Auto-protección de aplicaciones y su uso en sistemas SCADA en infraestructuras críticas: un mapeo sistemático de la literatura

Daniel Manrique, Carlos Neil, Jorge Kamlofsky

Universidad Abierta Interamericana, Facultad de Tecnología Informática,
Centro de Altos Estudios en Tecnología Informática, Buenos Aires, Argentina
Danielarnaldo.manrique@alumnos.uai.edu.ar
Carlos.Neil@uai.edu.ar
Jorge.kamlofsky@uai.edu.ar

Resumen. *Contexto*: Los sistemas industriales se enfrentan a un número cada vez mayor de amenazas a la ciberseguridad, especialmente con el auge de la Industria 4.0 y la integración de protocolos de comunicación. Como resultado, la protección de sistemas industriales críticos y líneas de producción contra amenazas cibernéticas se ha convertido en una preocupación cada vez mayor. *Objetivos*: es evidente que el desarrollo y la implementación de mecanismos de autoprotección para sistemas industriales desempeñan un papel crucial para garantizar la seguridad y confiabilidad de la infraestructura crítica, es por ello que este trabajo muestra y analiza los resultados obtenidos al realizar un mapeo sistemático de la literatura sobre tecnologías de auto-protección de aplicaciones, su uso en sistemas SCADA (Supervisory Control and Data Acquisition) en infraestructuras críticas y la utilización de la tecnología RASP (Runtime Application Self-protection) en entornos industriales. *Método*: se detalla la creación y ejecución de un protocolo que establece un conjunto de preguntas a responder y el procedimiento para la búsqueda, y posteriormente la aplicación de filtros para la selección de artículos. Finalmente, se procede al análisis para poder responder a las preguntas planteadas. *Resultados*: se puede observar que las tecnologías denominadas de auto-protección usadas ampliamente en los entornos IT pueden ser llevadas a los entornos OT, de allí que soluciones como los sistemas de detección de intrusiones (IDS), firewall de aplicaciones web (WAF) o la protección de ejecución de software en memoria pueden ser usadas en ambos entornos. *Conclusiones*: Si bien ya se han implementados diversos tipos de tecnologías de auto-protección en entornos industriales, no se pudo evidenciar en los artículos analizados que la tecnología RASP sea usada utilizada en los mismos.

Keywords: auto-protección, ics, rasp, scada, runtime application self-protection.

1 Antecedentes

Debido a que las amenazas a las infraestructuras criticas van cambiando del mundo físico al mundo cibernético, apoyándose en el uso cada vez más frecuente de las tecno-logías de la información para la provisión de servicios esenciales, su dependencia energética e interconexión, hace necesaria una revisión de todo el marco de gestión de seguridad que protegen a dichas infraestructuras a fin de generar protocolos acordes a las nuevas amenazas (Figueredo et al., 2021). Estos ciberataques son dirigidos a vulnerabilidades a las que antes estos sistemas críticos no estaban expuestos, previo a la convergencia con las redes IT (Kamlofsky et al., 2019)

A su vez, teniendo en cuenta que los sistemas SCADA son una parte importante de los procesos industriales, y una afección en su funcionamiento seria de un impacto muy alto a los servicios esenciales de las comunidades, se hace imprescindible tomar todas las acciones posibles de seguridad para protegerlos y mantenerlos asegurados (Anabalón & Donders, 2014).

La necesidad de proteger aplicaciones contra ataques en tiempo de ejecución ha llevado al desarrollo de sistemas de protección automática que detectan y mitigan amenazas sin intervención humana. Estos sistemas se enfocan en defender las aplicaciones desde su interior, reconociendo comportamientos erróneos y protegiendo contra ataques comunes. En el ámbito de la detección de intrusiones industrial, las infraestructuras de control, como los sistemas SCADA, son fundamentales para mantener operaciones continuas (Q. Chen & Abdelwahed, 2014).

