IPv6 First Hop Security

Fernando Gont

FLIP6 2012
Quito, Ecuador. Mayo 7-8, 2012

Motivación de esta Presentación

Motivación de esta presentación

- Tarde o temprano desplegarás IPv6
  - En realidad, seguramente ya lo has desplegado parcialmente
- IPv6 representa algunos desafíos en materia de seguridad: Qué podemos hacer al respecto?

Opción #1

Opción #2

Opción #3

Motivation de esta presentación (II)

- Analizar algunos de los desafíos existentes, con el fin de encararlos correctamente
- Describir problemas, proponiendo soluciones

IPv6 First Hop Security

IPv6 First Hop Security

- Mecanismos utilizados en una red local para mitigar posibles ataques
- Posibles puntos de acción:
  - sistemas finales (hosts)
  - switch local
  - router local (first-hop router)
- Conceptos ya conocidos del mundo IPv4:
  - Firewalls host-based/network-based
  - Monitoreo de resolución de direcciones (por ej. arpwatch)
  - FIltrado de paquetes en layer-2 (por ej. DHCP snooping)
  - etc

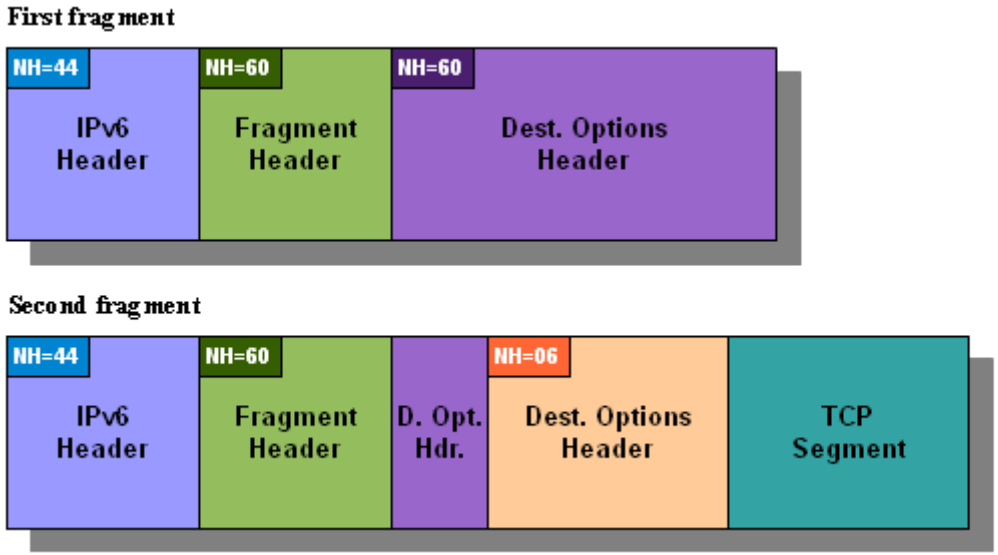
Firewalls en IPv6

Introducción

- Filtrado stateful
  - Necesita mantener estado para realizar su labor
  - Posible en firewalls basados en hosts
  - No aplicable en todos los firewalls basados en red (potencial de DoS)
- Filtrado stateless
  - No precisa mantener estado para realizar su labor
  - Requiere toda la información relevante en un mismo paquete
  - Particularmente interesante en firewalls basados en red (para evitar vectores de DoS)

Problema

- En IPv6, la cadena de encabezados puede ser virtualmente infinita – y fragmentada!



- El filtrado state-less se hace imposible.

Solución

- Propuesta relevante: draft-gont-6man-oversized-header-chains
  - Requiere que todos los encabezados estén en el primer fragmento
- En la práctica, dichos paquetes “patológicos” serán descartados

