Análisis de Seguridad del Proceso de Configuración Automática de Direcciones IPv6 Sin Estado (SLAAC)

Ernesto Sánchez[1], Daniel Arias Figueroa[2], Henri Alves de Godoy[3]

[1] Universidad Católica de Salta. Facultad de Ingeniería.
[2] Universidad Nacional de Salta. Facultad de Ciencias Exactas.
[3] Faculdade de Ciências Aplicadas. Universidade Estadual de Campinas.
esanchez@ucasal.edu.ar, daaf@cidia.unsa.edu.ar, henri.godoy@fca.unicamp.br

Abstract. El presente trabajo tiene por objetivo principal acompañar el despliegue del protocolo IPv6 mediante la propuesta de una plataforma de virtualización de redes basado en contenedores, que permite el despliegue de topologías para el análisis y comprensión de éste protocolo fundamentalmente en aspectos de seguridad. En base a las consideraciones descriptas en los RFC 7707, 6105 y 7113, se analizaron casos prácticos de ataques comunes al proceso de configuración automática de direcciones IPv6 sin estado en un entorno de red de área local. Con los resultados obtenidos de los análisis realizados, se proponen contramedidas basadas en reglas de filtrado a nivel de campos de encabezado IPv6, las cuales pueden extenderse para contrarrestar otros vectores de ataques a dicho protocolo.

Palabras Claves: IPv6, Virtualización, Redes, Seguridad, Contenedores, SLAAC

1 Introducción

A partir del anuncio realizado por el Registro de Direcciones de Internet de América Latina y Caribe (LACNIC) en el año 2020, en el cual se informa que se ha otorgado la reserva del último bloque disponible de direcciones IPv4, y sumado a la creciente demanda por parte de usuarios finales, generada por la necesidad de conectar dispositivos tales como smartphones, smartTVs, entre otros, y principalmente tecnologías emergentes como IoT, empujan a una solución de migración a IPv6 lo antes posible.

En un contexto general son varios los aspectos que demoran un despliegue definitivo de esta nueva versión. IPv6 es mucho más complejo que IPv4, lo cual traslada esta complejidad en implementaciones principalmente en aspectos de seguridad. Las Implementaciones de IPv6 llevan menos tiempo utilizándose en producción en relación a IPv4, por lo tanto si tiene una menor experiencia con IPv6 que con IPv4. Por otro lado se tiene menor soporte en productos de seguridad para IPv6 que para IPv4. Así mismo, la existencia de varias alternativas de tecnologías de transición implica el despliegue de entornos de redes mucho más complejos. Por

último, y relacionado de manera directa con todo lo anterior, aún no se cuenta con recursos humanos bien capacitados [1].

El presente trabajo tiene por objetivo principal acompañar el despliegue del protocolo IPv6 mediante la propuesta de una plataforma de virtualización de redes basado en contenedores, que permita el despliegue de topologías para el análisis y comprensión del protocolo IPv6 fundamentalmente en aspectos de seguridad.

Se presentará como caso práctico el análisis de vulnerabilidades y contramedidas en el proceso de configuración de direcciones IP para dispositivos finales mediante la alternativa SLAAC, (Stateless Address Autoconfiguration) [2] en entornos de redes locales, en base a las consideraciones descriptas en los RFC 7707 “Network Reconnaissance in IPv6 Networks” [3], RFC 6105 “IPv6 Router Advertisement Guard” [4] y el RFC 7113 “Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)” [5].

Este documento se organiza de la siguiente manera: en la sección 2 se describen los aspectos generales de la alternativa SLAAC para la asignación de direcciones IPv6 a dispositivos finales. En la sección 3 se exponen las implicancias de seguridad considerando los RFCs descriptos en el párrafo anterior junto a casos prácticos de ejemplos de ataques comunes, análisis de los mismos y propuestas de contramedidas. En la sección 4 se presentan las conclusiones obtenidas, aportes y trabajos futuros.