En resumen, la seguridad de las aplicaciones ha evolucionado para enfrentar desafíos cada vez más sofisticados, abordando amenazas en tiempo de ejecución, adaptándose a entornos cambiantes y protegiendo datos críticos en diferentes contextos, desde la web hasta el IoT y la industria. Anteriormente se realizaron aportes en esta línea a través de estudios de las arquitecturas de ciberseguridad centradas en soluciones usadas en las redes TI y trasladadas a redes OT (Kamlofsky et al., 2016)

2 Preguntas de investigación

Uno de los puntos más importantes de un mapeo sistemático es la lectura crítica del material seleccionado. Este análisis será direccionado por las siguientes preguntas de investigación:

Tabla 1. Preguntas guía del mapeo

PREGUNTAS DE INVESTIGACIÓN	MOTIVACIÓN
P1. ¿Qué trabajos identificaron previamente la tecnología de auto protección de aplicaciones como solución para la defensa ante ciberataques?	M1. Conocer el avance en el que se encuentra la utilización de esta tecnología.

P2. ¿Cuáles son las tecnologías de auto protección de aplicaciones que se están utilizando?	M2. Detectar cuales son las tecnologías más usadas para protección de las aplicaciones.
P3. ¿En qué tipo de industria se están utilizando?	M3. Poder entender que industria es la más madura en la utilización de esta tecnología.
P4. ¿RASP es una tecnología de auto protección usada para resguardar sistemas industriales?	M4. Identificar el nivel de adopción de esta tecnología en entornos OT.
P5. ¿Cuáles son los componentes de los ICS en los que se desplego RASP?	M5. Identificar los componentes candidatos para la integración de RASP con los ICS.

3 Métodos de revisión

En esta sección se utiliza el método propuesto por (Kitchenham et al., 2009) para realizar un mapeo sistemático de la literatura. Estableciendo un protocolo para la búsqueda y selección de artículos. Se realizan tres pasos básicos. Selección de bases de datos para la búsqueda de trabajos, detallada en la sección "Fuentes". Definición de una cadena de búsqueda en la sección "Definición de términos" y la selección de criterios de inclusión y exclusión utilizados para el filtrado de los artículos que se detalla en el apartado "Criterios de inclusión y exclusión".

3.1 Fuentes

Para obtener los artículos necesarios para este mapeo sistemático de la literatura se utilizaron repositorios o fuentes electrónicas masivas, es decir bases de datos que exponen documentos de diversos temas de investigación. La selección se basa en aquellos repositorios más populares y mayormente poblados de artículos para analizar:

IEEE Xplore Digital Library
ACM Digital Library
ResearchGate
Google Académico
Science Direct

3.2 Definición de términos

Siguiendo la metodología propuesta por (Kitchenham et al., 2009), se definió una cadena de búsqueda basándonos en dos elementos: la tecnologia de autoproteccion y el tipo de plataforma. Por lo que se obtuvo lo siguiente:

("application" AND "self-protection")

Al no producir los resultados esperados, debió refinarse la búsuqeda para que los artículos obtenidos sean más específicos del tema investigado. Para esto se definieron 4 términos principales y luego términos alternativos para cada uno de ellos.

Tabla 2. Términos utilizados para la búsqueda.

TÉRMINOS PRINCIPALES	TÉRMINOS ALTERNATIVOS
runtime application	rasp
	application security
critical infrastructure	Scada
	critical infrastructure protection
industrial control system	Ics
	industrial control system security
Protection	self protection

Utilizando estos términos alternativos, se pudo ampliar la cadena de búsqueda con nuevos criterios y, a la vez, con el conector lógico OR se concatenaron a los ya existentes. Las cadenas quedaron formuladas de la siguiente forma:

Tabla 3. Cadenas de búsqueda.

("runtime application" AND "protection")
("critical infrastructure" OR "industrial control system" AND "self protection")
("application security" AND "scada" OR "ics")
("industrial control system" OR "industrial control system security" AND "application security" OR "self protection")
("critical infrastructure" OR "scada" AND "rasp" OR "self protection")

Las cadenas de búsquedas se utilizaron en los buscadores propuestos en el apartado anterior arrojando resultados positivos para la búsqueda de sistemas de autoprotección. En ningun caso se pudo obtener articulos referidos a la utilización de tecnología RASP para la protección de sistemas SCADA.

3.3 Criterios de inclusión y exclusión

Los criterios de inclusión y exclusión fueron los siguientes:

Tabla 4. Criterios de inclusión y exclusión.

