Resultados de un Análisis de Seguridad de IPv6

Fernando Gont

SI6 NETWORKS

XI Foro de Seguridad de RedIRIS
Madrid, España. 25-26 de Abril de 2013

Acerca de...

- He trabajado en análisis de seguridad de protocolos de comunicaciones para:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- Actualmente trabajando para SI6 Networks
- Participante activo de la Internet Engineering Task Force (IETF)
- Más información en: http://www.gont.com.ar

Agenda

- Motivación de esta presentación
- Breve introducción a IPv6
- Discusión de aspectos de seguridad de IPv6
- Implicancias de seguridad de los mecanismos de transición/co-existencia
- Implicancias de seguridad de IPv6 en redes IPv4
- Áreas en las que se necesita más trabajo
- Conclusiones
- Preguntas y respuestas

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

Motivación de esta presentación (II)

- Muchos mitos creados en torno a IPv6:
  - La seguridad fue considerada durante el diseño
  - El paradigma de seguridad cambiará a host-centric
  - Aumentará el uso de IPsec
  - etc.
- Estos mitos tienen y han tenido un impacto negativo
- Esta presentación intentará:
  - Separar “mito” de “realidad”
  - Influenciar como pensás sobre “seguridad IPv6”

Breve introducción a IPv6

Breve comparación entre IPv6/IPv4

- Muy similares en *funcionalidad*, pero no así en *mecanismos*

	IPv4	IPv6
Direccionamiento	**32 bits**	**128 bits**
Resolución de direcciones	**ARP**	**ICMPv6 NS/NA (+ MLD)**
Auto-configuración	**DHCP & ICMP RS/RA**	**ICMPv6 RS/RA & DHCPv6 (opcional) (+ MLD)**
Aislamiento de fallos	**ICMPv4**	**ICMPv6**
Soporte de IPsec	**Opcional**	**Opcional**
Fragmentación	**Tanto en hosts como en routers**	**Sólo en hosts**

Consideraciones generales sobre seguridad IPv6

Algunos aspectos interesantes...

- Menor experiencia con IPv6 que con IPv4
- Implementaciones de IPv6 menos maduras que las de IPv4
- Menor soporte para IPv6 que para IPv4 en productos de seguridad
- La red Internet será mucho mas compleja:
  - Dos protocolos de Internet
  - Mayor uso de NATs
  - Mayor uso de túneles
  - Uso de otras tecnologías de transición co-existencia
- Pocos recursos humanos bien capacitados

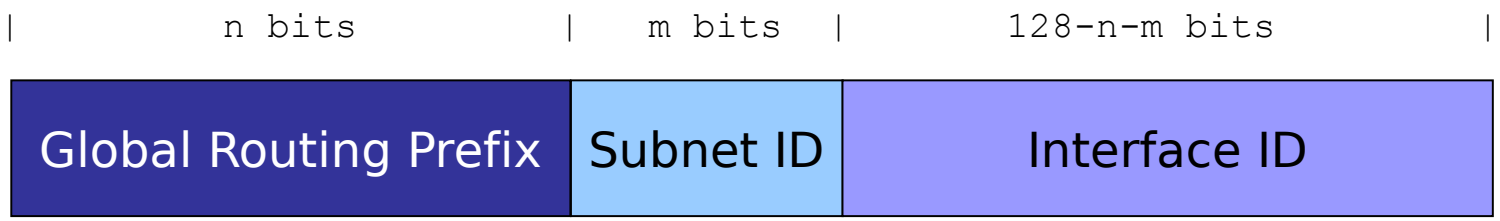
… así y todo tal vez sea la única opción para permanecer en el negocio

Implicancias de seguridad de IPv6

Direccionamiento IPv6
Implicancias en el escaneo de sistemas

SI6 NETWORKS

Direcciones Global Unicast



- El “Interface ID” es en general de 128 bits
- Se puede seleccionar con diferentes criterios:
  - Modified EUI-64 Identifiers
  - Privacy addresses
  - Configurados manualmente
  - De acuerdo a lo especificado por tecnologías de trasición