2 Autoconfiguración de direcciones IPv6 sin estado (SLAAC)

A diferencia de la versión anterior, en IPv6 los mecanismos para la asignación de direcciones IP automática son dos, la alternativa SLAAC es mandatoria, mientras que la alternativa DHCPv6 es opcional, por lo que abordaremos el estudio centrados en la primera. Otra característica distintiva con respecto a IPv4 es que para toda interfaz de red que conecta un dispositivo a una red, se le asigna una dirección link local y una o más direcciones globales, en particular nos centraremos en las direcciones IPv6 Global Unicast, ya que ésta es generada por el dispositivo host a partir de la información de prefijo que recibe mediante mensajes Router Advertisement enviados por el Router conectado al segmento de red. Queda fuera del alcance de este documento el mecanismo para la generación del Identificador de Interface (IID) que completa la dirección IPv6 Global Unicast, el cual se describe en el RFC 7217 “A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)”, el cual se recomienda como alternativa segura. A fin de comprender el funcionamiento de SLAAC, la siguiente figura muestra en términos generales los intercambios de mensajes y protocolos intervinientes, lo que posteriormente permitirá identificar los posibles vectores de ataques en este proceso.

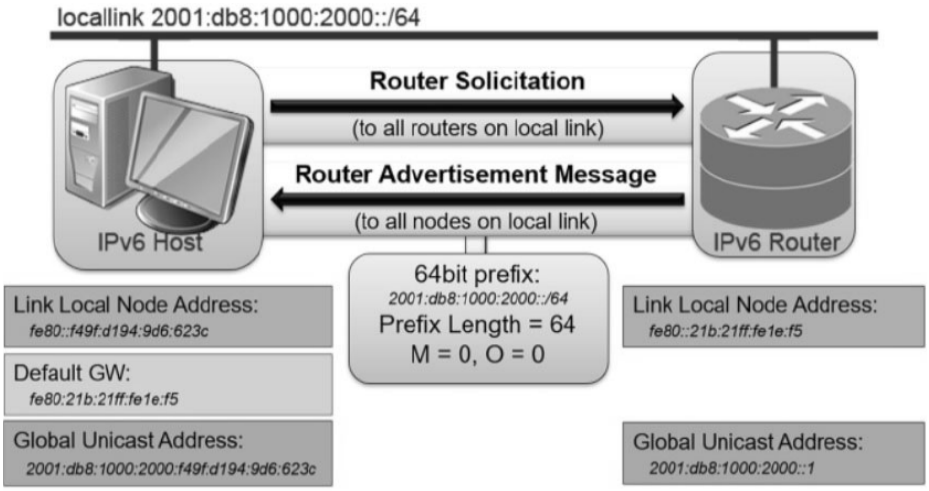

Fig. 1. Intercambio de mensajes ICMPv6 RS RA en SLAAC [6]

Cabe destacar que el proceso de generación de la dirección link local fue realizado previamente por el dispositivo host y no forma parte de SLAAC, sin embargo es necesario para su funcionamiento. Los mensajes Router Solicitation (RS) y Router Advertisement (RA) son parte del protocolo ICMPv6, el primero son enviados por los dispositivos hosts a la dirección IPv6 multicast ff02::2, (todos los routers), mientras que el mensaje RA son enviados por los routers a la dirección IPv6 multicast ff02::1, (todos los hosts), el alcance de ambos mensajes es dentro de un segmento de red local. El mensaje RA incluye el prefijo de IPv6 global y su longitud, a partir de esta información el dispositivo host puede autoconfigurar una dirección IPv6 unicast global y setea como default gateway la dirección link local del router. Para obtener un mayor detalle de la información que se incluye en estos mensajes, se puede consultar el RFC 4861 “Neighbor Discovery for IP version 6 (IPv6)”