Criterios de inclusión
Artículos redactados en idioma inglés y español
Artículos publicados hasta 2023
Artículos relacionados con tecnologías de autoprotección de aplicaciones
Artículos que respondan las preguntas de investigación
Artículos que abordan la problemática aplicada a infraestructuras críticas
Artículos utilizan la tecnología RASP para proteger sistemas SCADA
Criterios de exclusión
Artículos redactados en otros idiomas
Artículos publicados a partir de 2024
Artículos inaccesibles
Artículos que abordaban la autoprotección de hardware

4 Búsqueda de trabajos

Se realizó la busqueda de trabajos en las cinco fuentes mencionadas anteriormente. Previamente se definió el protocolo de revisión y se obtuvieron los siguientes resultados.

Gráfico 1. Fuentes.

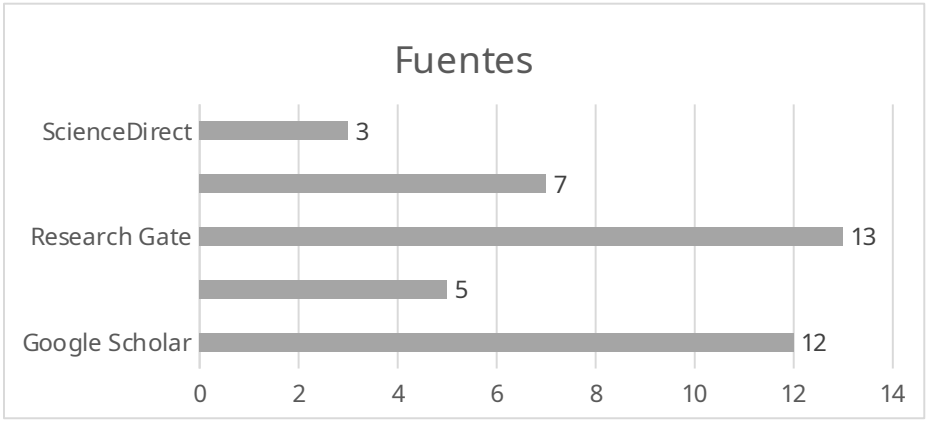


Gráfico 2. Cantidad de estudios por tipo.

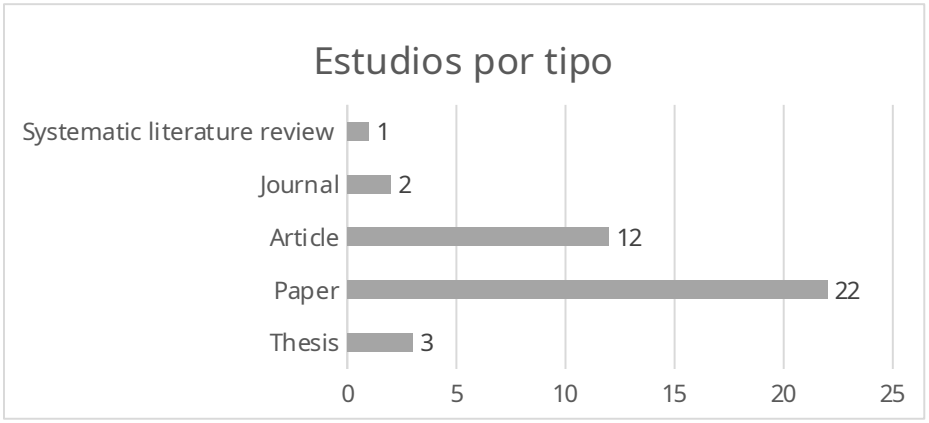
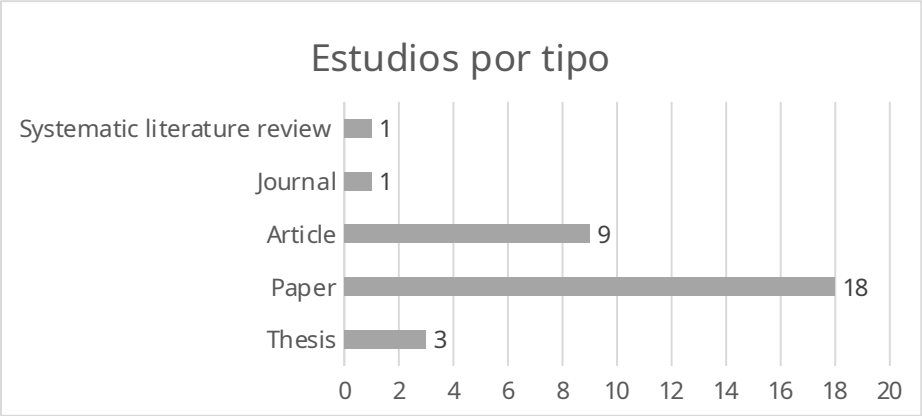


