

INSTITUTO TECNOLÓGICO SUPERIOR DE EL MANTE



Línea de Investigación: Seguridad en Protocolos de Internet

Tema: Propuesta de Seguridad para el protocolo BGP

por

M.C. José Paulino Ramírez Juárez
Ing. Miguel Ángel García Morales
M.D. Sergio Arana Tirado

Cd. Mante, Tamaulipas, Septiembre de 2014

Índice

1. Introducción	1
2. Definición del Problema	2
3. Objetivos	2
4. Hipótesis	2
5. Marco Teórico (Antecedentes)	2
5.1. BGP (Border Gateway Protocol)	2
5.2. Atributos BGP	3
5.3. Atributo WEIGHT	3
5.4. Atributo LOCAL PREFERENCE	4
5.5. Atributo MULTI-EXIT DISCRIMINATOR	4
5.6. Atributo ORIGIN	4
5.7. Atributo ASPATH	5
5.8. Atributo NEXT-HOP	6
6. Attack Tree	6
7. Ataques al protocolo BGP	7
7.1. Man In The Middle	7
7.2. Blackhole	7
8. Metodología	8
8.1. Recolección de Datos	8
8.2. Análisis de la Información	8
8.3. Modelado	9
8.4. Creación de Estrategias	9
8.5. Pruebas	9
8.6. Resultados	9
9. Referencias	10

Índice de figuras

5.1. Atributo Weight	3
5.2. Atributo Local Preference	4
5.3. Atributo Multi-Exit Discriminator	5
5.4. Atributo AS-Path	5
5.5. Atributo Next-Hop	6
7.6. Ataque Man In The Middle	7
7.7. Ataque Black Hole	8

Resumen

En el Ruteo Interdominio existe una gran variedad de ataques al protocolo BGP, lo cual ha llevado a plantear varias propuestas de seguridad a través de organismos centralizados a nivel global. En esta investigación se plantearán estrategias de seguridad analizando como se llevan a cabo los ataques a BGP por medio de la técnica de análisis llamada attack tree (árbol de ataque) y se pretende asegurar al protocolo a través de técnicas de verificación de ruta. Se cuantificará su desempeño por medio de pruebas entre portavoces BGP. Se espera que con esta nueva medida se obtengan resultados favorables.

1. Introducción

El protocolo BGP (Border Gateway Protocol)[2] es un protocolo de ruteo entre ASes (Sistemas Autónomos) mediante el cual se intercambian prefijos de los ISP (Internet Service Provider). Un sistema autónomo es un conjunto de routers que se encuentran bajo una misma administración y tienen las mismas políticas de ruteo.

BGP es usado para intercambiar información de ruteo para la internet y es el protocolo usado entre los ISPs. Clientes de redes tales como universidades y corporaciones, usualmente utilizan un IGP (Interior Gateway Protocol) tales como RIP o OSPF para el intercambio de información de ruteo con sus redes de trabajo. Los clientes se conectan a los ISPs y los ISPs usan BGP para intercambiar rutas entre clientes e ISPs. Cuando BGP es usado entre sistemas autónomos el protocolo es referido como External BGP (eBGP). Si un ISP está usando BGP para intercambiar rutas con un AS entonces el protocolo es referido como Interior BGP (iBGP).

El protocolo BGP es vulnerable a numerosos ataques los cuales se llevan a cabo proporcionando información falsa en las tablas de ruteo. Entre estos ataques se incluyen los mensajes falsos de OPEN, KEEPALIVE, NOTIFICATION y UPDATE. Estos mensajes falsos pueden generar problemas grandes tales como negación de servicios, que ASes sean inalcanzables y que un router suplante a otro y con esto puede desviar información, modificarla o eliminarla.

Es importante la seguridad en BGP ya que esta es crítica para la operación adecuada entre redes públicas y privadas y mantiene la infraestructura de ruteo en internet y es a través de este protocolo que se puede tener acceso a todo el mundo.

Actualmente existen varias propuestas para minimizar estos ataques. S-BGP, soBGP y psBGP[4]. Las cuales se basan en la implementación de llaves públicas y certificados de autenticidad pero no están basados en un análisis mediante verificación de ruta y solo se enfocan a resolver los problemas creados mediante los mensajes de UPDATE falsos.

