Avances Recientes en Seguridad IPv6

Fernando Gont

FLIP6 - LACNIC 2015
Lima, Peru. Mayo 18-22, 2015

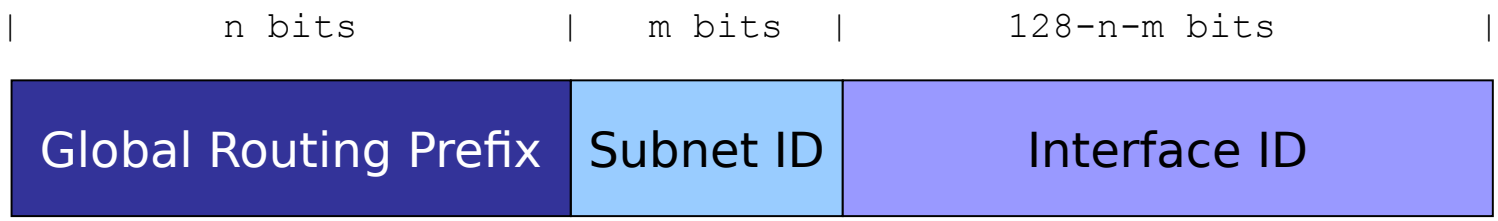
Acerca de...

- Security Researcher y consultor en SI6 Networks
- Publiqué:
  - 20 IETF RFCs (9 on IPv6)
  - 10+ active IETF Internet-Drafts
- Autor del SI6 Networks' IPv6 toolkit
  - http://www.si6networks.com/tools/ipv6toolkit
- Trabajé en proyectos de auditoría de seguridad de protocolos de comunicaciones para:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- Más información en: http://www.gont.com.ar

Direccionamiento IPv6

Breve reseñ

Direcciones IPv6 Global Unicast



- Existen distintas posibilidades para generar el Interface ID:
  - Embeber la dirección MAC (SLAAC tradicional)
  - Embeber la dirección IPv4 (por ej., 2001:db8::192.168.1.1)
  - Low-byte (e.g. 2001:db8::1, 2001:db8::2, etc.)
  - Wordy (e.g. 2001:db8::dead:beef)
  - De acuerdo a tecnologías de transición/co-existencia (6to4, etc.)

Direccionamiento IPv6
Revisión de Implicancias de Seguridad/Privacidad

Security Implications of IPv6 Addressing

- **Correlación de actividad de red en el tiempo**
  - porque el IID no varía en el tiempo
- **Correlación de actividad de red a través de redes**
  - porque el IID no varía de red en red
  - por ej.,2001:db8::**1234:5678:90ab:cdef** vs. fc00:1::**1234:5678:90ab:cdef**
- **Reconocimiento de Red**
  - porque los IIDs so predecibles
  - por ej., 2001:db8**::1**, 2001:db8**::2**, etc.
- **Ataques específicos de dispositiv**
  - porque el IID revela el fabricante de la placa de red
  - por ej., 2001:db8::**fad1:11**ff:fec0:fb33 -> Atheros

Direccionamiento IPv6
Mitigación de Implicancias de Seguridad/Privacidad

Direcciones Temporales (RFC4941)

- RFC 4941: direcciones temporales
  - IIDs aleatorios que varían en el tiempo
  - Generados **adicionalmente** a las direcciones SLAAC tradicionales
  - Direcciones tradicionales utilizadas para comunicaciones entrantes, y temporales para comunicaciones salientes
- Problemas operacionales:
  - Son difíciles de administrar!
- Problemas de seguridad:
  - No reemplazan a las direcciones SLAAC tradicionales (el “host tracking” **se mitiga solo parcialmente**)
  - **No mitigan** los ataques de host-scanning

SLAAC stable-privacy (RFC7217)

- Genera el Interface IDs mediante:

  F(Prefix, Net_Iface, Network_ID, Counter, Secret_Key)

- Where:
  - F() es una PRF (por ej., una función de hashing)
  - Prefix es el prefijo SLAAC o el prefijo link-local
  - Net_Iface es algun identificador de interfaz
  - Network_ID podría ser el SSID de una red wireless
  - Counter se utiliza para resolver colisiones
  - Secret_Key es desconocido para el atacante (y generado aleatoriamente por defecto)

SLAAC stable-privacy (RFC7217) (II)

- Cuando el host se “mueve”:
  - Prefix y Network_ID varían de una red a otra
  - Pero permanecen constantes dentro de cada red
  - F() varía de red en red, pero es constante dentro de cada red
- Esto resulta en direcciones que:
  - Son estables dentro de cada red
  - Tienen diferentes Interface-IDs cuando se cambia de red
  - EN general, poseen las mejores ventajas de ambos mundos
- Se incorporó una implementacion en Linux 4.0

DHCPv6's draft-ietf-dhc-stable-privacy

- Genera los Interface IDs como:

  F(Prefix | Client_DUID | IAID | Counter | secret_key)

- Where:
  - F() e una PRF (por ej., una función de hashing)
  - Prefix: Representa el “address pool” de DHCPv6 address pool
  - Client_DUID es el DHCPv6 DUID del cliente
  - IAID es un identificador unico para esta asociación de direcciones
  - Counter se emplea para resolver colisiones
  - Secret_Key es desconocido para el atacante (y se genera, por defecto, aleatoriamente)

DHCPv6's draft-ietf-dhc-stable-privacy (II)

- Permite que multiples servidores DHCPv6 operen en al misma red
- El estado de los “address leases” se comparte “algorítmicamente”
  - No se necesita de un nuevo protocolo
- Incluso si el archivo de DHCPv6 leases se corrompe, las direcciones serán estables
- El dhc wg está cnsiderando abandonar este trabajo (!?).

