Seguridad Informática

Ciberseguridad en Redes Operacionales

AUTORES:

Jorge Kamlofsky jorge.kamlofsky@uai.edu.ar
Daniel Manrique daniel.manrique@alumnos.uai.edu.ar
Jonatan Schmidt jonatan.schmidt@alumnos.uai.edu.ar
José Castro Tramontina JoseFederico.CastroTramontina@uai.edu.ar

FILIACION:
CAETI – Facultad de Tecnología Informática – Universidad Abierta Interamericana

LINEA DE INVESTIGACION:
Seguridad Informática

Ingeniería en Sistemas Informáticos

PALABRAS CLAVE:
ciberseguridad en OT, Criptografía en OT, Forensia en OT, ciberdefensa desplegable, IA en OT.

CONTEXTO:

Este proyecto se enmarca dentro la línea de Automatización y Robótica del CAETI. Se inició en Abril de 2014.

INTRODUCCIÓN Y PLANTEO DEL PROBLEMA:

Desde mediados del siglo XVIII, las revoluciones industriales han producido una explosión demográfica: creció fuertemente la esperanza de vida y se redujo notoriamente la pobreza, el analfabetismo y la mortalidad infantil. Estos cambios se lograron gracias al incremento de la mayor disponibilidad de bienes económicos y de calidad [1]. En estos tiempos, el sistema productivo global está transitando una nueva fase que se caracteriza por la digitalización y la conectividad [2]. Se presenta como un nuevo paradigma para la industria llamada Industria 4.0 [3]. Industria 4.0 se considera ya como la Cuarta Revolución Industrial. Contempla la introducción de las tecnologías digitales en la industria de la fabricación: IoT, cloud, big data, IA, sensores inalámbricos, dispositivos móviles, sistemas embebidos, entre otros [6].

Industria 4.0 se basa en la integración entre la tecnología de operación de planta (OT según sus siglas en inglés) con las tecnologías de la información (IT según sus siglas en inglés) presentes en las redes corporativas, con las tecnologías digitales mencionadas, así también con las redes de clientes y proveedores. Su interconexión propone grandes ventajas competitivas que puede lograr niveles de eficiencia inéditos. Se espera también, que Industria 4.0 ayude a resolver algunos desafíos mundiales tales como la eficiencia energética, producción urbana y el cambio demográfico [3].

Pero las redes OT se crearon para funcionar en aislamiento físico: su interconexión con otras redes expondría sus vulnerabilidades, lo que supone serias consecuencias [4, 5, 6]. Para evitar la materialización de estos riesgos, Industria 4.0 requiere la investigación de estándares, procesos y soluciones de ciberseguridad robustas [3]. Mientras que en OT se apelaba a la ilusión de la seguridad por ocultamiento dada por el aislamiento físico, en IT se poseían antecedentes robustos en ciberseguridad: estándares como ISO/IEC27000 [7], NIST SP800-30 [8], criptografía, forensia informática, anti-virus, entre otros.

Es inmediato, entonces, cuestionarse la validez de llevar directamente la experiencia de IT a OT. Un reparo a este cuestionamiento puede hallarse en que en IT, la ciberseguridad se basa en tres pilares: disponibilidad, integridad y confidencialidad, mientras que en OT, importa la disponibilidad por sobre los otros pilares [5]. Un segundo reparo, más técnico que filosófico, es el hecho de que en el despliegue de un sistema OT, dado que se requiere interactuar con una vasta cantidad de dispositivos, se requiere validar una gran cantidad de librerías. A partir de ese momento, cualquier actualización en cualquier librería podría causar fallos o paradas inesperadas de planta. A esto se lo denomina la rigidez de actualización, que se contrapone con los estándares y buenas prácticas de IT. Entonces, por lo expuesto, no puede trasladarse directamente a OT las experiencias de IT, Artificial para la detección temprana de ataques y criptografía para asegurar integridad y confidencialidad, cuya aplicación en estos sistemas novedosa.

RESULTADOS Y OBJETIVOS:

Resultados: Resultados anteriores a 2024 se detallan en [17]. Resultados recientes: se mencionan: dos artículos publicados [15, 19] y dos Trabajos Finales de Carrera aprobados [20, 21]. Se destaca la participación como expositores de Ekoparty: la feria de Hacking más importante de Latinoamérica [22]. Se plantea la publicación de al menos media docena de artículos en: WICC, JAIIO, CYBER.AR y en algún Journal especializado.

