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]*Facultad de Ciencias de la Administración, Universidad Nacional de Entre Ríos (UNER),*
[2]*Instituto de Investigación en Ciencias de la Computación, Universidad Nacional de Buenos Aires (UBA), Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET),*
[3]*Instituto de Ciencias e Ingeniería de la Computación (UNS-CONICET), Departamento de Ciencias e Ingeniería de la Computación, Universidad Nacional del Sur (UNS)*
[1]{graciela.etchart, carlos.alvez, carlos.teze}@uner.edu.ar, [2]mvmartinez@dc.uba.ar,
[3]gis@cs.uns.edu.ar

Resumen

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 son vulnerables a ataques que pueden comprometer su seguridad y privacidad. Para aumentar su seguridad, las técnicas de detección de intrusión son considerablemente útiles. En este trabajo se busca realizar la detección de ataques dirigidos al canal de comunicación utilizando argumentación rebatible con el propósito de proporcionar una estructura que favorezca una toma de decisiones de seguridad más informada. Se considera que el enfoque formal que brinda la argumentación complementará sustancialmente los sistemas de seguridad existentes en sistemas biométricos.

Palabras clave: Argumentación Rebatible, Sistemas Biométricos, Seguridad, Detección de intrusión

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*" [1, 2, 3].

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.

Introducción

En la actualidad, el acceso automático de las personas a los servicios es prácticamente una cuestión esencial. Esto ha dado lugar al desarrollo de diferentes métodos de autenticación. Un área tecnológica de relevancia en este sentido es conocida como reconocimiento biométrico o simplemente biometría [4]. El objetivo básico de la biometría es discriminar automáticamente entre sujetos - de forma fiable y según alguna aplicación- basándose en una o varias imágenes o señales derivadas de rasgos físicos o de comportamiento, como la huella dactilar, el rostro, el iris, la voz, la geometría de la mano o la firma escrita, entre otros.

Aunque el proceso biométrico presenta varias ventajas en la gestión de la identidad y en el control de acceso, es vulnerable a ataques que pueden disminuir su seguridad y comprometer la privacidad de los datos. Los sistemas de autenticación biométrica pueden recibir ataques

externos o sufrir una intrusión en la información privada del usuario [5], causando problemas graves y persistentes, ya que los datos biométricos son irreemplazables. En la literatura han sido descriptos puntos de ataques potenciales o puntos vulnerables en los sistemas biométricos [6-8]. El mayor número de esos puntos de vulnerabilidad involucran el tráfico de datos a través del canal de comunicación del sistema biométrico.

En el contexto de la seguridad en redes, los sistemas de detección de intrusos (IDS, por sus siglas en inglés) son una herramienta de creciente preponderancia. Según los datos de la auditoría, la detección de intrusión puede clasificarse como basada en *host* o basada en red. Un IDS basado en red analiza el tráfico del canal de comunicación, mientras que uno basado en *host* utiliza en su análisis de registros del sistema operativo o de las aplicaciones. Por otro lado, según la técnica de detección empleada, un IDS puede ser clasificado como sistema de detección de anomalías o sistema de detección de mal uso. 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. Si se detecta la intrusión, se puede iniciar una advertencia para prevenir o minimizar los daños que pueda sufrir el sistema. En diferentes escenarios se han estudiado y aplicado con efectividad sistemas de detección de intrusión [9]. 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 [10, 11]. El mecanismo de inferencia sobre el cual están basados, permite decidir entre conclusiones contradictorias y adaptarse fácilmente a entornos cambiantes.

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. En el marco de este trabajo, este proceso de razonamiento permite filtrar selectivamente información para detectar amenazas a la seguridad de los sistemas biométricos, sugerir acciones y acelerar la respuesta ante acontecimientos complejos como la presencia de una posible intrusión. 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) [12, 13], cuyo mecanismo de inferencia se base en el sistema argumentativo llamado Programación en Lógica Rebatible (DeLP, por sus siglas en inglés) [11]. Una consulta para un DeLP-server es un par (Co, L) donde L es una consulta DeLP y Co es el contexto para la consulta. El contexto puede ser cualquier programa DeLP. Un sistema basado en reglas como DeLP constituye una herramienta para el soporte a la toma de decisiones que brinda la posibilidad de explicar a los analistas humanos por qué se recomienda una acción y no otra. Además, este tipo de sistemas resulta adecuado para funcionar con un esquema "*human-in-the-loop*", donde los analistas humanos brindan retroalimentación que permite validar o rectificar los resultados del sistema.

Línea 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 [14-17] se utiliza argumentación para el desarrollo de

firewalls. En [18] 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 [19, 20] 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 [21]. El trabajo presentado en [22] 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 [21, 22] para aplicar el razonamiento basado en argumentación en la detección de ataque al canal de comunicación de sistemas biométricos.

Resultados y objetivos

Para supervisar la seguridad de la red en un sistema biométrico, se propone un framework que utiliza un DeLP-server. Los primeros resultados de este trabajo fueron publicados recientemente en [23]. Como se mencionó anteriormente, los servicios de razonamiento basados en DeLP, tienen la capacidad de representar conocimiento y responder consultas contextuales. En el framework propuesto, el contexto es información sobre alertas de intrusión al canal de comunicación del sistema biométrico.

