Seguridad IPv6

Fernando Gont

Seminario virtual organizado por LACNIC

Viernes 29 de Abril de 2011

Agenda

- Objetivos de este seminario
- Breve comparación de IPv6/IPv4
- Discusión de aspectos de seguridad de IPv6
- Seguridad de los mecanismos de transición/co-existencia
- Implicancias de seguridad de IPv6 en redes IPv4
- Áreas en las que se necesita progreso
- Conclusiones
- Preguntas (y posiblemente respuestas ☺)

Objetivos de este seminario

- Proveer un análisis objetivo de las implicancias de seguridad generales de IPv6
- Identificar y analizar algunos aspectos que deben ser considerados a la hora de desplegar IPv6
- Identificar y analizar las implicancias de seguridad de IPv6 en redes IPv4
- Identificar áreas en las que se requiere más trabajo
- Obtener algunas conclusiones respecto a la seguridad en IPv6

Consideraciones generales sobre seguridad IPv6

Aspectos interesantes sobre seguridad IPv6

- Se cuenta con mucha menos experiencia que con IPv4
- Las implementaciones de IPv6 son menos maduras que las de IPv4
- Los productos de seguridad (firewalls, NIDS, etc.) tienen menos soporte para IPv4 que para IPv6
- La complejidad de las redes se incrementará durante el periodo de transición/co-existencia:
  - Dos protocolos de red (IPv4 e IPv6)
  - Mayor uso de NATs
  - Mayor uso de túneles
  - Uso de otras tecnologías de transición
- Pocos recursos humanos bien capacitados

…y así y todo IPv6 será en muchos casos la única opción disponible para continuar en el negocio de Internet

Comparación entre IPv6 e IPv4

(qué cambia, y qué no)

Breve comparación de IPv4 e IPv6

- IPv4 e IPv6 son muy similares en términos de *funcionalidad* (no así de *mecanismos*)

	IPv4	IPv6
Direccionamiento	32 bits	128 bits
Resolución de direcciones	ARP	ICMPv6 ND/NA (+ MLD)
Auto-configuración	DHCP & ICMP RS/RA	ICMPv6 RS/RA & DHCPv6 (opcional) (+ MLD)
Soporte de IPsec	Opcional	Recomendado (**no** mandatorio)
Fragmentación	Tanto en hosts como routers	Sólo en hosts

Implicancias de Seguridad de IPv6

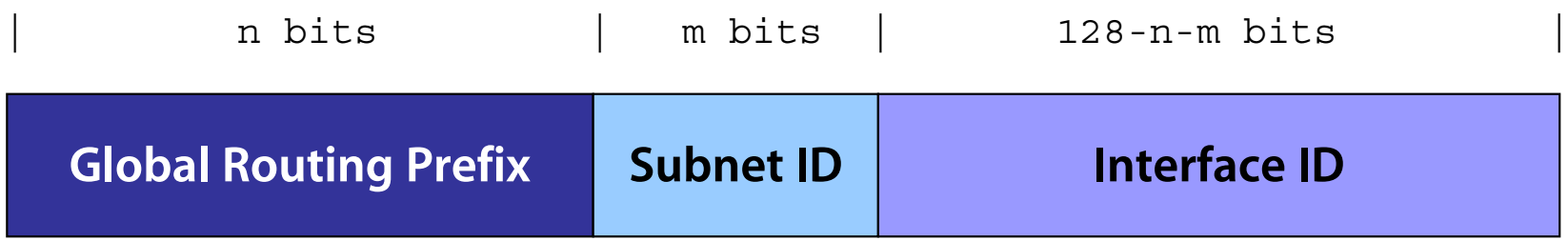
Direccionamiento

Breve reseña

- El principal motivador de IPv6 es su mayor espacio de direcciones
- IPv6 utiliza direcciones de 128 bits
- De manera similar a IPv4,
  - Las direcciones se “agregan” en prefijos para su ruteo
  - Se definen distintos tipos de direcciones (unicast, anycast, y multicast)
  - Se definen distintos alcances para las direcciones (link-local, global, etc.)
- Lo usual es que en un determinado instante, un nodo use varias direcciones, de distintos tipos y alcances

Breve reseña (II)

- Formato de las direcciones IPv6 unicast globales:



- El Interface ID es típicamente de 64 bits
- Las direcciones unicast globales pueden "generarse" con distintos criterios:
  - Formato EUI-64 modificado (embebiendo direcciones de capa de enlace)
  - Direcciones "temporales" (o sus variantes)
  - Patrones predeterminados por el administrador (por ej., PREFIJO::1)
  - De acuerdo a lo especificado por una tecnología de transición/co-existencia

