Automatización de la Detección de Intrusos a partir de Políticas de Seguridad

Javier Echaiz* Jorge R. Ardenghi Guillermo R. Simari
Laboratorio de Investigación de Sistemas Distribuidos (LISiDi)
Departamento de Ciencias e Ingeniería de la Computación
T.E.: +54 291–4595135 Fax: +54 291–4595136
Bahía Blanca – Buenos Aires – República Argentina
{je,jra,grs}@cs.uns.edu.ar

Resumen

La explosión de la Internet en esta última década involucra la búsqueda de "valor agregado" en las infraestructuras. Por esta razón, la seguridad de la información de los sistemas es una de las mayores preocupaciones de la actualidad. El control de acceso a un equipo, a una red, o a un dominio administrativo juega un papel esencial en un ambiente que se vuelve cada día más heterogéneo.

Las arquitecturas de seguridad en redes consisten de un número de componentes dedicados, como routers de filtrado y firewalls. El eje del enfoque tradicional de la seguridad en redes es separar la red en una zona segura y otra insegura. Típicamente, la interfase entre ellas está compuesta por un punto de único acceso que garantiza una determinada política de seguridad. Este enfoque tradicional presenta dos problemas significativos, reducida flexibilidad y escalabilidad. Adicionalmente los firewalls convencionales solamente son capaces de observar un único punto en la red y por lo tanto cuentan con información limitada (parcial) de su entorno. Por último, los ataques masivos, como el *Distributed Denial of Service* (DDoS), han demostrado categóricamente las limitaciones y debilidades de este modelo. La valoración de la seguridad en redes requiere entonces que estos problemas sean considerados profundamente.

El objetivo de esta investigación es crear metodologías de *Detección de Intrusos* efectivas que complementen a las tecnologías actuales y que sean capaces de responder a los nuevos desafíos.

Palabras Clave: Detección de Intrusos, Seguridad en Redes, Políticas de Seguridad, Sistemas Distribuidos, Computación Colaborativa, Automatización.

1. Introducción

La detección de intrusos constituye un campo de investigación que se encuentra en estudio desde hace unos 20 años. Sin embargo, las técnicas de detección de intrusos están lejos de ser perfectas. Los sistemas actuales, *Intrusion Detection Systems* (IDSs), presentan dos grandes inconvenientes: (1) suelen generar un gran número de falsos alertas (falsos positivos) y (2) no pueden detectar nuevos ataques (o variaciones de ataques conocidos). Adicionalmente, los IDSs actuales se basan en ataques (o anomalías) de bajo nivel, las cuales no pueden capturar los pasos lógicos o estrategias detrás de estos ataques. Consecuentemente, los IDSs existentes suelen generar una gran cantidad de alertas. Frente a situaciones de acciones de intrusión intensivas, no solamente los alertas reales se encontrarán mezclados con los falsos positivos, sino que

*Becario del "Consejo Nacional de Investigaciones Científicas y Técnicas" (CONICET), Argentina.

la cantidad de alertas a procesar puede rápidamente volverse inmanejable. Como resultado de ello, es difícil para el personal (especialmente para los Administradores de Sistemas y/o Administradores de Seguridad) o para los sistemas de respuesta a intrusos comprender las intrusiones detrás de las alertas y tomar las acciones apropiadas.

Los firewalls actuales son entidades de software o hardware que aplicando diversas formas de *Access Control Lists* (ACLs) controlan el tráfico de red entrante o saliente. Dado que se encuentran ubicados entre la red y los servidores tienden a convertirse en cuellos de botella debido a la gran cantidad de tráfico que manejan. Además, estos firewalls no tienen control sobre el tráfico interno de la red y por ende nada pueden hacer para neutralizar a uno de los tipos de ataque más frecuentes, aquellos causados por atacantes "internos" (pertenecientes a la misma organización). Los protocolos basados en estado suelen intercambiar mensajes de control para luego utilizar ports aleatorios que se emplean en la transferencia de datos. Esto indudablemente incrementa el nivel de complejidad de los firewalls en cuanto a sus ACLs y al requerimiento de mantener grandes volúmenes de información de estado.