El enfoque formal proporcionado por la argumentación rebatible permite manejar la inconsistencia de los datos que deben utilizarse en la toma de decisiones y extraer un conjunto coherente de reglas que puedan aplicarse para llegar a una decisión. Además, los argumentos que se construyen permiten explicar al responsable de la toma de decisiones humana los resultados del razonamiento, de manera que se aclare la situación y se mejore la calidad de las decisiones. 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.

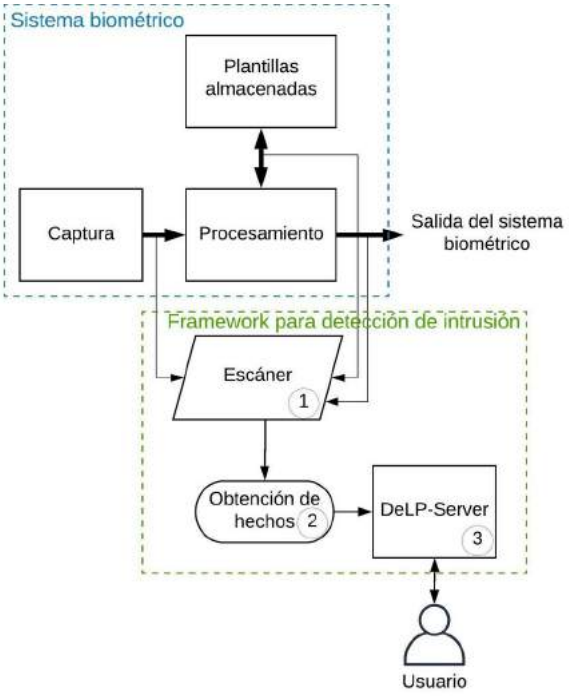

Figura 1. Componentes del framework.

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*[1], 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

[1] https://www.snort.org/

anómalos que se producen en el canal de comunicación en un período de tiempo determinado. En el framework propuesto, este conjunto de hechos luego conformará el conocimiento para contextualizar el pedido de recomendación que reciba el 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 que pueden realizarse sobre el canal de comunicación del sistema biométrico, 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.

Referencias

1 Alvez C., Etchart G., Ruiz S., Miranda E. and Aguirre J., "Extensión de una base de datos Objeto-Relacional para el soporte de datos de iris". XXIII Congreso Argentino de Ciencias de la Computación. Universidad Nacional de La Plata– Argentina, 2017.

2 Ruiz S., Etchart G., Alvez C., Miranda E., Benedetto M. and Aguirre J., "Iris Information Management in Object-Relational Databases". XXI Congreso Argentino de Ciencias de la Computación. Universidad Nacional del Noroeste de la Provincia de Buenos Aires, Junín - Argentina, 2015.

3 Etchart G., Luna L., Leal R., Benedetto M. and Alvez C., "Sistema adecuado a estándares de reconocimiento de personas mediante el iris". CGIV - XIV Workshop de Investigadores en Ciencias de la Computación, Universidad Nacional de Entre Ríos, Concordia - Argentina, 2012.

4 Alvez C., Benedetto M., Berón G., Etchart G., Luna L. y Leal C., "Desarrollo de un sistema multi-biométrico mediante reconocimiento de iris y voz, adecuado a estándares, para su aplicación en organismos públicos". SIE 2011 – Simposio de Informática en el Estado. Córdoba, 31 de agosto, 01 y 02 de septiembre de 2011. 40° JAIIO. pp. 206 - 220.

5 Rui, Z., and Yan, Z., "A Survey on Biometric Authentication: Towards Secure and Privacy-Preserving Identification". IEEE Access, 2019, 7, pp. 5994 – 6009.

6 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.

7 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.

8 Ratha, N., Connell, J., Bolle, R. "An analysis of minutiae matching strength". In Proc. AVBPA. LNCS, Vol. 2091. Springer, 2001, pp. 223–228.

9 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.

10 Simari, G.R. and Loui, R., "A mathematical treatment of defeasible reasoning and its implementation". Artificial Intelligence 53 (2–3). 1992, pp. 125–157.

11 García, A. and Simari, G.R., "Defeasible Logic Programming: An Argumentative Approach". Theory and Practice of Logic Programming 4(1). 2004, pp. 95–138.

12 García, A., Rotstein, N., Tucat, M. and Simari, G.R. "An argumentative reasoning service for deliberative agents". In KSEM, 2007, pp. 128–139.

13 García, A. and Simari, G.R., "Defeasible logic programming: Delpservers, contextual queries,

and explanations for answers". Argument & Computation 5. 2014, pp. 63-88.

14 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.

15 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.

16 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.

17 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.

18 Martinelli, F., Santini, F. and Yautsiukhin, A., "Network Security Supported by Arguments". 2015.

19 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.

20 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.

21 Guasco, L., Echaiz, J., and Ardenghi, J., "Framework para detección de intrusos usando DeLP". IX Workshop de Investigadores en Ciencias de la Computación, 2007.

22 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.

23 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.