Otros trabajos de IETF en este area

- draft-ietf-6man-ipv6-address-generation-privacy
  - Analiza las implicancias de privacidad del direccionamiento IPv6
- draft-ietf-6man-default-iids
  - Establece RFC7217 “por defecto”

IPv6 Extension Headers

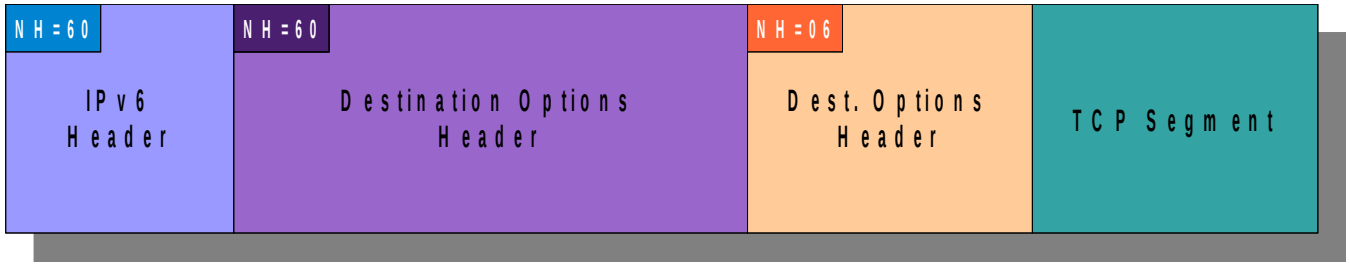
IPv6 Extension Headers

Breve reseña

SI6 NETWORKS

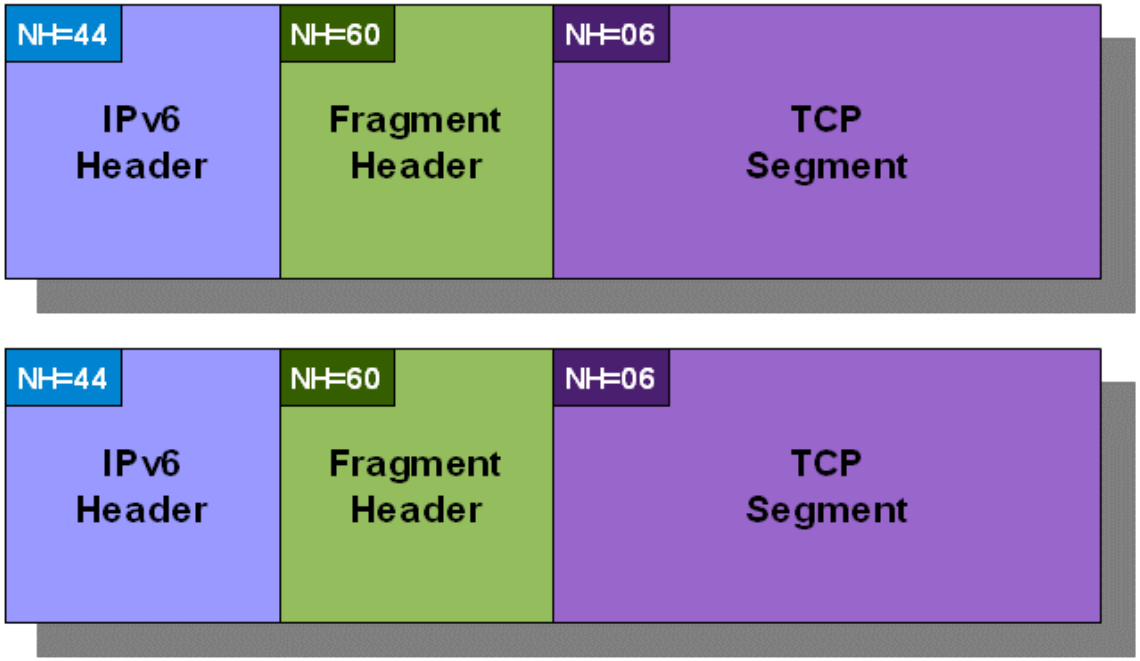
IPv6 Extension Headers

- Encabezado IPv6 base de longitud fija
- Las pciones se incluyen en diferentes “Encabezados de Extensión”
- El paquete sigue una estructura de “lista enlazada”



Fragmentación IPv6

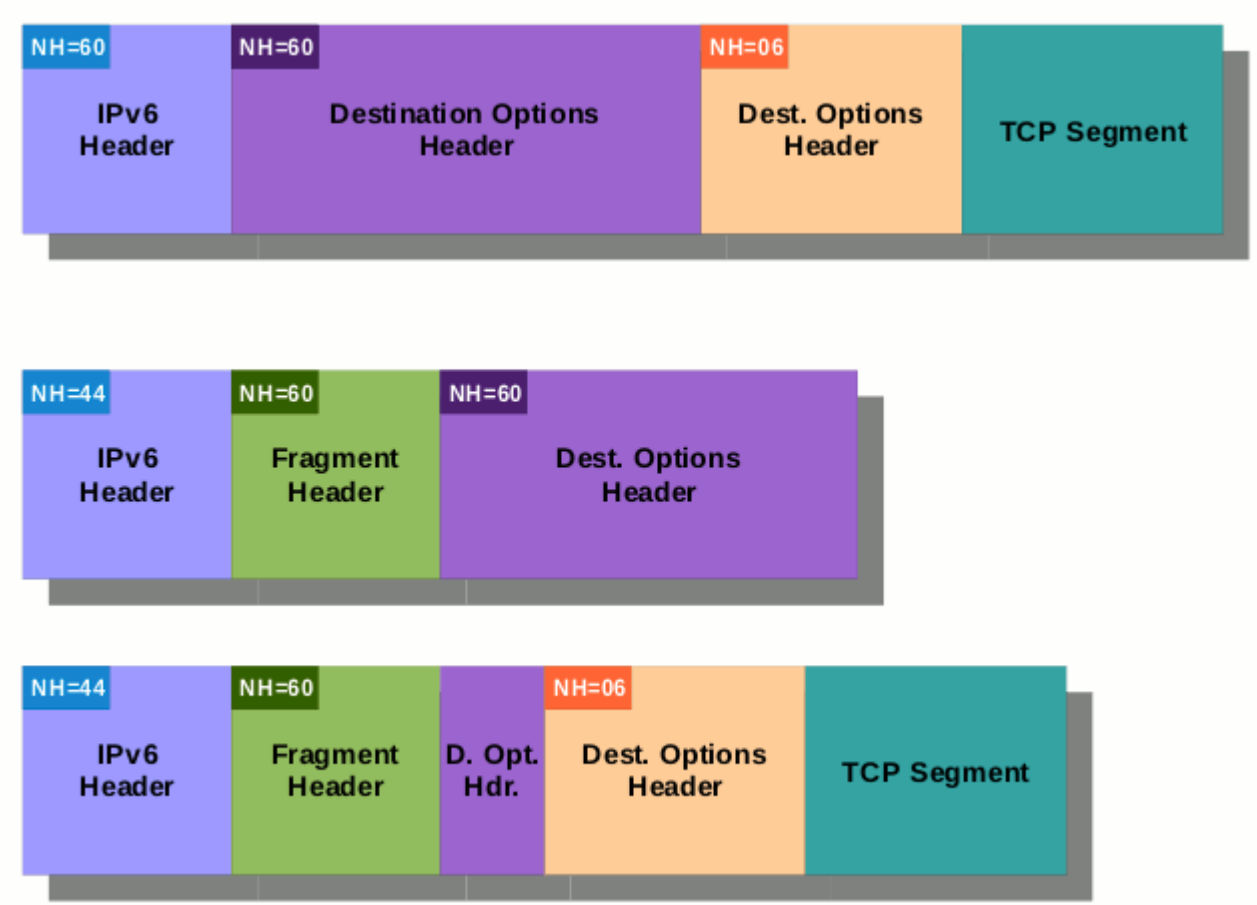
- Conceptualmente, igual que en IPv4
- Implementada con el IPv6 Fragmentation Header



