

XXI Workshop de Investigadores en Ciencias de la Computación

25 y 26 de abril de 2019 – San Juan – Argentina

LIBRO DE ACTAS

Facultad de Ciencias Exactas, Físicas y Naturales
Universidad Nacional de San Juan
Red de Universidades con Carreras de Informática (RedUNCI)

fcefn
Facultad de Ciencias Exactas, Físicas y Naturales
Universidad Nacional de San Juan

RedUNCI

XXI Workshop de Investigadores en Ciencias de la Computación -WICC 2019: libro de actas / Compilado por Nelson Rodríguez, María Murazzo, Manuel Ortega, María I. Lund. - 1a ed . - San Juan: Editorial UNSJ, 2019.

CD-ROM, PDF
Archivo Digital: descarga y online

ISBN 978-987-3984-85-3

1. Informática. 2. Informática Educativa. 3. Innovación Tecnológica. I. Rodríguez, Nelson, comp.
CDD 005 - 1118 páginas

ISBN 978-987-3984-85-3



Ciberseguridad en los Sistemas de Control Industrial: Clave para la Ciberdefensa de las Infraestructuras Críticas

Jorge Kamlofsky[1], Samira Abdel Masih[1], Hugo Colombo[1], Claudio Milio[1] y Pedro Hecht[2]

[1] CAETI - Universidad Abierta Interamericana
Av. Montes de Oca 725 – Buenos Aires – Argentina
{Jorge.Kamlofsky, Samira.Abdel Masih, Hugo.Colombo, Claudio.Milio}@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

La automatización de los procesos industriales se realiza mediante los sistemas de control industrial. Con lógica determinista, se diseñaron para funcionar con alta disponibilidad. Por ser robustos y efectivos, se los utiliza para la automatización de los procesos de las infraestructuras críticas: plantas de generación y distribución de energía, potabilizadoras de agua, sistemas de semaforización, entre otros.

Tradicionalmente su seguridad se basó en el aislamiento físico y en las enormes diferencias tecnológicas con los sistemas informáticos. Su interconexión con las redes administrativas y con Internet brindó mayor flexibilidad y eficiencia, pero quedaron expuestos a una gran cantidad de vulnerabilidades y amenazas.

En este proyecto se estudian las vulnerabilidades de estos sistemas y se proponen soluciones basadas en mejoras de procesos, comunicaciones y en criptografía e inteligencia artificial.

Palabras clave: seguridad en redes industriales, seguridad en scada, criptografía compacta, 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

La producción industrial a gran escala se automatiza mediante los Sistemas de Control Industrial (ICS, de sus siglas en inglés). Son sistemas de tele-mando y tele-control de procesos compuestos por autómatas industriales (según sus siglas en inglés): RTU (Remote Terminal Unit), PLC (Programmable Logic Controller), DCS (Distributed Control System) y/o PAC (Programmable Automation Controller) que pueden interconectarse [1]. Se les conectan entradas y salidas, discretas y/o analógicas como ser: micro-switches, sensores de temperatura, actuadores para encendido de motores, llaves, etc. Poseen procesadores de pequeño porte. Su lógica es determinista,

[1] CAETI: Centro de Altos Estudios en Tecnología informática, UAI.

lo cual favorece a la alta disponibilidad, esencial en el ambiente industrial [2].

Los ICS son monitoreados desde una Interfaz Hombre-Máquina (en inglés, HMI: Human Machine Interface). Se supervisan y controlan en tiempo real desde sistemas informáticos llamados SCADA (del inglés: Supervisory Control and Data Acquisition). Los SCADA suelen incluir terminales HMI visuales con pantallas táctiles, terminales para mantenimiento e ingeniería [2]. Los ICS son muy robustos, y por ello automatizan procesos que requieren uso continuo: plantas de potabilización de agua, producción y distribución de energía, transporte, siderúrgicas, entre otras. Es decir, están en las infraestructuras críticas de naciones. El aislamiento físico y las diferencias con la tecnología informática les dieron una falsa sensación de seguridad por ocultamiento [3, 4].

