CACiC 2023
CONGRESO ARGENTINO DE CIENCIAS DE LA COMPUTACIÓN

Utilizando Argumentación Rebatible en la Detección y Respuesta ante Intrusión en Sistemas Biométricos

Graciela R. Etchart[1], Juan C.L. Teze[1], Carlos E. Alvez[1],
María V. Martinez[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

Abstract. En las últimas décadas, la comunidad biométrica ha investigado la seguridad de los sistemas de reconocimiento biométrico identificando puntos de ataques potenciales, estudiando posibles amenazas y proponiendo contramedidas para superarlas. En este sentido, diversos trabajos apuntan a resolver situaciones de ataques dirigidos a la plantilla (o *template*) biométrica. En menor medida, se han encontrado propuestas orientadas a la detección y mitigación de intrusiones en el canal de comunicación del sistema biométrico. Para aumentar la seguridad en este punto, las técnicas de detección de intrusión son considerablemente útiles. En este trabajo se busca realizar la detección y respuesta ante ataques 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.

Keywords: Argumentación, Detección de intrusión, Sistemas biométricos.

1. Introducción

Los sistemas biométricos tienen varias ventajas con respecto a los métodos de autenticación tradicionales. Sin embargo, son vulnerables a ataques que pueden comprometer su seguridad y privacidad [1]. Varios trabajos han identificado y caracterizado puntos de ataques potenciales en los sistemas biométricos [2, 3]. Los puntos vulnerables se pueden agrupar en: ataques dirigidos hacia los equipos físicos y ataques orientados al canal de comunicación. En la literatura se han propuesto diferentes contramedidas para evitar o minimizar los riesgos derivados de los ataques de adversarios. Diversos trabajos apuntan a resolver situaciones de ataques dirigidos a la plantilla (o *template*) biométrica. En menor medida, se han encontrado propuestas dirigidas a la detección y mitigación de intrusión en el canal de comunicación del sistema biométrico.

Dentro del campo de la seguridad en redes, los sistemas detectores de intrusión (IDS, por sus siglas en inglés) son una herramienta de creciente preponderancia [4]. Estos sistemas procuran hallar acciones que puedan comprometer la confidencialidad, la integridad o la disponibilidad de un recurso. Los IDSs desde sus inicios han sido

objeto de una constante revisión y evolución. 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 y recomendar medidas para prevenir o minimizar los daños en el sistema.

Aunque numerosos IDSs han sido estudiados y efectivamente aplicados en diferentes escenarios de la vida real [5-6], la naturaleza dinámica del dominio en donde se producen los ataques en ocasiones conduce a situaciones de información en conflicto, principalmente cuando se razona en presencia de información incompleta y potencialmente contradictoria. En este escenario, los sistemas argumentativos [7, 8] pueden verse como una alternativa útil para hacer frente a estas cuestiones. 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 qué típicamente realizan las personas cuando buscan establecer qué conclusiones son aceptables en un contexto de desacuerdo. En el marco de este trabajo, el proceso de razonamiento permite filtrar selectivamente información para detectar amenazas, sugerir acciones y acelerar la respuesta ante la presencia de una posible intrusión.

2. Aportes realizados

Este trabajo se centra en introducir una arquitectura que extiende las capacidades de razonamiento de los sistemas biométricos incorporando argumentación al proceso de y respuesta a intrusiones. En la solución propuesta se utiliza un servicio de razonamiento basado en argumentación, para representar el conocimiento e inferir la acción de respuesta adecuada frente a una intrusión detectada en el canal de comunicación de un sistema biométrico, procurando minimizar el impacto del ataque en el funcionamiento habitual del sistema.

A continuación, se presenta el diseño arquitectónico del Sistema de Respuesta a Intrusión Basado en Argumentación (SRIBA) propuesto y una descripción de las operaciones del mismo, recurriendo a los formalismos Unified Modeling Language (UML) y modelo C4 de visualización de arquitectura de software[1]. El SRIBA presenta una arquitectura modular donde se pueden identificar tres contenedores bien diferenciados: el Escáner, el Gestor de Consulta Contextual (GCC) y el Razonador. En la Figura 1 se brinda una vista a alto nivel del sistema y se especifica el sistema externo con el cual interactúa el SRIBA (en este caso, el sistema biométrico). También se identifica la interacción con el usuario final que hará uso de la funcionalidad del sistema.

El Escáner es el responsable de obtener y registrar información del canal de comunicación monitorizado, analizando paquetes capturados en segmentos de red que conforman el sistema biométrico y detectando intrusiones al mismo. Uno de los componentes del Escáner es un sistema de detección de intrusión de uso indebido

[1] https://c4model.com/

basado en red, capaz de detectar accesos no autorizados utilizando un conjunto de reglas predeterminadas, y emitir alertas de posibles intrusiones.