Gráfico 3. Cantidad de estudios por año de publicación.

Los 40 artículos encontrados fueron registrados en una planilla excel y se aplicaron los criterios de exclusión obteniendo como resultado la selección de 32 estudios. Se comprobó el criterio de inclusión y se extrajeron las respuestas a las preguntas de investigación.

Gráfico 4. Cantidad de estudios por tipo.



5 Síntesis de datos extraídos

A continuación se realiza una síntesis de la información obtenida de los estudios analizados utilizando las preguntas de investigación.

P1. ¿Qué trabajos identificaron previamente la tecnología de auto protección de aplicaciones como solución para la defensa ante ciber-ataques?

En (Moldes Cruz et al., 2020) y (Iraqi & El Bakkali, 2019) se menciona que en los últimos años el número de Organizaciones afectadas por brechas de seguridad sufrió un incremento considerable provocando grandes daños a estas Organizaciones. Y las causas principales se debieron a la existencia de vulnerabilidades en el software corporativo asociado en parte a la necesidad de la velocidad en la demanda de la entrega de las soluciones. Planteando la solución de autoprotección como una manera de acompañar esa velocidad de entrega. Desde una perspectiva Gubernamental (C. Chen et al., 2019) muestra el mismo escenario de amenazas explorando la recolección de distintas fuentes de eventos como base para la construcción de un sistema de autoprotección de aplicaciones.

(Williams, 2015) describe también la necesidad de poder acompañar la velocidad y flexibilidad que necesitan los diseñadores de sistemas web para atender la demanda del negocio, sin embargo marca la diferencia entre los sistemas tradicionales de bloqueo por firmas con aquellos incorporados a las aplicaciones monitoreando y bloqueando eventos maliciosos y de esta manera autoprotegerse de las amenazas. Adicionalmente (Z. Zhang et al., 2020) (Sahin et al., 2020) (Mr. Rahul Suryawanshi et al., 2022) comentan que el software tradicional cuenta con protección insuficiente ante ataques desconocidos por lo que un abordaje distinto debe ser realizado para proteger las aplicaciones.

Se suma en (Aboughadareh & Csallner, 2016) un nuevo escenario que es el de las aplicaciones legacy, las cuales suelen ser complejas de modificar o monitorear y que

su interrupción podría tener un alto impacto, en este contexto es que se menciona una solución de autoprotección a nivel de procesos que corren en memoria.

Adicional a lo mencionado precedentemente, (Haupert et al., 2018) y (Lwanga & Kawanguzi, 2015) consideran que el aumento sin precedentes del uso de smartphones para aplicaciones de negocio expone un nuevo contexto en el cual la falta de actualizaciones en estos dispositivos expone a las aplicaciones a nuevas amenazas por lo tanto deben autoprotegerse para asegurar su integridad aun cuando los dispositivos sean comprometidos como por ejemplo se menciona en (N. Zhang et al., 2015) para dispositivos android. En (Elsabagh, 2017) se emplean técnicas automáticas para proteger las aplicaciones ante ataques específicos de denegación de servicios y code-reuse attacks.

Se pueden apreciar distintos escenarios en los cuales se dan indicios por los cuales es necesario dotar a las aplicaciones de características de autoprotección para mantenerlas seguras independientemente del entorno en las que se encuentren, el enfoque de (López et al., 2021) se centra además en las tecnologías IoT que trabajan de manera descentralizada y de esta manera desafiando las formas de mantenerlas seguras sin perder dicha característica, y protegiendo estos dispositivos de ataques como TOCTOU (Qin et al., 2020).

