Un Enfoque Proactivo Basado en Detección de Intrusos Distribuida (DIDS)

Pablo Davicino* Javier Echaiz Jorge Ardenghi

Laboratorio de Investigación en Sistemas Distribuidos (LISiDi)
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
Bahía Blanca - Buenos Aires - Argentina
email:{pmd,je,jra}@cs.uns.edu.ar

Resumen

En la actualidad la amplia interconexión entre sistemas, motivada por la existencia de múltiples medios de comunicación heterogéneos y dispositivos de bajo costo, naturalmente conlleva a la necesidad de contar con herramientas sofisticadas para proveer un marco de seguridad a las entidades participantes. En este contexto, un Sistema de Detección de Intrusos (IDS) provee la capacidad de poder detectar un uso indebido, no autorizado o un abuso de un recurso computacional. El eje central de esta línea de investigación se basa en el diseño de un sistema de detección de intrusos distribuido (DIDS), que permita obtener y correlacionar información proveniente de múltiples sensores, de forma de poder detectar la presencia de ataques y tomar una actitud proactiva en relación a los mismos. Se pretende que el sistema pueda desplegarse tanto en en una red de área local (LAN) como en una red de longitud y topología física arbitraria.

Palabras clave: *detección de intrusos, ids, dids, seguridad, sistemas distribuidos.*

*Becario de la Comisión de Investigaciones Científicas (CIC) de la Provincia de Buenos Aires

Contexto

El trabajo objeto del presente artículo se desarrolla en el Laboratorio de Investigación en Sistemas Distribuidos (LISiDi) del Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur.

La línea de investigación presentada es parte de los Proyectos "Automatización de la Detección de Intrusos a partir de Políticas de Seguridad" (24/ZN14) dirigido por el Mag. Lic. Javier Echaiz, y "Computación Distribuida de Alto Rendimiento y Disponibilidad"(24/N024) dirigido por el Mag. Ing. Jorge Ardenghi. Ambos proyectos son financiados por la Secretaria General de Ciencia y Tecnología de la Universidad Nacional del Sur, y se encuentran acreditados por la Universidad Nacional del Sur, Bahía Blanca.

Introducción

Un mecanismo de detección de intrusos pretende direccionar el problema referido a identificar accesos no autorizados, que tiendan a comprometer la integridad, confidencialidad o disponibilidad de un recurso computacional. El sistema debe contemplar las amenazas refe-

rentes tanto a atacantes externos, como a potenciales atacantes internos los cuales, a pesar de poseer un acceso autorizado al sistema, podrían intentar exceder sus privilegios en aras de comprometer los recursos utilizados.

La proliferación masiva de redes de computadoras heterogéneas ha tenido un serio impacto en lo que respecta al problema de detección de intrusos, dada la mayor oportunidad de obtener un acceso no autorizado a partir de la amplia oferta de conectividad brindada por las redes existentes. A su vez, la utilización de múltiples recursos computacionales distribuidos, también implica la necesidad de contar con un mayor control sobre los mismos.

Un sistema de Detección de Intrusos Distribuido (DIDS) [14, 1, 15] consiste en múltiples IDS, o agentes independientes cooperativos, interconectados mediante una red de comunicación. En particular, el sistema está compuesto por agentes que realizan monitoreos específicos sobre el *host* en el que se ejecutan (HIDS), y por agentes que monitorean diversos segmentos de red de interés (NIDS)[2]. Cada agente genera información específica en un formato bien determinado [7].

Para enfrentar el problema de la detección de instrusos distribuida a gran escala, debe contemplarse una clara división de trabajo, intercambio de información y coordinación entre los diversos *sensores* que componen el sistema. En particular, la correlación de información resulta un aspecto clave en la dinámica del sistema, dado que a partir de dicho proceso se podrá determinar la existencia de un ataque [4, 9].

El mecanismo de correlación resulta naturalmente complejo, dada la inherente distribución de la información generada por los diversos sensores. A su vez, la probabilidad de generar falsos positivos resulta un factor crítico, debido principalmente a que el sistema posee una actitud proactiva. Una errónea detección de un ataque mediante un conjunto de falsos positivos, podría implicar que el sistema impida el acceso a usuarios autorizados. En este sentido, el problema posee al menos dos aristas bien diferenciadas dado que, además de lo expuesto, un atacante podría utilizar como técnica la generación de falsos positivos para inducir al sistema a una negación total del servicio (DoS).

Diversos esquemas de detección de intrusos sobre un ambiente disitribuido han sido propuestos [15, 18], los cuales envían la información a auditar a un único nodo en el cual se efectúa su análisis. La escalabilidad de este tipo de modelos está totalmente limitada, dada la utilización de componentes centralizados. En aras de mejorar el factor de escala, otros sistemas han propuesto una estructura jerárquica [16] para organizar sus componentes.

