Wpływ wdrożenia IPv6 na bezpieczeństwo sieci

Piotr Lewandowski

Instytut Informatyki

Krzysztof Szczypiorski

Instytut Telekomunikacji

Politechnika Warszawska

24 marca 2009

Plan prezentacji

Zmiany w IPv6 wpływające na bezpieczeństwo

- Zmiana struktury nagłówków
- Adresacja w IPv6
- Nowe mechanizmy kryptograficzne

Zmiana struktury nagłówków

Najważniejsze zmiany

- stała długość nagłówka,
- brak sumy kontrolnej,
- fragmentacja dokonywana wyłącznie przez nadawcę,
- brak konieczności analizy rozszerzeń (za wyjątkiem hop-by-hop).

Efekt

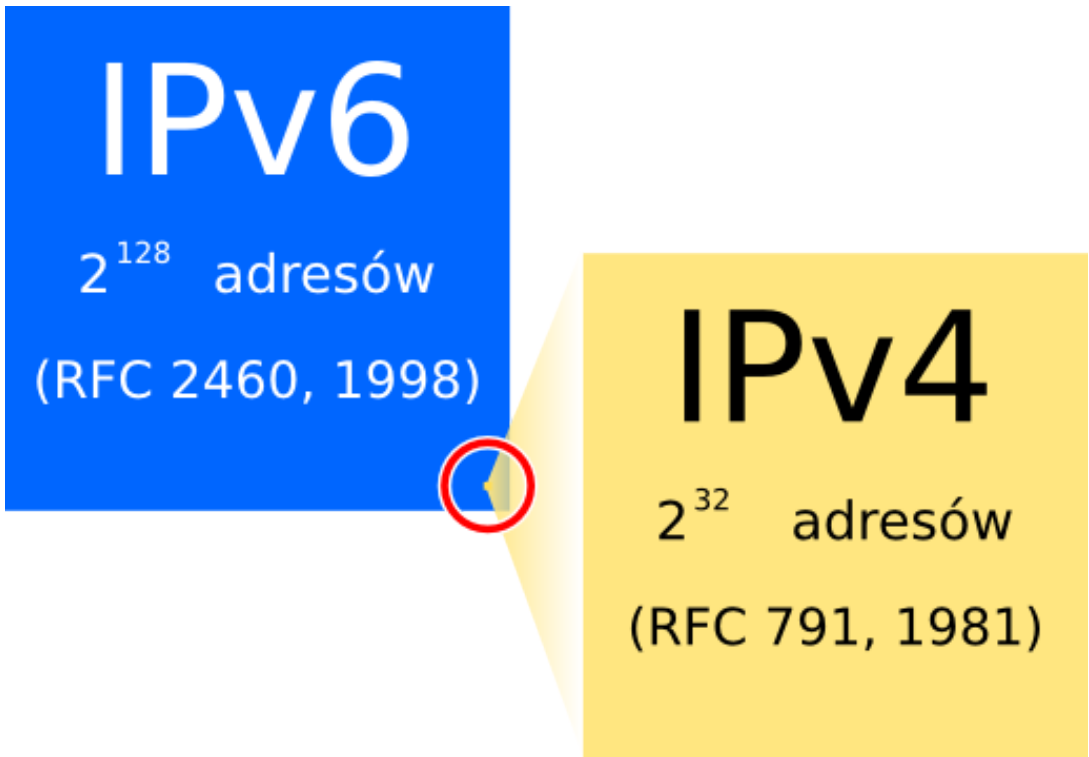
Potencjalnie większa odporność routerów na ataki typu denial-of-service.

Adresacja w IPv6

Adresacja

Najważniejsze zmiany

- większa przestrzeń adresowa ($2^{32} \rightarrow 2^{128}$ adresów),
- hierarchiczna adresacja sieci.



Network Address Translation w IPv6

NAT **nie jest** mechanizmem zapewnienia bezpieczeństwa!

Negatywne efekty NAT dla bezpieczeństwa sieci:

- gromadzenie logów połączeń z przestrzeni „prywatnej”,
- zwiększenie złożoności struktury sieci,
- obniżenie odporności sieci na ataki denial-of-service.

Ponadto:

- powoduje wzrost złożoności protokołów,
- uniemożliwia zastosowanie IPSec,
- dzieli użytkowników na dwie klasy.

Przyszłość ataków sieciowych

Skanowanie sieci na oślep – nieopłacalne.

↓

Konieczność znalezienia innych metod poszukiwania ofiary.

Potencjalne źródła adresów

- wewnętrzne serwery DNS,
- logi serwerów,
- sieci peer-to-peer,
- dostęp do lokalnego łącza,
- wyszukiwarki internetowe,
- czarny rynek (?).

Dotknięte społeczności

- włamywacze,
- spammerzy,
- twórcy robaków internetowych.

Nowe mechanizmy kryptograficzne

Bezpieczeństwo warstwy sieciowej w IPv6

IPv6 wprowadza obowiązkową implementację mechanizmów IPSec:

- Authentication Header (AH),
- Encapsulating Security Payload (ESP),
- Internet Key Exchange Protocol (IKEv2).

Efekty

- mniejsza złożoność nowych protokołów (np. OSPFv3),
- możliwość zabezpieczenia istniejących protokołów (DNS, Telnet),
- potencjalnie większa wydajność (sprzętowe układy kryptograficzne),
- mniejszy koszt tworzenia aplikacji.

Pomiędzy warstwą 2 a 3

Problem

Address Resolution Protocol (ARP) nie zapewnia żadnych mechanizmów bezpieczeństwa na poziomie warstwy łącza danych.

Rozwiązanie

Secure Neighbour Discovery (SEND) zabezpiecza komunikaty ICMPv6 w warstwie łącza danych.

- wykorzystuje CGA – powiązanie adresu i klucza publicznego,
- działa również z urządzeniami bez SEND,
- zapobiega atakom denial-of-service w Duplicate Address Detection,
- zapobiega atakom man-in-the-middle pomiędzy urządzeniami.

Dziękujemy za uwagę.
Prosimy o pytania.