Consideraciones de Seguridad en IPv6

Fernando Gont

SI6 NETWORKS

Experience IPv6 2017

Nairobi, Kenia. 6 de Junio de 2017

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)
  - 30 IETF RFCs
  - 10+ documentos (IETF I-Ds) de WG
- Más información en: https://www.gont.com.ar

Objetivos de esta presentación

Objetivos de esta presentación

- Discutir tendencias actuales en materia de seguridad IPv6
- Dar una mínima guía en materia de seguridad IPv6
- Objetivo personal:
  - Que no se duerman :-)

Breve comparación entre IPv6/IPv4

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**	**Mandatorio (a "opcional")**
Fragmentación	**Tanto en hosts como en routers**	**Sólo en hosts**

Consideraciones generales sobre seguridad IPv6

Algunos aspectos interesantes...

- Pocos recursos humanos bien capacitados
- Menor experiencia con IPv6 que con IPv4
- Implementaciones de IPv6 menos maduras que las de IPv4
- Menor soporte en productos de seguridad para IPv6 que para IPv4
- 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

… así y todo es la única opción para permanecer en el negocio

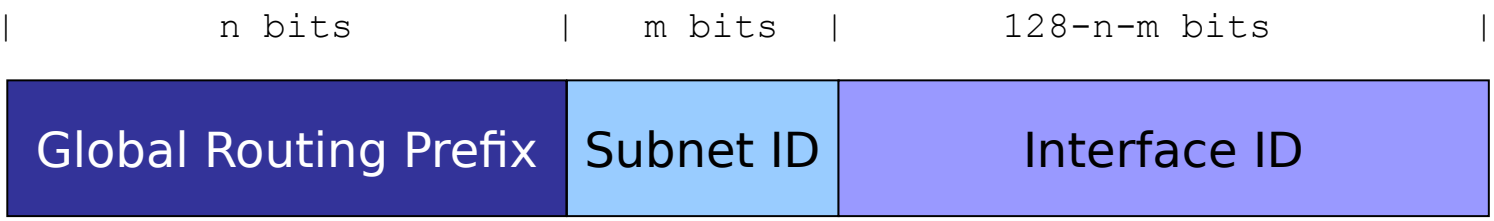
Tendencias en Seguridad IPv6

Direccionamiento IPv6
Breve Reseña

Breve revisión de direccionamiento IPv6

- El mayor espacio de direcciones es el “motivador” de IPv6
- Se utilizan direcciones de 128 bits
- Semántica muy similar a IPv4:
  - Se agregan direcciones en “prefijos” para el ruteo
  - Existen distintos tipos de direcciones
  - Existen distintos alcances para las direcciones
- Cada interfaz utiliza multiples direcciones, de multiples tipos y alcances:
  - Una dirección link-local unicast
  - Una o mas direcciones global unicast
  - etc.

Direcciones Global Unicast



- Global Routing Prefix y Subnet ID similares a IPv4
- El “Interface ID” análogo al Host-ID de IPv4 (pero de 64 bits)
- Se puede seleccionar con diferentes criterios:
  - Modified EUI-64 Identifiers (**SLAAC tradicional**)
  - Identificadores aleatorios (direcciones temporales)
  - Configurados manualmente
  - De acuerdo a lo especificado por tecnologías de transición

Direccionamiento IPv6
Reseña de las Implicancias de Seguridad

Impl. de seg. del direccionamiento IPv6

- Ataques a dispositivos especificos
- Correlación de actividades en el tiempo
- Correlación de actividades en el espacio
- Reconocimiento de redes

Ataques a dispositivos específicos

- Los IIDs basados en direcciones MAC revelan el fabricante de la tarjeta de red
- Es trivial identificar posibles “objetivos” de ataques con vulnerabilidades específicas de dichos fabricantes

Correlación de actividades en el tiempo

- Los IID de IPv6 IIDs son “globalmente únicos” y estables
- Ejemplo:
  - Dia #1: Veo actividad de 2001:db8:1::1111:22ff:fe33:4444
  - Dia #2: Veo actividad de 2001:db8:1::1111:22ff:fe33:4444
  - El IID “1111:22ff:fe33:4444” revela la identidad del nodo
    - Por lo tanto puedo hacer correlación de actividades
- Existía esto en IPv4?
  - No al mismo nivel
  - El espacio pequeño de direcciones (y los NAT!) son causantes de “colisiones” de IID