Implicancias en escaneo de sistemas

Mito: "*IPv6 hace que los ataques de escaneo de sistemas sean imposibles!*"

- Esto asume que las direcciones IPv6 se generan aleatoriamente
- Malone (*) midió y categorizó las direcciones de acuerdo a distintos patrones. Por ejemplo:
  - SLAAC (MAC address embebida en el Interface ID)
  - "Low byte" (2001:db8::1, 2001:db8::2, etc.)
  - Privacy addresses (Interface ID aleatorio)
- Las direcciones IPv6 siguen distintos patrones, explotables para reducir el "espacio de búsqueda" en ataques de escaneo

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

Algunas conclusiones

- Los ataques de escaneo **son posibles** en IPv6
- Se han econtrado “in the wild”
- Es esperable que no sean de “fuerza bruta”, y aprovechen:
  - Patrones de las direcciones
  - “Leaks” de la capa de aplicación
  - Direcciones multicast, Neighbor discovery, etc. (para ataques locales)
- Técnicas implementadas en **scan6** (SI6 Networks' IPv6 Toolkit)
- Recomendaciones:
  - Evitar patrones en las direcciones IPv6
    - Ver por ej. draft-ietf-6man-stable-privacy-addresses
  - Siempre considerar el uso de firewalls

Conectividad Extremo a Extremo

Breve reseña

- La red Internet se basó en el principio de “extremo a extremo”
  - Red tonta, extremos (hosts) inteligentes
  - La comunicación es posible entre cualquier par de nodos
  - La red no examina el contenido de los paquetes IP
- Se suele argumentar que este principio permite la innovación
- Los NATs lo han eliminado de Internet
- Se espera que con IPv6 no existan NATs, y se retorne al principio “extremo a extremo”

IPv6 y el principio “extremo a extremo”

Mito: “*IPv6 devolverá a Internet el principio 'extremo a extremo*'”

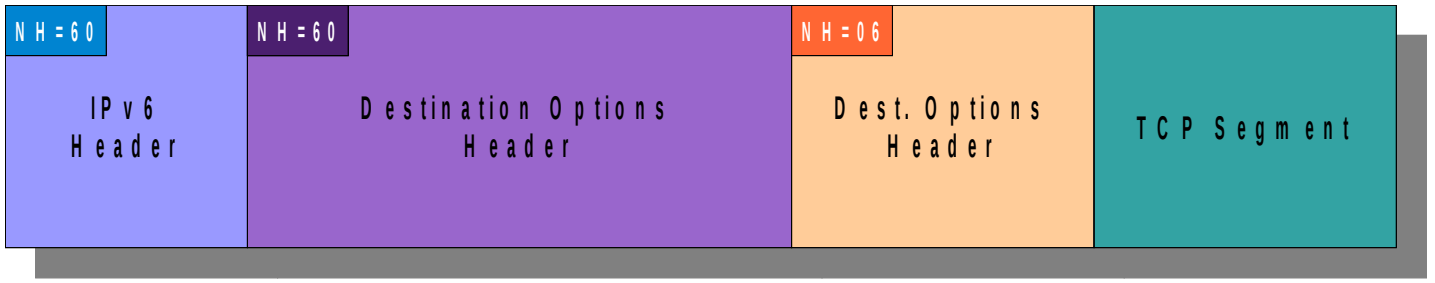
- Se asume que el gran espacio de direcciones devolverá este principio
- Sin embargo,
  - Las direcciones globales no garantizan conectividad extremo a extremo
  - La mayoría de las redes no tiene interés en “innovar”
  - Este principio aumenta la exposición de los sistemas
- En resumen,
  - La conectividad extremo a extremo no necesariamiente es deseable
  - La subred típica IPv6 solo permitirá “trafico saliente” (mediante firewalls)