En búsqueda de mayor flexibilidad y eficiencia, los desarrollos en tecnologías de la información y telecomunicaciones, incentivaron a interconectar los SCADA con las redes corporativas e incluso, a Internet. Así, los ICS quedaron expuestos a amenazas y riesgos que suponen serias consecuencias [5]. En 2010, el sistema SCADA de una planta de enriquecimiento de uranio de Irán fue atacada por un virus llamado Stuxnet [6]. La comunidad internacional mostró gran preocupación por la seguridad de las infraestructuras basadas en estas tecnologías [7-9] y trabaja en soluciones [10-12].

En el ámbito de las tecnologías informáticas se tiene amplia experiencia en Seguridad. Las sugerencias de las normas ISO 27000 y NIST SP800 [13,14] y una gran cantidad de soluciones técnicas, ayudan a proteger a los activos informáticos. En el ámbito industrial, las recomendaciones de la norma NIST SP800-82 [15] y el análisis de vulnerabilidades presentado en [20] son de gran ayuda. Sin embargo, la disponibilidad de soluciones es escasa. Para asegurar un sistema informático, se mencionan en [13] tres pilares básicos: disponibilidad, confidencialidad e integridad. Las soluciones para los ICS, deberían enfocarse, entonces, en mejorar la confidencialidad y/o integridad.

En este proyecto se analizan diferentes recomendaciones de seguridad y se proponen soluciones basadas en mejoras en los procesos y en las tecnologías y topologías de las redes. Se desarrollan soluciones que mejoren confidencialidad e integridad basadas en criptografía e Inteligencia artificial, cuya aplicación en estos sistemas novedosa.

Líneas de Investigación, Desarrollo e Innovación

En el proyecto se identifican tres líneas de investigación:

La primer línea de investigación se denomina Gestión de la Seguridad Informática. El punto de partida fue el análisis de normas [13-15]. Se extiende al análisis de técnicas y procesos de seguridad, topologías de redes, redes industriales, análisis de malware, hacking e informática forense, entre otros.

La segunda línea se denomina Inteligencia Artificial (IA) Aplicada a los ICS. Se dedica al estudio de técnicas de IA con la intención de implementarlas de diversas formas en los ICS.

La tercer línea se denomina Criptografía Aplicada a los ICS, trata la aplicación de algoritmia criptográfica clásica y criptografía post-cuántica basada en álgebra no conmutativa. Implementar criptografía en el interior del ICS es un novedoso desafío que permitiría de asegurar Confidencialidad en las comunicaciones. Y esto pareciera viable teniendo en cuenta que el criptosistema HK17 [16] es simple y compacto lo cual

permitiría su uso en estos sistemas sin comprometer la disponibilidad.

Resultados y Objetivos

En el marco del proyecto se han obtenido los siguientes resultados:

- **Convenios:** Convenio General de Colaboración entre la Universidad Abierta Interamericana (UAI) y la Universidad Fasta (UFASTA). Se firmó el 5/12/17. En 2018 se realizaron charlas de extensión en cada institución, articuladas desde UFASTA por el InFo-Lab y desde la UAI por el Caeti. Su objetivo es reforzar los conocimientos en Ciberseguridad de sus investigadores.
- **Dictado de Cursos, Charlas y Seminarios:** Taller de Criptografía (UAI, 27/9/17 y UFASTA 12/7/18 y 29/10/18). Conversatorio acerca de Alain Turing (UNGS, 10/11/17), Charlas Ciberseguridad para Gente Común (UAI, 23/9/16 y E.C. N°22, 4/9/18).
- **Extensión:** Jornadas de Informática Forense dictadas por los investigadores de UFASTA Juan Alberdi y Bruno Constanzo (UAI, 16/4/18 y 27/8/18).
- **Participación en Talleres de Ciberseguridad del MinSeg:** Hacia la construcción de un campo de I+D+i en Seguridad (MinCyT, 15/12/16), Taller Británico / Argentino: Tendencias Globales e Innovación en Ciberseguridad. Experiencias en Argentina y Gran Bretaña (MinSeg, 19/3/18 al 21/3/18).
- **Tesis:** Pablo Oviedo y defendió su tesis de Licenciatura en Matemática denominada: Fundamentos matemáticos de computación cuántica en el algoritmo de Shor, para la factorización prima de números enteros (UAI, 2017).
- **Patentes:** Res. de Derechos de Autor del algoritmo criptográfico HK17. RE-2017-23378132-APN-DNDA (6/10/17).
- **Concurso:** Presentación y aceptación del algoritmo HK17 [16] en CFP de la NIST [17] (USA, 30/11/17).
- **Publicaciones:** Publicación de siete trabajos con referato [18, 19, 21-25]. De ellos: [21, 23, 24] fueron premiados en los respectivos congresos. Los trabajos [8, 26-30] han citado a alguno de ellos.
- **Desarrollos:** Se desarrolló un ICS portable para demo y experimentación y se implementó un Honeypot industrial.