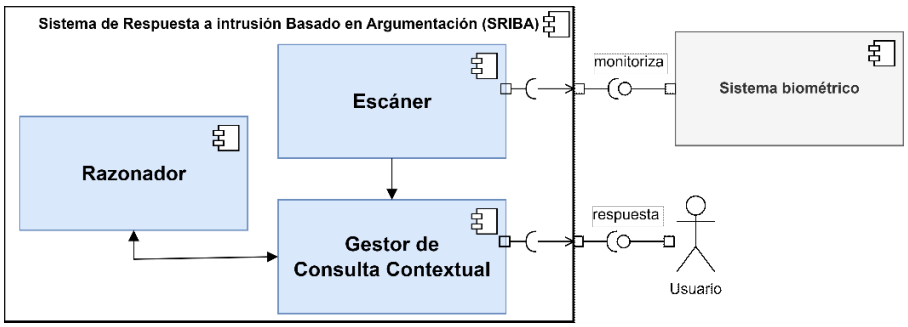

Fig. 1. Arquitectura del SRIBA

Por otro lado, el GCC tiene como responsabilidad procesar la información obtenida por el Escáner y generar hechos que expresan observaciones de los datos contenidos en las alertas. Estos hechos conforman el contexto enviado al componente razonador junto a la consulta. Una vez recibida la respuesta, el GCC la despliega al usuario del sistema.

En último lugar, el Razonador es la parte central de la arquitectura. Esta componente brinda un servicio de razonamiento argumentativo. Una propuesta para su implementación se enfoca en un sistema argumentativo en particular, denominado Programación en Lógica Rebatible (DeLP, por sus siglas en inglés) [9]. DeLP combina resultados de programación en lógica y argumentación rebatible, y posee flexibilidad en cuanto a su aplicación en diferentes dominios, con el propósito de proporcionar una estructura que favorezca una toma de decisiones de seguridad más informada. La argumentación rebatible proporciona un enfoque formal para manejar la inconsistencia de los datos que deben utilizarse en la toma de decisiones y permite extraer un conjunto coherente de reglas que puedan aplicarse para llegar a una decisión. Además, los argumentos que se construyen permiten explicar los resultados del razonamiento a los responsables de la toma de decisiones humanas, de manera que se aclare la situación y se mejore la calidad de las decisiones.

Como prueba de concepto para favorecer la comprensión del funcionamiento del Razonador, se realizan dos instanciaciones utilizando formalismos concretos para representar el conocimiento, las consultas y las respuestas. Para una instanciación se utiliza el concepto formal de servidor de razonamiento en Programación en Lógica Rebatible o DeLP-Servers [10, 11]. Los DeLP-Servers presentan un enfoque cliente-servidor caracterizado por permitir representar información o conocimiento público y responder consultas utilizando dicho conocimiento público junto con información privada provista por el cliente. De esta manera, el Razonador procesa la consulta recibida utilizando el contexto brindado por el GCC y, mediante un proceso argumentativo, brinda como respuesta la contramedida para contrarrestar los efectos de una intrusión detectada. Por otra parte, con el propósito de posibilitar la toma de decisiones multicriterio para la selección de la contramedida a desplegar frente a una intrusión, se instancia el proceso de razonamiento siguiendo un formalismo basado en reglas condicionales introducido por Burón Brarda et al. [12], el cual permite codificar

las preferencias entre criterios de comparación de acciones de respuestas en términos de requisitos y valores de tolerancia. En otras palabras, esta instanciación permite llevar a cabo el proceso de elección de la contramedida adecuada a partir de un proceso de decisión multicriterio basado en argumentación. De esta manera, es posible dar prioridad a aquellos atributos que mejor definen una recomendación relevante, en función de las políticas de seguridad que se deseen aplicar y diversas alternativas de acciones de respuesta. Una característica común en ambos formalismos y de gran relevancia, es que las conclusiones obtenidas pueden explicarse fácilmente mediante el proceso de razonamiento argumentativo, el cual permite ofrecer explicaciones como conjuntos coherentes de razones a favor o en contra de la acción de respuesta recomendada. De esta manera, se favorece una toma de decisión de seguridad más informada.