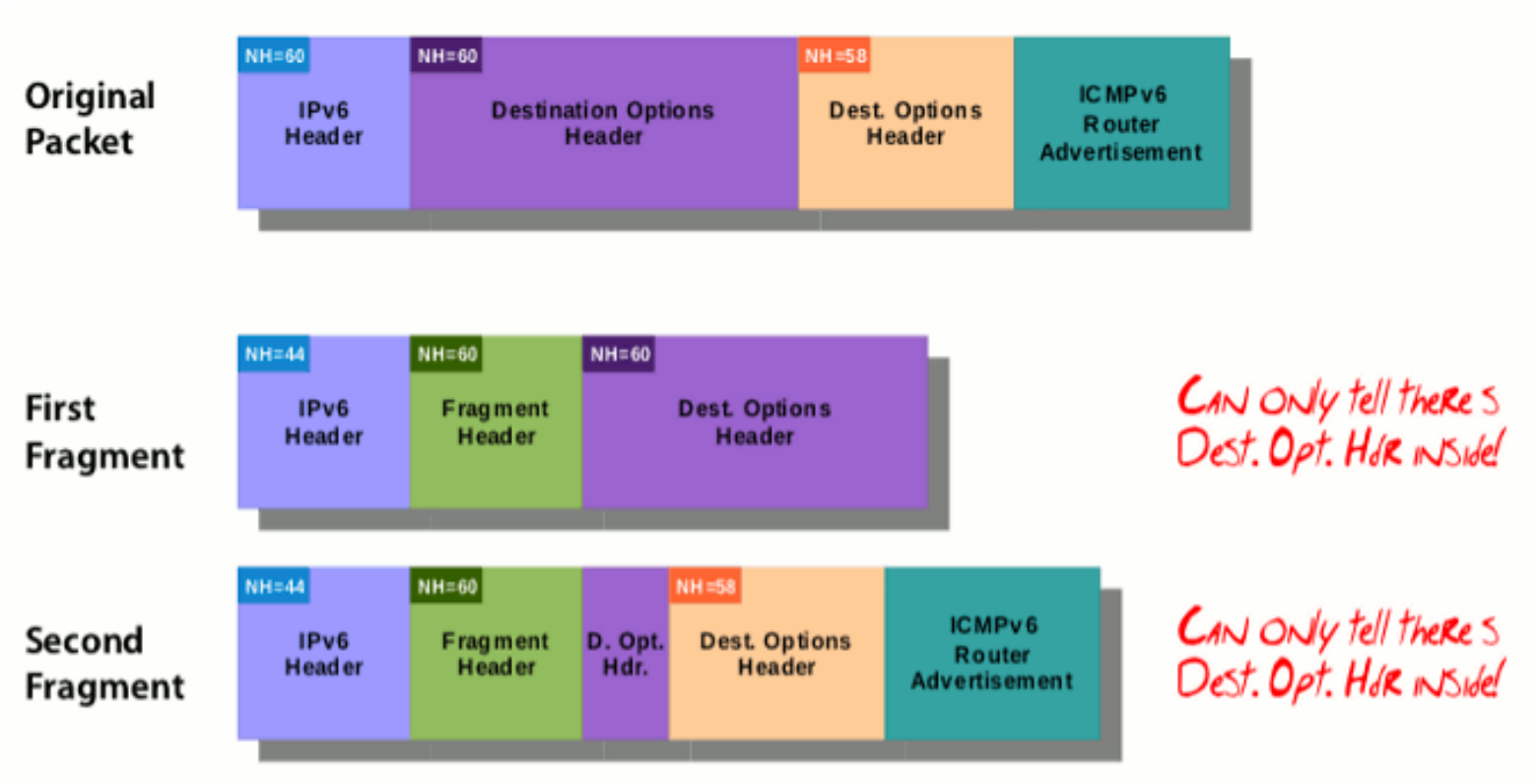
Seguridad IPv6 en Layer-2

Introducción

- Consiste básicamente en:
  - Inspeccionar tráfico de resolución de direcciones
  - Filtrado de tráfico de configuración de red
- Implementado en IPv4 mediante:
  - arpwatch
  - DHCP-snooping
  - etc
- La version IPv6 consistiría en:
  - Inspección de traffico de resolución de direcciones
  - Inspección de tráfico de auto-configuración y DHCPv6

Problema

- Complejidad del tráfico a procesar en layer-2
- Ejemplo:



Solución al filtrado en layer-2

- Descartar paquetes potencialmente maliciosos:
  - El primer fragmento no contiene la cadena de encabezados completa
  - El Hop Limit es 255
  - La dirección de origen o destino es utilizada en SLAAC o DHCPv6
- Propuestas relevantes:
  - draft-ietf-v6ops-ra-guard-implementation: Pasó el WGLC
  - draft-gont-opsec-dhcpv6-shield: recién publicado :-)

Solución al monitoreo en layer-2

- Prohibir el uso de fragmentación con Neighbor Discovery
- No es necesario!
  - Se puede enviar la misma información en multiples paquetes
- En posibles casos de uso, es indeseable:
  - Por ej. introduce un vector de DoS en SEND
- Propuestas relevantes:
  - draft-gont-6man-nd-extension-headers: en discusión en el 6man wg

Rastreo de direcciones IPv6

Introducción

- El rastreo “colaborativo” de direcciones es de suma utilidad.
- Ejemplo:
  - Se infecta un host, y realiza actividad maliciosa
  - Nos reportan la dirección IP del incidente
  - Deseamos saber “que sistema usó esa dirección IP en ese momento”
- Situación en el mundo IPv4:
  - La configuración de red se hace via DHCP
  - El servidor DHCP mantiene un registro de los mapeos IP->MAC address

Problema

- IPv6 utiliza SLAAC → cofiguración descentralizada
- No existe un log centralizado de IPv6 → MAC
- Muchos sistemas implementan direcciones temporales:
  - Las direcciones cambian permanentemente
  - No es posible mantener un registro “estatico”
- Si dificulta el “rastreo” de direcciones IPv6

Solución #1

- Monitorear el uso de direcciones IPv6
- Escribimos ipv6mon:
  - Realiza un escaneo local
  - Detecta nuevas direcciones
  - Prueba cada dirección para detectar cambios
- Publicaremos ipv6mon en el corto plazo
  - Licencia GPL
  - Portable (al menos Linux y *BSD)

Solución #2

- Deshabilitar el uso de direcciones temporales
- Desventajas:
  - Implicancias negativas en privacidad
  - Debe realizarse equipo por equipo
- Propuesta relacionada: draft-gont-6man-slaac-policy
  - Permite al router local especificar la politica de SLAAC deseada
  - Por ej. “solo direcciones estables”, sin preferencias”, etc.
  - I-D siendo discutido en el 6man wg

Solución #3

- Utilizar DHCPv6
- Ventajas:
  - Permite replicar en IPv6 nuestra experiencia del mundo IPv4
- Problemas:
  - Algunas plataformas no lo soportan
  - Requiere administraccion de SLAAC+DHCPv6
- Tema de frecuentes debates religiosos en la IETF!

Algunas conclusiones

KISS principle

- Es deseable tener paridad de funcionalidad con IPv4
- Asimismo, en la medida que sea posible y tenga sentido...

...utilizar mecanismos y conocimientos del mundo IPv4!

Trabajo a futuro

- El objetivo debería ser no repetir con IPv6 los mismos problemas de seguridad sufridos con IPv4
- Esto puede lograrse,
  - Haciendo mejoras en los protocolos (donde haya lugar)
  - Documentando problemas (incluso si no conocemos solución alguna)
  - Incrementando la producción de herramientas de “auditoría”.

Necesitamos IPv6...

y necesitamos que sea lo mas seguro posible

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com