Lo que se propone, es analizar los cuatro mensajes de BGP mediante attack tree y en base a ello proponer una estrategia de seguridad y cuantificar el desempeño de esta nueva medida. Se espera disminuir las probabilidades de éxito de estos ataques.

Existen ataques específicos que pueden ser ejecutados a través de los siguientes mensajes:

- OPEN
- KEEPALIVE
- NOTIFICATION
- UPDATE

BGP corre encima de TCP y por lo tanto es vulnerable a:

TCP SYN (SYN Flooding)

TCP SYN ACK

TCP ACK

TCP RST/FIN/FIN/FIN-ACK

BGP no tiene mecanismos internos que: garanticen la integridad y autenticidad de los routers y de los mensajes recibidos validen la autoridad de un AS para anunciar informaciones del NLRI aseguren la autenticidad y validez los atributos de camino de un AS.

Las estrategias de seguridad propuestas consisten en algoritmos que aplicados al protocolo BGP se puede dotar de seguridad.

Existen 3 propuestas principales. Cada una posee un método particular aunque son muy parecidos y las tres se enfocan solo en los ataques realizados por medio de los mensajes falsos de UPDATE y no involucra manipulación directa de BGP ni información contenida con BGP.

La propuesta más fuerte hasta ahora es S-BGP(Secure BGP)[5].

2. Definición del Problema

El protocolo BGP es vulnerable a ataques mediante el uso de mensajes de OPEN, KEEPALIVE, NOTIFICATION y UPDATE falsos. Por medio de estos mensajes falsos se puede irrumpir en las comunicaciones entre routers y se puede llegar a cometer violaciones de seguridad en los ASes tales como:

- Acceso no autorizado a los recursos y/o información.
- Revelación involuntaria/no autorizada de información.
- Negación de Servicios.

Actualmente solo existen propuestas para evitar los ataques a BGP mediante organismos centralizados que verifican la autenticidad de los sistemas autónomos involucrados en el recorrido del mensaje, mas no así para verificar si la ruta seguida es la real.

3. Objetivos

Realizar una propuesta de seguridad para el protocolo BGP mediante verificación de ruta entre sistemas autónomos y así prevenir ataques mediante mensajes con información de rutas falsas.

4. Hipótesis

La nueva propuesta de seguridad para el protocolo BGP pretende en incluir un nuevo mecanismo, el cual comprobará si la ruta recibida por medio de un mensaje de BGP existe dentro de la topología de red y si ese mensaje viajó por la trayectoria contenida en él.

5. Marco Teórico (Antecedentes)

5.1. BGP (Border Gateway Protocol)

BGP es un protocolo de ruteo muy robusto [3], evidenciado por el hecho de que BGP es el protocolo de ruteo empleado sobre la Internet. En el momento de esta escritura, en la Internet, BGP ha enviado más de 90,000 rutas. Para alcanzar la adaptabilidad en este nivel, BGP usa muchos parámetros de ruta llamados atributos para definir la política de ruteo y mantener un ambiente de ruteo estable.

Además BGP atribuye en el interdominio sin clases que encamina (CIDR) que es usado por BGP para reducir el tamaño de las tablas de ruteo de la Internet. Por ejemplo, asuma que un ISP posee el bloque de dirección de IP 195.10.x.x de la Clase tradicional C que dirige el espacio. Este bloque consiste en 256 bloques Clase C de dirección, 195.10.0.x por 195.10.255.x. Asuma que el ISP asigna un bloque Clase C a cada uno de sus clientes. Sin CIDR, EL ISP anunciaría 256 bloques Clase C de dirección a sus pares de BGP. CON CIDR, BGP puede poner en la red el espacio de dirección y anunciar un bloque, 195.10.x.x. Este bloque es

del mismo tamaño que un bloque de dirección Clase B tradicional. Las distinciones son dadas por CIDR, permitiendo a una reducción significativa del ruteo en BGP.

Los vecinos BGP cambian la información de ruteo cuando la conexión TCP entre vecinos primero es establecida. Cuando los cambios a la tabla de ruteo son descubiertos, los routers BGP envían a sus vecinos sólo aquellas rutas que se han cambiado. Routers BGP no envían actualizaciones de ruta periódicas, y las actualizaciones BGP que encaminan, anuncian sólo el camino óptimo a una red de destino.

