Machine Learning aplicado en Sistemas de Detección de Intrusos

Ignacio Peluffo[1,*] Marcela Capobianco[1] Javier Echaiz[2]

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

Resumen

En los últimos años los delitos informáticos de distinta envergadura han aumentado de manera considerable. Es cada vez más común la vulneración de sistemas de modo que queden inutilizables, el robo de información sensible o los ataques a redes de computadoras o bases de datos. El incremento de transacciones electrónicas y el desarrollo de aplicaciones y servicios web es cada día más notorio, por lo que las organizaciones exponen gran parte de su infraestructura a Internet, creando un significativo riesgo de potenciales ataques que podrían comprometer datos o recursos estratégicos. Frente a este problema han surgido diferentes herramientas desde el campo de la seguridad en sistemas, pero todas enfrentan el problema de ser extremadamente dependientes de un experto humano para que analice la información que se recolecta sobre posibles ataques y tome medidas para mitigarlos.

Para solucionar este inconveniente surgió la idea de usar técnicas de minería de datos para analizar la información recolectada por el sistema. De esta forma se pueden desarrollar herramientas automáticas que mejoren la seguridad de los sistemas y/o herramientas que asistan al administrador en la toma de decisiones. En particular en esta línea de investigación nos concentraremos en el desarrollo de sistemas de detección de intrusos asistidos mediante técnicas de minería de datos.

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

Palabras clave: Minería de Datos, Machine Learning, Seguridad en Sistemas, Sistemas de Detección de Intrusos

1. Contexto

La línea de investigación que estamos reseñando se encuentra en desarrollo en el seno del *Laboratorio de Investigación y Desarrollo en Inteligencia Artificial* (LIDIA), situado en el Departamento de Ciencias e Ingeniería de la Computación (DCIC) de la Universidad Nacional del Sur (UNS). El LIDIA cuenta con un gran número de estudiantes graduados con tesis doctorales y de maestría tanto completas como en progreso.

El tema propuesto conecta las áreas de Inteligencia Artificial, Sistemas Distribuidos y Seguridad en Sistemas, por lo que se mantendrá una estrecha colaboración con el *Laboratorio de Investigación en Sistemas Distribuidos* (LISiDi) del Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur, en donde funciona un grupo de trabajo que realiza investigación en Sistemas Distribuidos y Seguridad en Sistemas.

2. Introducción

La Seguridad en Sistemas es una amplia disciplina que abarca cuestiones tanto teóricas como prácticas que en los últimos años ha tomado una importancia significativa en diferentes ámbitos que varían desde

la industria bancaria, pasando por grandes corporaciones multinacionales, hasta en la vida cotidiana de cualquier usuario de computadoras. Desafortunadamente, aun cuando se utilicen nuevas políticas y mecanismos para proteger la seguridad de los sistemas, cada vez más organizaciones son vulneradas por delitos informáticos de media y gran escala, debido al notable crecimiento del uso de sistemas informatizados y del acceso a Internet. En la actualidad los sistemas informáticos generan de manera automática un conjunto de registros (logs) que contienen datos sobre diferentes aspectos, como el comportamiento de los distintos usuarios, la operatoria de los programas y la evolución de las bases de datos del sistema, entre otros. Estos datos pueden ser analizados para descubrir diversos tipos de ataques a la seguridad del sistema, pero debido al gran volumen de datos generados esta tarea resulta más que desafiante y el resultado obtenido depende mayormente de la pericia del administrador. Es en este sentido que consideramos que es posible desarrollar herramientas que descubran en forma automática ataques y/o potenciales amenazas a la seguridad del sistema, asistiendo de esta manera a los administradores en su tarea, por medio de la aplicación de distintas técnicas de minería de datos. La Minería de Datos se puede definir sucintamente como el proceso de extraer información útil a partir de grandes volúmenes de datos. Este área de la ciencia de la computación se ha transformado hoy en día en un elemento clave en diversas aplicaciones desde hacer uso de información histórica para predecir el éxito de una campaña de mercadeo, pasando por reconocer patrones en transacciones financieras con el objeto de descubrir operaciones ilegales, hasta el análisis del secuenciamiento del genoma humano.

Los Sistemas de Detección de Intrusos (*Intrusion Detection System, IDS*) son una herramienta de creciente preponderancia dentro del campo de la seguridad en sistemas. De acuerdo al Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology, NIST*) la Detección de Intrusos es el proceso de monitorear eventos que ocurren en sistemas de computación o redes, y analizan dichos procesos para detectar signos de posibles *incidentes* como ser violaciones, inminentes amenazas de violación de políticas de seguridad o uso de recursos en forma abusiva [11]. Dada esta definición se desprende la de IDS que se define como un software que automatiza el proceso de detección de intrusos [11]. Con el avance en el desarrollo de distintas implementaciones de IDS, han surgido distintas maneras de recolectar información de donde alimentar a los mismos [11, 9], que se enumeran a continuación:

1. Basado en el Host: en este caso la información recolectada proviene del sistema en el cual se encuentra funcionando el IDS.

