Un Sistema para la Detección de Intrusos basado en Agentes Autónomos

M. Canderle, G. Aguirre, F. Piccoli *

Líneas Agentes Inteligentes y Paralelismo y Distribución del
Laboratorio de Investigación y Desarrollo en Inteligencia Computacional
Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950
5700 - San Luis
Argentina
e-mail: {mpiccoli}@unsl.edu.ar

Resumen

Ante el crecimiento de las redes, los sistemas de computación son más vulnerables a ataques de intrusos. Generalmente el objetivo de un intruso es violar los mecanismos de seguridad tradicionales, comprometiendo la integridad, confidencialidad o disponibilidad de los recursos del sistema atacado. La detección de intrusos en la red resulta, entonces, de vital importancia para asegurar la integridad de una red de computadoras y sus usuarios.

Existen numerosos enfoques para diseñar un sistema para la detección de Intrusos en una red, IDS. En este trabajo se presenta el esquema básico de un IDS aplicando técnicas de inteligencia artificial, como son los Sistemas Multi-Agente.

Palabras Claves: Intrusos, Seguridad de Redes, Sistemas de Detección de Intrusos, Agentes, Sistemas Multi-Agente.

1. Introducción

Una red de computadoras puede ser vulnerada y/o atacada de muchas formas distintas. Generalmente los ataque se producen por fallas en el software utilizado, por ejemplo en el protocolo de comunicación[1]. Proteger a las redes y los usuarios de intrusos resulta una tarea prioritaria. Las tecnologías para la detección de Intrusos en una red son diseñadas para monitorear todas las actividades en la red y determinar las violaciones a la seguridad.

*Grupo subvencionado por la UNSL y ANPCYT (Agencia Nacional para la Promoción de la Ciencia y Tecnología)

Establecer qué actividad se corresponde con una violación a la seguridad de una red, depende de la organización a la que pertenece la red, no existe un detector de intrusos *universal*, mientras los principios, objetivos y métodos de seguridad son estándares, la determinación de seguridad es diferente para cada organización[4]. Si bien existen muchas formas de vulnerar y atacar una red de computadoras o a una computadora particular, los ataques más comunes son: la búsqueda de servicios a través de la exploración de los puertos de una computadora de la red y el ingreso de intrusos en una red o un nodo de la misma con el objetivo de hacer mal uso de los sistemas de información a acceder[14].

Las arquitecturas que implementan sistemas de detección de intrusos fueron modificándose y mejorando con el paso del tiempo y con la experiencia adquirida. Los primeros IDS eran herramientas de software rígidos, diseñados y realizados bajo la supervisión de un experto en seguridad de redes y según su experiencia personal. Consistían de un único programa, el cual realizaba todo el trabajo de control, no se pensaba en un control distribuido.

Existen dos tipos de IDS, ellos son:

- *orientados a Host*, HIDS: trabajan con la información recogida por un host de la red. Para proteger cada dispositivo de la red es necesario tener un HIDS por cada uno.

- *orientados a Red*, NIDS: trabajan con los datos que circulan a través de la red. Funcionan como un *sniffer*, detectando ataques según el tráfico.

Las nuevas tendencias se basan en el desarrollo de IDS híbridos y distribuidos. Estos IDS son semejantes a los NIDS, los sensores están distribuidos en diferentes puntos de la red y envían las alertas a un sistema centralizado o no, quien los analiza, coordina y determina la defensa apropiada. El desarrollo de estos IDS se basan fundamentalmente en dos principios básicos[2][4][6][7][11][12][13][15]:

- La utilización de Agentes Autónomos, quienes recogen información por separado, la cual será analizada, una parte por los agentes y la otra por una entidad coordinadora.

- Las arquitecturas basadas en la exploración de los datos en tiempo real.

Este trabajo propone el desarrollo de un IDS híbrido basado en una arquitectura de agentes autónomos para redes Windows.

2. IDS-MAS

El sistema para la detección de Intrusos basado en Agentes Autónomos se caracteriza por tratar de evitar y subsanar las limitaciones de los IDS tradicionales: HIDS y NIDS.