En (Q. Chen & Abdelwahed, 2014) se presentan los ataques a las infraestructuras críticas los cuales pueden tener un alto impacto en las comunidades, y teniendo en cuenta que las tecnologías actuales no son suficientes para prevenir estos eventos propone la utilización de nuevas tecnologías habilitando a los sistemas SCADA con características de autoprotección.

Al contar con una solución de autoprotección, las aplicaciones se adaptan a los cambios en el entorno y no requieren un alta intervención humana, según comenta (Yuan et al., 2014) y pueden de esta manera ser flexible, ágiles y costo efectivas. A medida que la industria avanza hacia sistemas autónomos, también debería hacerlo hacia sistemas resilientes y autoprotectores (Abdallah et al., 2017) (Ren et al., 2015).

P2. ¿Cuáles son las tecnologías de auto protección de aplicaciones que se están usando?

En (Moldes Cruz et al., 2020) identifica dos técnicas de protección, una de ellas se categoriza como prevención de vulnerabilidades y otra es la protección en tiempo real de las aplicaciones. Dentro de esta última se encuentra el Web Application Firewall (WAF), también mencionado en (Saha & Sanyal, 2014), que ofrece una capa adicional de detección y bloqueo ante ataques analizando el tráfico que tiene como destino la aplicación web. La siguiente es -Runtime Application Self-Protection (RASP) que se integra con la aplicación lo que permite analizar las entradas y flujos de datos como así también evaluar el comportamiento interno de la misma (Williams, 2015) (Gottipati, 2020). Esta combinación de tecnologías fue tenida en cuenta en (López et al., 2021) para mejorar la protección de las aplicaciones.

En (Salemi, 2020) se describe el uso de WAF y RASP como tecnologías de auto protección y adicionalmente las combina con un motor de Intrusion Detection System (IDS) para generar reglas de bloqueo en el WAF basado en el análisis de tráfico que

realiza el IDS y RASP. Sumado a la combinación de estas tecnologías (Riera et al., 2022) utiliza además un Intrusion Prevention System (IPS).

Otro solución planteada en (Aboughadareh & Csallner, 2016) es la de protección de procesos de memoria con Runtime Application Inventory (RAI) que consiste en tener un inventario dinámico de aplicaciones permitidas en memoria. O bien técnicas como la generación de perfiles de consumo de energía por cada proceso para detectar comportamientos anómalos de dichos procesos en tiempo de ejecución (Prakash et al., 2017). Además podemos ver en (Z. Zhang et al., 2020) otro tipo de técnica diferente basado en la diversidad natural del software, para crear distintas combinaciones de software y dinámicamente cada un período de tiempo cambiarlos para modificar la superficie de ataque y que esta no sea estática dificultando los ataques a la plataforma.

En (Elsabagh, 2017) se presentan dos alternativas, por un lado Radmin y Cogo como recursos para la detección de ataques de DoS, y en segundo lugar presenta a EigenROP y VCI como protección de binarios. Ambos se encuentran comprendidos dentro del paraguas de RASP para detectar cambios no esperados en el comportamiento y flujos de ejecución, en lugar de depender de la seguridad perimetral para bloquear posibles ataques.

Podemos encontrar en (Iraqi & El Bakkali, 2019) otra solución agregando instrumentación a la aplicación, esto se refiere a monitorear cualquier proceso para detectar intrusiones y bloquear amenazas basados en los datos que se recuperan de la aplicación.

Las plataformas móviles también pueden ser objeto de protección con este tipo de soluciones, como se menciona en (Lwanga & Kawanguzi, 2015), aquellas aplicaciones críticas con perfiles de alto riesgo deberían ser capaces de defenderse de manera autónoma y detectar amenazas en tiempo de ejecución.

Como se puede apreciar las tecnologías de auto protección se utilizan en distintos entornos incluido el uso de extensiones de protección de software de los procesadores Intel llamado GSX. En (Baumann et al., 2014) desarrollaron una aplicación que hace uso de GSX para proteger la ejecución de las aplicaciones denominadas legacy en los enclaves en memoria generados en por esta extensión.