2. Basado en la Red: a diferencia del caso anterior, el IDS recolecta toda la información posible del tráfico de la red que se genera en el ambiente que se encuentra funcionando. Se recolecta información interna como información externa (conexiones entrantes y salientes).

A pesar de los beneficios que los IDS proveen para mejorar la seguridad en sistemas, éstos funcionan bajo la configuración de un conjunto de reglas estáticas que son determinadas por los administradores de los sistemas quienes deben encargarse de mantener y configurar apropiadamente los IDS para que la seguridad ante posibles ataques sea realmente eficaz. Un problema de este mantenimiento manual es que crear reglas contra ataques sofisticados pueden tomar horas o días y requerir de personal altamente calificado en el tema, ya que generar reglas de calidad baja podría causar una avalancha de advertencias de falsos ataques que a fin de cuentas los mismos administradores tendrán que analizar que se terminará traduciendo en una gran pérdida de tiempo. A consecuencia de lo antes mencionado, se han presentado distintas aproximaciones a resolver este problema [13, 18] aunque hasta ahora no se ha creado una propuesta madura para ser utilizada de manera comercial o en ambientes de gran escala.

Todos los esfuerzos para implementar un IDS que sea independiente de la intervención de humanos han llevado a la propuesta de aplicar técnicas de Machine Learning (ML), Minería de Datos (*Data Mining*, DM) y algoritmos de estadística con el fin de automatizar completamente la detección de ataques maliciosos distinguiendo a los mismos del uso "normal" de la red. El área de ML y DM ofrecen un amplio aba-

nico de técnicas sustentadas por una fuerte base de estudio alcanzada a lo largo de los años [19, 8].

Algo realmente interesante para el ámbito científico e industrial es que estas técnicas pueden ser aplicadas de manera efectiva para tratar problemas de un extensivo número de áreas [7, 17]. La flexibilidad de aplicación de ML y DM ha hecho posible que la aplicación en el área de Seguridad en Sistemas haya avanzado de manera sustancial [10, 5] obteniendo resultados realmente interesantes, por ejemplo detección de operaciones con tarjetas de crédito ilegítimas, defensa contra el cyber-terrorismo, detección de botnets y otros [16].

En el caso particular del área de IDS, se han realizado diversos avances de investigación sobre la aplicación de ML y DM para la implementación de los mismos usando las distintas técnicas como Árboles de Decisión, Reglas de Decisión, Redes Neuronales, Algoritmos Genéticos, Support Vector Machines, entre otras [4, 6, 14]. El refinamiento de este tipo de sistemas será una de las direcciones en que orientaremos nuestra investigación.

3. Líneas de Investigación, Desarrollo e Innovación

La presente línea de investigación tiene como finalidad analizar el problema de aplicar técnicas de machine learning y minería de datos en la implementación de sistemas de detección de intrusos que resulten aplicables en forma práctica a problemas del mundo real. Si bien existen muchas propuestas en la literatura relacionadas con esta problemática creemos que es posible mejorar la precisión de los resultados obtenidos mediante la de manera combinada de más de una técnica para una misma implementación. Nuestro objetivo es crear un IDS con un porcentaje mayor de acierto al momento de diferenciar comportamiento normal de malicioso, disminuir la tasa de falsos positivos y disminuir los tiempos de procesamiento del sistema.

Dadas las pruebas que existen en relación a utilizar técnicas en forma combinada [12, 3], se buscará una combinación de técnicas de ML que perfeccionen la capacidad de un IDS haciendo que éste sea capaz de aprender a detectar nuevas amenazas de manera automática.

Para llevar a cabo una primera etapa de experimentación usaremos un conjunto de datos, utilizado en trabajos anteriores de investigación, conocido como KDD Cup 99 Data Set [2] con el fin de poder hacer una comparación con los resultados con otros estudios. Además de este conjunto de datos, se considera utilizar una variante mejorada del mismo conocida como NSL-KDD Data Set [15]. Por último, y para probar la real efectividad del modelo creado, se intentará generar un conjunto de datos a partir de la recolección de datos reales obtenidos de la red. Además, se considerara utilizar una herramienta de software ampliamente conocida en el área de ML y DM llamada WEKA [1] la cual permitirá agilizar las pruebas y poder visualizar de manera rápida la efectividad de nuestras decisiones.

4. Resultados y Objetivos

El propósito principal de las investigaciones enmarcadas en esta línea de investigación es perfeccionar el estado del arte en lo concerniente sistemas de detección de intrusos basados en técnicas de machine learning y/o minería de datos. Nos proponemos satisfacer este objetivo general a través de la prosecución de los siguientes objetivos específicos:

1. Realizar una revisión bibliográfica a fin de determinar el estado del arte del área de minería de datos. En esta etapa se procurará el material bibliográfico necesario y se estudiará y analizará el mismo a fin de contar con una sólida base teórica que permita trabajar con soltura en este primer eje.