Los sistemas multi-agente, MAS, poseen cualidades que los hacen especialmente adecuados para tratar con la detección de intrusos. Estos sistemas pueden lograr sus objetivos sin depender particularmente de alguna parte del software(agentes), consiguiéndose por la autonomía con que se desenvuelven los agentes componentes. Por ejemplo, se espera que los agentes puedan ingresar y salir libremente sin que se deteriore el funcionamiento general, además cada elemento puede ser depurado por separado y de antemano en entornos similares al real, en muchos casos cada uno suele realizar tareas simples pero gracias al intercambio de información con sus pares, en conjunto pueden lograr tareas mucho más complejas [5][16].

Los MAS poseen varias de las características requeridas en los IDS, entre ellas están:

- Pueden mantenerse funcionando constantemente. Algunas componentes pueden ser detenidas, por

ejemplo para su actualización, mientras tanto el resto de los agentes continúan trabajando para que el MAS siga brindando servicio.

- Control de la integridad. Cada agente puede ser regularmente controlado por algunos otros agentes, lográndose una verificación cruzada de la integridad de cada uno de los agentes componentes.

- Buena administración de recursos. Si los agentes están bien diseñados, requieren poco tiempo de procesador. Son activados para hacer una pequeña tarea y luego quedan inactivos.

- Fácilmente configurables. Los agentes pueden ser configurados mediante algunos parámetros según las características del host donde ejecutarán. Inclusive se pueden hacer cambios simples en el código para una configuración fina.

- Capaces de adaptarse a los cambios en el comportamiento. Incorporando en el agente capacidades de aprendizaje o de toma de decisiones, los agentes dinámicamente pueden adecuar su actividad a los cambios que se producen en el host. Además mediante el intercambio de información se pueden conseguir visiones y por lo tanto, adecuaciones, más generales.

- Escalabilidad. Nuevos agentes pueden ser incorporados en cada host para realizar nuevos controles sobre los recursos ya disponibles o para monitorear nuevos recursos. Incorporar nuevos agentes implica hacer crecer el IDS, esto implica un incremento de las comunicaciones entre los agentes y en la administración de la información generada. Este aspecto puede ser resuelto mediante una adecuada organización jerárquica de los agentes.

- Degradación adecuada de servicio. Si algún agente deja de funcionar se pierden solamente sus datos, los agentes dependientes de dichos datos deben tener prevista esta situación en su comportamiento y adecuarse a la nueva situación.

El trabajo propuesto es desarrollar un IDS basado en MAS. La implementación se realizará utilizando la plataforma JADE [8]. Dicha plataforma provee facilidades para garantizar la seguridad de los MAS. Estas facilidades están basadas en la tecnología de seguridad de JAVA para la autenticación y autorización de usuarios [9][10]. De manera similar a los sistemas operativos, los usuarios una vez acreditados serán responsables de otorgar acreditaciones a determinados agentes para usar los recursos creados.

$IDS - MAS$ aprovechará las ventajas brindadas por los MAS para la detección de intrusos en redes Windows. $IDS - MAS$ será un sistema de detección de intrusos dinámico, adaptivo, capaz de detectar posibles ataques a un nodo en particular de la red, HIDS, o a la red en sí, NIDS.

El trabajo se está desarrollando en etapas tendientes a la obtención de un IDS totalmente distribuido(recolección de información y control) y escalable. La arquitectura del sistema es mostrada en la figura 1

Como se puede observar, existirán varios niveles de agentes homogéneos por nivel. Los del nivel inferior serán responsables de la recolección de información. A partir del nivel 1, los agentes están encargados de analizar los datos suministrados por el nivel inferior y tomar decisiones. Actualmente se están desarrollando los agentes del nivel inferior, responsables de la recolección de la información.