Consideraciones de seguridad

- Asumiendo que las direcciones de los hosts están uniformemente distribuídas en la subred, sería muy difícil realizar un "escaneo por fuerza bruta"
- Sin embargo, estudios realizados (*) indican que este no es necesariamente el caso:
  - Para los clientes: 50% SLAAC, 20% IPv4-based, 10% Teredo, 8% "low-byte"
  - Para "infraestructura": 70% "low-byte", 5% IPv4-based
- En el caso de la infraestructura, usualmente no es critico que las direcciones sean predecibles
- En el caso de los "clientes", es recomendable (en la medida que sea posible) no asignar las direcciones de modo que las mismas sean predecibles -- por ej., utilizar direcciones "temporales"
- De cualquier modo, existen otros modos de identificar clientes (por ej. A través del DNS o de protocolos de aplicación)

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

Conectividad “extremo a extremo” (“end-to-end”)

Breve reseña

- Dado que IPv6 posee un gran espacio de direcciones, se espera que cada dispositivo conectado a la red cuente con una dirección IPv6 global unica.
- Es usual asumir que esto “devolverá” a la Internet el principio conocido como “end-to-end”:
  - La comunicación entre sistemas es transparente (por ej., los nodos intermedios no modifican los paquetes)
  - Cualquier sistema de la red es capaz de establecer una comunicación con cualquier otro sistema de la red
  - Usualmente se argumenta que esto permitiría la “innovación” en la red

Consideraciones varias

- El hecho de que cada sistema posea una dirección global única no garantiza la posibilidad de comunicación “extremo a extremo”
  - Esta no es necesariamente una propiedad “deseable” en una red de producción
  - Por tal motivo, es de esperar que una subred IPv6 típica (como ser una red hogareña) esté protegida por un firewall stateful que solo permita el tráfico “de retorno” (aquél en respuesta a comunicaciones iniciadas desde el interiore de la red)
- La realidad es que la mayoría de las redes de hoy en día no tienen como fin la innovación, sino que son un medio para trabajar o recrearse
- Y los servicios esperados por los usuarios son aquellos mismos que hoy se brindan en IPv4 sin conectividad “end-to-end” (web, email, redes sociales, etc.)

Resolución de Direcciones

Breve reseña

- Para resolver direcciones IPv6 en direcciones de capa de enlace se utiliza el mecanismo denominado “Neighbor Discovery”
- El mismo se basa en el protocolo ICMPv6
- Los mensajes ICMPv6 Neighbor Solicitation y Neighbor Advertisement cumplen una función an+aloga a la de ARP request y ARP reply en IPv4

Consideraciones de seguridad

- Como es de esperarse, en IPv6 se pueden realizar ataques análogos a los ataques “ARP spoofing” de IPv4
- Algunas técnicas de “mitigación” posibles son:
  - Desplegar SEND (SEcure Neighbor Discovery)
  - Monitorear el tráfico de Neighbor Discovery (por ej. con NDPMon)
  - Usar entradas estáticas en el Neighbor Cache
  - Restringir el acceso a la red
- Lamentablemente,
  - SEND es difícil de desplegar (requiere de una PKI)
  - Las herramientas de monitoreo son posibles de evadir
  - El uso de entradas estáticas “no escala” para el caso general
  - No siempre es posible restringir el uso a una red
- En síntesis, la situación no es tan diferente a la de IPv4

Autoconfiguración

Breve reseña

- Existen en IPv6 básicamente dos mecanismos para la autoconfiguración de hosts
  - Stateless: SLAAC (Stateless Address Auto-Configuration), basado en mensajes ICMPv6 (Router Solicitation y Router Advertisement)
  - Stateful: DHCPv6
- SLAAC es mandatorio, mientras que DHCPv6 es opcional
- Mediante el envío de mensajes "Router Advertisement", los router comunican información de configuración a los "hosts" del segmento de red en cuestión
  - Prefijos a utilizar
  - Rutas
  - Valores para distintos parámetros (Hop Limit, MTU, etc.)
  - Tiempos recomendados para la utilización de las direcciones generadas
  - etc.

Consideraciones de Seguridad

- Básicamente, mediante la falsificación de dichos mensajes el atacante puede realizar:
  - Ataques de denegación de servicio (DoS)
  - Ataques de tipo “Man in the Middle” (MITM)
- Algunas técnicas de “mitigación” posibles son:
  - Desplegar SEND (SEcure Neighbor Discovery)
  - Monitorear el tráfico de Neighbor Discovery (por ej. con NDPMon)
  - Utilizar RA guard (Router Advertisement guard)
  - Restringir el acceso a la red
- Lamentablemente,
  - SEND es difícil de desplegar (requiere de una PKI)
  - Las herramientas de monitoreo son posibles de evadir
  - Es posible evadir RA guard
  - No siempre es posible restringir el uso a una red
- En síntesis, la situación no es tan diferente a la de IPv4

Soporte de IPsec

Breve reseña y consideraciones…

- Actualmente, se el soporte de IPsec es mandatorio en toda implementación de IPv6 (y opcional en IPv4) – aunque la IETF está en proceso de cambiar este requerimiento
- Sin embargo, a los fines prácticos, esto es completamente irrelevante:
  - Es/era mandatorío el *soporte* de IPv6 – no así su *utilización*
  - Así y todo, existen muchas implementaciones IPv4 con soporte IPsec, como también implementaciones IPv6 sin soporte IPsec
- Existen en IPv6 básicamente los mismos problemas para el despliegue de IPsec que en IPv4
- Por tal motivo, no existen motivos para esperar más uso de IPsec con IPv6 que el que se tiene con IPv4

