UNIVERSIDAD/FACULTAD/CENTRO/INSTITUTO: Universidad Nacional de La Plata
OTROS TEMAS: Redes Académicas.
TÍTULO DEL TRABAJO: SEGURIDAD EN MOVILIDAD CON IPv6.
AUTOR(ES): Javier Díaz, Mauricio Demasi, Matías Robles, Germán Vodopivec
E-MAIL DE LOS AUTORES: jdiaz@unlp.edu.ar, mdemasi@cespi.unlp.edu.ar, mrobles@info.unlp.edu.ar, vodopivec@cespi.unlp.edu.ar
PALABRAS CLAVES: IPv6, movilidad, IPSec, Return Routability.

INTRODUCCIÓN

La movilidad a nivel IP permitirá que los usuarios se puedan desplazar libremente y, sin embargo, ser ubicados siempre por su misma dirección IP, además de mantener activas todas sus conexiones, por mas que el prefijo de la red a la que está conectado se modifique. Pero este proceso es vulnerable a distintos tipos de ataques que podrían imposibilitar su realización. Es necesario encontrar los métodos para eliminar, o reducir al mínimo, tales vulnerabilidades.

Este trabajo está compuesto en primer lugar de una breve explicación de IPv6, luego del protocolo de movilidad. A continuación se detallan los problemas que se encuentran en el proceso de binding y se explica como funcionan los métodos desarrollados para solucionar tales problemas. Por último, se dan las conclusiones del trabajo.

IPv6

A principios de la década del 90, los investigadores de la IETF empezaron a advertir ciertos problemas en el protocolo IPv4. Entre estos se encontraba la falta de direcciones disponibles para asignar, el crecimiento de las tablas de ruteo en los routers, etc. Además, la aparición de nuevas tecnologías evidenciaba problemas del protocolo para adaptarse a las mismas. Con el fin de solucionar estos problemas, se desarrolló el protocolo IPv6. Además de enmendar las carencias de IPv4, también se pretendió dotarlo de nuevas características.

IPv6 tiene direcciones de 128 bits contra los 32 bits de IPv4. Las direcciones se expresan con el formato *ipv6-address/prefix*, donde prefix es un número decimal que indica cuantos bits de la parte izquierda de la dirección pertenecen a la red. Las direcciones IPv6 permiten números hexadecimales y están compuestas por 8 grupos, de 4 números hexadecimales cada uno, separados por dos puntos cada grupo.

En IPv6, las direcciones se pueden configurar automáticamente, sin intervención de los usuarios finales. Para esto, se debe configurar en los routers un prefijo de red, entre otros datos. Esta información es enviada por los routers, en mensajes que se llaman Router Advertisement, a todos los nodos del enlace, a intervalos de tiempo determinados y configurables. Al recibir este anuncio, los nodos concatenan su dirección MAC, con algunas modificaciones, llamado identificador de interface, al final del prefijo enviado por el router. Si el prefijo tiene alcance a todo Internet, esta dirección también lo tendrá. Esto se conoce como autoconfiguración de direcciones. También se las puede configurar manualmente o a través de un servidor DHCPv6

Movilidad

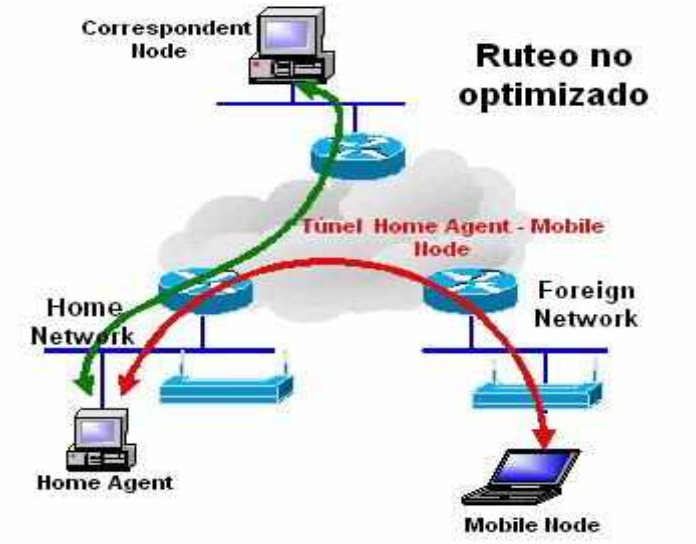
Se entiende por movilidad a la capacidad que tiene un nodo de una red para mantener la misma dirección IP, a pesar de que se desplace físicamente a otra red, y que, sin importar su ubicación en la red, puede seguir siendo accesible a través de su misma dirección IP original. Sin esta capacidad, los paquetes destinados a un mobile node, no podrían llegar a destino si dicho nodo se encuentre alejado de su enlace principal.