IPv6 Extension Headers
Realidad

Finding Upper-layer information

- Se hace difícil encontrar informaciónde layer-4



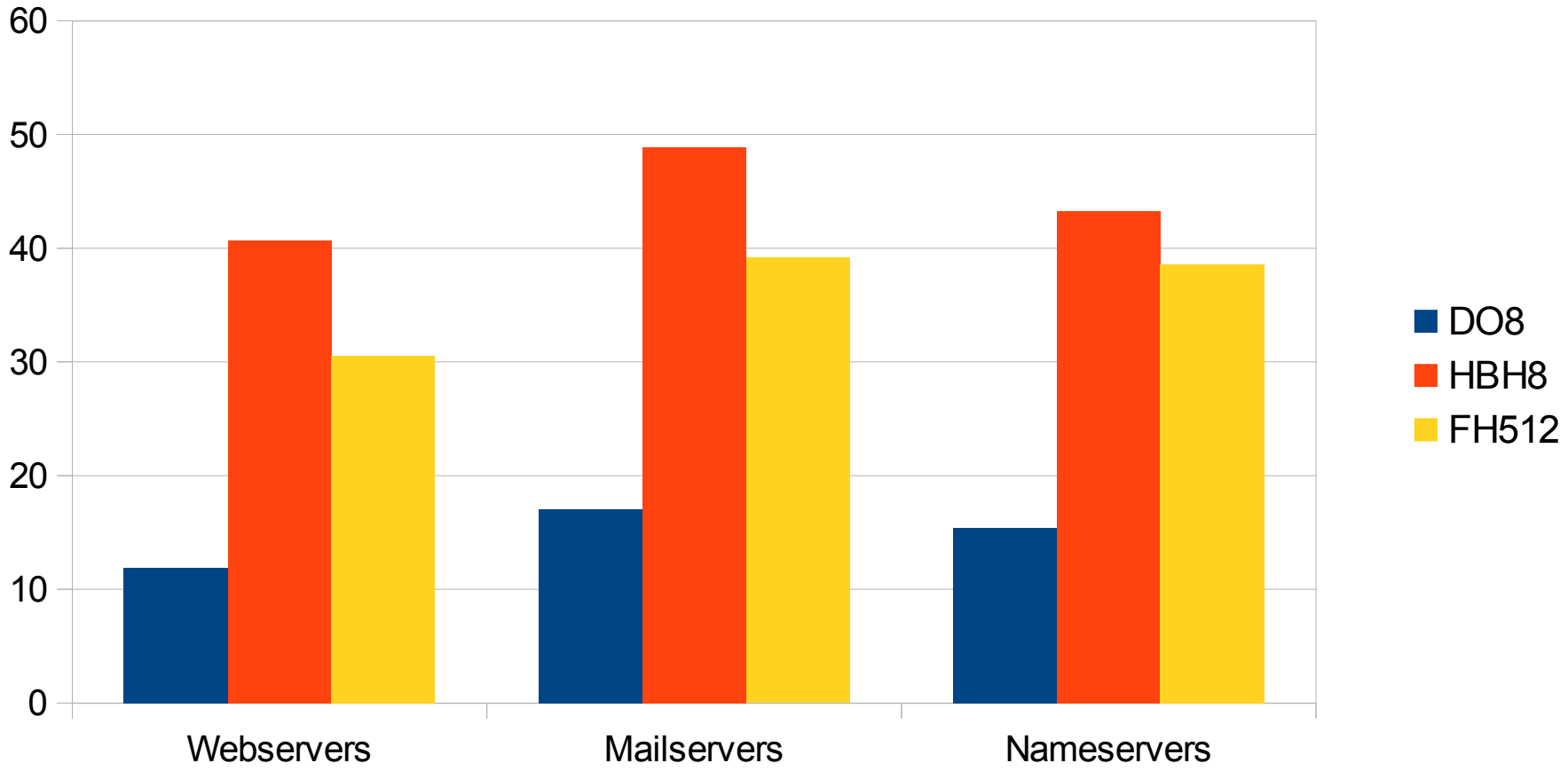
Procesamiento de encabezados

- Procesar la cadena de encabezados es costoso
  - Puede consumir mucho procesador
  - Algunas implementaciones puede “inspeccionar” sólo 128 bytes (u otro valor similar)
- La fragmentación de paquetes es considerada “insegura”
  - Vector de DoS
  - Evasion
  - Implementaciones defectuosas

