Avances recientes en seguridad IPv6

Fernando Gont

LACSEC 2013
Medellín, Colombia. Mayo 5-10, 2013

Introducción

- Durante los ultimos años hemos trabajado en mejoras de seguridad a IPv6
- Parte del trabajo ha incluido la publicación de IETF Internet-Drafts
  - La mayoría están camino a ser publicados como RFCs
  - Esta presentación describe algunos de esos esfuerzos
- También hemos producido herramientas de seguridad/auditoria

Herramientas de ataque/auditoría

Herramientas de ataque/auditoría

- SI6 Networks IPv6 Toolkit
  - Una decena de herramientas para evaluar seguridad IPv6
  - Portada a Linux, Mac OS, FreeBSD, NetBSD, y OpenBSD
  - Disponible en: http://www.si6networks.com
- THC's IPv6 Attack Toolkit:
  - Una decena de herramientas para evaluar vulnerabilidades específicas en IPv6
  - Basada en plataformas Linux
  - Disponible en: http://www.thc.org

Direccionamiento IPv6
Implicancias en seguridad/privacidad

SI6 NETWORKS

Problemas de seguridad

- Las direcciones SLAAC tradicionales resultan en patrones esécificos para las direcciones
- La existencia de patrones facilita (innecesariamente) los ataques de escaneo de direcciones
- Al momento no existia ninguna propuesta para mitigar estos ataques.

Problemas de privacidad

- Los IIDs “Modified EUI-64” son constantes para cada interfaz
- Si el host se mueve, el prefijo cambia, pero el IID no
  - el IID de 64 bits resulta ser una super-cookie!
- Esto introduce un problema no presente en IPv4: **host-tracking**
- Ejemplo:
  - En la red #1, el host configura la dirección: 2001:db8:1::1111:2222:3333:4444
  - En la red #2, el host configura la dirección: 2001:db8:2::1111:2222:3333:4444
  - El IID “1111:2222:3333:4444” identifica al host

“Mitigación” a host-tracking

- RFC 4941: privacy/temporary addresses
  - IIDs aleatorios que cambian en el tiempo
  - Generados **adicionalmente** a las direcciones SLAAC tradicionales
  - Las direcciones tradicionales se utilizan para conexiones entrantes, y las temporales para conexiones salientes
- Problemas operacionales:
  - Difíciles de administrar
- Problemas de seguridad:
  - Mitigan host-tracking **sólo parcialmente**
  - **No** mitigan los ataques de escaneo de direcciones

Direcciones/IIDs de Auto-configuración

	Estable	Temporales
Predecible	IEEE ID-derived	Ninguna
No predecible	**NINGUNA**	RFC 4941

- Nos faltan direcciones estables que tengan buenas propiedades de seguridad/privacidad
  - Que reemplacen las direcciones SLAAC tradicionales
  - Bastante ortogonales a las direcciones temporales
  - Probablemente “suficientemete buenas” para que en algunos casos no uses RFC 4941

draft-ietf-6man-stable-privacy-addresses

- Propone generar los Interface IDs como:

  F(Prefix, Iface_ID, Network_ID, secret_key)

- Donde:
  - F() es una PRF (por ej., una función de hash)
  - Iface_index es un número pequeño que identifica a la NIC
  - Network_ID podría ser, por ejemplo el SSID de una red inalámbrica
  - El resto de los parametros deberían ser obvios ;-)