Si bien la naturaleza jerárquica de estos enfoques logró mejorar la escalabilidad con respecto a los primeros desarrollos, su talón de Aquiles se ve reflejado en el proceso de correlación. Precisamente, si dos o más IDSs distantes en la jerarquía detectan un intruso común, dicha información no puede ser correlacionada hasta que los mensajes correspondientes alcancen un IDS común. En un sistema con una cantidad significativa de sensores, los mensajes deberían ser procesados por múltiples agentes, incurriendo en una sobrecarga tanto a nivel de comunicación como de procesamiento. De esta forma, la descentralización de componentes en una arquitectura totalmente distribuida corresponde a uno de los factores fundamentales para el desarrollo de un sistema de detección de instrusos distribuido.

Líneas de Investigación y Desarrollo

Uno de los objetivos de la línea de investigación presentada, radica en extender el concepto de detecciíon de intrusos a un sistema distribuido de gran escala interconectado mediante

una red física de topología arbitraria. Esta topología es transparente para cada sensor que compone el sistema, dado que los mismos se despliegan sobre una red lógica (overlay) sustentada bajo la utilización de Tablas Hash Distribuidas (DHTs) [5, 12].

Como eje adicional, se están investigando diversas técnicas basadas en High Performance Computing (HPC) aplicadas al proceso de agregación y correlación de información [9]. En particular, se desea acelerar el proceso de correlación de datos [6], mediante la distribución del cómputo de patrones específicos obtenidos a partir del análisis de la información generada por los distintos sensores que componen el sistema.

En relación con este último punto, se está estudiando la posibilidad de aplicar al proceso de análisis de información técnicas propias del campo de bases de datos [8, 11]. En particular, se pretende que dichas técnicas puedan aportar relaciones no triviales entre datos que puedan al menos modelar una alerta indicando la presencia de un potencial riesgo.

Resultados y Objetivos

Actualmente se está desarrollando la primer etapa del trabajo, en la cual se está realizando el despliegue de varios sensores sobre la infraestructura del LISiDi. Parte del proceso de despliegue, consiste en la implementación de los componentes específicos encargados del almacenamiento de la información generada por cada sensor.

En una segunda estapa del trabajo se abordará la implementación del mecanismo de correlación de datos. Se espera obtener resultados significativos en esta etapa con el objetivo de reducir la probabilidad de falsos positivos. De esta forma se pretende desarrollar una lógica específica sobre el sistema, de forma tal que el mismo pueda tomar una actitud proactiva ante la presencia de una amenaza.

Finalmente, se espera poder extender el sistema a una red de área amplia con el objetivo de demostrar la escalabilidad del mismo.

Formación de Recursos Humanos

El trabajo presentado corresponde a una de las principales líneas de investigación del Laboratorio de Investigación en Sistemas Distribuidos (LISiDi). La misma será una parte central de la Tesis de Maestría del Ing. Pablo Davicino.

A su vez, el LISiDi cuenta con recursos propios, sobre los cuales se despliegan los distintos componentes que conforman parte de la implementación del sistema considerado. Dicha infraestructura ha sido objeto de diversas Tesis de grado, desarrolladas por alumnos de las carreras Ingeniería en Sistemas de Computación y Licenciatura en Ciencias de la Computación, ambas dictadas por el Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur.

A continuación se detallan los cursos de pregrado relacionados con la línea de investigación presentada, dictados por los integrantes del grupo de investigación:

- **Sistemas Operativos.** Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas de Computación, Universidad Nacional del Sur.
- **Sistemas Distribuidos.** Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas de Computación, Universidad Nacional del Sur.
- **Sistemas Operativos y Distribuidos.** Materia obligatoria para los estudiantes de la carrera Licenciatura en Ciencias de la Computación, Universidad Nacional del Sur.

- **Sistemas Distribuidos I.** Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas, Facultad de Ingeniería, Universidad Nacional de la Pampa.

- **Sistemas Distribuidos II.** Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas, Facultad de Ingeniería, Universidad Nacional de la Pampa.

- **Seguridad en Sistemas.** Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas de Computación, y optativa para los de Licenciatura en Ciencias de la Computación, Universidad Nacional del Sur.

- **Redes de Computadoras.** Materia obligatoria para los estudiantes de la carrera Licenciatura en Ciencias de la Computación, Universidad Nacional del Sur.

Los siguientes cursos de posgrado, en relación con la línea de investigación presentada, son dictados por miembros del grupo de investigación:

- **Paradigmas de Programación Paralela.** Materia del Posgrado en Ciencias de la Computación, Universidad Nacional del Sur.