Correlación en el espacio

- Los IID de IPv6 IIDs son “globalmente únicos” y estables
- Cuando un host se mueve, cambia el prefijo pero **no** el IID
  - el IID de 64-bit IID se convierte en una super-cookie!
- Ejemplo:
  - En la red #1, el host configura: 2001:db8:1::1111:22ff:fe33:4444
  - En la red #2, el host configura: 2001:db8:2::1111:22ff:fe33:4444
  - El IID “1111:22ff:fe33:4444” revela la identidad de host
- Se introduce un problema no existente en IPv4: correlación de actividades en el espacio (**host-tracking**)

Reconocimiento de Red

- Se ha asumido que los ataques de escaneo de direcciones IPv6 son imposibles
- Las direcciones IPv6 siguen patrones
  - El espacio de búsqueda **no** es 2^{64}!
- Si bien el escaneo por fuerza bruta es “imposible”

Los ataques de escaneo que explotan patrones en las direcciones IPv6 son posibles

Direccionamiento IPv6
Mitigación tradicional

RFC4941: Direcciones temporales

- Direcciones con las siguientes características:
  - El IID es aleatorio
  - El IID varia en el tiempo
  - Se generan adicionalmente a las direcciones SLAAC tradicionales
- Utilización:
  - Las direcciones temporales se utilizan para conexiones salientes
  - Las direcciones estables se utilizan para conexiones entrantes
- Quedan sin mitigar:
  - Ataques a dispositivos específicos
  - Reconocimiento de redes
  - Host-tracking (correlación en el espacio)

Direccionamiento IPv6

Novedades/Mitigaciones

SI6 NETWORKS

Direcciones Auto-configuradas

	Estable	Temporal
Predecible	IEEE ID-derived	Ninguno
No Predecible	**RFC 7217**	RFC 4941

- RFC 7217 (stable privacy-enhanced IPv6 addresses (*)):
  - Reemplaza a las direcciones tradicionales, basadas en IEEE IDs
  - En buena medida es ortogonal a las direcciones temporales
  - Probablemente “lo suficientemente bueno” incluso sin RFC4941

(*) Ahora llamadas “Semantically Opaque Interface Identifiers”

RFC7217: Algoritmo

- Genera el Interface IDs mediante:

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

- Donde:
  - F() es una PRF (por ej., una función de hashing)
  - Prefix es el prefijo SLAAC o el prefijo link-local
  - Net_Iface es algún 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)

RFC7217: Propiedades

- Cuando el host se “mueve”:
  - Prefix y Network_ID varían de una red a otra
  - Pero permanecen constantes dentro de cada red
  - Resultado de F() varía de una red a otra, pero es estable dentro de cada red
- Esto resulta en direcciones que:
  - Son estables dentro de cada red
  - No siguen patrones
  - Tienen diferentes Interface-IDs cuando se cambia de red
  - En general, poseen las mejores ventajas de ambos mundos

RFC7217: Implementaciones

- Implementaciones
  - Linux kernel v4.0
  - NetworkManager v1.2.0-0.3.20151112gitec4d653.fc24
  - dhcpcd 6.4.0
- Sistemas operativos con soporte de RFC7217:
  - MacOS Sierra
  - Fedora 24

Direccionamiento IPv6
Consejos

Consejos

- Para sistemas en modo “roaming”, utilizar:
  - RFC7217 + RFC4941
  - Considerar el uso de MAC address randomization
- Para ambientes enterprise, utilizar:
  - RFC7217

Mas información

- RFC7721
  - Discute las implicancias de seguridad del direccionamiento IPv6
- RFC7707
  - Discute IPv6 network reconnaissance
- RFC7217:
  - Especifica “semantically-opaque addresses”
- RFC8064:
  - Recomienda la implementacion de RFC7217

Conectividad Extremo a Extremo

Breve reseña

- La red Internet se basó en el principio de “extremo a extremo”
  - Red tonta, extremos (hosts) inteligentes
  - La comuncación 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
- NATs (principalmente) y firewalls lo han eliminado de Internet
- Se esperaba que con IPv6 se retorne al principio “extremo a extremo”
- La consecuencia sería un paradigma de seguridad centrado en hosts (y no en red)

Consejos

- Desde el punto de vista de seguridad, siempre es preferible el “principio de menor privilegio”
- Permitir comunicación solo en casos necesarios
- Ejemplo:
  - En redes hogareñas, permitir por defecto sólo “conexiones salientes”
  - Este es el modelo aplicado por ej., Comcast en EE.UU.

