Seguridad en Redes las Industriales: Clave para la Ciberdefensa de las Infraestructuras Críticas

Jorge Kamlofsky[1], Samira Abdel Masih[1], Hugo Colombo[1], Daniel Veiga[1], Eugenio Costa[1], Claudio Milio[1], Marcelo Semería[1], Pedro Hecht[2]

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

Los procesos de producción industrial a gran escala se automatizan mediante los sistemas de control industrial. Por su robustez y efectividad, estos sistemas también fueron adoptados en la automatización de las infraestructuras críticas de las naciones: plantas de tratamientos de líquidos, distribución de energía, siderúrgicas y demás. La seguridad se basa en su aislamiento. Los nuevos requerimientos de mayor flexibilidad y eficiencia promueven su conexión con las redes corporativas, dejando expuestas sus vulnerabilidades a gran cantidad de amenazas provenientes de estas últimas.

En este proyecto se estudian las principales vulnerabilidades de estos sistemas, y se analizan y se desarrollan soluciones: algunas basadas en mejoras de procesos y herramientas tradicionales y otras basadas en esquemas compactos de criptografía adaptables a los dispositivos de las redes industriales.

Palabras clave: Seguridad en Redes Industriales, Seguridad en SCADA, Criptografía compacta, criptografía en PLCs, Infraestructuras críticas, ciberdefensa en redes industriales.

Contexto

Los proyectos radicados en el CAETI[1] se clasifican en cinco líneas de investigación. Este proyecto se enmarca dentro la línea de Seguridad Informática y Telecomunicaciones.

Se pretende obtener conocimiento teórico y desarrollar e implementar soluciones que permitan mejorar la situación de vulnerabilidad de estas redes lo que permitiría otorgar ciberseguridad a las infraestructuras críticas.

Introducción

Los Sistemas de Control Industrial (ICS de sus siglas en inglés) son redes de telemando y telecontrol de procesos compuestos por autómatas industriales llamados PLC (del inglés: Programmable

1 CAETI: Centro de Altos Estudios en Tecnología informática, dependiente de la Facultad de Tecnología informática de la UAI.

Logic Controller) interconectados entre sí y cada uno de ellos a sensores digitales o analógicos (caudalímetros, sensores de nivel, de temperatura, microswitches, etc.) y/o a actuadores (motores, válvulas, llaves, etc.). Fueron diseñados para supervisar y actuar en los procesos industriales. El aislamiento del proceso de producción, dio por muchos años una sensación de seguridad ilusoria gracias al ocultamiento [1, 2]. En la tecnología industrial, la prioridad siempre fue el proceso, y no la seguridad.

Los ICS son muy robustos, y por ello se los utiliza en sistemas que requieren uso continuo y permanente. Están presentes en plantas de potabilización de agua, producción y distribución de energía, transporte, telecomunicaciones, siderúrgicas, entre otras: están en infraestructuras críticas de naciones.

Los ICS se controlan desde el SCADA. Un SCADA (por sus siglas en inglés: Supervisory Control and Data Acquisition) es software que muestra gráficamente el estado de cada componente de la planta, con la posibilidad de actuar sobre ellos. Se diseñaron para controlar sistemas industriales, conectando PCs con las redes de autómatas industriales; conformando la interfaz hombre máquina. Originalmente los SCADA se instalaban en salas aisladas, con acceso restringido. Con el tiempo surgió la necesidad de vincularlos a la red corporativa e incluso a internet. Y esta tendencia es inevitable. Su interconexión dejó a los ICS expuestos a amenazas y riesgos provenientes desde el exterior, los que suponen serias consecuencias [3].

Hoy es posible, mediante dispositivos móviles, controlar un ICS, desde cualquier lugar del mundo con cobertura de red móvil [4], suponiendo un escenario ideal para explotar vulnerabilidades e inyectar malware. La tecnología corporativa y la industrial dejaron a la seguridad entre ambas [5].

Hasta hace pocos años, era impensable que un ICS se pudiera infectar con virus informático. En el año 2010 el sistema SCADA de las plantas de enriquecimiento de uranio de Irán fue atacado por un virus llamado Stuxnet. Esto desconcertó a analistas estratégicos de todo el mundo. La comunidad internacional mostró gran preocupación por la seguridad de las infraestructuras basadas en estas tecnologías [6 – 8], y se encuentra trabajando en soluciones [9 – 12].