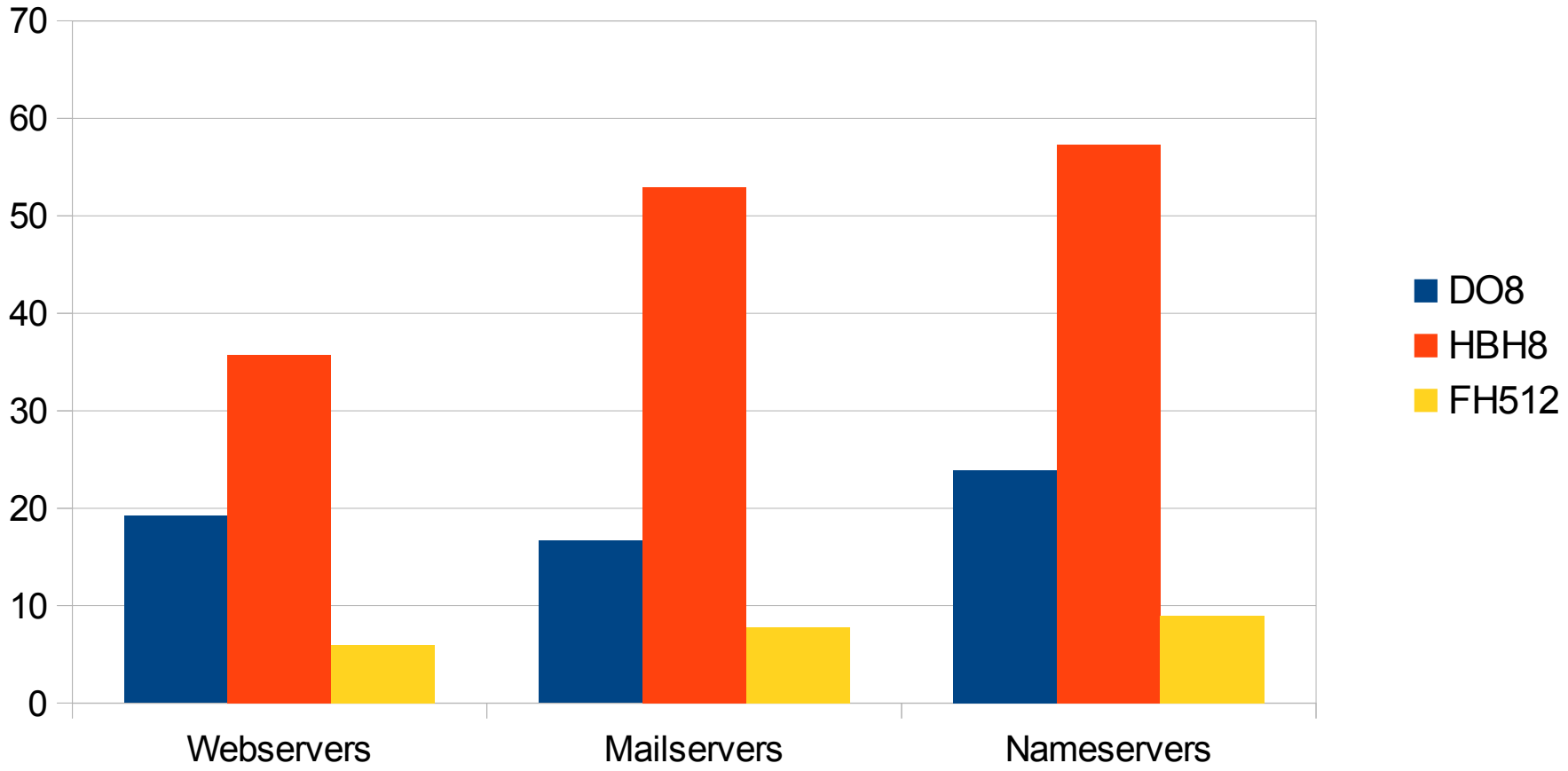
IPv6 EHs en el Mundo Real

- Muchos operadores descartan los paquetes que contienen encabezados de extensión, comoresultado de:
  - Cuestiones de seguridad asociadas a los EHs y fragmentación
  - No existe dependencia de estos encabezados
- Pero no existían mediciones públicas...
- Por lo que realizamos dichas mediciones nosotros mismos:
  - draft-ietf-v6ops-ipv6-ehs-in-real-world

