IDIDS: Un Sistema de Detección de Intrusos Distribuido Inteligente

Pablo Davicino[*,1,2] Marcela Capobianco [2] Javier Echaiz [1]

Laboratorio de Investigación en Sistemas Distribuidos (LISiDi) [1]
Laboratorio de Investigación y Desarrollo en Inteligencia Artificial (LIDIA) [2]
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
Bahía Blanca - Buenos Aires - Argentina
email:{pmd,mc,je}@cs.uns.edu.ar

Resumen

Un mecanismo de detección de intrusos permite identificar usos indebidos, accesos no autorizados o abusos, que puedan llegar a comprometer la integridad, confidencialidad o disponibilidad de un recurso computacional.

En la actualidad, 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. En este contexto, los Sistemas de Detección de Intrusos Distribuidos (DIDS) surgen como una herramienta clave para poder enfrentar las diversas y complejas problemáticas actuales.

El eje central de esta línea de investigación propone postular una nueva solución que permita resolver el acuciante problema de proveer un nivel de seguridad adecuado a partir de un sistema de detección de intrusos eficiente, inteligente, proactivo e inherentemente distribuido. A su vez, el desarrollo propuesto contempla el procesamiento eficiente de información de forma tal de filtrar falsos positivos y detectar de manera precisa alertas reales.

Palabras clave: seguridad, sistema de detección de intrusos, sistema de detección de intrusos distribuido, DIDS

[*]Becario del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)

Contexto

El trabajo objeto del presente artículo se desarrolla como un proyecto conjunto entre el Laboratorio de Investigación en Sistemas Distribuidos (LISiDi) y el Laboratorio de Investigación y Desarrollo en Inteligencia Artificial (LIDIA), ambos pertenecientes al Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur.

La línea de investigación presentada es parte de los Proyectos "Computación Distribuida de Alto Rendimiento y Disponibilidad"(24/N024) dirigido por el Mg. Ing. Jorge Ardenghi y codirigido por el Dr. Javier Echaiz, y "Requerimientos de Hardware y de Software en la implementación de un Sistema de Voto Electrónico Distribuido" (24/ZN23), dirigido por el Mg. Lic. Alejandro Stankevicius. 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 Sistema de Detección de Intrusos (IDS) corresponde a una herramienta que intenta proponer una solución al complejo problema de identificar accesos no autorizados, usos indebidos o abusos de recursos computacionales, perpetrados tanto por atacantes externos como por atacantes internos.

En la actualidad, la proliferación masiva de redes

de computadoras heterogéneas agrega un nivel de complejidad adicional al problema de detección de intrusos. La alta disponibilidad de conectividad, la cual se ha incrementado de forma siginificativa en los últimos años particularmente a partir del crecimiento vertiginoso de las redes inalámbricas, brindan mayores oportunidades de acceso a atacantes externos y facilita la evasión de la detección por parte de los intrusos.

En este contexto, los Sistemas de Detección de Intrusos se han convertido en una herramienta de seguridad cada vez más importante, principalmente en lo que respecta a prevenir eventos ilegales que podrían comprometer a un sistema. Un Sistema de Detección de Intrusos Distribuido (DIDS) [12] consiste en múltiples sensores IDS independientes interconectados mediante una red de comunicación. En este tipo de esquemas se deben tener en cuenta diversos aspectos críticos como el despliegue de los distintos sensores que componen el sistema, la detección de eventos ilegales, la generación y distribución de alertas, el procesamiento de información y la toma de decisiones inteligentes como respuesta a las amenazas.

Históricamente los sistemas de detección de intrusos han sido clasificados [1] en dos categorías: (1) detección por uso incorrecto y (2) detección por anomalías [5]. El primer modelo plantea la detección de intrusos mediante la comparación de los datos observados con despcripciones predefinidas de comportamiento intrusivo. Este enfoque es sumamente utilizado en productos comerciales pero posee un problema fundamental: las intrusiones son por lo general polimórficas y evolucionan constantemente, por lo que el mecanismo está sujeto a actualizaciones constantes de los patrones utilizados.

El segundo esquema se basa en la detección de un comportamiento anormal. Para esto se construyen modelos para el comportamiento esperado identificando patrones típicos de utilización. Todo patrón que represente una desviación de estos modelos es considerado anormal. Este tipo de esquema permite la detección de nuevos tipos de ataques, mediante la construcción de modelos adecuados. Sin embargo, la dificultad de este enfoque radica en identificar las fronteras entre el comportamiento normal y anormal por parte de los usuarios, lo que constituye un problema sumamente complejo de solucionar.

