Mýtus lepší bezpečnosti IPv6

- IPv6 má standardně IPsec -> větší bezpečnost než IPv4 ☹
  - Jak ochrání IPv6+IPsec před XSS?
  - Kdo používá IPsec?
  - IPsec je dnes i pro IPv4
  - V praxi SSL/TLS důležitější
- Jaká je vlastně bezpečnost IPv6 x IPv4?
  - *IPv6 does nothing IPv4 does not, though it promised to*
  - L2, L3, L4, …

L2 (1:1,5)

- Přenos unicast paketů na Ethernetu:
  - IPv4

  - IPv6

- Převod IPv4 na MAC = ARP (EtherType=0806, broadcast „Kdo má tuto IPv4 adresu“, falešná inzerce, platnost cache 20 min.)
- Převod IPv6 na MAC = Neighbor Discovery (multicast na Sol-Node „Kdo má tuto IPv6 adresu“, IPv6 protokol ICMPv6, falešná inzerce, navíc detekce dostupnosti a duplicity, platnost 1 den, RFC 3756 ND Trust Models and Threats)
- útoky DoS (znemožnění komunikace a flooding)

L2 (2:2,5)

- Přenos multicast paketů, cílová MAC adresa:
  - IPv4 multicast = 01-00-5E-dolních 23 bitů IPv4 group
  - IPv6 multicast = 33-33-dolních 32 bitů IPv6 group
- Standardně každý uzel poslouchá na all-nodes (FF01::1, FF02::1), pro každou unicast adresu X na sol-nodes (FF02::1:FFxx:xxxx, typicky 2), na multicast skupinách, do kterých se zařadil
- Filtrace příjmu multicastů je obecně problém (kolik různých lze na kartě nastavit)
- Uzly budou zbytečně zatíženy Ethernet multicasty pro cíle, které nepřijímají, ale projdou do systému, co když se některá standardní skupina namapuje stejně jako nějaký video stream?

L3 (2:4)

- konfigurace adresy a prefixu (hmm, IPv6 – která adresa?)
- staticky:
  - IPv4: není problém (pevná, nezměnitelná)
  - IPv6: link-local - prakticky nejde (win7 náhodná, jinak EUI-64)
  - IPv6: global unicast - je problém (pokud jde, nejde třeba router)
- dynamicky:
  - IPv4: DHCP - může být podvržena falešným DHCP serverem
  - IPv6: bezestavová automatická konfigurace SLAAC – RA, DAD, viz předchozí, bez záznamu v DNS, bez interakce se správcem
  - IPv6: temporary – RA, DAD (náhodná)
  - IPv6: stavová automatická konfigurace (DHCPv6), může být podvržena, je třeba vyvinout velké úsilí, aby nebyla použita jiná
  - IPv6: prefix a default router – lze získat pouze z RA (nejde z DHCPv6), snadno napadnutelné místo, odstaví všechny klienty v síti!

Odbočka 1: babylonské DHCPv6

- Dva tábory:
  - M&O: dokud nevidí klient M flag v RA, nezískává adresu pomocí DHCPv6, adresa získaná pomocí SLAAC je tak primární, případná DHCPv6 je sekundární (temporary adresa nejprimárnější)
    - Pokud je nastaven jen příznak O, použije se DHCPv6 pouze pro nastavení parametrů (DNS) a ne adresy
    - Kdo zajistí, že mají všechny routery stejné nastavení?
    - Co se stane, když nemají (jednou M, jednou ne)?
  - U&O: klient zkusí DHCPv6, pak SLAAC, pokud dostane DHCPv6 adresu, použije ji jako jedinou, flagy RA ignoruje

Odbočka 2: Statické DHCPv6

- IPv4: pro spravovanou síť je běžná centrální registrace MAC adres a přidělení statické IP adresy přes statický záznam v DHCP (identifikace uzlů, registrace v DNS, správa klientů)
- IPv6: v konfiguraci DHCPv6 **nelze prakticky** provést statické přiřazení IPv6 adresy danému klientovi:
  - Zásadní změna ve specifikaci – klient není identifikován MAC adresou (někdo byl příliš geniální), nýbrž pomocí DUID (DHCP Unique IDentifier), ten se jednak může lišit pro různé systémy (a liší), jednak není znám dopředu
  - Odpor – ISC dhcpd-4.2alpha zavádí pattern matching

