/0
```

# Na cestách: Road warrior

# Úkol: Road warrior

- Brána (a.example.net) nezná adresu připojovaného (b.example.net)
- Adresa připojovaného stroje je dynamická

# Openswan 2.6.33-1.fc15.x86_64

- Nefunguje IPv6 („Address family not supported by protocol“)
- Nefunguje IKEv2 (bez odpovědi)
- IKE démo si sám vybírá IPv4 adresu na rozhraní

# Řešení pro IPv4/IKEv1 (Openswan)

## Gateway (a.example.net)

```
conn test
    ...
    left=198.51.100.1
    ...
    right=%any
    ...
    ikev2=no
    auto=add
```

# Řešení pro IPv4/IKEv1 (Openswan)

## Warrior (b.example.net)

```
conn test
    ...
    left=198.51.100.1
    ...
    right=%defaultroute
    ...
    ikev2=no
    auto=route
```

# IPv4 NAT-Traversal

- Připojování na IPsec bránu přes IPv4 maškarádu
- Zapouzdření ESP do UDP
- Navazování spojení „zevnitř“

# Openswan 2.6.33-1.fc15.x86_64

- Nefunguje IKEv2

# IPv4 NAT-Traversal (Openswan)

## a.example.com, b.example.net: /etc/ipsec.conf

```
config setup
    ...
    nat_traversal=yes
    ...
```

## a.example.com, b.example.net: /etc/ipsec.d/test.conf

```
conn test
    ...
    ikev2=no
    ...
```

# IPsec tunely a VPN

# Tunelová varianta ESP

- Zapouzdření:
  IPv4/IPv6—ESP—IPv4/IPv6–ICMP/UDP/TCP
- První hlavička prozrazuje adresy obou konců tunelu
- Vnitřní adresy a porty jsou chráněny ESP

# Tunelová varianta (Openswan)

## a.example.com, b.example.net

```
conn test
    connaddrfamily=ipv6 # pouze pro IPv6
    type=tunnel
    ...
    left=2001:db8:0:0::a
    leftsubnet=2001:db8:a:a::/64
    ...
    right=2001:db8::b
    rightsubnet=2001:db8:b:b::/64
    ...
```

# Hybridní IPv4/IPv6 tunel

- IPv6 kanál: IPv6—ESP—IPv4/IPv6–ICMP/UDP/TCP
- IPv4 kanál: IPv4—ESP—IPv4/IPv6–ICMP/UDP/TCP
- Nezávislost vnitřního a vnějšího protokolu
- Technicky proveditelné a užitečné
- Speciální případ pro 6in4 řeší RFC 4891
- Nevím o žádné implementaci

# Kam dál...

# Konfigurace adres

- U IPv6 není nutná
- L2TP over IPsec (RFC 3193)
- IKEv1 + Mode CFG (Cisco)
- IKEv2 konfigurace adres (RFC 5996)
- DHCPv4 over IPsec (RFC 3456)

# Autentizace

- PSK (sdílená hesla)
- IKEv2 EAP (RFC 5996, RFC 5998)
- XAUTH (Cisco)
- PKI a certifikační autority (RFC 5280, RFC 4945)

http://data.pavlix.net/europen39/

pavlix@pavlix.net