Para que un nodo tenga la capacidad de movilidad, debe ser habilitada en el nodo. Este nodo, que se conoce como mobile node, debe tener una dirección IP fija por dos motivos, permite que el nodo sea accesible mediante una entrada válida en el DNS y esconde la movilidad a las capas superiores. Esta dirección fija se conoce como home address.

Mientras este nodo se encuentra en su red origen, su Home Network, opera como cualquier nodo IPv6. Los paquetes enviados a ese nodo serán ruteados utilizando los mecanismos de ruteo tradicionales. Las características de movilidad se invocan cuando el nodo se desplaza a otra red. Cuando esto sucede, el nodo adquiere una nueva dirección, conocida como care-of address, con igual prefijo de red al de la red visitada (Foreign Network). Una vez configurada esta dirección, debe informársela a un nodo ubicado en su Home Network, el Home Agent. Este proceso de asociar la home address con la care-of address se conoce como binding. Para realizarlo, el mobile node envía un mensaje Binding Update(BU) a su home agent informándole de su movimiento. Este es uno de los muchos mensajes Mobile IPv6 que se codifican en una nueva cabecera de extensión de IPv6 llamada

mobility header. La finalidad del BU es informarle al home agent de la nueva dirección del mobile node. Un mensaje Binding Acknowledgement(BA) es enviado en contestación al BU.

A partir de ahora, el home agent comienza a funcionar como proxy del mobile node. Cualquier paquete enviado a la home address del mobile node será recibido por su home agent. Este reenviará los paquetes, formando un túnel, a la care-of address del mobile node. Este túnel es bidireccional. Esto es, cuando el mobile node envía un paquete, primero lo manda, utilizando el túnel, al home agent quien lo desencapsula, obteniendo el mensaje original, y lo reenvía hacia su destino final. Esto se conoce ruteo triangular. El siguiente gráfico muestra este tipo de ruteo.



Movilidad con ruteo no optimizado

Todo el tráfico entre el mobile node y el correspondent node debe pasar por el home agent, lo cual lo convierte en un cuello de botella y en un punto central de falla. Si el home agent falla, todas las conexiones se pierden. Este tipo de ruteo debería evitarse porque es ineficiente. Para esto, el mobile node debe registrar su ubicación actual al correspondent node (además de registrarse con el home agent) enviándole un BU. A partir de ahora, el tráfico entre estos dos nodos se enviará directamente, sin pasar por el home agent. Los paquetes enviados por el correspondent node tendrán la care-of address en su dirección destino. Esto proceso se conoce como Route Optimization.