IPv6 Extension Headers

Implicancias de seguridad generales

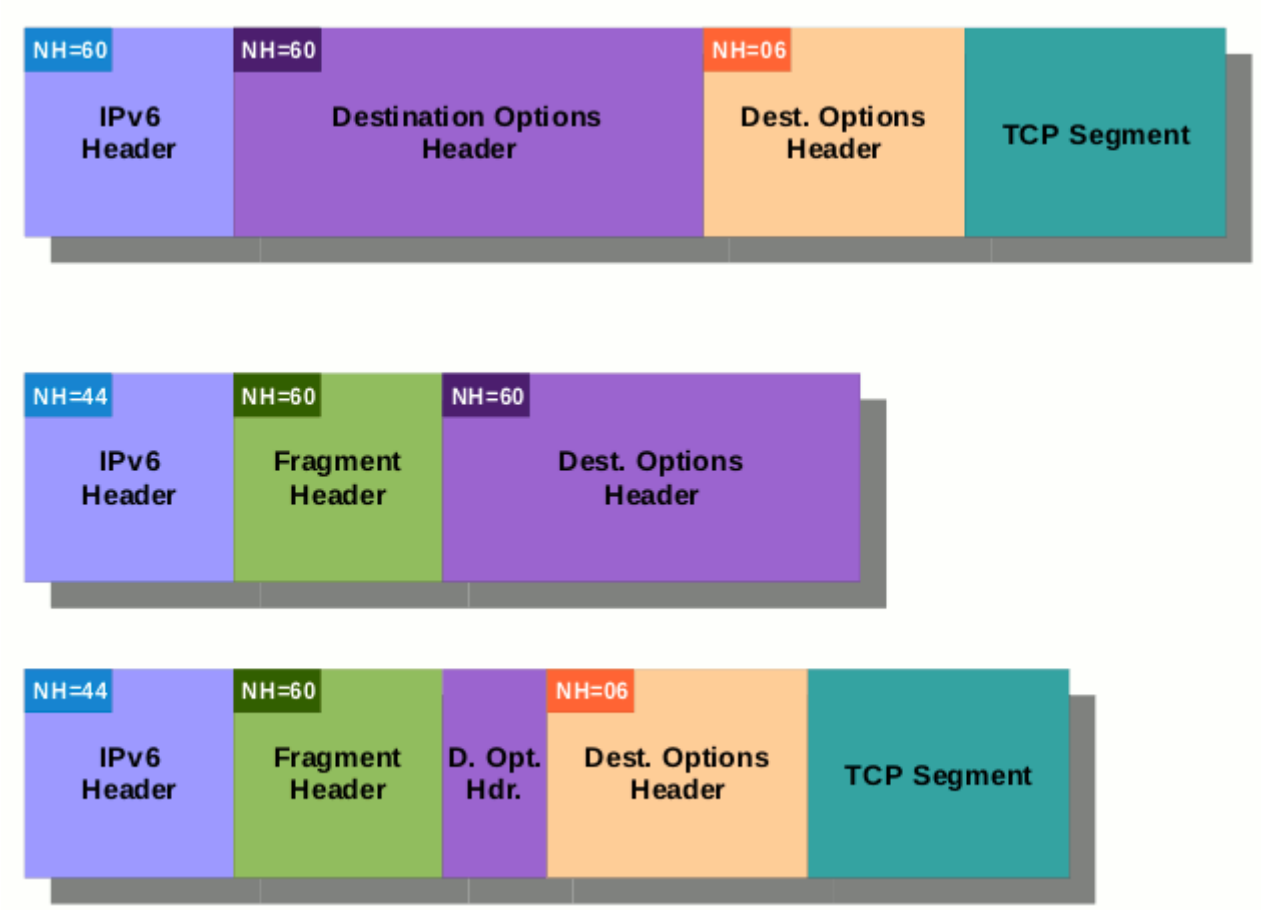
Estructura general de paquete IPv6

- Consiste en una cadena de encabezados y un payload (opcional)
- Formato típico de los Extension Headers: TLV (Type-Length-Value)
- Posibles multiples instancias de multiples encabezados
- Cada encabezado puede contener una cantidad arbitraria de opciones