Seguridad de los Mecanismos de Transición/Co-existencia

Breve reseña

- El plan original de transición era el uso de dual-stack (*si, este plan falló*)
- La estrategia actual es un plan de transición/co-existencia basado en un grupo de herramientas:
  - Dual Stack
  - Túneles “configurados”
  - Túneles automaticos (ISATAP, 6to4, Teredo, etc.)
  - Traducción (por ej., NAT64)
- Algunas variantes de túneles automáticos (como Teredo e ISATAP) están habilitados por defecto en Windows Vista y Windows 7

Consideraciones de seguridad

- La mayoría de estas tecnologías incrementan la complejidad de la red, y así las potenciales vulnerabilidades
- Muchas de estas tecnologías introducen Puntos Únicos de Falla ("Single Point of Failure") en la red.
- Algunas de ellas han sido explotadas para violar politicas de seguridad, ya que en ocasiones no son tenidas en cuenta por firewalls y NIDS
- Algunos de estos mecanismos merecen consideraciones de privacidad:
  - ¿Por dónde circula su tráfico Teredo y 6to4?
  - Esto puede (o no) ser importante para su red

Implicancias de seguridad de IPv6 en redes IPv4

Breve reseña

- Muchos sistemas tienen algun tipo de soporte IPv6 habilitado “por defecto” – soporte IPv6 nativo, y usualmente suporte de algún mecanismo de transición/co-existencia
- Por ejemplo, Linux, *BSD, y Windows Vista/7 tienen soporte IPv6 nativo habilitado “por defecto”
- Windows Vista/7 tienen, adicionalmente, soporte Teredo e ISATAP habilitado “por defecto”
- Es importante destacar que algunas tecnologías de transición, como Teredo, fueron diseñadas para funcionar incluso a través de NATs

Consideraciones de seguridad

- Un atacante con acceso a una red local podría realizar ataques contra SLAAC (falsificando RAs), haciendo que los hosts locales configuren direcciones IPv6
- Esto podría permitir que se evadan controles de filtrado de tráfico y/o NIDS
- El uso de tecnologías como Teredo podría resultar en que incluso hosts que están detrás de NATs quedaran expuestos a la red pública (Internet)
- Por tales motivos,
  - Incluso si una red no espera utilizar IPv6, debe tener en cuenta las implicancias de seguridad de este protocolo (por ej. en lo que respecta a filtrado y monitoreo)
  - Si se espera que en una red IPv4 no se utilicen mecanismos de transición/co-existencia, se deberían aplicar las políticas de filtrado correspondientes

Trabajo a futuro

Algúnas áreas clave en las que se necesita progreso

- Mejora de implementaciones IPv6
  - Las implementaciones de IPv6 todavía no han estado en el foco de los atacantes. Es muy probable que se descubran muchas vulnerabilidades y bugs en las implementaciones IPv6 actuales.
  - Existen muy pocas herramientas de ataque disponibles públicamente
- Soporte de IPv6 en dispositivos de seguridad
  - IPv6 no tiene el mismo nivel de soporte que IPv5 en dispositivos tales como firewalls, IDS/IPS, etc.
  - Esto es clave para poder aplicar en IPv6 políticas de seguridad comparables con las aplicadas en IPv4.
- Educación/Entrenamiento
  - Desplegar IPv6 sin un conocimiento aceptable del mismo podría llevar a resultados muy desfavorables
  - Se necesita entranamiento para ingenieros, técnicos, personal de seguridad, etc., previo al diseño y puesta en funcionamiento de una red IPv6.

20 million engineers need IPv6 training, says IPv6 Forum
The IPv6 Forum - a global consortium of vendors, ISPs and national research & Education networks - has launched an IPv6 education certification programme in a bid to address what it says is an IPv6 training infrastructure that is "way too embryonic to have any critical impact.“ (**http://www.itwire.com**)

Algunas conclusiones

Algunas conclusiones

- Pese a que IPv6 provee una funcionalidad similar a la de IPv4, muchos de los mecanismos utilizados son diferentes. Por tal motivo, requiere de un análisis cuidadoso.
- Las implicancias de seguridad de IPv6 deben ser consideradas previo a su despliegue, para evitar un impacto negativo en las redes correspodientes
- Dado que la mayoría de los sistemas de uso general cuenta con soporte IPv6, incluso los administradores de redes IPv4 deberían conocer las implicancias de seguridad de IPv6
- Incluso si todavía no lo ha planificado, es probable que necesite desplegar IPv6 en el corto plazo.
- Es hora de capacitarse, entrenarse, y experimentar con IPv6!

Preguntas?

Agradecimientos

- LACNIC (y Arturo Servín en particular), por la organización de este seminario

Fernando Gont

fernando@gont.com.ar

http://www.gont.com.ar

Foro de Seguridad de LACNIC

http://seguridad.lacnic.net