Ciberdefensa en Sistemas Operacionales

Jorge Kamlofsky[1], Hugo Colombo[1], Claudio Milio[1], Oscar Romero y Pedro Hecht[2]

[1] CAETI - Universidad Abierta Interamericana
Av. Montes de Oca 725 – Buenos Aires – Argentina
{Jorge.Kamlofsky, Hugo.Colombo, Claudio.Milio, Rauloscar.Romero}@uai.edu.ar

[2] Universidad de Buenos Aires, Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería. Maestría en Seguridad Informática, Buenos Aires, Argentina
phecht@dc.uba.ar

Resumen

Las revoluciones industriales fueron sin duda, los instrumentos que permitieron el impresionante desarrollo económico, tecnológico y humano de los últimos siglos. Industria 4.0 se plantea hoy, como una nueva revolución en los aspectos productivos: se presenta como la "Cuarta Revolución Industrial". Apalancado sobre nuevos protocolos de comunicación y sobre las tecnologías más disruptivas, propone una interconexión horizontal y vertical, que lograría altísimos niveles de eficiencia y eficacia en la producción.

En la integración vertical, se plantea la incorporación de las tecnologías operacionales (OT según sus siglas en inglés) dedicadas al proceso productivo con las tecnologías de la información (IT según sus siglas en inglés) dedicadas a la administración corporativa e incluso con Internet.

La Ciberseguridad se presenta aquí como un desafío: mientras que en el mundo IT se tiene amplia experiencia, OT se mantuvo seguro gracias al histórico aislamiento físico. La integración deja a los sistemas OT expuestos a una gran cantidad de vulnerabilidades y amenazas.

En este proyecto se estudian las vulnerabilidades de los sistemas OT y se proponen soluciones basadas en mejoras de procesos, comunicaciones y con el uso de criptografía e inteligencia artificial.

Palabras clave: seguridad en scada, seguridad en sistemas de control industrial, ciberseguridad en OT, ciberdefensa en infraestructuras críticas.

Contexto

Los proyectos radicados en el CAETI[1] se clasifican en tres líneas de investigación. Este proyecto se enmarca dentro la línea de Automatización y Robótica. Se inició en Abril de 2014.

Introducción

En los últimos años, la economía global comenzó a transitar una nueva fase que se caracteriza por la digitalización y la conectividad [1]. Una fase que se presenta tanto paradigmática como revolucionaria para la industria: Industria 4.0. Gracias a la implementación del protocolo IPv6[2], se permite la interconexión masiva de dispositivos a Internet. Así, IPv6 se plantea como uno de los puntos de partida de Industria 4.0 según su documento fundacional [2].

[1] CAETI: https://caeti.uai.edu.ar/ .

[2] IPv6 Forum: https://www.ipv6forum.com/

En [1] se presentan a las tecnologías utilizadas en las empresas: tanto las tecnologías de la información (IT), como la operacional (OT); creadas y desarrolladas con diferentes objetivos y finalidad: administración de la información (IT) y supervisión y control de la producción industrial (OT). Industria 4.0 se basa en la integración entre ambas tecnologías. Se plantea además, un gran desafío: la ciberseguridad [2].

Las tecnologías operacionales automatizan la producción industrial a gran escala mediante los Sistemas de Control industrial (ICS según sus siglas en inglés). Los ICS son sistemas de tele-mando y tele-control de procesos compuestos por autómatas industriales que pueden interconectarse [3]. Poseen procesadores de pequeño porte y lógica determinista, que favorece su alta disponibilidad, esencial para ambientes industriales [4].

Los ICS se supervisan y controlan en tiempo real desde los sistemas SCADA (del inglés: Supervisory Control and Data Acquisition). Estos suelen incluir interfases hombre-máquina (HMI según sus siglas en inglés) visuales con pantallas táctiles, terminales para mantenimiento e ingeniería [4]. Los ICS son muy robustos, y por ello se usan para la automatización procesos que requieren uso continuo: plantas industriales de todo tipo, y (por su robustez) en gran parte de las ingraestructuras críticas de naciones: plantas de potabilización de agua, producción y distribución de energía, transporte, siderúrgicas, entre otras.