Estructura general de paquete IPv6 (II)

- El tráfico resultante puede ser engorroso



Consideraciones generales

- Posibles implicancias negativas en performance
- Se hace dificultoso el DPI (difícil encontrar la información de layer-4!)
- Puede resultar imposible identificar qué tipo de trafico fue fragmentado

Resolución de direcciones

Breve reseña

- Resolución de direcciones: IPv6 → capa de enlace
- Realizada en IPv6 por “Neighbor Discovery”:
  - Basado en mesajes ICMPv6 (Neighbor Solicitation y Neighbor Advertisement)
  - Análogo a ARP Request y ARP Reply
  - Implementado sobre IPv6, y **no** sobre la capa de enlace

Vulnerabilidades y contramedidas

- Se pueden portar los ataques “ARP” de IPv4 a IPv6
  - Man in The Middle
  - Denial of Service
- Potenciales contramedidas:
  - Desplegar SEND
  - Monitorear tráfico de Neighbor Discovery
  - Utilizar entradas estáticas en el Neighbor Cache
  - Restringir el acceso a al red local
- Lamentablemente,
  - En la actualidad es dificultoso aplicarlas a escenarios reales
  - La situación es “algo mas complicada” que en IPv4

Auto-configuración

Breve reseña

- Dos mecanismos de autoconfiguración en IPv6:
  - Stateless Address Auto-Configuration (SLAAC)
    - Basado en ICMPv6
  - DHCPv6
    - Basado en UDP
- SLAAC es mandatorio, mientras que DHCPv6 es opcional
- Funcionamiento básico de SLAAC:
  - Los hosts solicitan información mediante ICMPv6 Router Solicitations
  - Los routers responden con Router Advertisements:

Vulnerabilidades y contramedidas

- Falsificando Router Advertisements se puede realizar:
  - Man In the Middle
  - Denial of Service
- Posibles contramedidas:
  - Desplegar SEND
  - Monitorear mensajes RS/RA
  - Desplegar Router Advertisement Guard (RA-Guard)
  - Restringir el acceso a la red local
- Lamentablemente,
  - En la actualidad es dificultoso aplicarlas a escenarios reales
  - La situación es “algo mas complicada” que en IPv4

Soporte de IPsec

Breve reseña y consideraciones

Mito: "*IPv6 es mas seguro que IPv4 porque la seguridad fue considerada durante el diseño del protocolo*"

- Debe su origen a que IPsec era opcional para IPv4, y mandatorio para IPv6 (hoy es opcional para ambos)
- En la práctica, esto fue/es irrelevante:
  - Es mandatorio el soporte, pero no así su uso
  - Las implementaciones no respetan el estándar
  - Existen en IPv6 los mismos obstáculos para IPsec que en IPv4
- Incluso la IETF reconoció esta situación
- Conclusión:
  - El despliegue de IPv6 no implica un mayor uso de IPsec

Implicancias de seguridad de los mecanismos de transición

Breve reseña

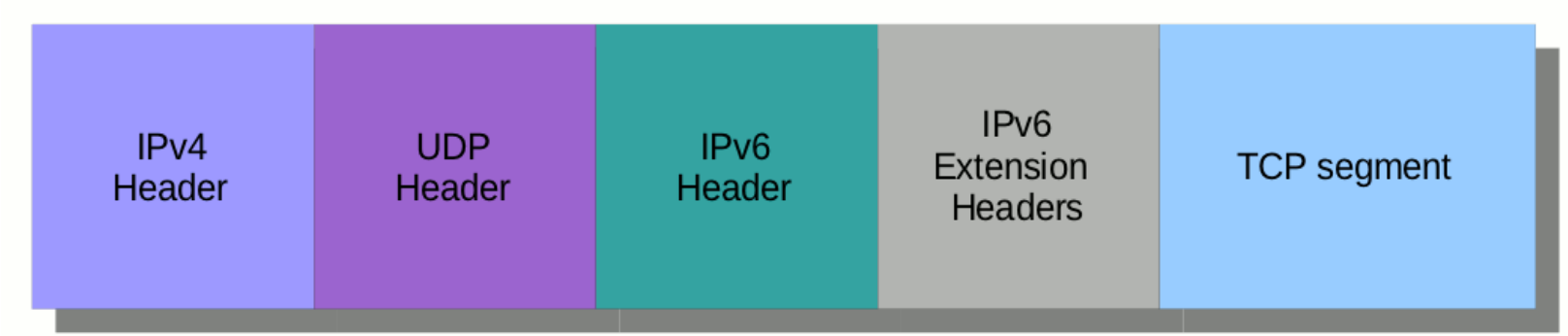
- Plan original de transición: doble pila (dual stack)
  - Desplegar IPv6 en paralelo con IPv4 **antes** de **necesitar** IPv6
  - Este plan **falló**
- La estrategia actual es transición/co-existencia basada en:
  - Doble pila
  - Túneles
    - Automáticos
    - Configurados
  - Traducción
    - CGN
    - NAT64
- La mayoria de los sistemas soportan algunos de estos mecanismos