3 Aspectos de Seguridad relacionados a SLAAC

El abordaje de los aspectos de seguridad relacionados al proceso de autoconfiguración de direcciones IPv6 sin estado tiene como punto de partida la revisión de las recomendaciones presentes en los RFCs 7707, considerando que el punto de partida al compromiso de la seguridad en una red se inicia en el escaneo de los dispositivos conectados a la misma. En el RFC referenciado se listan técnicas y herramientas utilizadas, así como un conjunto de recomendaciones para mitigar estas prácticas, básicamente se resume en el filtrado correcto de mensajes ICMPv6. Con respecto a la alternativa SLAAC, se consideraron los RFCs 6105 y 7113 donde se expone como problema principal la posibilidad del envío de mensajes RA falsos con el objetivo de realizar ataques de Hombre en el Medio y Denegación de Servicio en entornos de redes donde no se consideraron aspectos de seguridad relacionados el protocolo ICMPv6. Como contramedidas existen dos alternativas, la primera se describe en el RFC 3971 “SEcure Neighbor Discovery (SeND)”, la cual se basa en el uso de

criptografía y firma digital. La implementación de esta alternativa tiene la complejidad asociada al despliegue de una infraestructura de clave pública, generación y distribución de certificados y la implementación en los dispositivos de red, por otro lado existe escaso soporte en dichos dispositivos y puede afectar a la perfomance de la red. La segunda alternativa propone la implementación de la funcionalidad RA Guard, donde se examinan los mensajes RA para detectar y bloquear los anuncios no autorizados o maliciosos. La implementación de RA Guard puede variar según el dispositivo y el fabricante específico, puede estar integrado de manera nativa o bien ser necesario habilitar y configurarlo de manera explícita. Las técnicas utilizadas para identificar y bloquear los anuncios ilícitos, se basan en el filtrado de la fuente que envían los mensajes RA, inspección de campos opcionales ICMPv6, ya que los mismos pueden ser utilizados para evadir reglas preconfiguradas y por último, la frecuencia y los patrones de mensajes RA.

3.1 Plataforma propuesta para el análisis de seguridad en IPv6 SLAAC.

En base a la experiencia adquirida en trabajos previos, se utilizó la herramienta de software Containerlab [7] la cual permite la virtualización de entornos de redes basado en contenedores. Se configuró e implementó un escenario de red de área local IPv6 only para el análisis de seguridad en la asignación de direcciones IP mediante SLAAC [8]. La siguiente tabla muestra en detalle los dispositivos de red y hosts virtualizados.

Tabla 1. Detalle de dispositivos de red topología red Lan IPv6 SLAAC.

Dispositivo	Sistema Operativo	Direccionamiento IPv6
Switch	Nokia SRL Linux	-
Router	Nokia SRL Linux	Estático
PC1	Linux Kali distro	SLAAC
PC2	Linux Kali distro	SLAAC
PC3	Linux Alpine distro	SLAAC

Con el propósito de disponer de las herramientas necesarias para el análisis de los ataques a redes IPv6, los dispositivos PC1 y PC2 fueron configurados con las herramientas THC-IPv6 [9] e IPv6 Toolkit [10]. A continuación se describen los casos analizados:

3.2 Escenario 1: Análisis de escaneo local en redes IPv6

El primer caso analizado se basa en el análisis del comportamiento y técnicas utilizadas por las herramientas mencionadas anteriormente mediante la captura de tráfico de red. Según se describe en el RFC 7707, el ataque de escaneo local se realiza

enviando un mensaje ICMPv6 de solicitud de respuesta a la dirección multicast ff02::1, (todos los hosts) junto a una variante que enmascara esta solicitud en el campo Opciones del encabezado IPv6. Las siguientes figuras ilustran estas observaciones.

