Detección de Spoofing en Paquetes IP

Javier Echaiz* Jorge R. Ardenghi

Laboratorio de Investigación de Sistemas Distribuidos (LISiDi)
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur, Bahía Blanca (8000), Argentina
T.E.: 0291–4595135 (Ext. 2616 y 2605)
{je,jra}@cs.uns.edu.ar

Resumen

Los paquetes enviados mediante el protocolo IP incluyen en el *header* la dirección del nodo origen. Sin embargo el protocolo IP no hace ningún tipo de validación sobre esta dirección de origen, propiciando su falsificación (*spoofing*).
En esta línea de trabajo se estudia el problema y sus posibles soluciones con el objetivo de crear el marco necesario para futuras investigaciones y desarrollos en el campo de la detección de spoofing en paquetes IP.

Palabras Clave: Spoofing, IDS (*Intrusion Detection System*).

1 Introducción

Los paquetes enviados empleando el protocolo IP [Pos81] incluyen la dirección del nodo origen. El receptor responde a esta dirección de origen (emisor). Sin embargo, la autenticidad de esta dirección no es verificada por el protocolo. Este comportamiento trae aparejado el potencial problema de la falsificación de la dirección de origen del paquete (*spoofing*).

Las técnicas de spoofing son utilizadas por atacantes para diversos propósitos maliciosos. Estos incluyen:

- ocultar la dirección real del ataque;
- implicar a otro nodo como el origen del ataque;
- simular ser un nodo confiable (e.g. dirección IP de la red interna);
- interceptar (*hijacking*) tráfico;
- causar respuestas dirigidas a otro nodo.

Es entonces evidente que tener la capacidad de detectar paquetes falsificados se torna necesario. En algunos casos no sólo se pueden descubrir estos paquetes apócrifos sino que también es posible determinar la dirección real del atacante.

El spoofing puede ocurrir a diversos niveles (capas), e.g. a nivel de MAC Ethernet, tráfico no IP (e.g. IPX, Appletalk, NetBEUI), o spoofing de emails o de URLs. Si bien todos son importantes en este trabajo analizaremos únicamente el spoofing de paquetes IP.

Otros ataques relacionados con el aquí tratado también pueden provocar el ruteo a otro nodo (diferente al que el emisor pretende), e.g. [CWJ01, JGS+97] y ataques sobre el DNS [Bel95]. El spoofing de paquetes se restringe a direcciones de origen falsas en el header IP.

*Becario de la Comisión de Investigaciones Científicas de la Provincia de Buenos Aires, Argentina.

2 Spoofing de Paquetes IP

El spoofing de paquetes IP se encuentra generalmente asociado con diferentes tipos de ataque. Un factor común en los ataques que emplean spoofing es que el atacante salvo excepciones no necesita recibir respuestas directas de la víctima. Las respuestas simplemente no son necesarias, o pueden ser inferidas, o los paquetes pueden ser observados "en tránsito" (*sniffing*). En esta sección describiremos brevemente varios tipos de ataques de esta clase.

2.1 SYN-flood

Este es probablemente el ataque arquetipo de los denominados DoS (*Denial of Service*). En este caso las respuestas son irrelevantes. En el SYN-flood el atacante envía a la víctima un gran número de paquetes TCP `SYN`. Por cada paquete recibido el protocolo TCP/IP especifica que se debe enviar al emisor un paquete `ACK`. Obviamente el atacante no responde este paquete y por lo tanto la víctima queda esperando (hasta que expira el timeout), agotando inexorablemente la cantidad de conexiones.

Para que este ataque prospere se deben generar direcciones de origen falsas, pertenecientes a nodos inexistentes o apagados.

2.2 Smurf

En el ataque Smurf [CER98] el atacante envía paquetes ICMP `echo request` con dirección de origen falsa a una dirección broadcast de una subred. Esto provoca que cada nodo activo (encendido) envíe un `echo reply` al origen. En este ataque la dirección de la víctima se asigna como dirección de origen, causando un gran número de respuestas (potencial degradación de servicio). Nuevamente las respuestas no son importantes para el atacante.

Para que este ataque funcione el atacante debe tener acceso a una red broadcast que responda los ICMP `echo request`.

2.3 Spoofing de Conexión TCP

Este ataque necesita la coordinación de varios ataques, especialmente DoS de un host confiable y spoofing de paquetes de la víctima. De esta forma el atacante se puede hacer pasar por el host confiable falsificando la dirección de origen.

Este ataque no es sencillo dado que el protocolo TCP exige que los paquetes respuesta incluyan un número de secuencia correcto. Si el atacante no puede observar los paquetes en forma directa, todavía puede "adivinarlos". La RFC 1948 [Bel96] describe algunas técnicas para dificultar la predicción del número de secuencia. Sin embargo, aún hoy en día no solo se puede predecir, sino que no es una tarea extremadamente compleja.