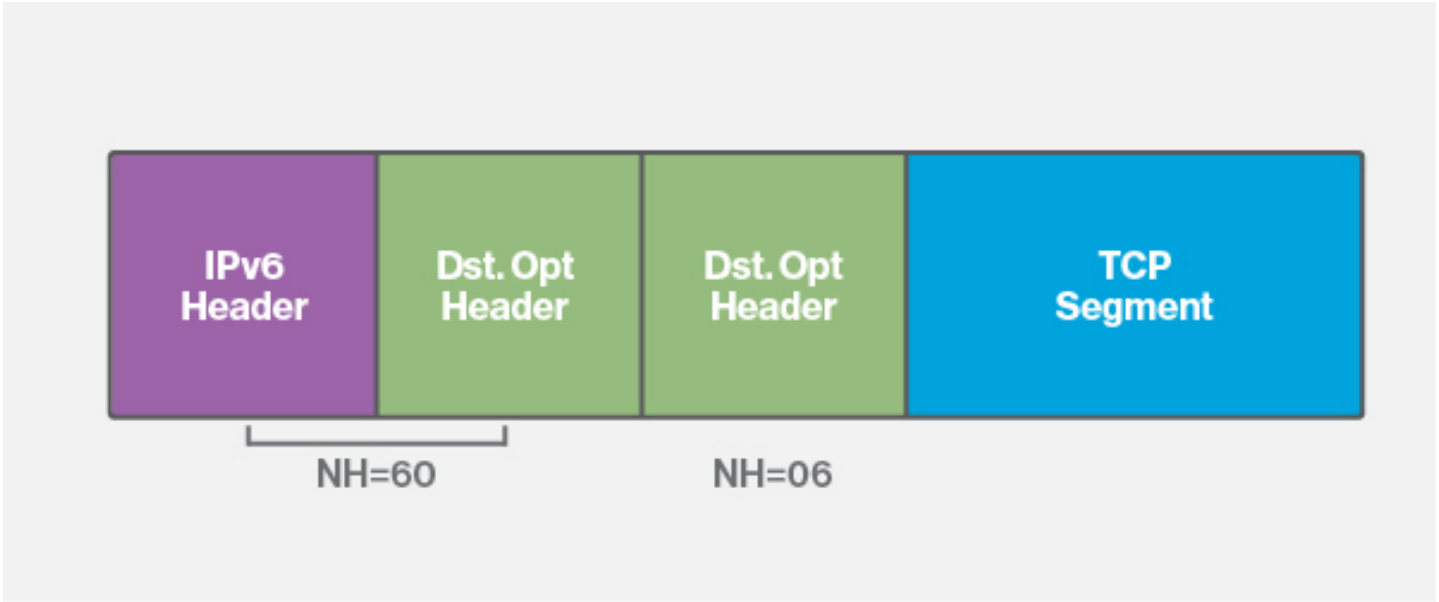
IPv6 Extension Headers

Breve reseña

SI6 NETWORKS

IPv6 Extension Headers

- Encabezado IPv6 base de longitud fija
- Las opciones se incluyen en diferentes “Encabezados de Extensión”
- El paquete sigue una estructura de “lista enlazada”
- Permiten la extensibilidad del protocolo



Implicancias de los IPv6 EHs

- El tráfico IPv6 puede ser dificil de inspeccionar
- Como consecuencia:
  - evasión de NIDS
  - DoS
  - etc.

IPv6 Extension Headers
Realidad

IPv6 EHs en el Mundo Real

- Muchos operadores descartan los paquetes que contienen encabezados de extensión:
  - Cuestiones de seguridad asociadas a los EHs
  - No existe dependencia de estos encabezados

Pero... que significa esto?