Finalmente, como se mencionó con anterioridad, en el SRIBA el Escáner opera mediante un sistema detector de intrusión basado en uso indebido. En este tipo de sistemas el costo de desarrollo y mantenimiento de los conjuntos de reglas constituye un importante problema. Con el propósito de mejorar la actualización de la base de datos de reglas para la detección (firmas) de esta componente, se realizó un estudio preliminar sobre distintas herramientas de aprendizaje automático. La motivación fue dar unos primeros pasos para proponer una solución aceptable para generar firmas orientadas a la detección personalizadas para el sistema biométrico. En esta tarea se estudió SIRUS (Stable and Interpretable RUle Set[2]), un nuevo algoritmo de reglas para la clasificación. Este algoritmo brinda un nivel útil de interpretabilidad en los modelos que genera, necesario para su traducción a una firma entendible por el sistema detector de intrusión.

3. Posibles líneas de investigación a futuro

En el contexto de esta investigación los resultados son preliminares pero promisorios en cuanto a su aplicación efectiva en el contexto de aplicación en el mundo real. La arquitectura presentada constituye una propuesta a alto nivel, perfectible en trabajos posteriores. Además, se considera que esta propuesta supone un avance para conseguir un proceso de reconocimiento más seguro y una toma de decisiones sobre seguridad más informada; sin embargo, la investigación debe seguir persiguiendo garantizar la confidencialidad, la integridad y la disponibilidad de un sistema biométrico.

El SRIBA parte de una arquitectura general que puede ser modularizada e implementada de diversas maneras. Además, este enfoque puede aplicarse también a otros sistemas tecnológicos, y su utilidad no se limita a los sistemas biométricos.

En la búsqueda de soluciones y mejoras a las diferentes cuestiones planteadas, han surgido nuevas ideas e inquietudes que constituyen algunas líneas de investigación. Uno de estos trabajos futuros consiste en estudiar cómo aprovechar los conceptos propuestos para desarrollar aplicaciones con otros formalismos de razonamiento, como podría ser ontologías. Otra tarea consiste en lograr un comportamiento proactivo en el

[2] https://cran.r-project.org/web/packages/sirus/

SRIBA. Para esto es necesario utilizar algoritmos de predicción de ataques de tal manera que el sistema de respuesta pueda ejecutar la acción de respuesta frente a una intrusión antes que ésta se lleve a cabo. Una vez que el tipo de ataque ha sido predicho, la inferencia de la respuesta adecuada se realizaría siguiendo el proceso de razonamiento propuesto en este trabajo. También, es posible profundizar el estudio de métricas de seguridad y de metodologías utilizadas para su obtención, a fin de ampliar la arquitectura propuesta con módulos que gestionen la obtención de dichas métricas.

Referencias

1. Rui, Z., and Yan, Z.: A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. IEEE Access, 7, 5994-6009 (2019).
2. Ratha, N., Connell, J., and Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40, 614-634 (2001).
3. Jain, R., and Kant, C.: Attacks on Biometric Systems: An Overview. International Journal of Advances in Scientific Research, 1, 283-288 (2015).
4. 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).
5. Hamed, T., Ernst, J.B., and Kremer, S.C.: A Survey and Taxonomy of Classifiers of Intrusion Detection Systems. In Daimi K. (eds) Computer and Network Security Essentials. Springer, Cham, 21-39 (2018).
6. Ozkan-Okay, M., Samet, R., Aslan, Ö., and Gupta, D.: A Comprehensive Systematic Literature Review on Intrusion Detection Systems. In IEEE Access, 9, 157727-157760 (2021).
7. Paredes J., Simari G.I., Martinez M.V., Falappa, M.: Detecting malicious behavior in social platforms via hybrid knowledge- and data-driven systems, Future Generation Computer Systems, 125, 232-246 (2021)
8. Leiva, M., García, A., Shakarian, P. and Simari, G.I.: Argumentation-Based Query Answering under Uncertainty with Application to Cybersecurity. Big Data Cogn. Comput., 6, 91 (2022).
9. García, A. and Simari, G.R.: Defeasible logic programming: An argumentative approach. Theory and Practice of Logic Programming (TPLP), 4, 95-138 (2004).
10. García, A., Rotstein, N.D., Tucat, M., and Simari, G.R.: An Argumentative Reasoning Service for Deliberative Agents. In Zhang, Z., Siekmann, J. (eds) Knowledge Science, Engineering and Management. KSEM 2007. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 4798, 128-139 (2007).
11. Tucat, M.: Grupos de Servicios de Razonamiento para el Procesamiento de Consultas Contextuales en Paralelo. PhD thesis, Universidad Nacional del Sur, Bahía Blanca, Argentina. (2011).
12. Burón Brarda, M.E., Tamargo, L.H., and García, A.: An approach to enhance argument-based multi-criteria decision systems with conditional preferences and explainable answers. Expert Systems with Applications, 126, 171-186 (2019).