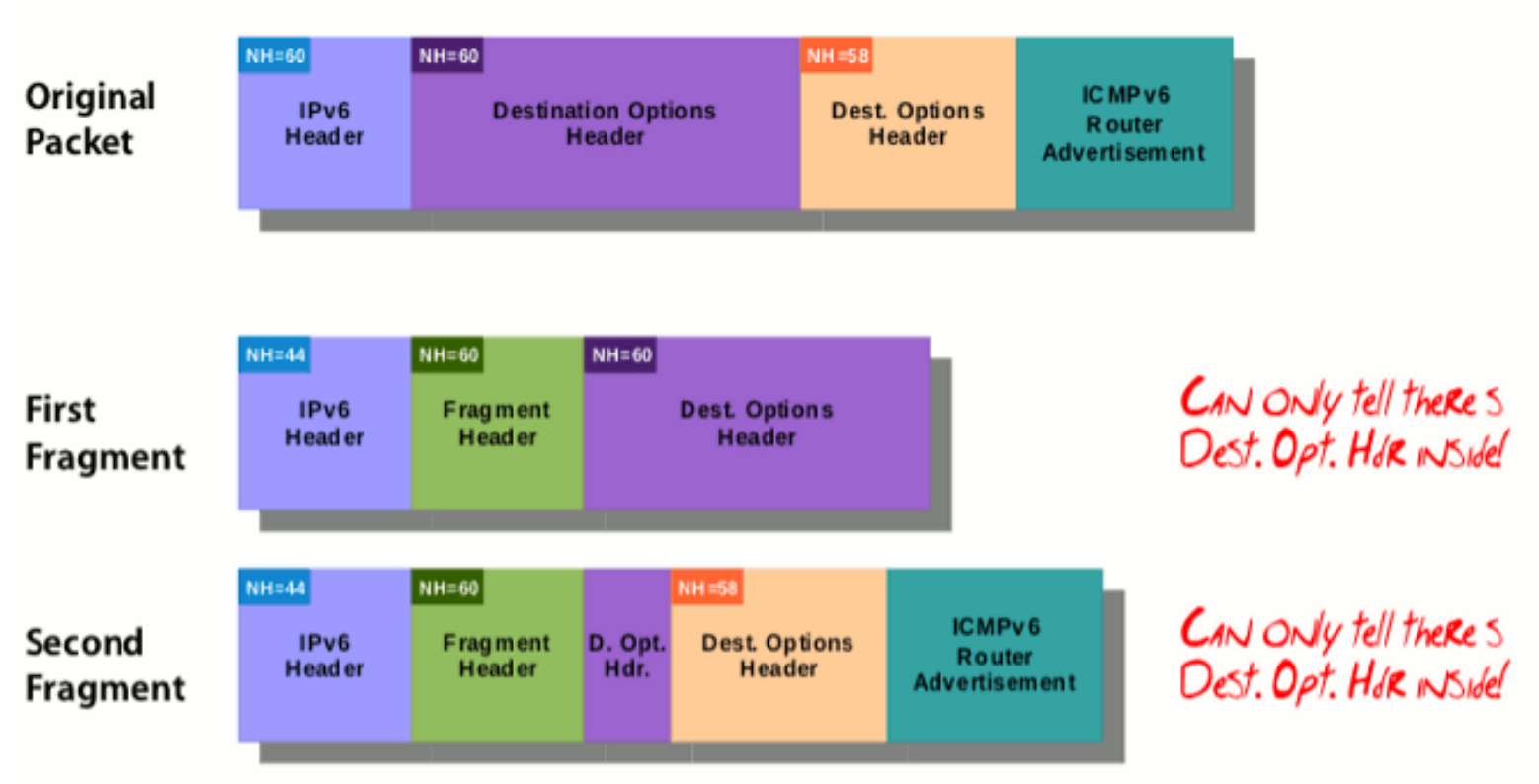
draft-ietf-6man-stable-privacy-addresses

- Esta función proporciona direcciones que:
  - No son predecibles
  - Son estables en una misma subred (importante para O&M)
  - cambian al moverse de una red a otra
- Próximo a ser publicado como RFC

Fragmentación IPv6

Problemas vinculados a Ext Headers

- Resulta en tráfico complejo
- Ejemplo:



SI6 NETWORKS

draft-ietf-6man-nd-extension-headers

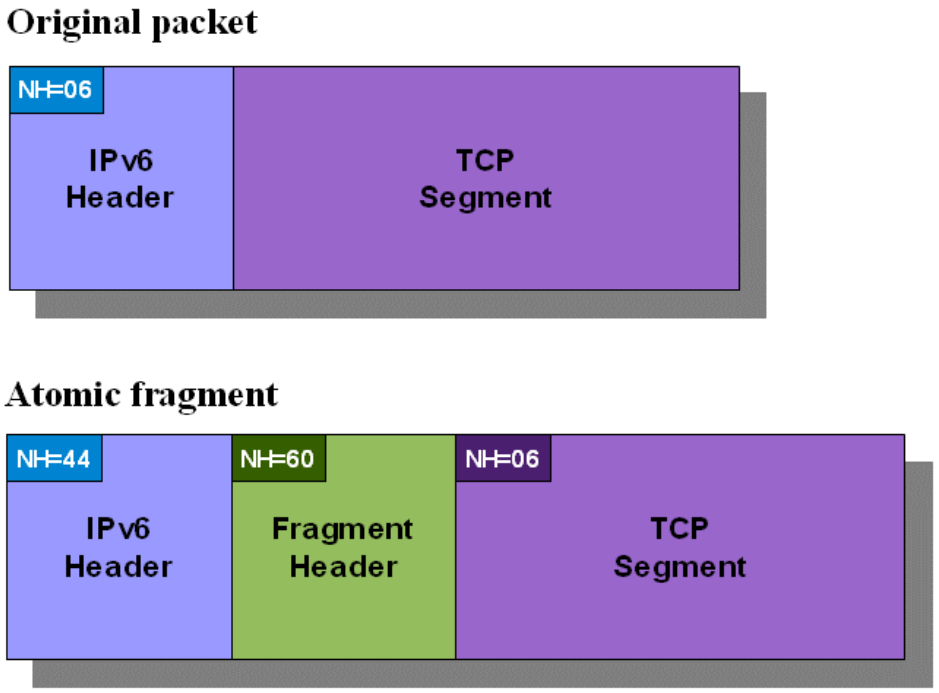
- La fragmentación no es necesaria para Neighbor Discovery
- Esta propuesta prohíbe el uso de fragmentación con Neighbor Discovery