Las transacciones electrónicas se están volviendo cada día más populares, haciendo necesaria la apertura de parte de la red a proveedores, partners y clientes. Indudablemente esto agrega una capa adicional de complejidad. Por otro lado, el *e-commerce* también afecta la criptografía *end-to-end* debido a que los firewalls deben actuar como intermediarios en las conexiones seguras. Por último, manejar la seguridad únicamente en el perímetro de la red no previene ataques masivos (como el *Distributed Denial of Service* (DDoS)).

Solamente a modo de ejemplo de la magnitud del problema que atacaremos en esta línea de investigación, basta con decir que desde el año 2000 el costo de los ataques de seguridad en el mundo se estima que es de 1600 mil millones de dólares según InformationWeek Research y PriceWaterHouseCoopers. Este estudio también indica que el 50 % de todas las compañías con presencia en Internet fueron atacadas para el año 1998, pero que sin embargo este número escaló al 74 % en 2002. Con el advenimiento masivo de las redes de banda ancha es de esperarse que cada día este número sea aun mayor. Por todo esto las soluciones de seguridad deben tener en cuanta las nuevas características de las redes: banda ancha generalizada, soporte de calidad de servicio (QoS), movilidad, etc. Más aun, la seguridad debe tratarse de acuerdo con una gestión de QoS y en menor medida (aunque también importante) según la heterogeneidad de las redes de acceso (fijas o móviles).

Otro problema se origina con el rápido crecimiento de nuevos servicios y protocolos (estándares abiertos o propietarios), particularmente en los dominios de la multimedia y de los juegos de video. Típicamente los proveedores y administradores actualizan los protocolos y servicios asociados, pero generalmente las soluciones de seguridad son estáticas y procesadas manualmente. Los límites de este enfoque pueden verse en la actualidad cuando aplicaciones pertenecientes a estos dominios abren canales de comunicación e introducen restricciones de tiempo real. Por simplicidad discutiremos el caso del dominio de la multimedia solamente en dos tipos de medios: medios discretos (una foto, un texto) y streams contínuos (audio, video). El último caso implica restricciones de tiempo, más o menos restrictivas según el tipo de aplicación empleado. Análogamente esto mismo sucede si consideramos el dominio de los juegos, como por ejemplo los juegos de estrategia, donde los jugadores se encuentran separados geográficamente (y también en términos de red) por grandes distancias, pero que sin embargo, deben conocer constantemente las posiciones de todos los actores en el "mundo virtual" creado por el juego, prácticamente en tiempo real.

Considerando el objetivo de tener en cuenta estas aplicaciones y sus protocolos asociados, la arquitectura de seguridad de nuestro sistema completo debe replantearse. En particular, con la

tecnología de Internet 3G (aparecida en el año 2007 en nuestro país), la movilidad y el constante incremento de los anchos de banda, es necesario combinar los mecanismos de seguridad con los mecanismos de procesamiento de datos a alta velocidad y movilidad de los usuarios.

2. Línea de investigación

2.1. Objetivos generales

Esta línea de investigación incluye entonces la creación de un *framework* que gestione adecuadamente las políticas de seguridad, a su vez capaces de adaptarse efectiva y eficientemente a estos cambios. Estas políticas de seguridad deben definirse de forma flexible pero segura y deben poder aplicarse tanto a la totalidad de la red de una organización como solamente a una parte de la misma. Las relaciones con otras entidades (*partners*) deben poder traducirse a reglas dinámicas, instaladas posiblemente como un overlay, sin cambiar la seguridad "base" de los demás nodos. Adicionalmente el sistema de seguridad debe poder interactuar y tomar decisiones de forma automática en función a dichas políticas.

Por otro lado, no es suficiente contar con la capacidad de proteger únicamente a los servidores de ataques provenientes del interior trabajando con la cadena completa entre clientes y servidores, sino que también es necesario preservar cada red dentro de un dominio frente a otras redes interconectadas. Por ejemplo, nuestra investigación debería ser capaz de presentar una solución que evite la propagación de ataques DDoS entre diferentes dominios de red, fundamental desde el punto de vista de los administradores de sistemas y de vital importancia para los usuarios de sistemas distribuidos geográficamente. Esta línea permite entonces un nuevo enfoque para los intercambios entre los diferentes actores (administradores, usuarios, proveedores).