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

IPv6 Extension Headers
Consejos

Consejos

- En el borde de una red organizacional, utilizar una “lista blanca”
  - Solo permitir EHs necesarios para los servicios de la red en cuestión
- En proveedores de tránsito, utilizar una lista negra
  - Descartar paquetes con EHs “maliciosos” (por ej., RHTO)
- Consultar la documentación de los sistemas involucrados respecto del procesamiento de EHs
  - Por ej., procesar una cadena de EHs completa podría requerir el procesamiento “lento” de un paquete
  - En determinados escenarios, podría ser necesario descartar todos los paquetes con EHs

Más información

- RFC7872
  - Mediciones sobre el soporte de IPv6 EHs en Internet
- draft-gont-v6ops-ipv6-eh-packet-drops
  - Análisis de las razones para descartar con paquetes con EHs
- draft-ietf-opsec-ipv6-eh-filtering
  - Recomendaciones sobre el filtrado de paquetes con EHs
- RFC7113
  - Evasión de RA-Guard

Neighbor Discovery & DHCPv6

Breve Reseña

Breve reseña

- Dos mecanismos de autoconfiguración en IPv6:
  - Stateless Address Auto-Configuration (SLAAC)
    - Basado en mensajes ICMPv6 RS/RA
  - DHCPv6
    - Basado en UDP
- La resolución de direcciones (equivalentes a ARP de IPv4) esta basada en mensajes ICMPv6 NS/NA
- A diferencia de IPv4:
  - Todos ellos son mas inependientes de la tecnología de red
  - Pero el tráfico resultante es mas complejo

Neighbor Discovery & DHCPv6
Implicancias de Seguridad

Implicancias de seguridad

- Autoconfiguración:
  - DoS
  - Man-In-The-Middle
- Resolución de direcciones:
  - DoS
  - Man-In-The-Middle

Neighbor Discovery & DHCPv6

Consejos

Consejos

- Preguntarse: Se utilizan contramedidas para los mecanismos analogos del mundo IPv4?
  - DHCP-Guard, etc.
- Para lograr paridad de seguridad, implementar:
  - RA-Guard
  - DHCPv6-Shield
  - IPv6 Source Guard/SAVI
- **Comprobar si dichos mecanismos son evadibles**

Más información

- Cisco First Hop Security:
  - http://docwiki.cisco.com/wiki/FHS
- RA-Guard
  - RFC6105
  - RFC7113
- IPv6 Source Guard
  - RFC7039

Implicancias de seguridad de IPv6 en redes IPv4

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”
  - Enviando Router Advertisements
  - Habilitando tecnologías de transición/co-existencia
- Las tecnologías de transición pueden aumentar la exposición de sistemas
- La conectividad IPv6 puede llevar a fugas de tráfico
  - Por ejemplo, software VPN que solo soporta IPv4

Implicancias de seguridad de IPv6 en redes IPv4

Consejos

Consejos

- No existen redes IPv4 “puras”
- Siempre se deben considerar las implicancias de seguridad de IPv6
- Si no desea utilizar IPv6, asegúrese que ese sea el caso

Herramientas de seguridad IPv6

Herramientas de seguidad IPv6

- Por años, THC's IPv6 attack suite (http://www.thc.org) fue el único set de herramientas IPv6 públicamente disponible
- En el 2009, publicamos “SI6 Networks IPv6 toolkit”
  - Un nuevo grupo de herramientas para seguridad y trouble-shooting
  - Portable (Linux, *BSD, Mac OS, OpenSolaris)
  - Poderoso y flexible
  - Buena documentación
- Disponible en: https://www.si6networks.com/tools/ipv6toolkit
  - Repositorio GIT en: https://github.com/fgont/ipv6-toolkit.git

Conclusiones

Conclusiones

- Hay mucho por aprender en materia de seguridad IPv6
- En algunas áreas, IPv6 es un “moving target”
- Tarde temprano estarás lidiando con IPv6
  - Es hora de empezar!

Preguntas?

Contacto

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

https://www.si6networks.com/community/

www.si6networks.com