Consideraciones de seguridad

- Se incrementa la complejidad de la red
- Se introducen “Puntos Únicos de Fallo” (Single Points of Failure)
- Algunas tecnologías tienen implicancias de privacidad:
  - ¿Por dónde circula su tráfico Teredo, 6to4, o de túneles configurados?
  - Esto puede (o no) ser problemático para su organización

Consideraciones de seguridad (II)

- La complejidad del tráfico aumenta notablemente
- Se dificulta la realización de “Deep Packet Inspection”
- Ejemplo: Estructura de un paquete “Teredo”:



- “Ejercicio”: construir filtro libpcap para capturar paquetes destinados al host 2001:db8::1, puerto TCP 25

Implicancias de seguridad de IPv6 en redes IPv4

SI6 NETWORKS

Breve reseña

- La mayoría de los sistemas tiene algún tipo de soporte IPv6 habilitado “por defecto”
  - Doble pila
  - Teredo
  - ISATAP
  - etc
- Por ende,
  - La mayoría de las “redes IPv4” tienen al menos un **despliegue parcial de IPv6**

Consideraciones de seguridad

- Se puede habilitar la conectividad IPv6 “durmiente”
- El uso de IPv6 podría ocasionar que el tráfico de red circule por fuera de una VPN (Virtual Private Network)
- Las tecnologías de transición pueden aumentar la exposición de sistemas
  - Teredo permite el “traspaso” de NATs por sistemas externos
- En conclusión,
  - No existen redes IPv4 “puras”
  - Siempre se deben considerar las implicancias de seguridad de IPv6
  - Si no desea utilizar IPv6, asegurese que ese sea el caso

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/tools
- 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

Áreas en las que se necesita más trabajo

Áreas en las que se necesita mas trabajo

- Seguridad de implementaciones
  - Todavía no han sido foco de ataque
  - Pocas herramientas de auditoria
  - Se descubrirán muchos bugs y vulnerabilidaes
- Soporte de IPv6 en dispositivos de seguridad
  - Se necesita paridad de funcionalidad IPv6/IPv4
  - Caso contrario, no se pueden aplicar las misms políticas de seguridad
- Educación/Entrenamiento
  - Se necesita entrenamiento para todo el personal involucrado
  - Primero entrenarse, luego desplegar IPv6

Algunas conclusiones

Algunas conclusiones....

- Estar atentos al marketing y mitología sobre IPv6
  - Confiar en ellos tiene sus implicancias
- IPv6 provee una *funcionalidad* similar a IPv4
  - Los *mecanismos* utilizados son distintos
  - En dichas diferencias pueden aparecer las “sorpresas”
- La mayoría de los sistemas tiene soporte IPv6
  - Usualmente no existen redes IPv4 “puras”
  - Toda red debe considerar las implicancias de seguridad de IPv6
- Tarde o temprano desplegarás IPv6
  - Es hora de capacitarse y expetimentar con IPv6
  - Sólo después debe desplegarse el mismo

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com