5.2. Atributos BGP

Las rutas aprendidas vía BGP han asociado las propiedades que son usadas para determinar la mejor ruta a un destino cuando múltiples caminos existen a un destino particular. Estas propiedades se mencionan como BGP atributos, y entender como estos atributos influyen en la selección de ruta es necesario para diseñar redes robustas. A continuación se describen los siguientes atributos.

- Weight
- Local preference
- Multi-exit discriminator
- Origin
- ASpath
- Next hop

5.3. Atributo WEIGHT

El peso es un atributo que Cisco ha definido como un atributo local de un Router. El atributo de peso no es anunciado a routers vecinos. Si el router aprende más que una ruta al mismo destino, la ruta con el peso más alto será preferida. En la Figura 5.1, el router recibe un anuncio para la red 172.16.1.0 de los routers B y C. Cuando el router un recibe el anuncio del router B, el peso asociado es puesto a 50. Cuando el router un recibe el anuncio del router C, el peso asociado es puesto a 100. Ambos caminos para la red 172.16.1.0 estarán en la tabla de ruteo BGP, con sus pesos respectivos. La ruta con el peso más alto será instalada en el IP de la tabla del router.

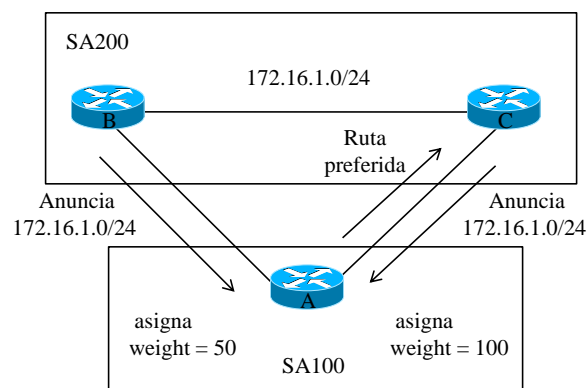


Figura 5.1: Atributo Weight

5.4. Atributo LOCAL PREFERENCE

El atributo local de preferencia es usado preferir un punto de salida del sistema local autónomo.

A diferencia del atributo de peso, el atributo local de preferencia es propagado en todas partes del AS local. Si hay múltiples puntos de salida del AS, el atributo local de preferencia es usado para seleccionar el punto de salida para una ruta específica. En la Figura 5.2, AS 100 recibe dos anuncios para la red 172.16.1.0 de AS 200. Cuando el router A recibe el anuncio para la red 172.16.1.0, la preferencia correspondiente local es puesta a 50. Cuando el router B recibe el anuncio para la red 172.16.1.0, la preferencia correspondiente local es puesta a 100. Estos valores locales de preferencia serán cambiados entre routers A y B. Como el router B tiene una preferencia más alta local que el router A, la del router B será usado como el punto de salida de AS 100 para alcanzar la red 172.16.1.0 en AS 200.

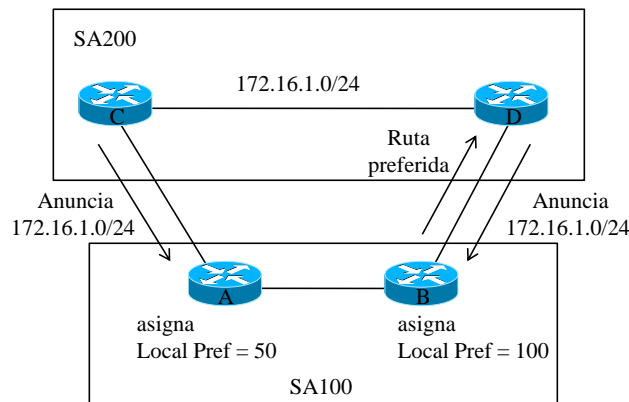


Figura 5.2: Atributo Local Preference

5.5. Atributo MULTI-EXIT DISCRIMINATOR

El discriminador multisalida (MED) o el atributo métrico es usado como una sugerencia a un AS externo, en cuanto a la ruta preferida en el AS esto hace anuncios a el métrico. El término sugerencia es usado porque el AS externo que recibe el MED puede usar otros atributos de BGP para la selección de ruta. En la Figura 5.3, el router C anuncia la ruta 172.16.1.0 con un métrico de 10, mientras la ruta D anuncia 172.16.1.0 con un métrico de 5. El valor inferior de los métricos es el preferido, para 100 seleccionará la ruta al router D para la red 172.16.1.0 en AS 200. MEDs son anunciados en todas partes del AS local.