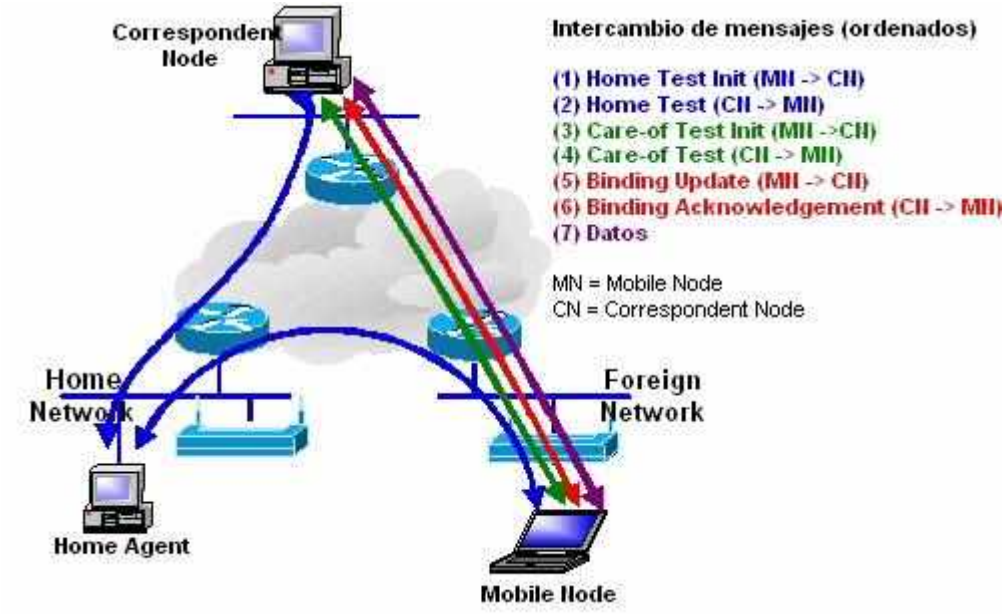
Problemas de Seguridad en Mobile IPv6

El primer problema de seguridad se encuentra en el momento en el que el mobile node registra su movimiento con su home agent (home registration). Por ejemplo, un atacante podría enviar un Binding Update al Home Agent indicándole una care-of address falsa, indicándole que el mobile node está en una ubicación distinta de la cual está. El túnel entre el home agent y el mobile node sería incorrecto. Con el fin de evitar cualquier tipo de ataque, los dos nodos deben definir una asociación de seguridad, usando IPSec, para proteger la autenticidad e integridad de los mensajes intercambiados en el proceso (Binding Update y Binding Acknowledgement).

El segundo problema se presenta en el proceso de Route Optimization. Si los Bindings Updates no son autentificados, el nodo correspondiente puede ser utilizado como cómplice involuntario del ataque. Por ejemplo, un nodo podría enviarle un Binding Update al correspondent node indicándole una nueva care-of address para una home address determinada. Esto haría que todo el tráfico sea redirigido hacia esta nueva dirección. La care-of address elegida por el atacante podría ser su propia dirección IP, o cualquiera que él desee.

Para prevenir o mitigar las amenazas de seguridad del proceso de Route Optimization, se integró con el protocolo un mecanismo básico de seguridad llamado Return Routability (RR). No elimina todas las amenazas, pero limita los posibles atacantes a aquellos que son capaces de monitorear el path entre el home agent y el correspondent node. Permite que éste último tenga una seguridad razonable de que el mobile node es direccionable, tanto en su home address como en su care-of address. Unicamente después que este procedimiento tuvo éxito, el correspondent node procesa el Binding Update y realiza la optimización del ruteo.

El mecanismo básico del Return Routability consiste de dos chequeos diferentes, el de la home address y de la care-of address. Para el primero, el mobile node envía un mensaje Home Test Init (HoTI), a través del home agent, al correspondent node, quien le contesta con un mensaje Home Test (HoT), también por medio del home agent. Para el segundo, el mobile node envía un mensaje Care-of Init Test (CoIT) directamente al correspondent node, quien le contesta con un Care-of Test (CoT). Una vez que el mobile node ha recibido las dos contestaciones le envía el Binding Update al correspondent node.

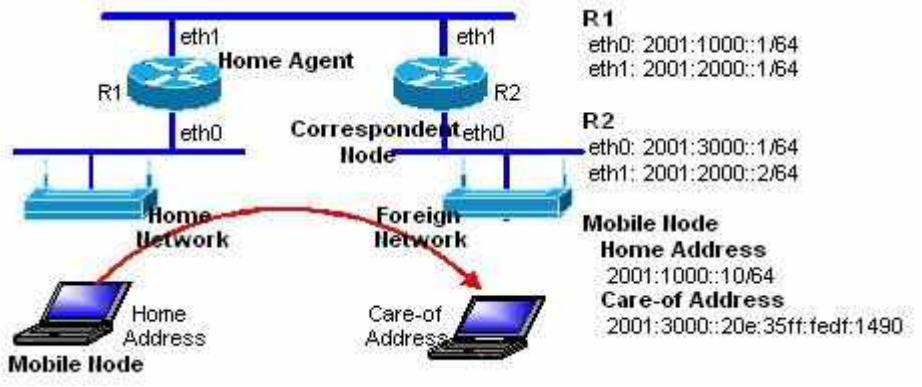


Ruteo optimizado con Return Routability

Implementación de las soluciones

Para solucionar el primer problema se debe utilizar IPSec. Este es un protocolo de seguridad de la capa de red, que debe se incluye en toda implementación de IPv6. Mobile IPv6 lo utiliza para proteger los mensajes del protocolo que el home agent y el mobile node intercambian entre sí. Para lograr esto, es necesario que ambos nodos se pongan de acuerdo en aspectos tales como el algoritmo usado para encriptar y/o autentificar, claves, etc.