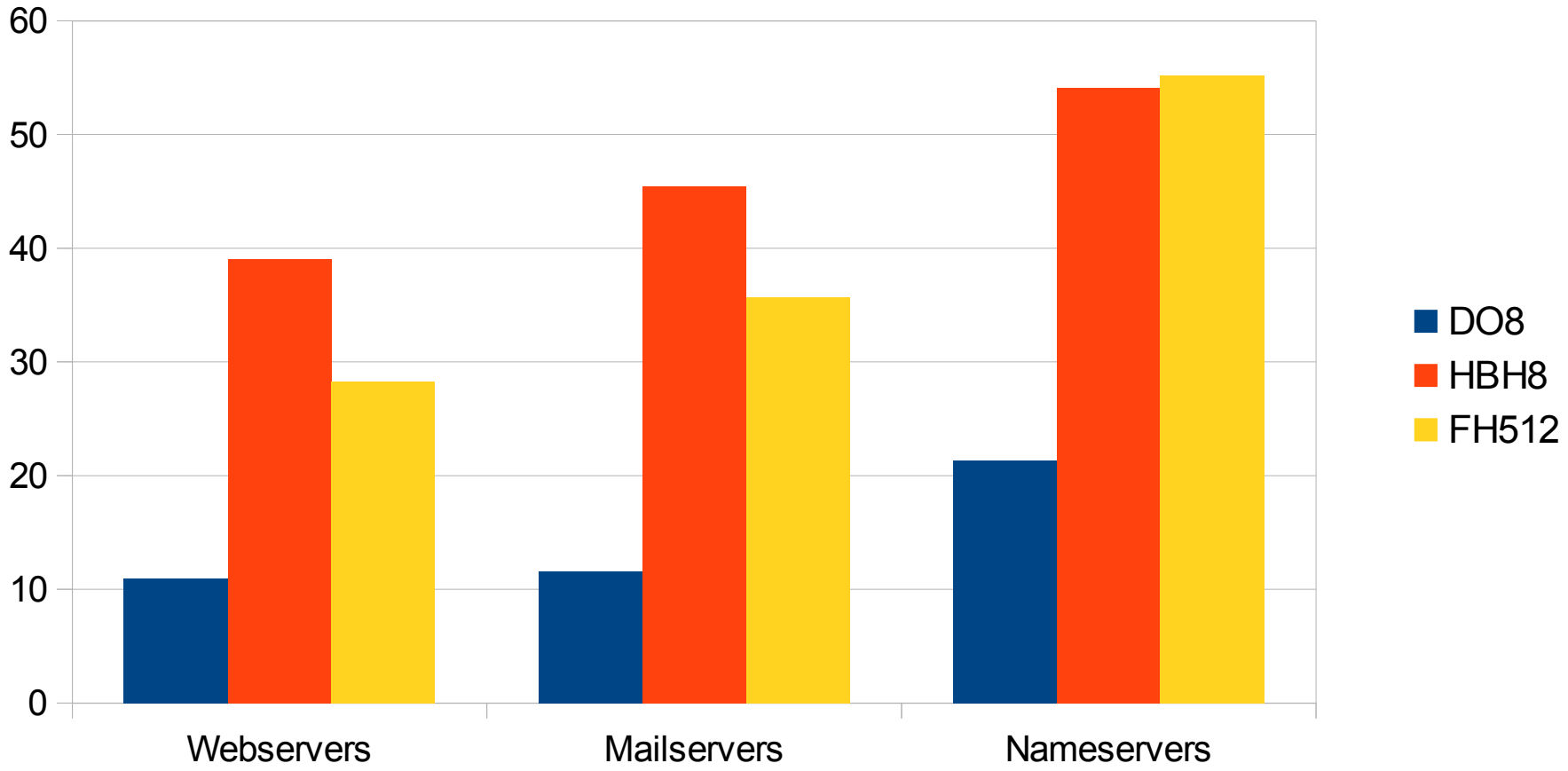
WIPv6LD dataset: Packet Drop rate



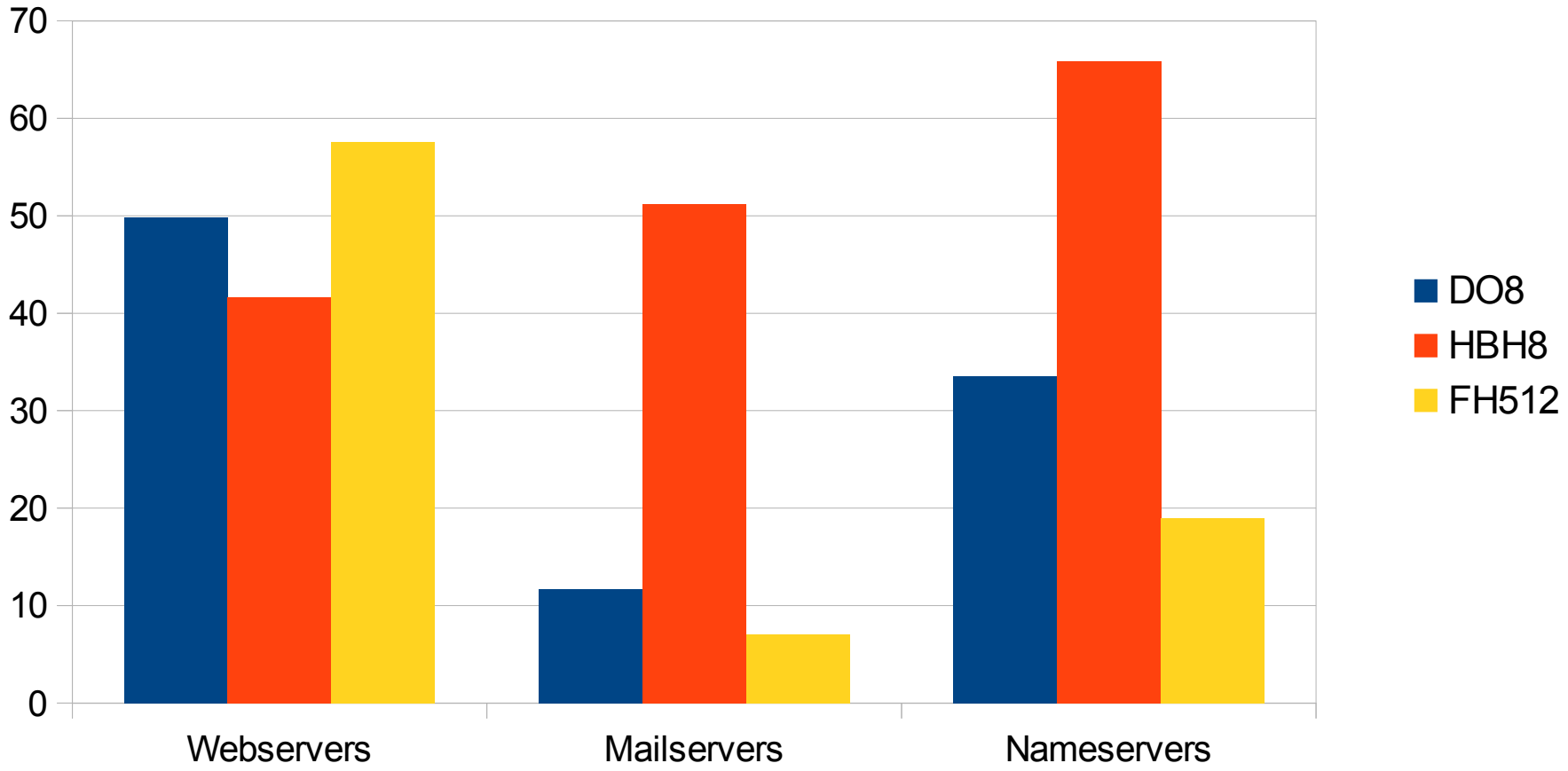
WIPv6LD dataset: Drops by diff. AS



Alexa dataset: Packet Drop rate



Alexa dataset: Drops by diff. AS



Pero... que significa est?

