

INSTITUTO TECNOLÓGICO SUPERIOR DE EL MANTE

Línea de Investigación

Seguridad en Redes de Cómputo e Internet

M.C. José Paulino Ramírez Juárez

Cd. Mante Tamaulipas a 10 de junio de 2016

LÍNEA DE INVESTIGACIÓN: PROTOCOLOS SEGUROS EN REDES DE COMPUTADORAS E INTERNET

RESULTADOS O PRODUCTOS ESPERADOS

Producir documentos de alta calidad técnica que influyan en la manera de diseñar y manejar las redes de computadoras en internet de tal manera que esta mejore su desempeño. En internet existen ataques que llevan a violaciones de seguridad tales como:

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

En esta línea de investigación se pretende desarrollar propuestas de seguridad para los diferentes protocolos de comunicación en distintas capas del modelo OSI.

Algunos ejemplos son:

- En la capa de Enlace: Seguridad inalámbrica. WEP y WPA
- En la capa de Red: IPsec, BGP
- En la capa de Transporte: SSL (TLS)
- En la capa de Aplicación: PGP

Estos documentos incluyen estándares de protocolos, buenas prácticas, simulaciones y documentos con información relevante.

También se pretende generar artículos que puedan ser sometidos a arbitraje para su publicación en revistas a nivel nacional e internacional.

PROYECTOS DESARROLLADOS RELACIONADOS CON ESTE PROYECTO

- Sistemas de detección de intrusos
- Herramientas estadísticas de tráfico en Internet
- Sistemas de prevención de ataques

INTRODUCCIÓN

Día a día el uso de Internet se encuentra en aumento, y es por eso que cada vez más compañías se ven en la necesidad de poder acceder a sus sistemas informáticos desde cualquier lugar, ya sea desde la misma ciudad donde se reside o desde otro país. Es fundamental proteger los recursos dentro de la compañía y saber otorgar los derechos de acceso ya sea a clientes y proveedores. Este mismo procedimiento se aplica cuando se permite el acceso a través de Internet.

En internet existen ataques que llevan a violaciones de seguridad tales como:

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

Es a través de la investigación, propuestas y desarrollo de nuevos protocolos, la manera de alcanzar mayor seguridad dentro de las redes de computadoras en Internet.

Algunos proyectos relacionados con esta línea de Investigación son:

- Sistemas de detección de intrusos
- Herramientas estadísticas de tráfico en Internet
- Sistemas de prevención de ataques

Todo esto nos lleva a elevar la seguridad de la información y de los sistemas, y que los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Los principales objetivos de la seguridad en Internet son los siguientes:

- **Integridad.** En los datos que son enviados y recibidos a través de la red.
- **Confidencialidad.** Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad.** Garantizar el correcto funcionamiento de los sistemas de cómputo.
- **Evitar la Negación de Servicios.** Garantizar que no se pueda negar una operación realizada.
- **Autenticación.** Asegurar que sólo los individuos autorizados tengan acceso a los recursos.

ANÁLISIS DE SEGURIDAD DEL PROTOCOLO BGP

VULNERABILIDADES Y RIESGOS

BGP no tiene mecanismos internos que proveen de protección a la integridad, y autenticación de peers de los mensajes en una comunicación bgp peer to peer.

No han sido especificados mecanismos dentro de BGP para validar la autoridad de un AS para anunciar información NLRI.

No han sido especificados mecanismos dentro de BGP para asegurar la autenticidad de los atributos de trayectoria anunciados por un AS.

AMENAZAS

Las amenazas pueden provocar

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

Los ataques a las comunicaciones se clasifican en ataques pasivos y activos. En los pasivos el atacante solo observa la información que circula por la red violando la confidencialidad y también identifica los medios por los cuales puede realizar ataques más fuertes.

En los ataques Activos el atacante modifica los datos en tránsito.