Por ultimo, buscaremos también dar respuesta a la necesidad de poder detectar/solucionar las intrusiones en los *Distributed Processing Environments* (DPEs), especialmente en aquellos sistemas cuyos nodos se encuentran distribuidos geográficamente, como por ejemplo en *grid computing*. Para este fin será también analizada la problemática del paradigma *peer-to-peer*, como el anonimato, la alta escalabilidad y la inherente distribución de recursos relacionados con la propuesta aquí planteada.

2.2. Finalidades Específicas

Las tecnologías actuales están lejos de poder solucionar de forma efectiva el problema de la seguridad en redes, básicamente los firewalls únicamente toman decisiones de muy bajo nivel y los sistemas de detección de intrusos (quienes también analizan el bajo nivel sin considerar entornos ni eventos previos) no son capaces de detectar nuevos ataques (o modificaciones de ataques conocidos). Adicionalmente la gestión de la seguridad se hace de forma manual, por parte de los administradores de sistemas.

A través del desarrollo de esta línea de investigación esperamos desarrollar una solución de seguridad nueva y general que resuelva el acuciante problema de proveer seguridad combinando las tecnologías clave pertenecientes a varias áreas, en particular:

- Algoritmos y metodologías para la detección de intrusos.
- Técnicas basadas en políticas de seguridad que apunten a la configuración automática y toma de decisiones del sistema.
- Técnicas de implementación flexible para el procesamiento de paquetes a alta velocidad.

3. Trabajos futuros

Nuestra hipótesis de partida propone generar metodologías capaces de mejorar la efectividad y eficiencia de los sistemas de seguridad actuales. Para ello se combinan principalmente firewalls (filtrado y QoS), sistemas de detección de intrusos, análisis y procesamiento automático a partir de políticas de seguridad. A todo esto se le suman metodologías provenientes del campo de la computación distribuida (clusters disponibles) y de la inteligencia artificial.

En primer término se estudiarán en profundidad las tecnologías antes mencionadas. A continuación se propondrán nuevas metodologías y algoritmos, con el correlato de mesuras y experimentos a desarrollar en el *Laboratorio de Investigación en Sistemas Distribuidos* (LISiDi) de la UNS.

El objetivo general del proyecto es desarrollar nuevos componentes de red que posibiliten entornos de servicio seguro de una forma eficiente y efectiva. Esta línea de investigación incluye:

- Diseñar e implementar una nueva arquitectura que provea un ambiente distribuido controlado de detección de intrusos y que a su vez conjugue filtrado de paquetes de alta velocidad (incluyendo QoS y control de tráfico) en base a las restricciones planteadas en la política de seguridad. El objetivo en este punto es lograr una solución completa de seguridad que satisfaga las necesidades de los usuarios y de los proveedores de servicios.
- Desarrollar nuevas técnicas de detección de intrusos capaces de detectar un amplio espectro de violaciones a las políticas de seguridad preestablecidas. No sólo se tratará de minimizar la posibilidad de ataques DDoS, sino también poder detectar e identificar todo tipo de fallas, incluyendo incluso actividades no mal intencionadas que puedan causar interrupciones de servicios. Mejorar las capacidades de detección de intrusos actuales diseñando e implementando soluciones efectivas y flexibles para el monitoreo distribuido del tráfico de las aplicaciones.
- Establecer técnicas inteligentes (conceptos provenientes del área de la Inteligencia Artificial) que den respuesta a las violaciones de seguridad.
- Asegurar igualdad y coherencia en la aplicación de las políticas de seguridad gestionando y controlando los componentes del sistema propuesto.
- Crear aplicaciones y *testbeds* para esta nueva tecnología.

Referencias

[1] S. Weber, P. A. Karger, and A. Paradkar, "A software flaw taxonomy: aiming tools at security," *SIGSOFT Softw. Eng. Notes*, vol. 30, no. 4, pp. 1–7, 2005.

[2] V. Ahuja, *Network and Internet security.* San Diego, CA, USA: Academic Press Professional, Inc., 1996.