- **Sistemas Peer-To-Peer y sus Aplicaciones.** Materia del Posgrado en Ciencias de la Computación, Universidad Nacional del Sur.

- **Seguridad, Auditoría y Control de Sistemas de Información (SACS).** Módulo obligatorio perteneciente a la Maestría en Sistemas de Información de la Facultad de Ciencias de la Administración de la Universidad Nacional de Entre Ríos (UNER).

Referencias

[1] Abraham, A., Jain, R., Thomas, J., and Han, S. Y. D-scids: distributed soft computing intrusion detection system. *J. Netw. Comput. Appl. 30* (January 2007), 81–98.

[2] Bai, Y., and Kobayashi, H. Intrusion detection system: Technology and development. *Advanced Information Networking and Applications, International Conference on 0* (2003), 710.

[3] Banković, Z., Moya, J. M., Araujo, A., Fraga, D., Vallejo, J. C., and de Goyeneche, J.-M. Distributed intrusion detection system for wireless sensor networks based on a reputation system coupled with kernel self-organizing maps. *Integr. Comput.-Aided Eng. 17* (April 2010), 87–102.

[4] Bass, T. Intrusion detection systems and multisensor data fusion. *Commun. ACM 43* (April 2000), 99–105.

[5] Caesar, M., Castro, M., Nightingale, E. B., O'Shea, G., and Rowstron, A. Virtual ring routing: network routing inspired by dhts. *SIGCOMM Comput. Commun. Rev. 36* (August 2006), 351–362.

[6] Cuppens, F., and Miège, A. Alert correlation in a cooperative intrusion detection framework. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy* (Washington, DC, USA, 2002), IEEE Computer Society, pp. 202–.

[7] Cuppens, F., and Ortalo, R. Lambda: A language to model a database for detection of attacks. In *Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection* (London,

UK, 2000), RAID '00, Springer-Verlag, pp. 197–216.

[8] Dasarathy, B. V. *Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security 2009*. Society of Photo Optical, 2009.

[9] Debar, H., and Wespi, A. Aggregation and correlation of intrusion-detection alerts. In *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection* (London, UK, 2001), RAID '00, Springer-Verlag, pp. 85–103.

[10] Gunawan, L. A., Vogel, M., Kraemer, F. A., Schmerl, S., Slåtten, V., Herrmann, P., and König, H. Modeling a distributed intrusion detection system using collaborative building blocks. *SIGSOFT Softw. Eng. Notes 36* (January 2011), 1–8.

[11] Kavitha, B., Karthikeyan, S., and Chitra, B. Efficient intrusion detection with reduced dimension using data mining classification methods and their performance comparison. In *Information Processing and Management*, V. V. Das, R. Vijayakumar, N. C. Debnath, J. Stephen, N. Meghanathan, S. Sankaranarayanan, P. M. Thankachan, F. L. Gaol, and N. Thankachan, Eds., vol. 70 of *Communications in Computer and Information Science*. Springer Berlin Heidelberg, 2010, pp. 96–101.

[12] Lua, E. K., Crowcroft, J., Pias, M., Sharma, R., and Lim, S. A survey and comparison of peer-to-peer overlay network schemes. *IEEE Communications Surveys and Tutorials 7* (2005), 72–93.

[13] Patil, N., Das, C., Patankar, S., and Pol, K. Analysis of distributed intrusion detection systems using mobile agents. *Emerging Trends in Engineering and Technology, International Conference on 0* (2008), 1255–1260.

[14] Shetty, P. *DISTRIBUTED INTRUSION: Detection Systems*. VDM Verlag, Saarbrücken, Germany, Germany, 2010.

[15] Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, L. T., Ho, C.-L., Levitt, K. N., Mukherjee, B., Smaha, S. E., Grance, T., Teal, D. M., and Mansur, D. Internet besieged. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1998, ch. DIDS (distributed intrusion detection system) motivation, architecture, and an early prototype, pp. 211–227.

[16] Spafford, E. H., and Zamboni, D. Intrusion detection using autonomous agents. *Comput. Netw. 34* (October 2000), 547–570.

[17] Valeur, F., Vigna, G., Kruegel, C., and Kemmerer, R. A. A comprehensive approach to intrusion detection alert correlation. *IEEE Trans. Dependable Secur. Comput. 1* (July 2004), 146–169.

[18] Vigna, G., and Kemmerer, R. A. Netstat: A network-based intrusion detection system. *Journal of Computer Security 7* (1999), 37–71.

[19] Yang, X.-y., Gao, K., and Zhang, W.-g. Study of intrusion detection system based on improved bp neural networks. In *First International Workshop on Artificial Intelligence in Grid Computing* (New York, NY, USA, 2007), AIGC '07, ACM, pp. 5:1–5:4.