Originalmente, su seguridad radicaba en una seguridad ilusoria: la seguridad por ocultamiento dada por el aislamiento físico [5]. Pero Industria 4.0 plantea una integración tanto vertical (entre tecnologías IT y OT) como horizontal (entre los sistemas de la empresa con clientes y proveedores). Así, los ICS quedaron expuestos a amenazas y riesgos que suponen serias consecuencias [6].

En 2010, el sistema SCADA de una planta de enriquecimiento de uranio de Irán fue atacada por un virus llamado Stuxnet [7]. La comunidad internacional mostró gran preocupación por la seguridad de las infraestructuras basadas en estas tecnologías, en especial, las infraestructuras críticas [8-10] y trabaja en diferentes desarrollos y propuestas [11-13].

En el ámbito de las tecnologías de la información se poseen experiencias reconocidas en Seguridad. Las recomendaciones de las normas ISO 27000 y NIST SP800-30 [14,15] y un gran plexo normativo, ayudan a proteger a los activos informáticos. Asimismo, en el ámbito industrial, las recomendaciones de las normas ISA/IEC 62443 [16] y NIST SP800-82 [17] y otras ayudan a abordar este problema.

En este proyecto se investigan mejoras a la ciberseguridad en los sistemas de control industrial (ICS según sus siglas en inglés), como parte de las tecnologías operacionales. Se soportan en tres pilares: Gestión de la Seguridad en ICS para la prevención, uso de Inteligencia Artificial para la detección temprana de ataques y criptografía para asegurar integridad y confidencialidad, cuya aplicación en estos sistemas novedosa.

Líneas de Investigación, Desarrollo e Innovación

En el proyecto se identifican tres líneas de investigación:

La primera línea de investigación se denomina Gestión de la Seguridad en ICS. El punto de partida fue un análisis de la base de incidentes RISI[3] que

[3] Vínculo a RISI: https://www.risidata.com/

desembocó en un artículo [18] muy bien recibido por la comunidad. Se extendió al análisis de técnicas y procesos de seguridad, topologías de redes, redes industriales, análisis de malware, hacking e informática forense, entre otros. En 2023 se entregó a MinCYT una guía de recomendaciones en el marco de un proyecto PDTS[4]. Los detalles de este trabajo pueden hallarse en el artículo [19].

La segunda línea se denomina Inteligencia Artificial (IA) aplicada a ciberseguridad de los ICS. 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. Se basa en el proyecto Infoscopia [20] de la Facultad de Ingeniería del Ejército (FIE[5]), de quienes se recibe apoyo en el desarrollo experimental.

La tercera línea se denomina Criptografía Aplicada a los ICS. Trata la aplicación de algoritmia criptográfica (originalmente: moderna y luego: post-cuántica). Implementar criptografía en el interior de un ICS es un desafío novedoso, aunque muy difícil. Esto permitiría asegurar Confidencialidad en las comunicaciones. La idea se basa en la existencia del protocolo Modbus TLS y de PLCs que utilizan dicho protocolo, lo que permitiría armar una infraestructura PKI sobre este protocolo. Se cuenta con el apoyo de las empresas Trend Ingeniería[6] y Levex[7] para soporte de las experiencias.

[4] Definición de PDTS según Conicet: https://vinculacion.conicet.gov.ar/proyectos-de-desarrollo-tecnologico-y-social/

[5] FIE: https://www.fie.undef.edu.ar/

[6] Trend: http://www.trendingenieria.com.ar/

[7] Estudio Levex: https://estudiolevex.com.ar/

Resultados y Objetivos

Los resultados más destacados obtenidos en el proyecto pueden agruparse como sigue:

- Convenios: Convenio General de Colaboración entre la UAI y la Universidad Fasta (UFASTA). Se realizaron charlas de extensión en cada institución, articuladas desde UFASTA por el InFo-Lab[8] y desde la UAI por el Caeti con el objetivo es reforzar los conocimientos en Ciberseguridad de sus investigadores. También se firmó un Convenio General de Colaboración entre la UAI y la FIE. Se hicieron trabajos experimentales conjuntos sobre ICS. Un convenio entre la UAI y la empresa Trend Ingeniería aporta know-how y soporte en tecnologías de la operación.
- Patentes: Reserva de Derechos de Autor del algoritmo criptográfico HK17.
- Concurso: Presentación y aceptación del algoritmo HK17 [21] en CFP de la NIST [22], USA.
- Proyecto PDTS: Entre FIE, UFASTA y UAI, finalizado en 2023.
- Publicaciones: Publicación más de una docena de artículos con referato, de los cuales, tres fueron premiados en los respectivos congresos [23-25].
- Desarrollos: Se desarrolló un ICS portable para demo y experimentación. Se desarrolló también, el sistema de intercambio de claves poscuántico HK17.
- Tesis / Trabajo Final de Carrera finalizados: Dos Trabajos Finales de la Carrera Licenciatura en Matemáticas (UAI), cinco trabajos Finales de la Carrera Licenciatura en Gestión de Tecnología Informática (UAI).

El objetivo general del proyecto es:

- Crear soluciones que mejoren la seguridad en las redes OT.

[8] Info-Lab: https://info-lab.org.ar/

Los objetivos específicos más destacados son:

- Aplicar modelos de IA para identificar intentos de ataques.
- Aplicar criptografía para asegurar confidencialidad e integridad sin comprometer la disponibilidad
- Mejorar procesos y topologías de red para asegurar la inter-conexión de las redes OT con las redes IT y con Internet.

Formación de Recursos Humanos

El proyecto está dirigido por el Mg. Lic. Jorge Kamlofsky quien está cursando un Doctorado. Los resultados colaborarán con el desarrollo de su Tesis Doctoral.

En el proyecto participan los siguientes investigadores: el Dr. Pedro Hecht, el PhD. Hugo Colombo, el Ing. Claudio Milio y el Esp. Lic. Oscar Romero quienes en el desarrollo del proyecto van adquiriendo mayores conocimientos.

Es de gran importancia la colaboración en el desarrollo del proyecto de estudiantes que se encuentran realizando sus trabajos finales de carrera y/o tesis de posgrado, a saber: Leonardo Scussolin, Darío Zatti, Esteban Mass y Jessica Ingrao se encuentran realizando su Trabajo Final de la Carrera Licenciatura en Gestión de IT (UAI). Oscar Romero desarrolla su Trabajo Final de la Especialización en Criptografía y Seguridad Informática (FIE); mientras que Daniel Manrique, José Castro Tramontina y Diego Chiza están realizando sus Tesis Doctorales (UAI).

La colaboración se complementa con la participación de más de medio centenar de alumnos de carreras de grado, que han participado en diferentes oportunidades realizando tareas puntuales.

El problema que se estudia en este proyecto se encuentra latente en las infraestructuras críticas e industriales del mundo. Resulta muy atractivo tanto para docentes como para estudiantes.

Otras actividades han aportado a la capacitación de recursos humanos:

- Dictado de Cursos, Charlas y Seminarios: Talleres de Criptografía, (UAI, UFASTA). Conversatorio acerca de Alain Turing (UNGS), Charlas acerca de Ciberseguridad (UAI, U-Experience Brazil).
- Extensión: Jornadas varias de Informática Forense dictadas por los investigadores de UFASTA.
- Clases Magistrales: Desde 2017 se dictan clases de Ciberseguridad en la Diplomatura en Ciberseguridad (UAI)
- Talleres del MinSeg: Participación de talleres de ciberseguridad con personal de las FFSS.

Referencias

[1] Basco, A. I., Beliz, G., Coatz, D., & Garnero, P. (2018). *Industria 4.0: fabricando el futuro* (Vol. 647). Inter-American Development Bank.

[2] Kagermann H., Wahlster W. & Helbig J. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. Acatech, (2013).

[3] Miguel. *¿DCS, PLC, PAC o RTU?,* Control Real Español, (2015). Disponible en: https: // controlreal.com / es / dcs - o - plc – o – pac – o - rtu/. [Consultado: 24/02/2024].

[4] Romero Mestre, H. *Ciberseguridad en sistemas de control industrial o ICSs*. Trabajo Final de Master. Incibe, UOC, URB, Universitat Autonoma de Barcelona, (2018).