En el ámbito de las tecnologías corporativas se tiene experiencia en Seguridad. Las recomendaciones de las normas ISO27000 [13] y NIST SP800-30 revisión 1 [14] y los múltiples desarrollos realizados, ayudan a proteger la seguridad de los activos informáticos. La criptografía es clave para asegurar sistemas informáticos. Es posible dar seguridad criptográfica a dispositivos con baja capacidad de cómputo gracias al desarrollo de algoritmia criptográfica de clave pública basada en estructuras algebraicas de anillos no conmutativos [15-17] la cual a fecha actual es inmune a ataques cuánticos y esquemas simétricos compactos como el presentado en [18].

Este proyecto pretende desarrollar soluciones en las redes industriales: en los SCADA usando avances en la seguridad de redes corporativas, y en la profundidad de la red industrial mediante soluciones criptográficas basadas en álgebra no conmutativa integrándolas con esquemas simétricos compactos.

Líneas de Investigación, Desarrollo e Innovación

El equipo de investigación trabaja en dos ramas: matemático-criptográfica y redes-sistemas.

La rama matemático-criptográfica trabaja estudiando las estructuras de anillos no conmutativos y no asociativos y su posibilidad de aplicarlos criptográficamente como sistema de intercambio seguro de claves. Las variantes generadas se programan y se las pone a prueba en ambientes de simulación controlados.

La rama de redes-sistemas se encuentra estudiando las normas de seguridad en sistemas de información más importantes y los protocolos de comunicaciones intervinientes con la intención de lograr implementar los algoritmos generados. Se estudian las vulnerabilidades más frecuentes en estos sistemas.

Resultados y Objetivos

La rama matemático-criptográfica ha logrado implementar el protocolo presentado en [15] y ha llegado a mejoras en tiempos de ejecución usando cuaterniones [16], en diferentes conjuntos numéricos [17]. También se analiza el funcionamiento del algoritmo de Shor para computación cuántica [19]

La rama de Redes-Sistemas analizó ataques a infraestructuras críticas publicados en [20] y ha propuesto un enfoque para disminuir los efectos de ciber ataques [21]. Hoy se encuentra analizando en detalle las normas ISO27000 [13], la NIST [14] y NIST
específica de los ICS [22].

El objetivo final del proyecto es el desarrollo de soluciones de Seguridad que puedan implementarse en las redes de los ICS. El problema en cuestión es crítico y se encuentra latente en toda la infraestructura crítica e industrial del mundo.

Se espera lograr transferencia de resultados a la comunidad y a la industria. La transferencia a la comunidad se logrará mediante cursos de extensión universitaria. La transferencia a la industria consistirá en el patentamiento de métodos y algoritmos que permitirán incrementar la seguridad de las redes industriales.

Formación de Recursos Humanos

El proyecto está dirigido por el Esp. Lic. Jorge Kamlofsky y la Dra. Samira Abdel Masih. Tiene la colaboración especial del Dr. Pedro Hecht. Integran el proyecto los siguientes docentes de la Facultad de Tecnología Informática de la UAI: el PhD. Hugo Colombo, los ingenieros Marcelo Semería, Eugenio Costa, Claudio Milio y el Lic. Daniel Veiga.

El equipo de investigación se completa con alumnos de la Facultad de Tecnología Informática de la UAI: Matías Sliafertas, Juan Manuel Pedernera, Oscar Morales, Pablo Oviedo, Jesica Valente, Christian Martin, Damián Romero. Daniel Sola, Enrique Belaustegui, Facundo Coronel, Federico Romero, Federico Tabarez Rosa, Fernando Ribas, Matías iacobuzio, Sandra Biondini, Joan Mutti Ferreyra, Andrés Perez, Angel Orlauskas, Rodrigo Gomez, Nicolás Mayer, Maximiliano Ríos, Nicolás Carella, Nicolás Salas, Gastón Suarez y Montserrat Patiño.

Los docentes integrantes del proyecto adquieren conocimientos y técnicas de seguridad que pueden complementar los conocimientos por ellos enseñados en las diferentes materias que integran.