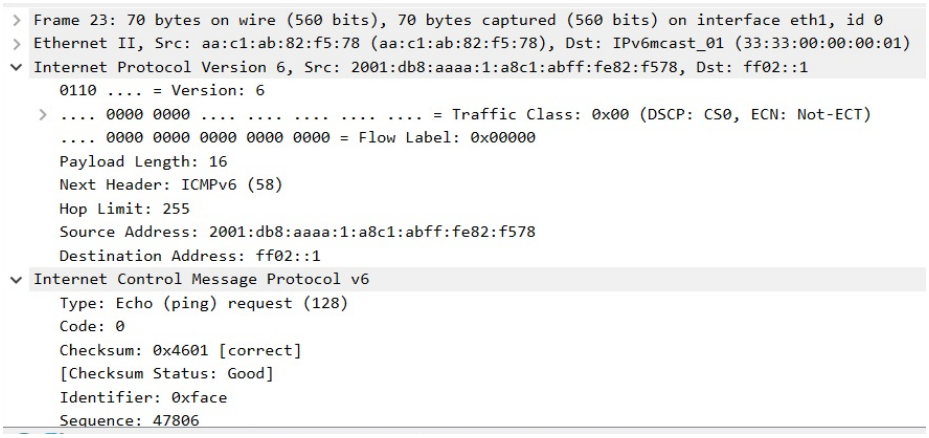

Fig. 2. Captura de tráfico de red en escaneo de una red local IPv6

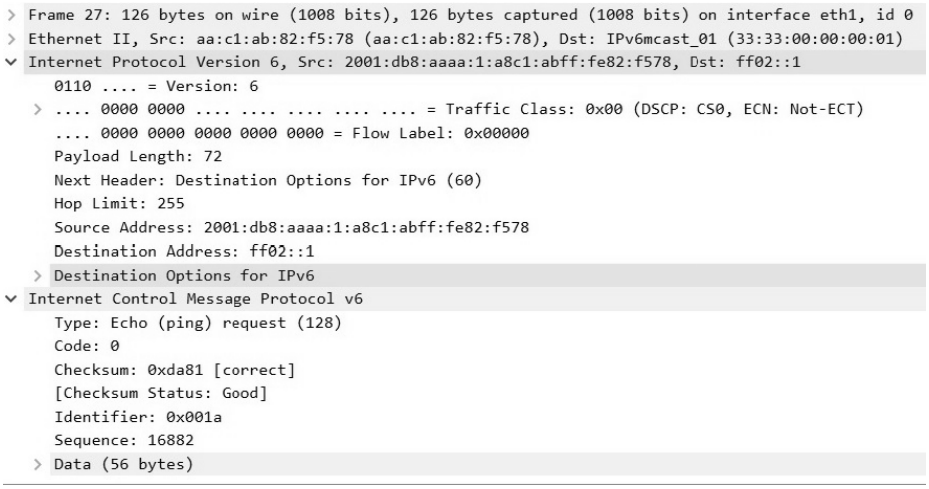

Fig. 3. Captura de tráfico de red en escaneo de una red local IPv6, (continuación)

Tabla 2. Detalle de captura ataque escaneo Figura 2.

Encabezado IPv6	Origen	Destino
Next Header ICMPv6 (58) ICMPv6 Type 128 Code 0	IPv6 addr global unicast PC1	ff02::1

Tabla 3. Detalle de captura ataque escaneo Figura 3.

Encabezado IPv6	Origen	Destino
Next Header Dest Opt for IPv6 (60) ICMPv6 Type 128 Code 0	IPv6 addr global unicast PC1	ff02::1

Teniendo en cuenta las observaciones anteriores se propone como contramedida a un ataque de escaneo la siguiente regla de filtrado:

```
acl {
        ipv6-filter ipv6ra {
            entry 60 {
                action {
                    drop {
                        log true
                    }
                }
                match {
                    next-header 60
                    destination-ip {
                        prefix ff02::/128
                    }
                }
            }
            entry 70 {
                action {
                    drop {
                        log true
                    }
                }
                match {
                    next-header icmp6
                    destination-ip {
                        prefix ff02::/128
                    }
                }
            }
```

El política de seguridad se completa aplicando la ACL anterior a las interfaces del dispositivo de capa 2 (Nokia SRL Linux).

3.3 Escenario 2: Análisis de ataque anuncios Router Advertisement falsos

Según se describe en el RFC 6105, el concepto detrás de la técnica de mitigación RA Guard se basa en el filtrado de mensajes Router Advertisement aplicado en dispositivos de red de capa 2 según diferentes criterios. El primer criterio a aplicar es descartar los mensajes RA que no provienen de puertos autorizados para tal fin. Claramente la eficiencia de aplicar esta técnica recae en la habilidad de los dispositivos de capa 2 para identificar los mensajes RA. Más allá de este requerimiento, existen técnicas de evasión basadas en la utilización de los campos de encabezado IPv6 Extension Headers.