En la última década diversos acercamientos al problema se han realizado por medio de técnicas basadas en inteligencia computacional [20]. Dentro de este campo se han utilizado varias técnicas para implementar algoritmos de detección de intrusos, como redes neuronales [16, 18, 21], computación evolutiva [11, 15], machine learning [17], sistemas inmunológicos artificiales [19] y soft computing [2, 14].

Los enfoques basados en inteligencia computacional realizan una clasificación cuantitativa. Estas técnicas, si bien resultan adecuadas para muchos escenarios, son limitadas dado que no permiten explicar las razones que llevaron a realizar una determinada acción. En base a lo expuesto, resulta sumamente importante el desarrollo de nuevas técnicas inteligentes capaces de combinar un análisis cualitativo y cuantitativo de los patrones de comportamiento.

En las últimas décadas, la *argumentación rebatible* [7] evolucionó para convertirse en un mecanismo exitoso para modelar el razonamiento de sentido común cualitativo. En este sentido se cuentan la *programación en lógica rebatible* (PLR) [10] y sus especializaciones, la *programación en lógica rebatible probabilística* (PLRP) [4] y la *programación en lógica rebatible con observaciones* (PLRO) [3]. Estos sistemas de razonamiento se han aplicado con éxito a diversas áreas como *teorías de agencia*, *clustering* y *negociación*.

Creemos entonces que los diversos enfoques existentes no contemplan las necesidades actuales en lo que respecta a la problemática de detección de intrusos, dada su incapacidad de adaptarse a ataques cada vez mas complejos y dinámicos. Por esta razón, surge la necesidad de invertir esfuerzos de investigación para el desarrollo de un IDS inteligente que sea capaz de direccionar las problemáticas actuales. Para esto desarrollaremos sistemas innovadores que utilicen los enfoques de inteligencia computacional mencionados anteriormente, utilizando técnicas cuantitativas y cualitativas.

Líneas de investigación y desarrollo

Esta línea de investigación y desarrollo pretende continuar los trabajos presentados en [8, 9], explorando la incorporación de técnicas de *inteligencia artificial* a los mismos.

En particular, la *argumentación rebatible* ya ha sido utilizada en ArgueNet [6], para diseñar un sistema de recomendaciones que clasifique los resultados de búsqueda de acuerdo a un conjunto de criterios de preferencia especificados por el usuario. Este enfoque permite integrar de forma novedosa un motor de búsqueda tradicional con un framework argumentativo. La presente línea de I+D pretende dar continuidad a esta idea, con el objetivo de mejorar la clasificación realizada por los algoritmos tradicionales utilizados en los sistemas de detección de intrusos.

Como eje adicional, se está estudiando la aplicación de diversas técnicas propias del campo de bases de datos [13] al proceso de análisis, agregación y correlación de información. Se pretende que dichas técnicas puedan aportan relaciones no triviales entre los datos, que puedan modelar una alerta indicando la presencia de un riesgo potencial.

Resultados y objetivos

Esta línea de investigación y desarrollo espera conseguir resultados que tiendan a solucionar el problema referente a obtener un mecanismo de detección de intrusos inteligente, que pemita correlacionar la información obtenida por los diversos sensores que componen el sistema facilitando la administración del mismo. A su vez, se espera que el sistema pueda reaccionar de forma proactiva ante la presencia de ameanzas.

Los enfoques basados en inteligencia computacional realizan una clasicación cuantitativa. Estas técnicas, si bien resultan adecuadas para muchos escenarios, son limitadas, dado que no permiten explicar las razones que llevaron a realizar una determinada clasificación. En base a lo expuesto anteriormente, juzgamos que un paso importante para avanzar en el área del diseño e implementación de sistemas de detección de intrusos, es el desarrollo de nuevas técnicas inteligentes capaces de combinar un análisis cualitativo y cuantitativo de los patrones de comportamiento. En particular, se espera que el desarrollo contemple el agregado de las siguientes funcionalidades:

- Algoritmos de detección de intrusos basados en técnicas cualitativas.
- Algoritmos de detección de intrusos mixtos (basados en técnicas cualitativas combinadas con técnicas cuantitativas).
- Integración con componentes inteligentes como el sistema de la PLR y/o sus extensiones, la PLRO y la PLRP.

Con respecto al proceso de agregación y correlación de información, se han obtenido resultados positivos los cuales fueron publicados en [8]. Se espera mejorar dicho desarrollo a partir de la incorporación de algoritmos inteligentes y técnicas de minería de datos.