El objetivo general del proyecto es crear soluciones de seguridad para los ICS.

Los objetivos particulares más destacados son: aplicar modelos de IA y criptografía en los ICS y mejorar procesos y topologías de red para asegurar la conexión del ICS/SCADA a la red corporativa y a Internet. Algunos objetivos específicos son: solucionar los ataques presentados al algoritmo HK17 [19, 31], desarrollar modelos de IA y criptografía para detectar conexiones anómalas y ataques a la red.

Objetivos subyacentes: difundir conocimientos que ayuden al abordaje del problema de estudio y además, mejorar la participación de los alumnos en los resultados del proyecto.

Formación de Recursos Humanos

El proyecto está dirigido por el Esp. Lic. Jorge Kamlofsky quien está cursando un Doctorado. Los resultados colaborarán con el desarrollo de su Tesis Doctoral. Está co-dirigido por la Dra. Samira Abdel Masih quien se enfoca en las tutorías de Tesis de Licenciatura en Matemática. En el proyecto colabora el Dr. Pedro Hecht. Integran el proyecto el PhD. Hugo Colombo y el Ing. Claudio Milio, docentes de la Facultad de Tecnología Informática de la UAI quienes adquieren nuevos conocimientos de ciberseguridad.

El equipo de investigación se completa con alumnos de la Facultad de Tecnología Informática de la UAI: Nicolás Carella, Federico Tabarez Rosa, Daniel Sola, Alejandro Vassallo Lagos, Sebastian Caldarola, Ricardo Goffi, Juan Di Modugno, Jonatan Schmidt, Valeria Galván, Federico Arango, Federico Romero, Lucas Barros, Nahuel Perez, Enrique Belaustegui, Angel Orlauskas, Nicolás Mayer, Fernanda Lopez y Cecilia Prieto. Se desempeñan como auxiliares de investigación. El conocimiento adquirido se incorporará en sus trabajos finales de carrera. Enrique Belaustegui es un alumno avanzado de Ingeniería en Sistemas con experiencias con ICS, tiene un rol destacado en el proyecto. Fernanda Lopez y Cecilia Prieto están realizando sus Tesis de final de Licenciatura en Matemática tratando temas de criptografía poscuántica. Los alumnos Juan Perdiguizzi y Yahel Bayarsky se encuentran realizando sus prácticas en el marco de la materia Práctica Profesional Supervisada de la carrera Ingeniería en Sistemas. Juan Perdiguizzi logró el desarrollo de un ICS portable, para experimentación y demostración. Yahel Barbasky está elaborando un documento que resume las normas de seguridad de la información [13, 14].

En el proyecto también participan alumnos de otras instituciones: Pablo Pizio y Nicolás Ferella están iniciando su tesina de Licenciatura en Ciencias de la Computación de la Universidad Nacional de La Plata acerca de Criptografía poscuántica. Juan Ferreyra es alumno del Instituto IESI Itemed, y estudia aspectos de la Informática Forense.

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.

Referencias

[1] Miguel. “¿DCS, PLC, PAC o RTU?,” Control Real Español, (2015). Disponible en: https: // controlreal.com / es / dcs - o - plc – o – pac – o - rtu/. [Consultado: 8/03/2017].

[2] Romero Mestre, H. “Çiberseguridad en sistemas de control industrial o ICSs.” Trabajo Final de Master. Incibe, UOC, URB, Universitat Autonoma de Barcelona, (2018).

