Facultad de Ciencias de la Administración
UNER

ASI

Utilizando Argumentación Rebatible en la Detección de Intrusión en Sistemas Biométricos

Graciela R. Etchart[1], Juan C.L. Teze[1], Carlos E. Alvez[1], M. Vanina Martínez[2], Gerardo I. Simari[3]
[1]{graciela.etchart, carlos.alvez, carlos.teze}@uner.edu.ar, [2]mvmartinez@dc.uba.ar, [3]gis@cs.uns.edu.ar

Introducción

Hoy en día, las tecnologías biométricas representan un componente integral en sistemas de gestión de la identidad y de control de acceso. Sin embargo, los sistemas biométricos pueden recibir ataques externos o sufrir una intrusión en la información privada del usuario [1], causando problemas graves y persistentes, ya que los datos biométricos son irreemplazables. En la literatura se han descripto puntos de ataques potenciales en los sistemas biométricos [2-4]. El mayor número de esos puntos de vulnerabilidad involucran el tráfico de datos a través del canal de comunicación.

En el contexto de la seguridad en redes, los sistemas de detección de intrusos son una herramienta de creciente preponderancia. En relación a los procesos biométricos, la detección de intrusión puede ser utilizada como una capa de defensa contra los ataques que surgen en el canal de comunicación. En diferentes escenarios se han estudiado y aplicado con efectividad sistemas de detección de intrusión [5]. Sin embargo, la naturaleza dinámica del dominio donde se producen los ataques en ocasiones conduce a situaciones donde la información que se maneja es incompleta o potencialmente contradictoria. Este contexto constituye un escenario ideal para los sistemas argumentativos [6,7]. En inteligencia artificial, el área de argumentación computacional se especializa en modelar el proceso de razonamiento humano de manera tal de establecer qué conclusiones son aceptables en un contexto de desacuerdo. Este trabajo se centra en una arquitectura que extiende las capacidades de razonamiento de los sistemas biométricos incorporando argumentación al proceso de detección de intrusión. En la solución propuesta se utiliza el concepto formal de servidor de razonamiento en DeLP (DeLP-server) [8,9], cuyo mecanismo de inferencia se basa en el sistema argumentativo llamado Programación en Lógica Rebatible (DeLP, por sus siglas en inglés) [7].

Resultados y objetivos

Para supervisar la seguridad de la red en un sistema biométrico, se propone un framework que utiliza un DeLP-server. En el contexto de este trabajo, el proceso de argumentación llevado a cabo por el DeLP-server, filtra selectivamente información para el diagnóstico de ataques al canal de comunicación del sistema biométrico y para proporcionar una estructura que informe al analista acerca de una intrusión y posibles contramedidas a adoptar. Los primeros resultados de este trabajo fueron publicados recientemente en [10].

El framework propuesto consta de tres componentes (Figura 1). Uno de los componentes es el escáner (1 en la Figura 1); encargado de obtener y registrar información sobre el tráfico del canal de comunicación, analizando paquetes capturados en segmentos de red que conforman el sistema biométrico. Para la implementación de este componente se utiliza la herramienta open source *Snort*, la cual además de su tipo de licencia de uso, presenta como ventaja la posibilidad de configuración para obtener información ampliada de las alertas. Otro de los componentes del framework es el módulo para la obtención de hechos (2 en la Figura 1), que consiste en un módulo computacional específico para generar hechos que expresan observaciones de los datos registrados por el escáner. Estos hechos resumen los eventos anómalos que se producen en el canal de comunicación en un período de tiempo determinado. En el framework propuesto, este conjunto de hechos conforma el conocimiento para contextualizar el pedido de recomendación enviado al DeLP-server (3 en la Figura 1). En esta propuesta, el conocimiento público del DeLP-server está representado en una base de conocimiento mediante un programa DeLP con hechos y reglas que permiten detectar posibles ataques e indicar la contramedida que puede adoptarse frente a ellos. Para el armado de la base de conocimiento es necesaria la participación del experto humano en seguridad para identificar características de los ataques, y para considerar políticas generales de seguridad.

Actualmente, se están desarrollando algoritmos que permitan implementar el módulo computacional para la generación de los hechos que denoten observaciones sobre los datos registrados por el escáner.

Formación de Recursos Humanos

En la presente línea de investigación se enmarca el desarrollo de una tesis para la Maestría en Sistemas de la Información de la Universidad Nacional de Entre Ríos.

Líneas de Investigación y Desarrollo

Esta línea de investigación se enfoca sobre la problemática involucrada en la utilización de argumentación rebatible para la detección de intrusión. Diversas técnicas de inteligencia artificial se han utilizado para la detección y/o prevención de intrusión en redes de computadoras. En este contexto, cabe mencionar algunos trabajos que aplican argumentación en cuestiones relacionadas con la seguridad informática. En [11-14] se utiliza argumentación para el desarrollo de firewalls. En [15] los autores analizan la aplicación de un marco de argumentación abstracta para el análisis general de la seguridad de la red de un sistema. Por otra parte, en los trabajos [16,17] se utiliza la argumentación para abordar el problema de la atribución cibernética. Una propuesta preliminar para el desarrollo de un sistema de detección de intrusión basado en representación de conocimiento y razonamiento rebatible para un entorno de red LAN, se encuentra en [18]. El trabajo presentado en [19] considera el uso de argumentación para la correlación de alerta y el análisis de intrusión. En el presente trabajo se consideran principalmente los aportes de [18, 19] para aplicar el razonamiento basado en argumentación en la detección de ataque al canal de comunicación de sistemas biométricos.