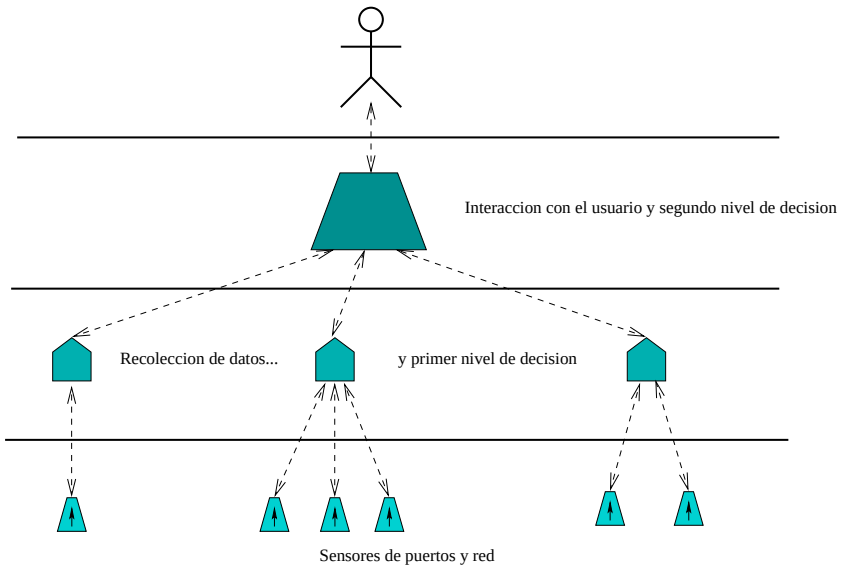

Figura 1: Arquitectura del MAS para IDS-MAS

3. Conclusiones

El desarrollo de un IDS a través de un MAS permitirá analizar la aplicabilidad de alternativas no convencionales de programación, además del desarrollo de $IDSs$ flexibles, distribuidos, híbridos y escalables. En el diseño de la herramienta deben considerarse muchos aspectos, no sólo relacionados a las redes, sino también a las características de los MAS: definición del lenguaje de los agentes, función de cada agente, comunicación entre agentes, entre otras.

En esta propuesta convergen, con un objetivo común, dos líneas de investigación: línea de Sistemas Distribuidos y Paralelos y línea de Agentes Inteligentes.

Referencias

[1] Comer, D. E.. *Computer Networks and Internet* - Second Edition - Prentice Hall - 1999 - ISBN: 0-13-083617-6

[2] Crosbie, M., Spafford, G.. *Active Defense of a Computer System using Autonomous Agents*. Technical Report N**?** 95-008. Purdue University. 1995.

[3] Crosbie, M., Spafford, E.. *Defending a computer system using autonomous agents*. 2003.

[4] Crothers, T.. *Implementing Intrusion Detection Systems*. Wiley. 2003.

[5] Ferber, J.. *Multi-agent systems*. Addison-Wesley. 1999.

[6] Frank, J.. *Artificial intelligence and intrusion detection:current and futere directions*. 1994.

[7] Frank, J.. *Artificial Intelligence and Intrusion Detection: Current and Future Directions*. Division of Computer Science. University of California.

[8] *JADE security guide*. JADE Board. 2005.

[9] *JAVA security overview*. White paper, 2005.

[10] *User authentication and authorization in JAVA plataform]*

[11] Koza, J. - Genetic Programming: On the Programming of Computers by means of Natural Selection. MIT Press. 1992.

[12] Kurmar, S., Spafford, G.. *A Pattern Matching model for Misuse Instrusion Detection*. Proceedings of the 17th National Computer Security Conference. October 1994.

[13] Maes, P.. *Modeling Adaptive Autonomous Agents*. Artificial Life, Vol 1, N**?** 1 / 2. MIT Press. 1993.

[14] Scambray, J. , McClure, S., Kurtz, G.. *HACKER: Secretos y soluciones para la Seguridad de Redes*. McGraw Hill. 2001.

[15] Spafford, E. H., Zamboni, D.. *Intrusion detection using autonomous agents*. 2003.

[16] Wooldridge, M.. *A Introduction to Multiagent systems*. Wiley. 2002.