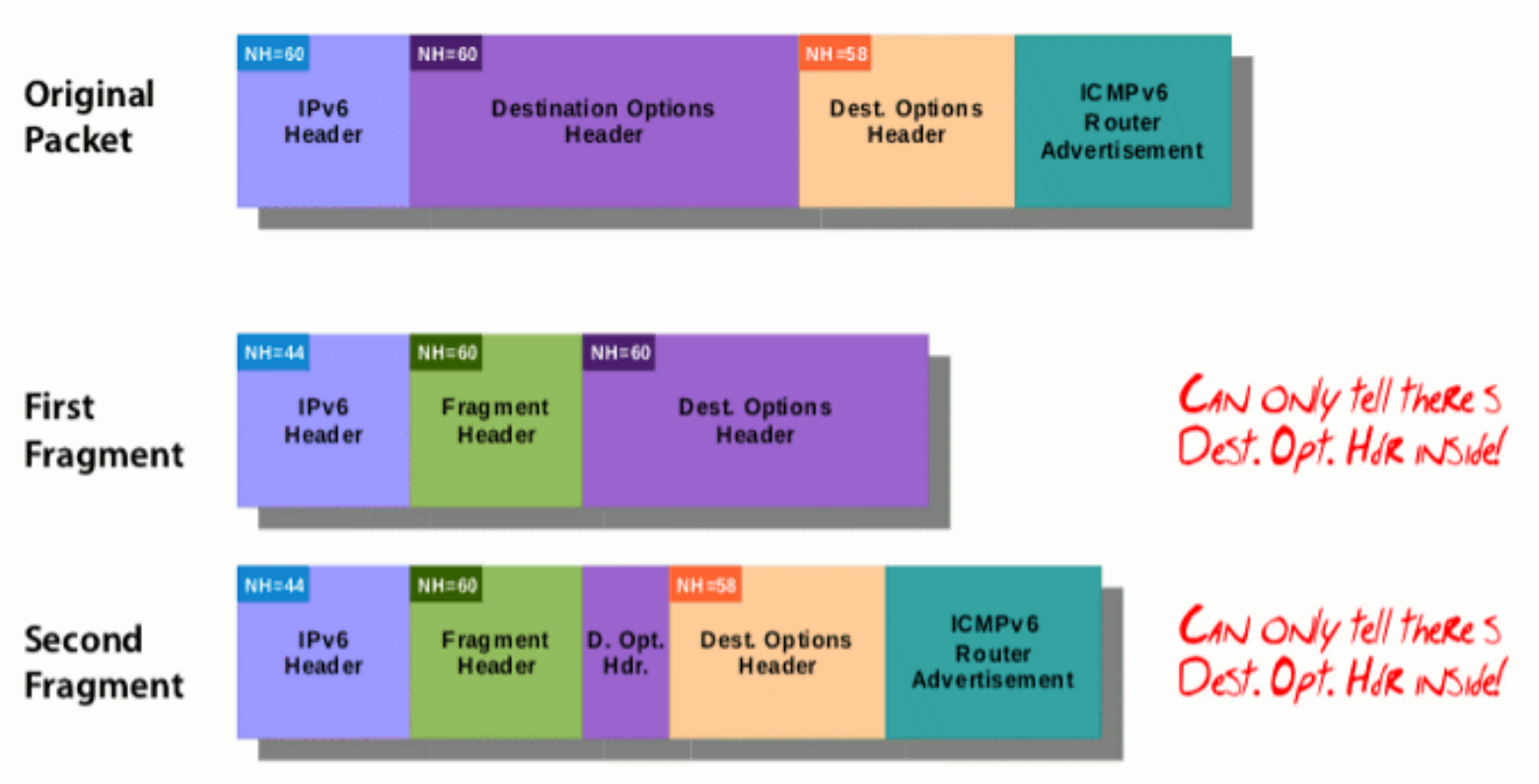
- Buena suerte con utilizar IPv6 EHs en la Internet!
  - Los paquetes en cuestión son ampliamente descartados
- Los IPv6 EHs no son “tan cool” para evasión, tampoco
  - Es probable que tus paquetes ni lleguen a su “objetivo