Odbočka 2: perličky DHCPv6

- Perlička 1: takto vypadá DUID v ISC DHCPD /var/db/dhcpd6-leases (u klienta podobně):
  `ia-na "C\"\000\016\000\001\000\001\0227\315 \372\000#T\201\025e"` (kdo mě sdělí jaká to je MAC adresa?)
- Perlička 2: DUID je uloženo u Vista/Win7 v registry – při klonování počítačů se nemění (zoufalé dotazy, jak zrušit DUID, když je máme duplicitní?)

Odbočka 3: chyby DHCPv6

- Windows XP nemá DHCPv6 vůbec (ale taky neumí DNS přes IPv6, takže to nevadí)
  - problém, pokud chceme vypnout SLAAC (viz O4)
- Windows Vista a 2008 server:
  - Špatná interpretace RFC – domain search suffix
- **Závěr:** v praxi je DHCPv6 jen složitým mechanismem, jak vnutit klientům IPv6 DNS servery

Odbočka 4: jak přinutit Windows k poslušnosti?

- Interface-id u Link-local a SLAAC adresy je implicitně náhodný (což je z hlediska ochrany soukromí v pořádku, nicméně pro správu velké sítě katastrofa), lze zakázat:
  - `netsh interface ipv6 set global randomizeidentifiers=disabled`
- Klienti používají implicitně jako zdrojovou adresu náhodnou temporary adresu (platná 1den, expiruje po 7 dnech), lze zakázat:
  - `netsh interface ipv6 set privacy state=disabled`

Odbočka 4:

- Když lze pomocí M/O z RA přinutit klienta použít DHCPv6, nejde z RA zakázat SLAAC?
  - **jde to!** (ale ne u všech routerů)
  - BSD rtadvd.conf:

    ```
    em0:raflags#136:addr="2001:718:802:8b2::":
    pinfoflags#128:prefixlen#64:
    ```
  - zrušit implicitně nastavený Prefix Information Option Autonomous (128=Onlink, 64=Autonomous)
  - Pak má klient pouze jednu globální IPv6 adresu (hurá)
  - Jenže pak mě v síti nefunguje Mac, Win XP a BSD/Linuxy (pokud nemají implicitně DHCPv6 klienta) ☹
  - Nelze vypnout RA a vnutit z DHCPv6 IPv6 prefix a router!
- *SLAAC set out to solve a problem that no one had (with IPv4 clients management)*

Odbočka 5: Jak se s ním spojit?

- IPv4: fixní adresa, v DNS, lze se spojit na uzel jménem
- IPv6: link-local nepoužitelná, temporary nepoužitelná, dhcpv6 nepoužitelná, SLAAC nepoužitelná (Exchange server z nějakého důvodu změnil svou adresu, klienti se do restartu nejsou schopni s ním spojit, pokud EUI, pak výměna síťovky stejný problém)
  - jedině statická adresa skutečně funguje
  - lze zakázat SLAAC a staticky přidělit DHCPv6, pak není problém záznam v DNS, ale viz předchozí odbočka

L3 (3:5,5)

- konfigurace adresy routeru
  - IPv4: staticky, DHCP nebo rdisc
  - IPv6: staticky (často nejde) nebo RA (napadnutelné lépe než DHCP, DHCP je vždy diskrétní, RA funguje pro všechny v síti!)
- Redirect:
  - IPv4 ICMP
  - IPv6 ICMPv6
  - Funguje úplně stejně, stejné nebezpečí

Odbočka 6: chyby RA

- RA lze snadno podvrhnout (kdo si myslí, že SEND to zachrání?), důsledky jsou daleko fatálnější než falešný DHCP server
- RA flags – pouze 8 bitů, z nich jen 2 volné, std. RFC 5175 doplňuje Expanded Flags Option (nikdo neumí)
- Exp. RFC 5006 doplňuje RDNSS Option (adresy DNS serverů) – nikdo neumí

L3 (3:6)