[3] S. M. Bellovin, "Security problems in the tcp/ip protocol suite," *SIGCOMM Comput. Commun. Rev.*, vol. 19, no. 2, pp. 32–48, 1989.

[4] B. Caswell, J. Beale, and A. R. Baker, *Snort Intrusion Detection and Prevention Toolkit.* Syngress Publishing, 2007.

[5] A. Molitor, "An architecture for advanced packet filtering," in *SSYM'95: Proceedings of the 5th conference on USENIX UNIX Security Symposium*, (Berkeley, CA, USA), pp. 11–11, USENIX Association, 1995.

[6] A. D. Keromytis and J. M. Smith, "Requirements for scalable access control and security management architectures," *ACM Trans. Inter. Tech.*, vol. 7, no. 2, p. 8, 2007.

[7] H. Julkunen and C. Chow, "Enhance network security with dynamic packet filter," 1998.

[8] L. M'e and C. Michel, "Intrusion detection: A bibliography," Tech. Rep. SSIR-2001-01, Sup'elec, Rennes, France, September 2001.

[9] D. Anderson, T. Frivold, A. Tamaru, and A. Valdes, "Next-generation intrusion detection expert system (nides), software users manual, beta-update release," Tech. Rep. SRI–CSL–95–07, Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025-3493, May 1994.

[10] A. K. Jones and R. S. Sielken, "Computer system intrusion detection: A survey," tech. rep., University of Virginia Computer Science Department, 1999.

[11] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, E. H. Spafford, and D. Zamboni, "An architecture for intrusion detection using autonomous agents," in *ACSAC*, pp. 13–24, 1998.

[12] T. Lane and C. E. Brodley, "An application of machine learning to anomaly detection," in *Proc. 20th NIST-NCSC National Information Systems Security Conference*, pp. 366–380, 1997.

[13] S. M. Bellovin, "Problem areas for the IP security protocols," in *Proceedings of the Sixth Usenix UNIX Security Symposium*, 1996.

[14] S. R. Snapp, J. Brentano, G. V. Dias, T. L. Goan, L. T. Heberlein, C. lin Ho, K.Ñ. Levitt, B. Mukherjee, S. E. Smaha, T. Grance, D. M. Teal, and D. Mansur, "DIDS (distributed intrusion detection system) - motivation, architecture, and an early prototype," in *Proceedings of the 14th National Computer Security Conference*, (Washington, DC), pp. 167–176, 1991.

[15] M. Medina, "A layered framework for placement of distributed intrusion detection devices," in *Proc. 21st NIST-NCSC National Information Systems Security Conference*, pp. 76–83, 1998.

[16] T. Lane and C. E. Brodley, "Detecting the abnormal: Machine learning in computer security," tech. rep., Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, Jan. 1997.

[17] T. Lane and C. E. Brodley, "Sequence matching and learning in anomaly detection for computer security," in *AI Approaches to Fraud Detection and Risk Management* (Fawcett, Haimowitz, Provost, and Stolfo, eds.), pp. 43–49, AAAI Press, 1997.

[18] R. A. Sinnappan, "A reconfigurable approach to tcp/ip packet filtering," 2001.

[19] J. R. Vacca, *Internet Security Secrets*. Foster City, CA, USA: IDG Books Worldwide, Inc., 1995.

[20] "Pbit, a pattern-based testing framework for iptables," in *CNSR '04: Proceedings of the Second Annual Conference on Communication Networks and Services Research*, (Washington, DC, USA), pp. 107–112, IEEE Computer Society, 2004.

[21] C. Krügel, R. Lippmann, and A. Clark, eds., *Recent Advances in Intrusion Detection, 10th International Symposium, RAID 2007, Gold Goast, Australia, September 5-7, 2007, Proceedings*, vol. 4637 of *Lecture Notes in Computer Science*, Springer, 2007.

[22] N. J. Puketza, K. Zhang, M. Chung, B. Mukherjee, and R. A. Olsson, "A methodology for testing intrusion detection systems," *IEEE Transactions on Software Engineering*, vol. 22, no. 10, pp. 719–729, 1996.