5.6. Atributo ORIGIN

El atributo de origen indica como BGP ha aprendido una ruta particular. El atributo de origen puede tener uno de tres valores posibles:

IGP la ruta es interior al AS de origen. Este valor es puesto cuando la orden de configuración del router de red es usado para inyectar la ruta en BGP.

EGP la ruta es aprendida vía el Protocolo de Entrada de Frontera Exterior (EBGP).

Incompleto. El origen de la ruta es desconocido o aprendido de algún otro modo. Un origen incompleto ocurre cuando una ruta es redistribuida en BGP.

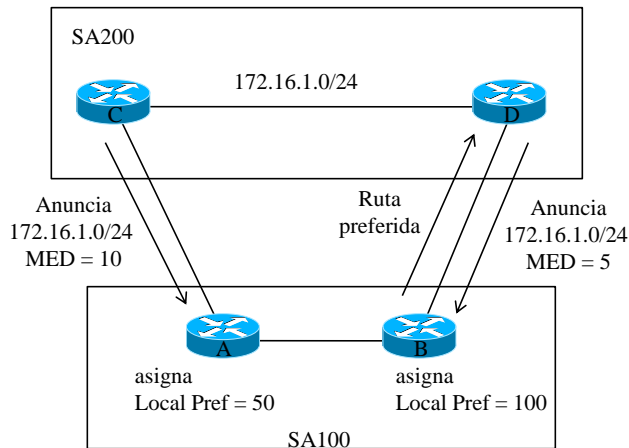


Figura 5.3: Atributo Multi-Exit Discriminator

5.7. Atributo ASPATH

Cuando un anuncio de ruta pasa por un sistema autónomo, el numero del AS es añadido a una lista ordenada de números AS que el anuncio de ruta ha atravesado. La figura 5.4 muestra la situación en la cual una ruta pasa por tres sistemas autónomos.

AS1 origina la ruta a 172.16.1.0 y anuncia esta ruta a AS2 Y AS3, con el atributo de ASPATH igual a 1. AS3 hará anuncios atrás a AS1 con el atributo de ASPATH 3,1, y AS2 hará anuncios atrás a AS1 con el atributo de ASPATH 2,1. AS1 rechazará estas rutas cuando su propio número AS sea descubierto en el anuncio de ruta. Este es el mecanismo que BGP suele utilizar para descubrir lazos en las rutas. AS2 Y AS3 propagan la ruta el uno al otro con sus números AS añadidos al atributo de ASPATH. Estas rutas no serán instaladas en el IP de la tabla del router porque AS2 Y AS3 aprenden una ruta a 172.16.1.0 de AS1 con una lista de ASPATH más corta.

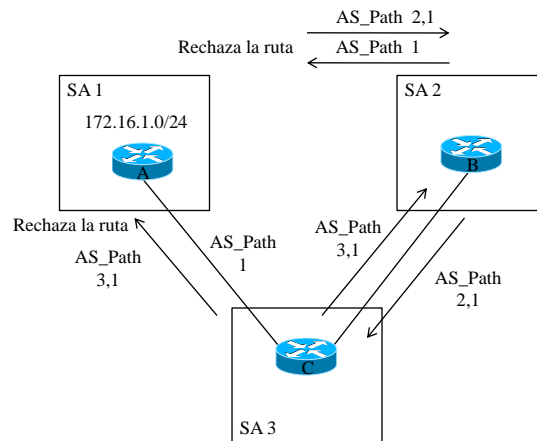


Figura 5.4: Atributo AS-Path

5.8. Atributo NEXT-HOP

El atributo de next-hop EBGP es la dirección de IP que es usada para alcanzar el router anunciado. Ya que EBGP mira detenidamente, la dirección de salto siguiente es la dirección de IP de la conexión entre los pares. Para IBGP, la dirección de salto siguiente EBGP es llevada en el AS local, como se ilustra en la Figura 5.5.