VULNERABILIDADES EN MENSAJES BGP

- OPEN
- KEEP ALIVE
- NOTIFICATION
- UPDATE

VULNERABILIDADES A TRAVES DE OTROS PROTOCOLOS

BGP corre encima del protocolo TCP por el puerto 179 por lo tanto es vulnerable a ataques por medio de los mensajes:

- TCP SYN
- TCP SYN ACK
- TCP ACK
- TCP RST/FIN/FIN-ACK
- Dos y DDos

DAÑOS GENERADOS POR ATAQUES A BGP

- Starvation
- Network Congestion
- Black hole
- Delay
- Looping
- Eavesdrop
- Partition
- Cut
- Churn
- Instability
- Overload
- Resource Exhaustion
- Address Spoofing

ATAQUES

BGP dentro de sí mismo puede caer dentro de los siguientes ataques.

- Replay
- Message Insertion
- Message Deletion
- Message Modification
- Man in the middle
- Denial of Service

La meta primaria de seguridad en BGP es proveer datos a los operadores de Ases para habilitar a los BGP speakers a rechazar avisos de update que no son válidos.

AREAS A ASEGURAR

Las principales areas a asegurar son:

- The data payload del protocolo
- The data semantics de el protocolo

Una manera de asegurar los datos recibidos por los BGP speakers es verificarlos criptográficamente y de esta manera evitar los replay data.

Pero al requerir validación criptográfica pudiera abrir vectores para Denial of Service y esto es debido a la inundación del procesador con paquetes falsos los cuales tienen que ser invalidados criptográficamente antes de ser descartados. Esta validación criptográfica se realiza por medio de del standard del IETF llamado IPsec.

Hay preguntas que deben hacerse acerca de la información contenida en un Update recibido:

¿El AS originario está autorizado a propagar el prefijo que hemos recibido?

¿El AS_PATH recibido vía update representa una trayectoria válida en la red?

De esta última consideración surgen 2 más las cuales van de la menos a la más rigurosa:

¿El AS_PATH especificado, existe como una trayectoria en la topología de la red y es posible atravesar esa trayectoria para alcanzar el prefijo dado?

¿El update recibido ha viajado por la trayectoria que anuncia ese update?

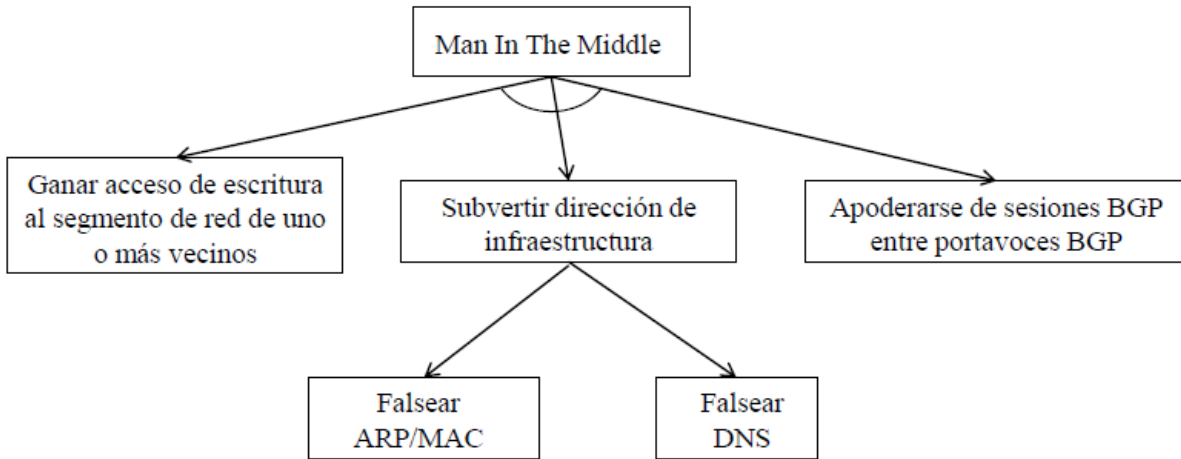
Ataques al protocolo BGP

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

En los arboles 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.

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.



REFERENCIAS

Toda la información es recopilada de los drafts de los grupos de trabajo de la IETF

The Internet Engineering Task Force (IETF), Disponible en la web: <http://www.ietf.org/>, 2016

The Internet Assigned Numbers Authority (IANA), Disponible en la web: <http://www.iana.org/>, 2016

The Internet Corporation for Assigned Names and Numbers (ICANN), Disponible en la web: <http://www.icann.org/>, 2016