2.4 Bounce Scan

Éste es uno de los casos en donde es fundamental para el atacante recibir paquetes de respuesta. Por lo tanto se suele asignar el IP de otra máquina (inexistente o apagada) en el mismo segmento a la dirección de origen y luego monitorear (sniffing) las respuestas dirigidas a este nodo. Sin embargo las redes switcheadas dificultan este ataque. Una alternativa más sofisticada sería observar indirectamente las respuestas de la víctima [Ant01].

Este ataque aprovecha la naturaleza regular del campo `identification number` del header IP. En la mayoría de las implementaciones este número se incrementa en uno por cada paquete

enviado. El ataque bounce emplea esta técnica enviando paquetes `SYN` falsificados a un *port* de la víctima. Si el port se encuentra cerrado la víctima responde con un `RST` (reset) y la máquina falsificada no toma ninguna acción al recibirlo [CWJ01]. Si el port está abierto la víctima responde a la dirección falsificada con un `ACK`, sin embargo como esta máquina no inició la conexión con el `SYN` envía un `RST` al destino e incrementa el `id number`.

En el bounce scan deben seguirse tres pasos: (i) conseguir el número de id de la máquina a "reemplazar"; (ii) enviar el paquete de "scan" falsificado a la víctima; (iii) conseguir nuevamente el número de id de la máquina a "reemplazar". De esta forma el atacante puede determinar si un port dado se encuentra o no abierto: si el número de id se incrementó en 1, está cerrado, si se incrementó en 2, entonces se encuentra abierto.

2.5 Zombies

Los ataques DDoS (*Distributed Denial of Service*) como Trinoo, Tribe Flood Network (TFN), Stacheldraht [LRST00], Trinity, Shaft, TFN2K y MStream entre otros, envían mensajes de control a sus *zombies*. Esto permite al atacante controlar a sus zombies sin necesidad de observar las respuestas y como consecuencia puede falsificar el origen de los mensajes de control. Además, teniendo en cuenta que los mensajes son típicamente *one-way* se puede utilizar virtualmente cualquier protocolo (facilitando el traspaso de firewalls).

Al igual que en el ataque mencionado en la subsección anterior los mensajes de control pueden ser enviados indirectamente.

Los ejemplos de ataque arriba mencionados explicitan la necesidad de poder determinar si un paquete tiene su dirección fuente falsificada o no. Esta determinación puede ayudar a prevenir posibles fuentes de ataque, evitar determinaciones falsas del origen, estimar el nivel de sofistificación, y posiblemente descubrir el origen real del ataque.

3 Detección del IP Spoofing

Los métodos de detección pueden clasificarse en aquellos que requieren soporte por parte de los routers, o métodos a nivel del nodo (activos o pasivos).

Por cuestiones de espacio estos métodos se describirán muy brevemente. Se recomienda al lector interesado consular la bibliografía.

3.1 Detección Mediante Soporte en Routers

Los routers son capaces de determinar por cual de sus interfases de red llegó cada paquete. Pueden entonces filtrar paquetes de origen falsificado siguiendo simplemente las recomendaciones de la RFC 2827 [FS00]. Por ejemplo un router (o un firewall *dual-homed*) que recibe por su placa de red "externa" un paquete con una dirección fuente perteneciente a la clase de la red "interna", se encuentra frente a un paquete erróneo, probablemente malintencionado.

Por otro lado, los routers pueden tomar un rol activo en la detección del spoofing participando de lo que se conoce como *traceback* [SDS00, SC95].

3.2 Detección a Nivel del Nodo

Un nodo puede analizar un paquete y así determinar si se trata de un paquete auténtico o no. Para ello puede emplear métodos activos o pasivos; son activos cuando el nodo debe efectuar

alguna acción en la red para validar la dirección de origen de los paquetes y son pasivos cuando no requieren acciones de este tipo.

3.2.1 Métodos Activos

Los métodos activos envían paquetes de consulta (*query*) para determinar el origen real del paquete (reactivos) o envían paquetes con comandos específicos esperando una determinada respuesta (proactivos). La ventaja de estos métodos por sobre los que se apoyan en routers es que no necesitan la cooperación entre ISPs y pueden ser efectivos aún si el atacante se encuentra en la misma subred que la víctima.

Los métodos activos requieren respuestas del supuesto fuente y solamente funciona si el nodo que esta haciendo el spoofing se encuentra activo (i.e., conectado a la red y recibiendo y procesando paquetes). Cuando los nodos no responden a ninguna sonda (*probe*) se vuelve necesario corroborar mediante métodos pasivos.

Ejemplos de los métodos activos son las sondas basadas en el análisis del `TTL` (*time to live*), los basados en el `id number`, la identificación del S.O., los basados en TCP (control de flujo, retransmisión de paquetes) y `traceroute`.