IPv6 Extension Headers

Ataques

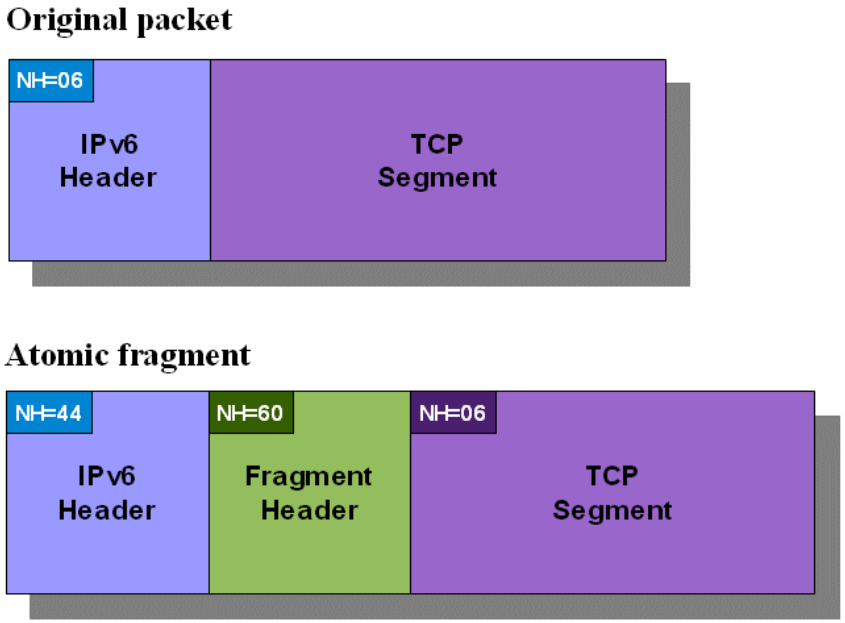
Viejo/obvio/aburrido

- e.g. evasión de RA-Guard



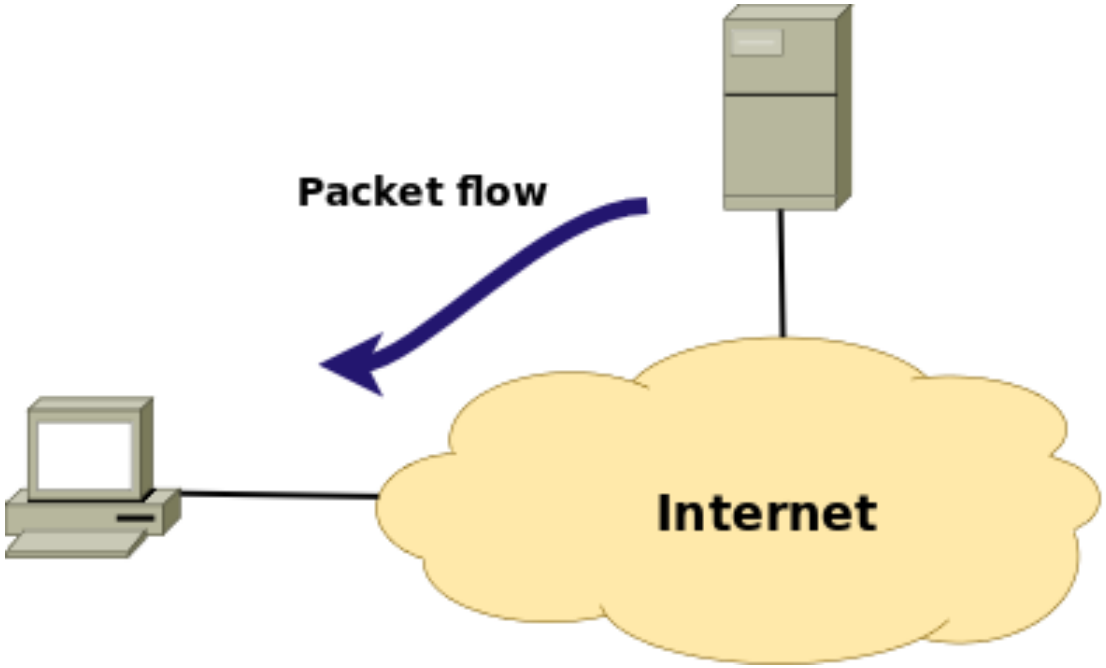
Algo mas interesante

- Si se descartan ampliamente los fragmentos IPv6... qué tal si dispararamos intencionalmente el uso de fragmentación?
  - Enviar un ICMPv6 PTB con MTU<1280
  - El nodo en cuestión generará “IPv6 atomic fragments”
  - Los paquetes se descartarán



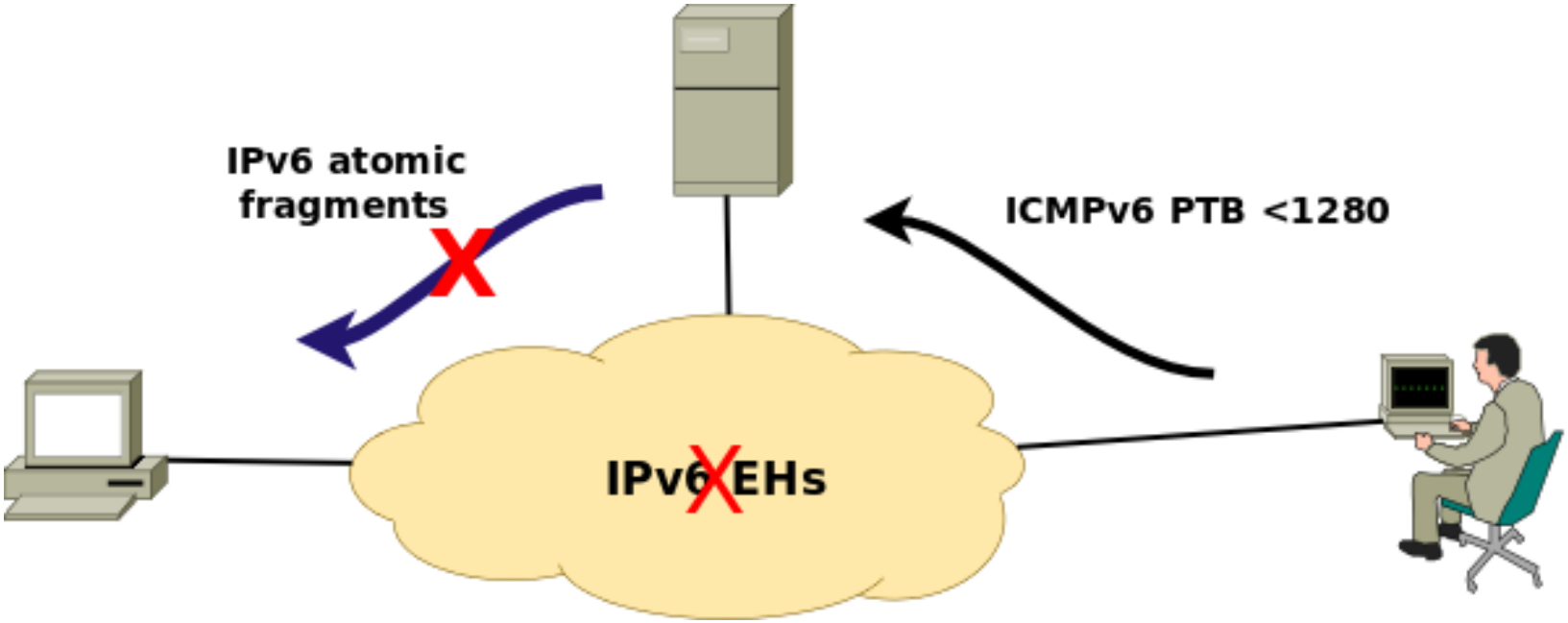
Escenario de ataque #1

- Un cliente se comunica con un servidor



Attack Scenario #1 (II)