Gran parte de los alumnos que se desempeñan como auxiliares de investigación inician experiencias en la investigación científica adquiriendo la correspondiente metodología, en una temática que resulta ser muy atractiva. Otros se encuentran promediando la

carrera, y el conocimiento adquirido se incorporará en sus trabajos finales de carrera. En particular Oscar Morales, Jesica Valente y Pablo Oviedo están finalizando las tesis de final de la carrera Licenciatura en Matemática.

Referencias

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

[2] Menezes, A., Van Oorschot, P., and Vanstone, S. *Handbook of applied cryptography*. CRC press, 1996.

[3] Sánchez P. *Sistema de Gestión de la Ciberseguridad Industrial* [En línea]. Universidad de Oviedo, (2013). [Consulta: 11/02/15]. Disponible en: <http:// dspace.sheol.uniovi.es / dspace / bitstream / 10651/17741 / 1 / TFM%20-%20PABLO %20SANCHEZ.pdf>.

[4] Opto 22, *Press Release: Updates groov to Easily Connect Modbus/TCP Devices with Smartphones and Tablets* [En línea], (2015). Disponible en: <http:// www.modbus.org / member_docs / OPTO22-Jan2015.pdf> [Consulta: 14/08/2015].

[5] Carrasco Navarro, O. y Villalón Puerta, A. *Una visión global de la ciberseguridad de los sistemas de control*. Revista SIC: ciberseguridad, seguridad de la información y privacidad 106, (2013), pp. 52-55.

[6] Veramendi, R. *Ataques a la Seguridad Informática y Telecomunicaciones en el Contexto Internacional*. Revista del Instituto de Estudios Internacionales IDEI-Bolivia, 45(2), (2012), pp. 4-11.

[7] Vazquez, S. *Ciberseguridad en Paraguay*. III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, 2015.

[8] 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.

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

[10] Simoes, P., Cruz, T., Proença, J. and Monteiro, E. *Honeypots especializados para Redes de Control Industrial*. VII CIBSI. Panamá, 2013.

[11] Arias, D. *Seguridad en Redes Industriales.* Trabajo Final, Universidad de Buenos Aires, 2013.

[12] Paredes, I. *La protección de infraestructuras críticas y ciberseguridad industrial*. Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones 62, (2013), pp. 49.

[13] ISOTools, *ISO 27001* [En línea], (2015). Disponible en: <https:// www.isotools.org / normas / riesgos-y-seguridad / iso-27001>. [Fecha de consulta: 14 de Agosto de 2015].

[14] NIST. *Special Publication 800 – 30, revision 1: Information Security.* National Institute of Standards and Technology, U.S. Departament of Commerce, [En línea] (2012). Disponible en: <http:// nvlpubs.nist.gov / nistpubs / Legacy / SP / nistspecialpublication800-30r1.pdf> [Consulta: 8/3/2017].

[15] Hecht J. *Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos.* V CIBSI, Montevideo, 2009.

[16] Kamlofsky J., Hecht J., Abdel Masih, S. Hidalgo Izzi, O. *A Diffie Hellman compact model over conmutative rings using quaternions*. VIII CIBSI, Quito, 2015.

[17] KAMLOFSKY, Jorge. *Improving a Compact Cipher Based on Non Commutative Rings of Quaternion*. XXII Congreso Argentino de Ciencias de la Computación (CACIC 2016), 2016.

[18] Castro Lechtaler, A., Cipriano, M., García, E., Liporace, J., Maiorano, A., y Malvacio, E.. *Model design for a reduced variant of a Trivium Type Stream Cipher*. Journal of Computer Science & Technology, 14.

[19] Shor, Peter W. *Algorithms for quantum computation: Discrete logarithms and factoring*. Foundations of Computer Science,

1994 Proceedings., 35th Annual Symposium on. IEEE, 1994.
[20] Security Incidents Organization, *RISI: The Repository of Industrial Incidents* [En línea], (2015). Disponible en: <http:// www.risidata.Com / Database> [Consulta: 14/08/2015].
[21] Kamlofsky J, Colombo H, Sliafertas M y Pedernera J, *Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Criticas.* III CONAIISI, Buenos Aires, 2015.
[22] NIST. *Special Publication 800 – 82, revision 2: Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology, U.S. Departament of Commerce, [En línea] (2015). Disponible en: <http: // nvlpubs.nist.gov / nistpubs / Legacy / SP / NIST.SP.800-82r2.pdf> [Consulta: 8/3/2017].