2. Realizar una revisión bibliográfica a fin de determinar el estado del arte del área de seguridad en sistemas. En esta etapa se procurará el material bibliográfico necesario y se estudiará y analizará el mismo a fin de contar con una sólida base teórica que permita trabajar con soltura en este segundo eje.

3. Tomar contacto con el área de investigación en el cual convergen estos dos ejes, esto es, la aplicación de técnicas de minería de datos a la seguridad en sistemas, con el objeto de analizar propuestas relacionadas que nos permitan orientar el trabajo de investigación a realizar. Identificar campos de aplicación en el contexto de la seguridad en sistemas en los cuales las técnicas de minería de datos existentes en la actualidad puedan ser perfeccionadas, proponiendo nuevos algoritmos que permitan refinar esas técnicas.

4. Implementar los algoritmos propuestos para validar las soluciones obtenidas mediante su aplicación a problemas de seguridad concretos en diversos entornos, a manera de verificación de las hipótesis planteadas por la presente investigación. La intención es realizar esta implementación tomando como punto de partida herramientas licenciadas como software libre, las cuales nos permiten acceder al código fuente. Esto posibilitará desarrollar prototipos a corto plazo a fin de concentrar el esfuerzo principalmente en el refinamiento de los algoritmos inteligentes.

5. Formación de Recursos Humanos

Esta línea de trabajo tiene el potencial de desempeñar un importante rol en la misión educativa de nuestra unidad académica. Las tareas asociadas al desarrollo de esta línea de investigación contribuyen a la formación de estudiantes de grado y posgrado y las mismas están integradas en el programa de materias del Departamento de Ciencias e Ingeniería de la Computación.

Por el momento esta línea de investigación formará parte del trabajo que está realizando un becario doctoral del conicet. Se anticipa que otros estudiantes de posgrado, y también de grado, se sumen a lo largo de su desarrollo.

Referencias

[1] Weka. "`http://www.cs.waikato.ac.nz/ml/weka/index.html`".

[2] Kdd cup 99. `https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html`, 1999.

[3] Atefi, K., Yahya, S., Dak, A. Y., and Atefi, A. A hybrid intrusion detection system based on different machine learning algorithms. *Proceedings of the 4th International Conference on Computing and Informatics, ICOCI 2013* (2013).

[4] Azad, C., and Jha, V. K. Data mining in intrusion detection: A comparative study of methods, types and data sets. *I.J. Information Technology and Computer Science* (2013).

[5] Barbará, D., and Jajodia, S. *Applications of Data Mining in Computer Security*. Advances in Information Security. Springer US, 2002.

[6] Bloedorn, E., Christiansen, A. D., Hill, W., Skorupka, C., Talbot, L. M., and Tivel, J. Data mining for network intrusion detection: How to get started. *Technical Report, MITRE* (2001).

[7] Chitra, K., and Subashini, B. Data mining techniques and its applications in banking sector. *International Journal of Emerging Technology and Advanced Engineering 3* (2013).

[8] Han, J., Kamber, M., and Pei, J. *Data Mining: Concepts and Techniques*, 3rd ed. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2011.

[9] Jaiganesh, V., Mangayarkarasi, S., and Sumathi, D. P. Intrusion detection systems: A survey and analysis of classification techniques. *International Journal of Advanced Research in Computer and Communication Engineering 2* (2013).

[10] Maloof, M. A. *Machine Learning and Data Mining for Computer Security: Methods and Applications (Advanced Information and Knowledge Processing)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.

[11] Scarfone, K., and Mell, P. Guide to intrusion detection and prevention systems (idps) - recommendations of the national institute of standards and technology. *NIST Special Publication 800-94* (2007).

[12] Sinclair, C., Pierce, L., and Matzner, S. An application of machine learning to network intrusion detection. In *ACSAC* (1999), IEEE Computer Society, pp. 371–377.

[13] Suarez-Tangil, G., Palomar, E., de Fuentes, J. M., Blasco, J., and Ribagorda, A. Automatic rule generation based on genetic programming for event correlation.

[14] S.V.Shirbhate, V.M.Thakare, and S.S.Sherekar. Data mining approaches for network intrusion detection system. *International Journal of Computer Technology and Electronics Engineering* (2011).

[15] Tavallaee, M., Bagheri, E., Lu, W., and Ghorbani, A. A. A detailed analysis of the kdd cup 99 data set. *Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009)* (2009).

[16] Thuraisingham, B., Khan, L., Masud, M. M., and Hamlen, K. W. Data mining for security applications. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (2008).

[17] Tzanis, G., Katakis, I., Partalas, I., and Vlahavas, I. Modern applications of machine learning. *Proceedings of the 1st Annual SEERC Doctoral Student Conference* (2006).

[18] Vollmer, T., Alves-Foss, J., and Manic, M. Autonomous rule creation for intrusion detection. *2011 IEEE Symposium on Computational Intelligence in Cyber Security* (2011).

[19] Witten, I. H., Frank, E., and Hall, M. A. *Data Mining: Practical Machine Learning Tools and Techniques*, 3 ed. Morgan Kaufmann, 2011.