A las soluciones anteriores se suma el cifrado de datos basado en hardware (Wang et al., 2019) para resguardar la información en tiempo de ejecución en sistemas embebidos, esto se logra cifrando el dato antes de ser almacenado y además se verifica su integridad evitando alteraciones. Toda esta operación es realizada de manera automática. Y podemos encontrar además soluciones con cifrado por software (Qin et al., 2020).

Y por último, en (Mubarak et al., 2021) (Dehlaghi-Ghadim et al., 2023) la técnica usada es el uso de machine Learning para analizar diferentes datasets públicos de SCADA y generar con ello perfiles de detección basados en comportamiento para ser usado en la detección de intrusiones sobre sistemas industriales.

P3. ¿En qué tipo de industria se están utilizando?

La utilización de las tecnologías de auto protección de aplicaciones son ampliamente usadas en distintas industrias como veremos a continuación, sin embargo su utilización en entornos industriales es insipiente.

En desarrollo de software (Moldes Cruz et al., 2020) o procesos de DevSecOps (López et al., 2021) se puede ver la utilización de RASP y WAF como así también en e-commerce o servicios web (Williams, 2015) (Salemi, 2020) (Riera et al., 2022) (Iraqi & El Bakkali, 2019). Incluso en el intercambio de criptomonedas (Gottipati, 2020).

Otras áreas de aplicación son en Gobierno (C. Chen et al., 2019) y en (Saha & Sanyal, 2014) para ciberdefensa. Además de aplicaciones móviles (Haupert et al., 2018) (Lwanga & Kawanguzi, 2015)..

Lo mencionado previamente se podría enmarcar dentro del paraguas de tecnologías aplicadas a IT, adicionalmente se encuentran también en sistemas legacy (Aboughadareh & Csallner, 2016) (Baumann et al., 2014), embedded systems (Wang et al., 2019) o IoT (N. Zhang et al., 2015) (Qin et al., 2020).

Y por último su aplicabilidad en ICS o sistemas SCADA (Abdallah et al., 2017) (Mubarak et al., 2021) (Dehlaghi-Ghadim et al., 2023) (Q. Chen & Abdelwahed, 2014).

P4. ¿RASP es una tecnología de auto protección usada para resguardar sistemas industriales?

En el análisis de estudios realizado no se pudo encontrar la aplicación de la tecnología RASP en entornos industriales. Sin embargo, se encuentra presente en diversos entornos de IT.

P5. ¿Cuáles son los componentes de los ICS en los que se desplegó RASP?

Debido a que no se encontraron trabajos que hayan realizado el análisis de RASP en entornos industriales, no fue posible responder esta pregunta de investigación dejando una espacio para futuros trabajos.

6 Conclusiones

Luego del análisis realizado de los estudios seleccionados se pudo encontrar que las tecnologías de autoprotección existentes son diversas, y se aplican en distintos entornos, desde la seguridad en el perímetro de las redes con WAF, pasando por la protección en tiempo de ejecución con RASP, hasta trabajar con el control de procesos de memoria e incluso controles por hardware para resguardar los sistemas en tiempo de ejecución.

Adicional a lo mencionado precedentemente, se encontraron otras tecnologías que trabajan en combinación con las anteriores que son los IDS e IPS que nutren con reglas de comportamiento a los sistemas de bloqueo de tráfico.

Estas tecnologías son utilizadas en una gran variedad de industrias como ser Gobierno, desarrollo de software, comercio electrónico, intercambio de criptomonedas e incluso en entornos de aplicaciones móviles.

No obstante, la búsqueda del uso de RASP en entornos industriales no arrojó resultados positivos, dejando una oportunidad para explorar este tipo de soluciones para los entornos OT.

Cabe destacar además que se evaluaron 3 trabajos con IA generativa para determinar la inclusión o no en el análisis, resultando que dos de los cuales respondieron las preguntas de investigación y otro no cumplió con este criterio de inclusión quedando descartado. Se utilizó https://www.chatpdf.com para realizar el análisis que cuenta con tecnología de ChatGPT.