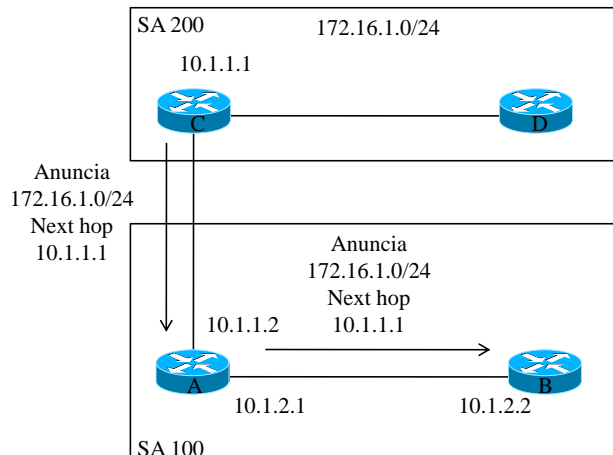


Figura 5.5: Atributo Next-Hop

El router C anuncia la red 172.16.1.0 con un siguiente salto de 10.1.1.1. Cuando el router A propaga esta ruta dentro de su propio AS, la información de salto siguiente EBGP es conservada. Si el router B no tiene la información de encaminamiento en cuanto al siguiente salto, la ruta será desechada. Por lo tanto, es importante tener un IGP corriendo para propagar el salto siguiente que encamina la información.

6. Attack Tree

Los árboles de ataque categorizan sistemáticamente las diferentes maneras en las cuales un sistema puede ser atacado.

Un árbol de ataque es un árbol en el cual los nodos representan ataques. El nodo raíz del árbol es la meta global de el atacante. Los hijos de un nodo son refinamientos de esta meta y las hojas por consiguiente representan ataques, que no pueden ser refinados. Un refinamiento puede ser conjuntivo (agregación) o disjuntivo (opción).

Una vez construido un árbol (modelado en attack tree) el árbol puede ser usado para analizar atributos de la seguridad del sistema. Por ejemplo: Posibilidad, imposibilidad, costo, y si se requieren herramientas especiales.

El análisis procede en dos pasos: primero el valor de cada hoja de nodo es determinado. Segundo, los valores en los nodos sin hojas es sintetizado de el valor de sus hijos. Así, la creatividad sobre la parte de el análisis es solamente necesitada en entender bien los valores de los nodos hojas, como las reglas de síntesis en ambos, los conjuntivos y disjuntivos casos, es usualmente determinado por la naturaleza de el atributo.

El resultado de un análisis puede ser el valor de un atributo en el nodo raíz (por ejemplo, el costo de el ataque más barato), pero esto podría también ser un sub-árbol consistente de nodos adheridos a algunos predicados, por ejemplo, el costo de esos ataques es menos que 100K euros o esos ataques que no requieren de un equipo especial.

También valores de diferentes atributos (calidades) pueden ser definidos. Por ejemplo: para determinar el ataque más barato no usando equipo especial.

7. Ataques al protocolo BGP

BGP y otros protocolos han recibido atención crítica tanto como la conciencia en toda la internet en cuanto a seguridad se refiere se ha incrementado. A continuación se presentan dos ataques muy comunes al protocolo por medio de la herramienta de árboles de ataque.

En los árboles de ataque se presentan los operadores “OR” y “AND”. El operador “OR” especifica que solo se requiere una acción para llevar a cabo el proceso del nodo. En cambio el operador “AND” nos indica que se deben cumplir todas las acciones, y este operador se representa por medio de una ligadura. El operador “OR” no lleva ninguna liga[6].

7.1. Man In The Middle

El ataque man in the middle permite a un adversario apoderarse efectivamente de una comunicación entre dos partes permitiendo que cualquier dato sea leído o alterado. Aunque no es imposible conducirlo después de que una sesión ha sido establecida, el ataque puede lograrse más fácil antes del inicio de sesión[6].