Las pruebas se realizaron usando dos PC Routers con Linux 2.6.15 y, una notebook con el mismo sistema operativo. Linux no trae la movilidad incorporada en el kernel, se debe instalar una implementación, de la Universidad de Helsinki, conocida como Proyecto MIPL. Esta consta de dos partes, una que es un parche para el kernel y otra son las aplicaciones del usuario. La funcionalidad de IPSec viene incorporada en el kernel. El siguiente gráfico muestra la configuración de la red de prueba.



Red de prueba en el LINTI - UNLP

A continuación se muestran dos mensajes Binding Update, el primero sin encriptar y el segundo encriptado (algunos campos se han eliminado por simplicidad):

Internet Protocol Version 6
Source address: 2001:3000::20e:35ff:fedf:1490
Destination address: 2001:1000::1
Destination Option Header
Next header: Mobile IPv6 (0x87)
Option Type: 201 (0xc9) - Home Address Option
Home Address : 2001:1000::10 (2001:1000::10)
Mobile IPv6
Mobility Header Type: Binding Update (5)
Binding Update
1... .... = Acknowledge (A) flag: Binding Acknowledgement requested
.1.. .... = Home Registration (H) flag: Home Registration
..0. .... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility
...0 .... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
Lifetime: 74 (296 seconds)
Mobility Options
Alternate care-of address: 2001:3000::20e:35ff:fedf:1490 (2001:3000::20e:35ff:fedf:1490)

Binding Update sin encriptar

Internet Protocol Version 6
Source address: 2001:3000::20e:35ff:fedf:1490
Destination address: 2001:1000::1
Destination Option Header
Next header: ESP (0x32)
Option Type: 201 (0xc9) - Home Address Option
Home Address : 2001:1000::10 (2001:1000::10)
Encapsulating Security Payload
SPI: 0x000007d0
Sequence: 7
Data (60 bytes)

Binding Update encriptado

En este último mensaje toda la información transportada en la cabecera de Mobile IPv6 está encriptada. Además, el paquete está autentificado lo que detectaría cualquier modificación involuntaria o no sobre los datos del mismo.

Return Routability

A continuación se muestran los mensajes intercambiados en un proceso de Return Routability, con los cookies y tokens intercambiados entre ámbos nodos. El primer mensaje es del tipo Home Test Init (HoTI), que es enviado desde el mobile node al correspondent node, a través del home agent. Le envía su Home Init Cookie, un valor aleatorio de 64 bits. Este cookie se usa para verificar que el mensaje Home Test coincide con el Home Test Init.

Internet Protocol Version 6
Source address: 2001:3000::20e:35ff:fedf:1490
Destination address: 2001:1000::1
Internet Protocol Version 6
Source address: 2001:1000::10
Destination address: 2001:3000::1
Mobile IPv6
Mobility Header Type: Home Test Init (1)
Home Test Init
Home Init Cookie: 0x8d7123ab72588572

A través del home agent, el correspondent node le contesta al mobile node enviándole un mensaje Home Test (HoT). El valor del cookie es igual al enviado en el Home Test Init. Además, envía su home keygen token, que es un valor de 64 bits.

Internet Protocol Version 6
Source address: 2001:1000::1
Destination address: 2001:3000::20e:35ff:fedf:1490
Internet Protocol Version 6
Source address: 2001:3000::1
Destination address: 2001:1000::10
Mobile IPv6
Mobility Header Type: Home Test (3)
Home Test
Home Nonce Index: 1
Home Init Cookie: 0x8d7123ab72588572
Home Keygen Token: 0x6c1e23a3ddc0f2e0

Además del Home Test Init, el mobile node le envía un mensaje Care-of Test Init al correspondent node, pero lo hace directamente, no a través del home agent. El único dato que envía es el Care-of Init Cookie, que es un valor de 64 bits, y cumple la misma función que el Home Init Cookie en los mensajes Home Test.

Internet Protocol Version 6
Source address: 2001:3000::20e:35ff:fedf:1490
Destination address: 2001:3000::1
Mobile IPv6
Mobility Header Type: Care-of Test Init (2)
Care-of Test Init
Care-of Init Cookie: 0x505158eeef3ac99b

El correspondent node le contesta, directamente, al mobile node enviándole un mensaje Care-of Test. Además de reenviarle el Care-of Init Cookie, le envía un Care-of Keygen Token, que también es un valor de 64 bits.