[5] Courtois, N. *The dark side of security by obscurity, and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime.* IACR Cryptology ePrint. 137, (2009).

[6] Sanchez, P. *Sistema de Gestión de la Ciberseguridad Industrial.* Trabajo Final de Master. Univ. Oviedo, (2013).

[7] Englert, M. *Cyber meets nuclear Stuxnet and the cyberattacks on Iranian centrifuages.* Deutschen

Physikalischen Gesellschaft, (2013).
[8] Socarrás, H. E., & Santana, I. (2019). *Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM. Revista Ibérica de Sistemas e Tecnologias de Informação,* (32), 83-96.
[9] García Arias, J. A. *Ciberseguridad aplicada a los sistemas de control industrial con énfasis en el sector energético*. (2018)
[10] CEEAG *La Ciberguerra. Sus Impactos y Desafıos.* Centro de Estudios Estratégicos de la Academia de Guerra, Ejército de Chile, (2018).
[11] Pérez Ignacio, E. *Estudio y desarrollo de un enfoque de pentesting para sistemas de control industrial*, (2019).
[12] Saiz Miranda, Javier. *Arquitecturas y seguridad en sistemas de control industrial e IoT para infraestructuras críticas.* (2022).
[13] Rojas Castro, Álvaro Roberto. *Protección en infraestructuras críticas: análisis de seguridad de los sistemas de control industrial.* (2019).
[14] ISOTools. *ISO 27001*. (2015). Disponible en: https: // www.isotools.org ⁄ normas ⁄ riesgos-y-seguridad ⁄ iso-27001. [Consultado: 26/02/2024].
[15] NIST. *Special Publication 800 - 30, revision 1*. Information Security. National Institute of Standards and Technology, U.S. Departament of Commerce, (2012).
[16] International Standard of Automation (ISA), *ISA/IEC 62443 Series of Standards*, (2020). Disponible en: https: // www.isa.org / standards – and – publications / isa – standards / isa – iec – 62443 – series – of - standards. [Consultado: 26/02/2024].
[17] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M. and Hahn, A. *Guide to Industrial Control Systems (ICS) Security.* NIST. Special Publication 800 / 82, revision 2. U.S. Departament of Commerce, (2015).
[18] 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).
[19] Kamlofsky, Jorge, Gerardo Gonzalez, and Santiago Trigo. *Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021, Chilecito, La Rioja).* 2021.
[20] Liporace, Julio César, et al. *Metodología para el análisis de incidentes de ciberseguridad o ciberataques durante las acciones de ciberdefensa de las infraestructuras críticas de la defensa nacional–infoscopia–. XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, San Juan).*. 2019.
[21] Hetch, P. and Kamlofsky, J. *HK17: Post Quantum Key Exchange Protocol Based on Hypercomplex Numbers.* NIST: National Institute of Standards and Technology, U.S. Departament of Commerce, Post Quantum Cryptography Project, (2017). Disponible en: https: // csrc.nist.gov / CSRC / media / Projects / Post-Quantum-Cryptography / documents / round-1 / submissions / HK17.zip [Consultado: 26/02/2024].
[22] Chen, L., Moody, D. And Liu, Y. *Post Quantum Cryptography, Call for Proposal*. NIST: National Institute of Standards and Technology, U.S. Departament of Commerce, Post Quantum Cryptography Project, (2017). Disponible en: https: // csrc.nist.gov / Projects / Post-Quantum-Cryptography / Post-Quantum-Cryptography-Standardization / Call-for-Proposals. [Consultado: 20/01/2019].
[23] Kamlofsky, J. and Hecht, P. *Post-Quantum Cryptography Using Hyper-Complex Numbers.* XXIII Congreso Argentino de Ciencias de la Computación, La Plata, (2017).
[24] Kamlofsky, J. and Mieres, J. *A Graph Approach to Improve Crimeware Analysis and Classification.* IX Congreso Iberoamericano de Seguridad Informática, Buenos Aires, (2017).
[25] Kamlofsky, J. *Improving a Compact Cipher Based on Non Commutative Rings of Quaternions.* XXII Congreso Argentino de Ciencias de la Computación, San Luis, (2016).