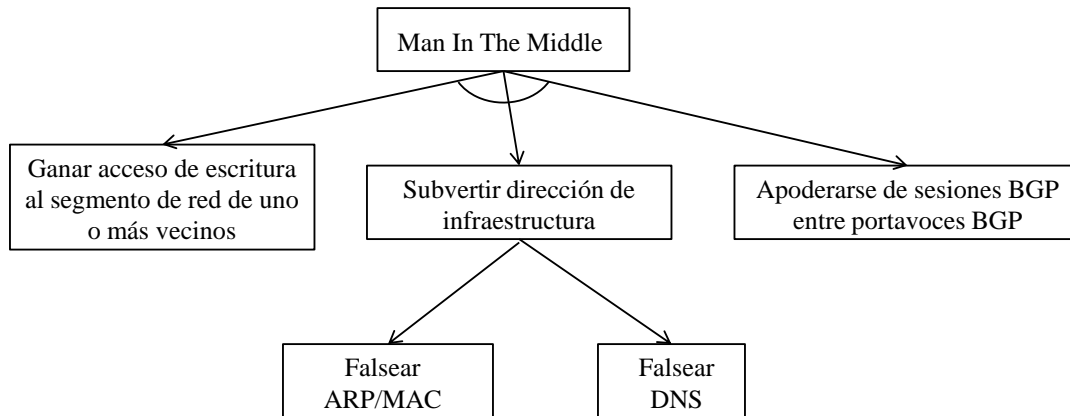


Figura 7.6: Ataque Man In The Middle

7.2. Blackhole

BGP puede ser usado para hacer tráfico Blackhole. Si un adversario ha accedido al forwarding path del sistema objetivo, el puede completamente descartar o arrojar el tráfico mientras continua funcionando como un portavoz BGP. El adversario también puede afectar las tablas BGP de sus vecinos usando anuncios BGP de tal manera que estos podrían enviar tráfico al destino incorrecto. Una manera de que esto pueda ser llevado a cabo es a través de la originación de un prefijo no autorizado[6].

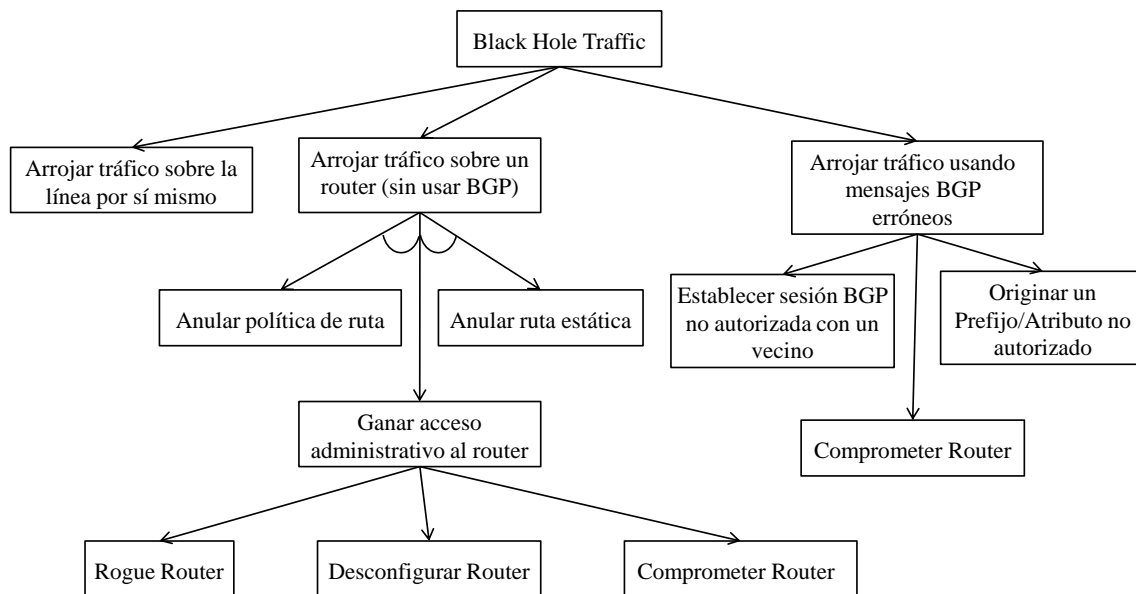


Figura 7.7: Ataque Black Hole

8. Metodología

El tipo de investigación que se llevará a cabo es el del tipo no experimental. Tal es el caso de desarrollar una nueva estrategia de seguridad y nuevos mecanismos al protocolo BGP para sus mensajes de comunicación, y a través de una simulación verificar la ruta de los mensajes enviados y recibidos.

Los primeros pasos de esta investigación son analizar el funcionamiento de mensajes BGP en una simulación, tal y como lo hacen en la realidad. Observar cómo funcionan normalmente y después introducir los ataques más comunes y esperados.

Observar en la simulación que existe un desvío de información, y que los paquetes enviados no llegan a su destino final.