Referencias

Abdallah, E., Ul Alam, M. S., Liem, C., O'Connor, J., Okoye, C., & Janes, S. (2017). Runtime Self-Protection in a Trusted Blockchain-inspired Ledger. Conference: 15th ESCAR EUROPEAt: Berlin, Germany. https://www.researchgate.net/publication/326243461_Runtime_Self-Protection_in_a_Trusted_Blockchain-inspired_Ledger

Aboughadareh, S., & Csallner, C. (2016). Detecting rootkits with the RAI runtime application inventory. *ACM International Conference Proceeding Series*, *05-06-December-2016*. https://doi.org/10.1145/3015135.3015138

Anabalón, J., & Donders, E. (2014). Una revisión de ciberdefensa de infraestructura crítica. *Estudios de Seguridad y Defensa Nº 3*. https://doi.org/10.1109/TSMCA.2010.2048028

Baumann, A., Peinado, M., & Hunt, G. (2014). Shielding applications from an untrusted cloud with Haven. *Proceedings of the 11th USENIX Symposium on Operating Systems Design and Implementation*, 267. https://doi.org/10.1145/2799647

Chen, C., Wang, R., Li, H., & Wang, Y. (2019). Key Technology Research on Backtracking Attack Eventof Government Website Comprehensive Protection System. *2019 2nd International Conference on Mechanical, Electronic and Engineering Technology (MEET 2019)*. http://166.62.7.99/conferences/AEASR/MEET%202019/MEET12.pdf

Chen, Q., & Abdelwahed, S. (2014). Towards realizing self-protecting SCADA systems. *ACM International Conference Proceeding Series*, 105–108. https://doi.org/10.1145/2602087.2602113

Dehlaghi-Ghadim, A., Moghadam, M. H., Balador, A., & Hansson, H. (2023). Anomaly Detection Dataset for Industrial Control Systems. *IEEE (Institute of Electrical and Electronics Engineers)*. https://arxiv.org/abs/2305.09678v1

Elsabagh, M. (2017). Protection from Within: Runtime Hardening Techniques for COTS Binaries. *George Mason University - ProQuest LLC*.

Figueredo, A. F., Vales, J., Norberto, A., & García, F. (2021). La ciberseguridad en las infraestructuras críticas. *Centro Universitario de La Defensa de Marín*. http://calderon.cud.uvigo.es/handle/123456789/485

Gottipati, H. (2020). A proposed cybersecurity model for cryptocurrency exchanges. *Submitted to the Faculty of Graduate Studies, Concordia University of Edmonton in Partial Fulfillment of the Requirements for the Final Research Project for the Degree*. https://doi.org/10.7939/R3-MJA6-E058

Haupert, V., Maier, D., Schneider, N., Kirsch, J., & Müller, T. (2018). Honey, i shrunk your app security: The state of android app hardening. *Springer*, *10885 LNCS*, 69–91. https://doi.org/10.1007/978-3-319-93411-2_4

Iraqi, O., & El Bakkali, H. (2019). Application-Level Unsupervised Outlier-Based Intrusion Detection and Prevention. *Hindawi Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/8368473

Kamlofsky, J., Masih, S. A., Colombo, H., Milio, C., & Hecht, P. (2019). Ciberseguridad en los sistemas de control industrial: clave para la ciberdefensa de las infraestructuras críticas. *In XXI Workshop de Investigadores En Ciencias de La Computación (WICC 2019, Universidad Nacional de San Juan)*. http://sedici.unlp.edu.ar/handle/10915/77258

Kamlofsky, J., Masih, S. A., Colombo, H., Veiga, D., & Hecht, P. (2016). Ciberdefensa en redes industriales. *XVIII Workshop de Investigadores En Ciencias de La Computación*, 882–885. http://sedici.unlp.edu.ar/handle/10915/53249

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. In *Information and Software Technology* (Vol. 51, Issue 1, pp. 7–15). Elsevier. https://doi.org/10.1016/j.infsof.2008.09.009

López, Ó., Blasi, J., Uriarte, M., Lacalle, I., Galiana, G., Palau, C. E., Garro, E., Ganzha, M., Paprzycki, M., Lewandowski, P., Wasielewska, K., Votis, K., Stavropoulos, G., & Papoutsoglou, I. (2021). DevSecOps Methodology for NG-IoT Ecosystem Development Lifecycle – ASSIST-IoT perspective. *Journal of Computer Science and Cybernetics*. https://doi.org/10.15625/1813-9663/37/3/16245