draft-ietf-6man-oversized-header-chain

- Requiere que la cadena de encabezados entera esté en rl primer fragmento
- Esto permite el filtrado de paquetes sin estado

draft-ietf-6man-ipv6-atomic-fragments

- Los IPv6 atomic fragments son paquetes que:
  - Poseen un IPv6 Fragment Header
  - El Fragment Offset es igual a 0
  - El flag “M” es igual a 0



draft-ietf-6man-ipv6-atomic-fragments (II)

- Resultan al recibir un ICMPv6 PTB < 1280
- Suelen ser de utilidad para los traductores IPv6/IPv4
- Muchas implementaciones “mezclan” estos paquetes con tráfico realmente fragmentado
- Esto permite ataques basados en fragmentación
- Solución: procesar estos fragmentos independientemente de otros paquetes

draft-ietf-6man-predictable-fragment-ids

- Muchas implementaciones utilizan Fragment IDs predecibles
- Las implicancias de seguridad son conocidas el mundo IPv4
- draft-ietf-6man-predictable-fragment-ids:
  - Describe las implicancias de seguridad correspondientes
  - Actualiza el standard para que estos problemas sean evitados

IPv6 First-Hop Security

SI6 NETWORKS

draft-ietf-v6ops-ra-guard-implementation

- RA-Guard apunta a filtrar Router Advertisements incorrectos/maliciosos en capa 2
- La mayoria de las implementaciones de RA-Guard son trivialmente evadibles mediante el us de IPv6 Extension Headers
- Describe problemas existentes en implementaciones de RA-Guard
- draft-ief-v6ops-ra-guard-implementation
  - Describe el problema
  - Propone una solución

draft-ietf-v6ops-dhcpv6-shield

- Especifica “DHCP-snooping” para IPv6
- Apunta a evitar los problemas ya encontrados en implementaciones de mecanismos similares (RA-Guard)

Operación de IPv6

draft-ietf-opsec-vpn-leakages

- Mucho software de VPN no soporta IPv6
- Es completamente agnóstico al mismo
- Esto puede llevar a “VPN leakages”
  - Un sistema pide registros A y AAAA para un dominio
  - Si recibe AAAA, puede preferirlos sobre los A
  - El tráfico puede salir por fuera de la VPN

draft-ietf-opsec-ipv6-host-scanning

- Durante mucho tiempo se consideró que era virtualmente imposible
- draft-ietf-opsec-ipv6-host-scanning describe alternativas para realizar IPv6 network reconnaissance
  - Basadas en DNS
  - Basadas en aplicaciones
  - Inspección de archivos de configuración y log files
  - Inspección de estructuras de datos del sistema operativo
  - etc.
- Objetivo: Ayudar a prevenir estos ataques, y posibilitar penetration tests

draft-ietf-opsec-ipv6-implications-on-ipv4-nets

- Describe implicancias de seguridad de IPv6 en redes IPv4
  - En la práctica, no existe cosa tal como redes “IPv4-only”
- Problemas de seguridad:
  - Evasión de politicas de seguridad mediante mecanismos de transición co-existencia
  - Rogue RAs
  - VPN leakages
  - etc
- Este I-D discute distintas formas de mitigar dichas implicancias de seguridad

Conclusiones

Thanks!

Fernando Gont

fgont@si6networks.com

@FernandoGont

SI6 Networks

www.si6networks.com

@SI6Networks