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 Doctoral del Ing. Pablo Davicino y se desarrolla en colaboración con el Laboratorio de Investigación y Desarrollo en Inteligencia Artificial (LIDIA).

A su vez, diversas tesinas de grado 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, abordan la temática referente a detección de intrusos, utilizando la presente línea de I+D como punto de referencia.

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 distintas tesinas 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.
- **Paradigmas de Computación Paralela y Distribuida.** Materia optativa para los estudiantes de las carreras Ingeniería en Sistemas de Computación y 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] Axelsson, S. Intrusion detection systems: A survey and taxonomy. Tech. rep., 2000.

[2] Balas, V. E., Fodor, J., and Vrkonyi-Kczy, A. R. *Soft Computing Based Modeling in Intelligent Systems*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[3] Capobianco, M., Chesñevar, C. I., and Simari, G. R. Argumentation and the dynamics of warranted beliefs in changing environments. *Journal of Autonomous Agents and Multiagent Systems 11* (2005), 127–151.

[4] Capobianco, M., and Simari, G. A proposal for making argumentation computationally capable of handling large repositories of uncertain data. In *Proceedings of the third international conference on scalable uncertainty management* (2009).

[5] Chebrolu, S., Abraham, A., and Thomas, J. Feature Deduction and Ensemble Design of Intrusion Detection Systems. *Computers and Security 24*, 4 (2005), 295–307.

[6] Chesñevar, C. I., and Maguitman, A. ArgueNet: An Argument-Based Recommender System for Solving Web Search Queries. In *Proc. of Intl. IEEE Conference on Intelligent Systems IS-2004. Varna, Bulgaria* (June 2004).

[7] Chesñevar, C. I., Maguitman, A. G., and Loui, R. P. Logical Models of Argument. *ACM Computing Surveys 32*, 4 (2000), 337–383.

[8] Davicino, P., Echaiz, J., and Ardenghi, J. A framework for implementing a distributed

intrusion detection system with interoperability and information analysis. *XVII Congreso Argentino de Ciencias de la Computación* (2011), 221–230.

[9] Davicino, P., Echaiz, J., and Ardenghi, J. Un enfoque proactivo basado en detección de intrusos distribuida (dids). *XIII Workshop de Investigadores en Ciencias de la Computación* (2011), 753–757.

[10] García, A., and Simari, G. Defeasible Logic Programming: An Argumentative Approach. *Theory and Practice of Logic Programming 4*, 1 (2004), 95–138.

[11] Gong, R. H., Zulkernine, M., and Abolmaesumi, P. A software implementation of a genetic algorithm based approach to network intrusion detection. In *Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks* (Washington, DC, USA, 2005), IEEE Computer Society, pp. 246–253.

[12] Huang, M.-Y., Jasper, R. J., and Wicks, T. M. A large scale distributed intrusion detection framework based on attack strategy analysis. *Computer Networks 31*, 2324 (1999), 2465 – 2475.

[13] 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.

[14] Melin, P., and Castillo, O. *Hybrid Intelligent Systems for Pattern Recognition Using Soft Computing: An Evolutionary Approach for Neural Networks and Fuzzy Systems*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[15] Pillai, M. M., Eloff, J. H. P., and Venter, H. S. An approach to implement a network intrusion detection system using genetic algorithms. In *Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (, Republic of South Africa, 2004), SAICSIT '04, South African Institute for Computer Scientists and Information Technologists, pp. 221–221.

[16] Ryan, J., jang Lin, M., and Miikkulainen, R. Intrusion detection with neural networks. In *ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS* (1998), MIT Press, pp. 943–949.

[17] Sinclair, C., Pierce, L., and Matzner, S. An application of machine learning to network intrusion detection. In *Proceedings of the 15th Annual Computer Security Applications Conference* (Washington, DC, USA, 1999), ACSAC '99, IEEE Computer Society, pp. 371–.

[18] Tan, K. The application of neural networks to unix computer security. In *In Proceedings of the IEEE International Conference on Neural Networks, Vol.1* (1995), IEEE Press, pp. 476–481.

[19] Williams, P. D., Anchor, K. P., Bebo, J. L., Gunsch, G. H., and Lamont, G. D. Cdis: Towards a computer immune system for detecting network intrusions. In *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection* (London, UK, 2001), RAID '00, Springer-Verlag, pp. 117–133.

[20] Wu, S. X., and Banzhaf, W. Review: The use of computational intelligence in intrusion detection systems: A review. *Appl. Soft Comput. 10*, 1 (2010), 1–35.

[21] 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.