Comprobar que mediante los nuevos mecanismos diseñados con verificación de ruta, se evitan estos mensajes con información falsa, y que los portavoces BGP rechazan la información maliciosa.

8.1. Recolección de Datos

La información es obtenida durante la simulación del protocolo BGP. Cuando el protocolo funciona normalmente, los datos son tomados desde que se realiza el envío de paquetes con los mensajes BGP, verificando que la ruta seguida es la indicada dentro de los parámetros y con las métricas descritas por las tablas de ruteo. Cuando un ataque es introducido se vuelven a tomar los datos proporcionados por las tablas de ruteo

8.2. Análisis de la Información

Tomando en cuenta la información obtenida durante la simulación, se analiza cuáles son los cambios que surgen durante los ataques al protocolo BGP, tales como cambios en las rutas establecidas por los ruteadores, los cambios en los atributos y cabeceras de los mensajes BGP y como cambia el flujo de la información en la topología de red. Todo esto con el fin de proponer una estrategia de seguridad.

8.3. Modelado

La simulación se lleva a cabo mediante programas tales como simulink, matlab o C-BGP. No se toman consideraciones especiales en el diseño de la topología de red, solo lo previsto por las características de los ruteadores, tales como sistema operativo, comandos y funciones utilizadas. En cuanto al protocolo BGP, las rutas y sus atributos son los predefinidos y no se añaden otras funciones.

8.4. Creación de Estrategias

Se analizan y determinan las posibles estrategias de solución, tales como la verificación de la ruta seguida por los mensajes a través de la topología de red. También se explora la posibilidad de crear nuevos mecanismos de operación del protocolo, como puede ser la introducción de un nuevo tipo de mensaje o sistemas basados en llaves públicas para autenticar la información enviada en ellos y de esta manera evitar ataques y eliminar los puntos de debilidad en los mensajes de BGP.

8.5. Pruebas

Las pruebas de desempeño de las estrategias propuestas se llevan a cabo en el simulador. Primero se simula BGP en una topología en la cual no está presente el mecanismo de seguridad, es decir, de la manera en que opera actualmente el protocolo. Después se introduce un router adicional, el cual envía a sus vecinos mensajes con información de rutas falsas con el propósito de cambiar sus tablas de ruteo. Después se confirma que los routers cambiaron sus tablas de ruteo por las enviadas por el router atacante. Una vez comprobado que los ataques se llevan con éxito, se implementa el mecanismo de seguridad, el cual consiste en verificar la ruta seguida por los mensajes. Se vuelve a correr la simulación y se comprueba que en efecto los routers no atacantes no agregan esta información a sus tablas de ruteo.

8.6. Resultados

El resultado de esta investigación es una nueva medida de seguridad que aplicada al protocolo BGP logra evitar que los ataques se lleven a cabo mediante los mensajes de comunicación.

Se propone el método de verificación de ruta para comprobar que la información recibida en los mensajes BGP sea real y de esta manera prevenir la agregación de rutas falsas en los routers. Mediante la simulación se comprueba que el nuevo mecanismo ayuda a la detección de información falsa en los mensajes y contribuye con la adecuada operación del protocolo BGP y además evita posibles ataques.

9. Referencias

- [1] Foundations of Attack Trees, Sjouke Mauw Eindhoven, University of Technology and Martijn Oostdijk Radboud University Nijmegen
- [2] Rekhter, Li, and Hares, RFC 4271 - A Border Gateway Protocol 4 (BGP-4), October 2005”, Disponible en la web: <<http://www.ietf.org/ietf/lid-abstracts.txt>> 2014
- [3] Cisco Documentation, Disponible en la web: <<http://www.cisco.com>>, 2014
- [4] On Tao Wan, Evangelos Kranakis, P.C. van Oorschot, Pretty Secure BGP (psBGP), School of Computer Science, Carleton University, Ottawa, Canada, November 2004 Routing Security and Pretty Secure BGP (psBGP) P. C. Van Oorschot, Tao Wan, and Evangelos Kranakis, Carleton University
- [5] The Internet Engineering Task Force (IETF), Disponible en la web: <<http://www.ietf.org/>>, 2014
- [6] S.Convery, D.Cook, M.Franz, An Attack Tree for the Border Gateway Protocol, IETF Internet Draft, draft-ietf-rpsec-bgpattack-00, Disponible en la web: <<http://www.ietf.org/>>, 2014