- Více adres pro jeden IPv6 uzel:
  - na úrovni L2 musí být pro každou záznam v NC
  - IPv6 router musí mít patřičně větší FDB (oproti IPv4 minimálně 4x)
  - IPv4 router vystačí s ARP, platnost údajů dlouhodobá
  - IPv6 router musí dělat RA, ND, DAD, NUD, atd., platnost sice dlouhodobá, ale změny stavu co pár sekund (S,P,D,R) – co to udělá v síti s pár tisícem klientů?!
- Adresový prostor:
  - IPv4: omezený, nutný NAT (klient není dostupný zvenku)
  - IPv6: není nutný NAT (klient snadněji napadnutelný)
  - IPv4: není problém Internet scan
  - IPv6: remote scan je problém, lokální ne (ping6 ff02::1)

L3 - konektivita

- IPv4 – konektivita buď je nebo není
- IPv6 – když není nativní IPv6 konektivita, pak
  - zkusím 6to4 tunel
  - zkusím ISATAP tunel
  - zkusím Teredo tunel
  - Všechny Windows se usilovně snaží získat IPv6 konektivitu přes IPv4 síť!
  - Často se jim to podaří, ale s velkou ztrátovostí paketů
  - Tunelovaný traffic obchází firewall a je neviditelný (máte filtr na IPv4 protokol 41?)
  - Umí interní firewall filtrovat IPv6? A umí tunelovaný IPv6?

L3 - fragmentace paketů

- IPv4: každý router po cestě
- IPv6: jen odesílatel (funkčnost PMTU discovery), ale:
  - z hlediska IDS a cílového uzlu je to jedno, musí mít buffer na spojování fragmentovaných paketů, lze DoS nebo záměrně rozházené fragmenty pro obejití IDS stejně jako u IPv4
  - díky možnosti vkládání vícenásobných hlaviček lze zaplnit první fragment tak, že neobsahuje TCP/UDP hlavičku – nelze pak spolehlivě filtrovat pravidly na úrovni L4 (mohou být obcházena)

L4

- TCP/UDP zůstává beze změny:
  - DoS na TCP/UDP porty = stejné (i chyby)
  - SYN, FIN TCP útoky = stejné
  - aplikace nad TCP/UDP = stejné
- TCP Wrapper:
  - IPv4 – služba/adresa/síť, není probleém
  - IPv6 – služba/adresa/síť, ekvivalentní, ale
    - co když přijde ze sítě IPv6 paket se zdrojovou adresou ::ffff:127.0.0.1?
    - máte v TCP wrapperu povoleno ::ffff:localnet?
    - IPv4 mapped adresy je doporučeno nepoužívat! (Linux stále implicitně dovoluje)

L5 (3:6,5)

- Konfigurace DNS serveru:
  - IPv4: staticky nebo DHCP (stačí DHCP)
  - IPv6: staticky nebo DHCPv6 (kromě RA musí fungovat i DHCPv6, navíc musí být nastaven RA flag M nebo O konzistentně na všech routerech, jinak se nic nestane nebo vznikne zmatek)
- fragmentace TCP/UDP paketů

Stabilita (3:7)

- IPv4 se používá 40 let:
  - chyby v implementacích nejsou
  - implementace mají odstraněné známé problémy
  - existuje hw podpora na straně L2 aktivních prvků (DHCP snooping, IP lockdown, atd.)
- IPv6 se prakticky nepoužívá:
  - řada chyb (Vista, FreeBSD, XORP, ISC DHCPv6)
  - mnohé chyby takového rázu, že něco vůbec nefunguje (jak to, že na to ještě nikdo nepřišel)
  - dokud se nezačne používat, chyby zůstanou

Závěr

- IPv6 je pro normální aplikace 2x zranitelnější než IPv4 ☺
- Dokud se nezačne v praxi používat, tak se to nezmění
- IPv6 bude brzy 20 let, nelze pořád čekat, až bude dokonalé
- Nebát se IPv6, lepší je začít používat co nejdříve, dokud není nosným protokolem a je prostor pro experimentování
- Pokud v IPv6 něco dnes nefunguje, máme vždy k dispozici IPv4 (zásadně jiný stav než v době zavádění Internetu)