Internet Protocol Version 6
Source address: 2001:3000::1
Destination address: 2001:3000::20e:35ff:fedf:1490
Mobile IPv6
Mobility Header Type: Care-of Test (4)
Care-of Test
Care-of Nonce Index: 1
Care-of Init Cookie: 0x505158eeef3ac99b
Home Keygen Token: 0x4c955e8da5e31cd7

Con el fin de aumentar la seguridad, es recomendable que los mensajes Home Test Init y Home Test sean protegidos usando IPSec en la parte que la conexión es entre el mobile node y el home agent.

Utilizando los tokens recibidos, el mobile node genera la Binding Managment Key ejecutando una función hash a la concatenación de dichos tokens. Esta clave es usada para proteger el Binding Update enviado al correspondent node. Aunque cualquier nodo puede recibir los tokens y generar la clave, los mensaje Home Test y Care-of Test son enviados por distintas rutas hacia el mobile node, además el Home Test es encriptado entre el home agent y el mobile node. Un atacante debería tener acceso a ambas rutas para poder obtener los dos tokens. El siguiente es un mensaje Binding Update después que el RR se ejecutó con éxito.

Internet Protocol Version 6
Source address: 2001:1000::10
Destination address: 2001:3000::1
Destination Option Header
Next header: Mobile IPv6 (0x87)
Option Type: 201 (0xc9) - Home Address Option
Home Address : 2001:3000::20e:35ff:fedf:1490
Mobile IPv6
Mobility Header Type: Binding Update (5)
Binding Update
1... .... = Acknowledge (A) flag: Binding Acknowledgement requested
.0.. .... = Home Registration (H) flag: No Home Registration
..0. .... = Link-Local Compatibility (L) flag: No Link-Local Address Compatibility
...0 .... = Key Management Compatibility (K) flag: No Key Management Mobility Compatibility
Lifetime: 64 (256 seconds)
Mobility Options
Nonce Indices
Home nonce index: 1
Care-of nonce index: 1
Binding Authorization Data
Authenticator: 9729318DC6F719D4480C4D82

Este Binding Update es diferente al mostrado mas arriba. En la opción Mobility Options lleva valores que utiliza el correspondent node para comprobar la validez del mensaje.

CONCLUSIONES

El proceso de registración de un mobile nodo con su home agent, o con el correspondent node, es simple y rápido, sin embargo, puede ser blanco de distintos tipos de ataques que comprometan dicho proceso. En primer lugar, el uso de IPSec para proteger todo el intercambio de mensajes de Mobile IPv6 entre el mobile node y su home agent es altamente recomendable. En cambio, el proceso Return Routability es obligatorio pero depende de que el correspondent node tenga la capacidad de movilidad habilitada. RR no es un protocolo criptográfico tradicional pero sirve para evitar la mayoría de los ataques.

REFERENCIAS

Kent, S. y R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Noviembre 1998.

Kent, S. y R. Atkinson, "IP Authentication Header", RFC 2402, Noviembre 1998.

Kent, S. y R. Atkinson, "IP Encapsulating Security Payload", RFC 2406, Noviembre 1998

Deering, S. y R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Diciembre 1998.

Narten, T., Nordmark, E. y W. Simpson, "Neighbor Discovery for IP Version 6", RFC 2461, Diciembre 1998.

Thomson, S. Y T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Diciembre 1998.

Conta, A. y S. Deering, "Internet Control Message Protocol (ICMPv6) for IPv6 Specification", RFC 2463, Diciembre 1998.

Hinden, R. and S. Deering, "Internet Protocol Version 6 Addressing Architecture", RFC 3513, Abril 2003

D. Johnson , C. Perkins y J. Arkko – “Mobility support in IPv6”, RFC 3775, Junio 2004

Arkko, J., Devarapalli, V. y F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, Junio 2004.

IEEE 802.11 – Wireless LAN Médium Access Control (MAC) and Physical Layer Specifications

MIPL Mobile IPv6 for Linux - http://www.mobile-ipv6.org/

Lars Mars - Linux Mobile IPv6 HOWTO - Abril 2004

Dr. Dimitrios Kalogeras – Introduction to Mobile IPv6, Noviembre 2004

Cisco Systems – Mobile IPv6 overview, Diciembre 2004