Del mismo modo que se procedió en el Escenario 1, se analizaron alternativas de ataques mediante las herramientas THC IPv6 e IPv6 Toolkit, analizando tráfico de red capturado. A continuación se describen los casos de estudio y resultados obtenidos:

Caso 1: El atacante envía un mensaje de RA falso anunciando un prefijo de red con el propósito de que los dispositivos hosts, configuren una dirección IPv6 automática y agreguen como Gateway default la dirección IP del atacante. La siguiente figura muestra la captura de tráfico de red obtenida:

```
> Frame 4: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface eth1, id 0
> Ethernet II, Src: aa:c1:ab:3c:b6:00 (aa:c1:ab:3c:b6:00), Dst: IPv6mcast_01 (33:33:00:00:00:01)
> Internet Protocol Version 6, Src: fe80::a8c1:abff:fe3c:b600, Dst: ff02::1
v Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x19dc [correct]
    [Checksum Status: Good]
    Cur hop limit: 255
  > Flags: 0x08, Prf (Default Router Preference): High
    Router lifetime (s): 2048
    Reachable time (ms): 0
    Retrans timer (ms): 1024
  > ICMPv6 Option (MTU : 1500)
  > ICMPv6 Option (Prefix information : 2001:db8:dddd:1::/64)
  > ICMPv6 Option (Source link-layer address : aa:c1:ab:3c:b6:00)
  > ICMPv6 Option (Route Information : High ::/0)
  > ICMPv6 Option (Route Information : High 2000::/3)
  > ICMPv6 Option (Route Information : High fc00::/7)
  > ICMPv6 Option (Recursive DNS Server ff02::fb)
```

Fig. 4. Captura de tráfico de red ataque Router Advertisement Falso

Tabla 4. Detalle de captura ataque RA Figura 4.

Encabezado IPv6	Origen	Destino
ICMPv6 Type RA (134) Code 0 ICMPv6 Option Prefix: 2001:db8:dddd:1::/64 ICMPv6 Option Route info: High	IPv6 addr link local PC2	ff02::1

Analizada la técnica utilizada por el ataque, la contramedida propuesta se basa en la identificación de los mensajes RA teniendo en cuenta los campos de encabezado ICMPv6 Type 134, Code 0 y tomando como acción DROP en los puertos del dispositivo de capa 2 que conectan a dispositivos finales.

Caso 2: El atacante utiliza una variante de la técnica descripta en el Caso 1, mediante la cual se evade la comprobación del mensaje RA, insertando el mismo dentro de los campos Extension Header del encabezado IPv6. La siguiente figura muestra el resultado de la captura de tráfico y el análisis de los campos de encabezado.