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

[4] Menezes, A., Van Oorschot, P., Vanstone, S. "Handbook of applied cryptography”. CRC press, (1996).

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

[6] Englert, M. ”Cyber meets nuclear Stuxnet and the cyberattacks on Iranian centrifuages." Deutschen Physikalischen Gesellschaft, (2013).

[7] Corvalan, F. "Seguridad de Infraestructuras Críticas: Visión desde la Ciberdefensa." III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, (2015).

[8] CEEAG "La Ciberguerra. Sus Impactos y Desafıos." Centro de Estudios Estratégicos de la Academia de Guerra, Ejército de Chile, (2018).

[9] Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. and Timorin, A. Industrial control systems vulnerabilities statisttics." Kaspersly Labs, (2016).

[10] Sajid, N., Patel, S. and Patel, D. ”Assessing and augmenting SCADA cybersecurity: A survey of techniques." Computers and Security 70, (2017): 436-454.

[11] Blackmer, M. ”Cibersecurity for Industrial Control Networks." III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, 2015.

[12] Simoes, P., Cruz, T., Proenca, J. and Monteiro, E. "Honeypots especializados para Redes de Control Industrial." VII Congreso Iberoamericano de Seguridad Informática, Panamá, 2013.
[13] ISOTools. ”ISO 27001." (2015). Disponible en: https:// www.isotools.org / normas / riesgos-y-seguridad / iso-27001. [Consultado: 20/01/2019].
[14] NIST. "Special Publication 800 - 30, revision 1." Information Security. National Institute of Standards and Technology, U.S. Departament of Commerce, (2012).
[15] 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).
[16] 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: 20/01/2019].
[17] 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].
[18] Kamlofsky, J., Hetch, P., Izzi, O. and Abdel Masih, S. "A Diffie Hellman compact model over conmutative rings using quaternions." VIII Congreso Iberoamericano de Seguridad Informática, Quito, 2015.
[19] 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).
[20] INL "Vulnerability Analysis of Energy Delivery Control Systems." Idaho National Laboratory, INL/EXT-10-18381, (2011).
[21] Kamlofsky, J. "Improving a Compact Cipher Based on Non Commutative Rings of Quaternions." XXII Congreso Argentino de Ciencias de la Computación, San Luis, 2016.
[22] Kamlofsky, J., Hecht, P. and Abdel Masih, S. "Post-Quantum Cryptography: An Elementary and Compact Key Exchange Scheme Based on Octonions." IX Congreso Iberoamericano de Seguridad Informática, Buenos Aires, 2017.
[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., Abdel Masih, S., Colombo, H., Veiga, D., Costa, E., Milio, C., Semeria, M. y Hecht, P. "Seguridad en las Redes Industriales: Clave para la Ciberdefensa de las Infraestructuras Críticas." XIX Workshop de Investigadores en Ciencias de la Computación, Buenos Aires, 2017.
[26] Castro Lechtaler, A., Cipriano, M., Garcia, E., Liporace, J., Maiorano, A., Malvacio, E., Tapia, N., Dulio, N. y Perez, P. "Secuencias Seudoaleatorias para Criptología." XVIII Workshop de Investigadores en Ciencias de la Computación, Concordia, 2017.
[27] Hecht, J. "Post-Quantum Cryptography: S381 Cyclic Subgroup of High Order." ArXiv preprint arXiv:1704.07238, (2017).
[28] Durcheva, M. and Karailiev, K. "New public key cryptosystem based on quaternions." AIP Conference Proceedings 1910, 060014, (2017).
[29] Arzzolini, C. "Ciberseguridad en la República Argentina y su Perspectiva Futura." Trabajo Final Integrador, Instituto de Inteligencia de las Fuerzas Armadas, 2018.
[30] Remache Rubio, E. "Modelo para la Mitigación de Vulnerabilidades Informáticas en los Servicios Web." Trabajo Final de

Maestría. Pontificia Universidad Católica del Ecuador, 2018.
[31] Li, H., et al. "Cryptanalysis of HK17." IACR Cryptology ePrint Archive 2017: 1259}, (2017).