3.2.2 Métodos Pasivos

Los métodos pasivos se basan en la observación de paquetes con valores predecibles que no se corresponden a paquetes previos. El sistema aprende qué valores pueden esperarse y entonces dictamina que los paquetes con valores inesperados son sospechosos.

Siendo que los valores de `TTL` son función del S.O., del protocolo del paquete y de la topología de la red, pueden emplearse para detección pasiva, a diferencia del `id number`.

4 IDSs y la Detección del IP Spoofing

La detección de paquetes con orígenes falsificados puede implementarse como un sensor en un IDS (*Intrusion Detection System*) o como módulo en un firewall. Para el primer caso, un paquete marcado como potencial spoofing alerta al sistema IDS, en un firewall el paquete puede descartarse (*drop*) o pasar (*accept*) pero con la marca adicional de posible spoofing. Los sistemas de monitoreo de seguridad pueden emplear esta información en la detección de ataques.

Todo sistema robusto y eficiente de detección de spoofing debe combinar métodos para lograr correctas determinaciones. Es nuestra intención experimentar con un sistema que emplee en primer término métodos pasivos y a continuación, y sólo para los paquetes sospechosos, técnicas activas. Además deben ser enviadas y analizadas varias clases de sondas para lograr resultados más precisos. El sistema debe generar *logs* que justifiquen la decisión de marcar un paquete como apócrifo no sólo para fines prácticos (para el administrador de red) sino también como ayuda para minimizar futuros falsos positivos y falsos negativos y para que comprendamos mejor las relaciones entre redes.

Si bien es posible analizar cada paquete, por cuestiones de eficiencia es aconsejable emplear estas técnicas únicamente por demanda y como extensión del sistema IDS.

Nuestra investigación concluirá con una implementación de un sistema de detección de spoofing capaz de generalizar a partir de paquetes anómalos detectados previamente a fin de lograr una mayor efectividad tratando de no incrementar los falsos positivos. Es claro que detectar los paquetes con origen falsificado es sólo la mitad de la solución: debemos también

poder determinar el verdadero origen de los paquetes. Para lograrlo existen soluciones a nivel de routers especializados [SDS00, Dun00], o cambios en los protocolos de red subyacentes [KA98]. Si bien estas técnicas atacan de forma correcta el problema creemos que son más atractivas las soluciones que no se basan en estos fuertes requerimientos.

El interés en este campo reside en la fuerte dependencia de la mayoría de los ataques actuales provenientes de las redes y el empleo de técnicas de spoofing. Es entonces interesante poder detectar y posiblemente prevenir este tipo de ataque como método general para fortalecer la seguridad en las redes.

Bibliografía

[Ant01] Antirez. New TCP scan method, Febrero 2001.

[Bel95] Steven M. Bellovin. Using the domain name system for system break-ins. En *Proceedings of the 5th USENIX Security Symposium*, páginas 199–208, Utah, Junio 1995. USENIX.

[Bel96] S. Bellovin. RFC 1948: Defending against sequence number attacks, Mayo 1996.

[CER98] CERT. Smurf IP denial of service attacks. CERT, Advisory CA-1998-1, Computer Emergency Response Team, Enero 1998.

[CWJ01] Ho-Yen Chang, S. Felix Wu y Y. Frank Jou. Real-time protocol analysis for detecting link-state routing protocol attacks. *ACM Transactions on Information and System Security*, 4(1):1–36, Febrero 2001.

[Dun00] T. Dunigan. Backtracking spoofed packets, 2000.

[FS00] P. Ferguson y D. Senie. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. Request For Comments (RFC) 2827, Best Current Practice (BCP) 0038, Mayo 2000.

[JGS+97] Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun Felix Wu y W. Rance Cleaveland. Architecture design of a scalable intrusion detection system for the emerging network infrastructure. Reporte Técnico CDRL A005, MCNC Information Technologies Division, Research Triangle Park, N.C. 27709, Abril 1997.

[KA98] Stephen Kent y Randall Atkinson. Security architecture for the Internet Protocol. Internet Request for Comment RFC 2401, Internet Engineering Task Force, Noviembre 1998.

[LRST00] F. Lau, S. Rubin, M. Smith y Lj. Trajkovic. Distributed denial of service attacks. En *Proceedings of the 2000 IEEE Int. Conf. on Systems, Man, and Cybernetics, Nashville, TN*, páginas 2275–2280, Octubre 2000.

[Pos81] J. Postel. Internet Protocol DARPA Internet Program Protocol Specification. RFC 791, Internet Society (IETF), 1981.

[SC95] L. T. Heberlein S. Staniford-Chen. Holding intruders accountable on the Internet. En *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, páginas 39–49, Oakland, CA, Mayo 1995.

[SDS00] Dan Schnackenberg, Kelly Djahandari y Dan Sterne. Infrastructure for intrusion detection and response. En *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX 2000)*. IEEE Computer Society Press, Enero 2000.