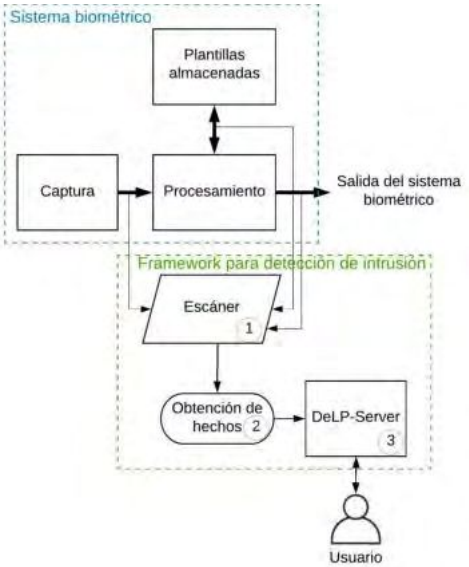

Figura 1: Componentes del framework.

Contexto

Este trabajo se da en el marco del Proyecto PID *"Modelos de Machine Learning para la mejora de la precisión, seguridad y eficiencia en la gestión de datos biométricos"*, que da continuidad a los Proyectos PID07/G035 "*Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos estatales*" y PID07/G044 "*Gestión de datos biométricos en base de datos objeto - relacionales*".

Además, este trabajo se realiza en el marco del desarrollo de una tesis para la Maestría en Sistemas de la Información de la Universidad Nacional de Entre Ríos.

Referencias

1. Rui, Z., and Yan, Z., "A Survey on Biometric Authentication: Towards Secure and Privacy-Preserving Identification". IEEE Access, 2019, 7, pp. 5994 – 6009.
2. Marcel, S., Nixon, M. S., and Li, S. Z., Eds., "Handbook of Biometric Anti-Spoofing - Trusted Biometrics under Spoofing Attacks". ser. Advances in Computer Vision and Pattern Recognition. Springer, 2014.
3. Galbally, J., Cappelli, R., Lumini, A., Gonzalez-de-Rivera, G., Maltoni, D., Fierrez, J., Ortega-Garcia, J., Maio, D., "An evaluation of direct attacks using fake fingers generated from ISO templates". Pattern Recognition Letters, Vol. 31, Issue 8, 2010, pp. 725-732.
4. Ratha, N., Connell, J., Bolle, R. "An analysis of minutiae matching strength". In Proc. AVBPA. LNCS, Vol. 2091. Springer, 2001, pp. 223–228.
5. Hamed, T., Ernst, J.B., Kremer, S.C. "A Survey and Taxonomy of Classifiers of Intrusion Detection Systems". In Daimi K. (eds) Computer and Network Security Essentials. Springer, Cham. 2018.
6. Simari, G.R. and Loui, R., "A mathematical treatment of defeasible reasoning and its implementation". Artificial Intelligence 53 (2–3). 1992, pp. 125–157.
7. García, A. and Simari, G.R., "Defeasible Logic Programming: An Argumentative Approach". Theory and Practice of Logic Programming 4(1). 2004, pp. 95–138.
8. García, A., Rotstein, N., Tucat, M. and Simari, G.R. "An argumentative reasoning service for deliberative agents". In KSEM, 2007. pp. 128–139.
9. García, A. and Simari, G.R., "Defeasible logic programming: Delpservers, contextual queries, and explanations for answers". Argument & Computation 5. 2014, pp. 63-88.
10. Etchart G., Teze J.C., Alvez C., Martínez M.V., Simari G.I., "Hacia la Detección de Intrusión en Sistemas Biométricos Utilizando Argumentación Rebatible". 8vo Congreso Nacional de Ingeniería Informática – Sistemas de Información (CoNaIISI). Universidad Tecnológica Nacional - Facultad Regional San Francisco – Argentina, noviembre de 2020.
11. Applebaum, A., Levitt, K., Rowe, J., and Parsons, S., "Arguing about firewall policy in COMMA". ser. Frontiers in Artificial Intelligence and Applications, Verheij, B., Szeider, S., and Woltran, S. (eds), Vol. 245. IOS Press, 2012, pp. 91–102.
12. Bandara, A., Kakas, A., Lupu, E., and Russo, A., "Using argumentation logic for firewall policy specification and analysis", in DSOM, ser. LNCS, R. State, S. van der Meer, D. O'Sullivan, and T. Pfeifer, Eds., Vol. 4269. Springer, 2006, pp. 185–196.
13. Bandara, A., Kakas, A., Lupu, E., and Russo, A., "Using argumentation logic for firewall configuration management". In Integrated Network Management. IEEE, 2009, pp. 180–187.
14. Rajkhowa, P., Hazarika, S.M., Simari, G.R. "An Application of Defeasible Logic Programming for Firewall Verification and Reconfiguration". In Singh, K., Awasthi, A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine, Vol 115. Springer, Berlin, Heidelberg, 2013.
15. Martinelli, F., Santini, F. and Yautsiukhin, A., "Network Security Supported by Arguments". 2015.
16. Shakarian, P., Simari, G.I., Moores, G., Parsons, S., and Falappa, M., "An Argumentation-based Framework to Address the Attribution Problem in Cyber-Warfare". Proceedings of the 3rd ASE International Conference on Cyber Security, 2014.
17. Nunes, E., Shakarian, P., Simari, G.I. and Ruef, A., "Argumentation models for cyber attribution", IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, 2016, pp. 837-844.
18. Guasco, L., Echaiz, J., and Ardenghi, J., "Framework para detección de intrusos usando DeLP". IX Workshop de Investigadores en Ciencias de la Computación, 2007.
19. Applebaum, A., Levitt, K., Li, Z., Parsons, S., Rowe, J., Sklar, E., "Cyber reasoning with argumentation: Abstracting from incomplete and contradictory evidence". MILCOM 2015 - IEEE Military Communications Conference, 2015, pp. 623-628.