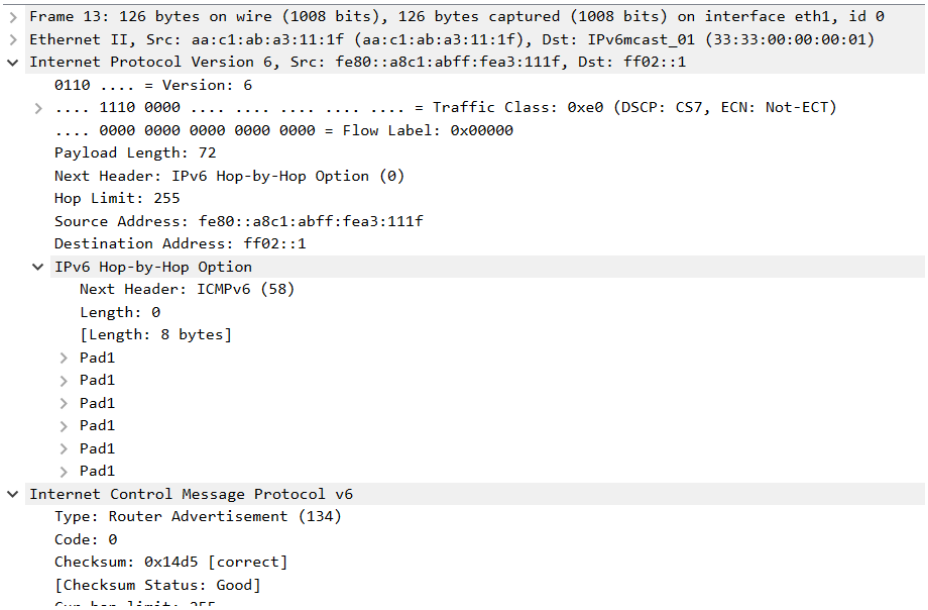

Fig. 5. Captura de tráfico de red ataque evación RA Guard.

Tabla 5. Detalle de captura ataque evasión RA Guard Figura 5.

Encabezado IPv6	Origen	Destino
Next Header IPv6 Option 0 IPv6 Hop by Hop Option Next Header ICMPv6 (58) ICMPv6 Type RA (134)	IPv6 addr link local PC2	ff02::1

Analizada la variante utilizada como ataque, la contramedida adoptada consta en una nueva regla que tiene como acción DROP de los paquetes IPv6 con campo de encabezado Next Header Option 0. Se aplica dicha regla a los puertos del dispositivo de capa 2 que conectan a dispositivos finales.

4 Conclusiones, aportes y trabajos futuros

Como aporte principal de las actividades descriptas en éste artículo, se cumplió con el objetivo de poner a disposición un entorno de prueba basado en la herramienta de virtualización de redes Containerlab, que permita fundamentalmente comprender y analizar el funcionamiento del protocolo IPv6 en el proceso de asignación de direcciones IP a dispositivos finales, con énfasis en aspectos de seguridad.

De los resultados obtenidos en el análisis de ataques comunes en el proceso de autoconfiguración automática de direcciones IPv6 (SLAAC), se proponen contramedidas mediante la implementación de reglas de filtrado aplicadas al tráfico de red. La elección del Sistema Operativo de Red Nokia SRL se fundamenta en la potencialidad que presenta para la configuración de dichas reglas a nivel de campos de encabezado IPv6, sin la necesidad del despliegue de dispositivos de seguridad adicionales. Los ejemplos de configuraciones de seguridad aplicados, se pueden extender a otros dispositivos de red que soporten la implementación de las mismas.

Como futuros trabajos se propone el análisis de otros ataques a protocolos propios de IPv6 tales como el descubrimiento de vecinos que reemplaza al protocolo ARP de IPv4, DHCPv6, entre otros, siguiendo la metodología de análisis de comportamiento de los ataques y las consideraciones en los RFCs pertinentes. Así mismo se propone realizar un análisis de perfomance en cuanto al consumo de recursos de procesamiento y memoria de los dispositivos de red, como resultado de aplicar tales reglas de filtrado.

Referencias

1. Gont, F.: Seguridad IPv6. Webinar online video. https://www.youtube.com/watch?v=wQE-yhfD9ac. (2021)
2. Thomson, F., Narten, T., Jinmei., T.: RFC 4862 IPv6 Stateless Address Autoconfiguration. https://datatracker.ietf.org/doc/html/rfc4862. (2007)
3. Gont, F., Chown, T.: RFC 7707 Network Reconnaissance in IPv6 Networks. https://datatracker.ietf.org/doc/html/rfc7707. (2016)
4. Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., Mohacsi, J.: RFC 6105 IPv6 Router Advertisement Guard. https://datatracker.ietf.org/doc/html/rfc6105. (2011)
5. Gont, F.: RFC 7113 Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard). https://datatracker.ietf.org/doc/html/rfc7113. (2014)
6. Hughes, L.: Third Generation Internet Revealed. Reinventing Computers Networks with IPv6, pp 210. Apress, Frisco, TX, USA. (2022).
7. Containerlab. https://containerlab.dev/
8. IPv6 Security Lab based in Containerlab. https://github.com/ernestosv73/ipv6seclab
9. THC-IPv6. https://www.kali.org/tools/thc-ipv6/
10. IPv6 Toolkit. https://www.si6networks.com/research/tools/ipv6toolkit/