- Atacando comunicaciones cliente-servidor



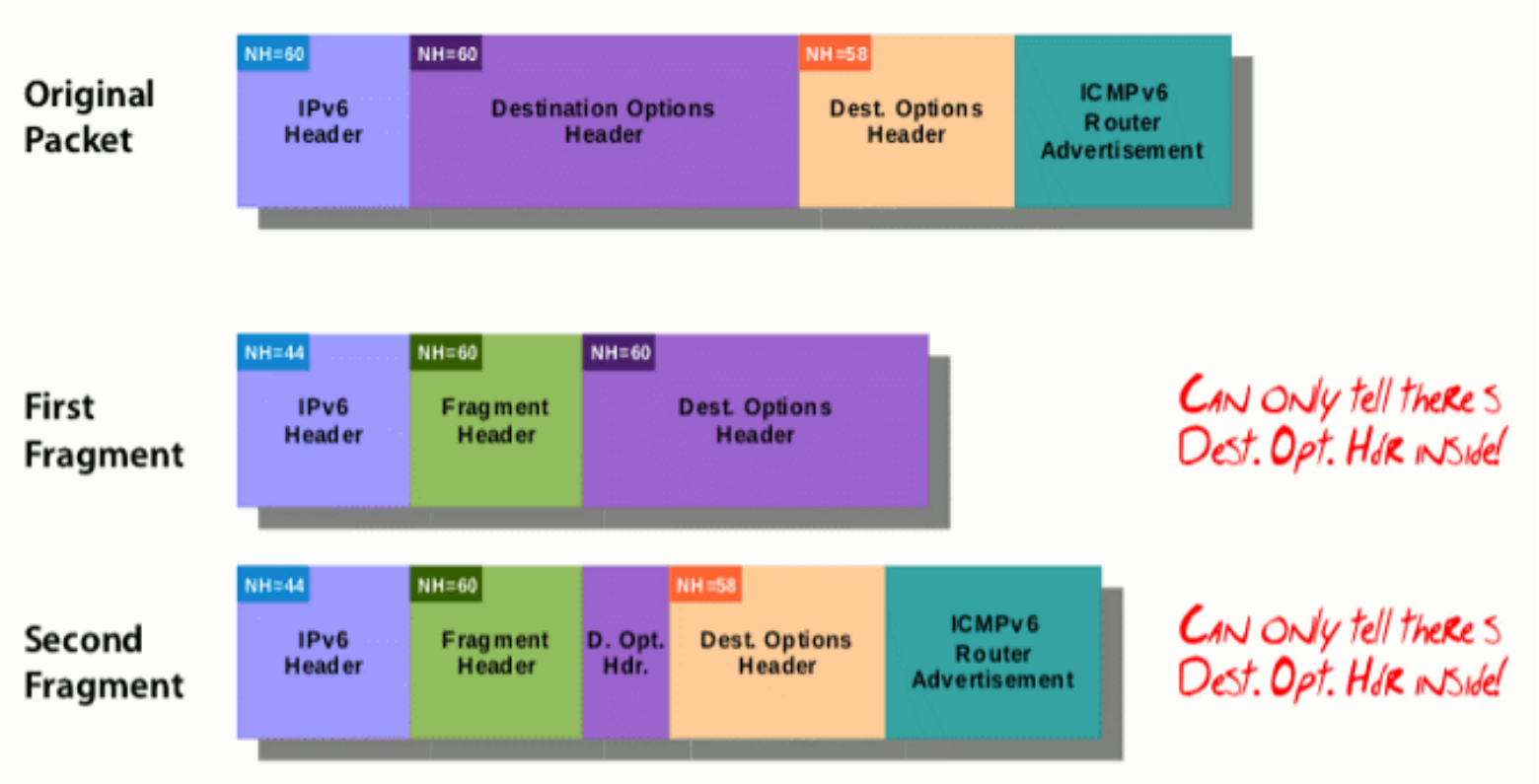
Otro escenario de ataque: BGP

- Asumamos que:
  - Tenemos dos BGP peers
  - Descartan los fragmentos IPv6 “por cuestiones de seguridad”
  - Pero procesan los ICMPv6 PTBs
- Ataque:
  - Enviar un ICMPv6 PTB <1280 (tal vez uno en cada dirección)
- Resultado:
  - Los paquetes se descartarán (a pesar de TCP MD5, IPsec, etc.)
  - Denegación de Servicio

IPv6 Extension Headers
Mejoras

Oversized IPv6 Header Chains

- RFC 7112 prohibe las cadenas de EHs muy largas:



Fragmentación y Neighbor Discovery

- La fragmentación dificulta el filtrado en capa 2
- RFC 6980 prohibe el uso de fragmentación con eighbor Discovery

Generación de IPv6 atomic fragments

- draft-ietf-6man-deprecate-atomfrag-generation
  - “No generar fragmentos atómicos en respuesta a ICMPv6 PTB < 1280”
  - Uctualiza SIIT (IPv6/IPv4 translation) para que no dependa de los mismos

Filttrado de IPv6 Extension Headers

- No existía guía en este área
- Publicamos draft-ietf-opsec-ipv6-eh-filtering
  - Aconseja respecto al filtrado de paquetes que contienen IPv6 Extension Headers

Algunas conclusiones

- Todavía mucho por hacer en el area de seguridad IPv6
  - Mejorar las especificaciones
  - Parchear tu IPv6 stack
  - Escribir código que demuestre nuevas ideas
- **Aprendé IPv6 a fondo antes que sea demasiado tarde!**

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com