Lwanga, N., & Kawanguzi, N. (2015). Recent Advances in Mobile Security: Mobile Application Security. *Makerere University College of Computing & Informatics Sciences, Kampala, Uganda*. https://www.researchgate.net/publication/288667600

Moldes Cruz, R., Del Canto Rodríguez, P., & Pous, H. R. (2020). Runtime application self-protection (RASP). *Universitat Oberta de Catalunya*. https://openaccess.uoc.edu/handle/10609/117866

Mr. Rahul Suryawanshi, Aniket Sorte, Kunal Sahare, & Sahil Tembhare. (2022). Runtime Application Self Protection. *International Journal of Advanced Research in Science, Communication and Technology*, 689–692. https://doi.org/10.48175/IJARSCT-4885

Mubarak, S., Habaebi, M. H., Islam, M. R., Rahman, F. D. A., & Tahir, M. (2021). Anomaly Detection in ICS Datasets with Machine Learning Algorithms. *Computer Systems Science and Engineering*, *37*(1), 33–46. https://doi.org/10.32604/CSSE.2021.014384

Prakash, A., Fauzi, M., Abbas, B., & Srikanthan, T. (2017). Power profile based runtime anomaly detection. *School of Computer Science and Engineering Nanyang*

Technological University, Singapore. https://doi.org/10.23919/TRONSHOW.2017.8275074

Qin, Y., Liu, J., Zhao, S., Feng, D., & Feng, W. (2020). RIPTE: Runtime Integrity Protection Based on Trusted Execution for IoT Device. *Security and Communication Networks*. https://doi.org/10.1155/2020/8957641

Ren, J., Qi, Y., Dai, Y., Wang, X., & Shi, Y. (2015). AppSec: A safe execution environment for security sensitive Applicationst. *VEE 2015 - Proceedings of the 11th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, 187–199. https://doi.org/10.1145/2731186.2731199

Riera, T. S., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Herráiz, J. J. M. (2022). Systematic Approach for Web Protection Runtime Tools' Effectiveness Analysis. *CMES - Computer Modeling in Engineering and Sciences*, *133*(3), 579–599. https://doi.org/10.32604/CMES.2022.020976

Saha, A., & Sanyal, S. (2014). Application Layer Intrusion Detection with Combination of Explicit-Rule- Based and Machine Learning Algorithms and Deployment in Cyber-Defence Program. *International Journal of Advanced Networking and Applications 06(02)*. https://arxiv.org/abs/1411.3089v1

Sahin, M., Hebert, C., & Santana De Oliveira, A. (2020). Lessons Learned from SunDEW: A Self Defense Environment for Web Applications. *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2020*. https://doi.org/10.14722/madweb.2020.23005

Salemi, M. (2020). Automated rules generation into Web Application Firewall using Runtime Application Self-Protection. *Ecole Polytechnique de Louvain, Université Catholique de Louvain*. https://dial.uclouvain.be/downloader/downloader.php?pid=thesis%3A25351&datastream=PDF_01

Wang, W., Zhang, X., Hao, Q., Zhang, Z., Xu, B., Dong, H., Xia, T., & Wang, X. (2019). Hardware-enhanced protection for the runtime data security in embedded systems. *Electronics - MDPI*, *8*(1). https://doi.org/10.3390/ELECTRONICS8010052

Williams, J. (2015). Protection from the Inside: Application Security Methodologies Compared. *SANS ANALYST PROGRAM*. https://www.ten-inc.com/presentations/HP_Protection_Inside_2015.pdf

Yuan, E., Esfahani, N., & Malek, S. (2014). A Systematic Survey of Self-Protecting Software Systems. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, *8*(4). https://doi.org/10.1145/2555611

Zhang, N., Yuan, K., Naveed, M., Zhou, X., & Wang, X. (2015). Leave me alone: App-level protection against runtime information gathering on android. *Proceedings - IEEE Symposium on Security and Privacy*, *2015-July*, 915–930. https://doi.org/10.1109/SP.2015.61

Zhang, Z., Liu, Z., Liu, H., Zhang, G., & Chen, Y. (2020). Active Defense Technology Based on Natural Software Diversity in Java Web Services. *Journal of Physics: Conference Series*, *1550*(3), 032024. https://doi.org/10.1088/1742-6596/1550/3/032024