Objetivos: El objetivo general es proponer procesos y soluciones para mejorar la ciberseguridad en redes OT. Los objetivos específicos más destacados son: Aplicar modelos de IA para identificar intentos de ataques por Ransomware o conexiones no autorizadas. Probar el uso de herramientas de Forensia en vivo para ayudar en la prevención de ataques en ICS. Implementar soluciones criptográficas que aseguren confidencialidad e integridad sin comprometer la disponibilidad. Desarrollar procesos y soluciones que permitan desplegarse en instalaciones industriales afectadas por incidentes de ciberseguridad.

CONTRIBUCIÓN ORIGINAL:

Implementar criptografía en una red OT le daría a estas redes 2 de los 3 pilares de la cibereguridad, incrementándola por diseño: integridad y confidencialidad. Se analiza su implementación. Por otro lado, Tiene originalidad el uso de herramientas forenses para prevención de ciberataques. Se propone también, el desarrollo de herramientas de despliegue de ciberdefensa para sistemas industriales y críticos, lo cual es novedoso.. Por otro lado, mediante el uso de técnicas de IA, se busca hallar patrones que permitan identificar acciones de Ransomware en instancias de Pre-ataque, y así evitar la efectivización del ataque.

FORMACION DE RECURSOS HUMANOS:

El proyecto está dirigido por el Mg. Lic. Jorge Kamlofsky quien está cursando un Doctorado. En el proyecto participan los siguientes investigadores: Daniel Manrique, José Castro Tramontina, Hernán Bottinelli, Jonatan Schmidt, Oscar Romero y los Auxiliares de investigación (alumnos): Gonzalo y Valentina Heinen, Mateo Wrobel y Juan Arias. José Castro Tramontina y Daniel Manrique avanzan en el desarrollo de sus respectivas tesis doctorales. Oscar Romero y Hernán Bottinelli se encuentran realizando sus respectivas tesis de maestría. Llos auxiliares de investigación adquieren experiencias en el proyecto colaborando con tareas diversas.

REFERENCIAS:

[1] Montagut Contreras, E. (2017). La transición demográfica en la Revolución Industrial. Los ojos de Hipatía.
[2] Basco, A. I., Beliz, G., Coatz, D., & Garnero, P. (2018). Industria 4.0: fabricando el futuro (Vol. 647). Inter-American Development Bank.
[3] Kagermann H., Wahlster W. & Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Acatech.
[4] Sanchez, P. Sistema de Gestión de la Ciberseguridad Industrial. Trabajo Final de Master. Univ. Oviedo, (2013).
[5] Kamlofsky, J., Colombo, H., Sliafertas, M. y Pedernera, J. "Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas." III Congreso Nacional de Ingeniería Informática / Sistemas de Información (CONAIISI, 2015), ISSN: 2346-9927. (2015).
[6] Ybzunza Cortes C. El Entorno de la Industria 4.0: Implicaciones y Perspectivas Futuras. En Conciencia Tecnológica n°54, 2017.
[7] ISO/IEC. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018). International Organization for Standardization.
[8] NIST. "Special Publication 800 - 30, revision 1." Information Security. National Institute of Standards and Technology, U.S. Departament of Commerce, (2012).
[15] Heinen, G., Milano, M. A., & Kamlofsky, J. (2025). Uso de técnicas de machine learning para la detección temprana de Ransomware. In XXVII Workshop de Investigadores en Ciencias de la Computación (WICC). Mendoza, 10 y 11 de abril de 2025.
[16] Kamlofsky, J., & Romero, R. O. (2022). Live Forensic Analysis on an ICS / SCADA. Sexta Conferencia Nacional de Informática Forense 2022, 30-38.
[17] Kamlofsky, J., Colombo, H. R., Milio, C., Romero, O., & Hecht, P. (2024). Ciberdefensa en sistemas operacionales. In XXVI Workshop de Investigadores en Ciencias de la Computación (WICC). Puerto Madryn, 18 y 19 de abril de 2024.
[18] Kamlofsky, J., Castro Tramontina J. & Manrique, D. (2025). Ciberseguridad en Ambientes Industriales: Desafíos y Aportes. Ekoparty 2025. En Researchgate.net
[19] Heinen, G. H., & Heinen, V. L. (2025). Prototipado de una Plataforma SCADA Portátil para el Análisis de Vulnerabilidades en Redes OT. Revista Abierta de Informática Aplicada, 9(1), 124-140.
[20] Scussolin, L. A. (2024). Implementación de infraestructura de clave pública (PKI) en sistemas SCADA. Universidad Abierta Interamericana.
[21] Bernardi, F. A. (2025). Seguridad de entornos SCADA basada en infraestructura de clave pública PKI. Universidad Abierta Interamericana.
[22] Manrique, D., Castro, J. & Kamlofsky J. (2025). Ciberseguridad en Ambienes Industriales: Desafíos y Aportes, Video en Youtube: https://www.youtube.com/watch?v=Ukw2KRfa3js