Ciberdefensa en Redes Industriales

Jorge Kamlofsky, Samira Abdel Masih, Hugo Colombo, Daniel Veiga, Pedro Hecht
CAETI - Universidad Abierta Interamericana
Av. Montes de Oca 725 – Buenos Aires – Argentina
(+54 11) 4301-5323; 4301-5240; 4301-5248
{Jorge.Kamlofsky, Samira.Abdel Masih, Hugo.Colombo, Daniel.Veiga}@uai.edu.ar,
phecht@dc.uba.ar

Resumen

Los sistemas de control industrial han logrado la automatización de los procesos de producción en las industrias de manera robusta y eficiente. Gracias a ello, también fueron adoptados en infraestructuras críticas de las naciones: plantas potabilizadoras, distribución de energía, y demás. Nuevos requerimientos de mayor flexibilidad y eficiencia promueven su conexión con las redes corporativas, las que poseen gran cantidad de falencias y dejan expuestas a las redes industriales a sus vulnerabilidades y fallas.

En este proyecto se estudian las principales vulnerabilidades, ataques publicados, y se analizan y se desarrollan soluciones criptográficas basadas en el álgebra no conmutativa aptas para procesadores de menor porte, lo que permitirá otorgar seguridad criptográfica a los dispositivos de las redes industriales.

Palabras clave: Seguridad en Redes Industriales, Seguridad en Sistemas SCADA, Criptografía en PLCs, Ciberdefensa en SCADA, 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 investigación 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.

Introducción

La disminución de los costos de chips y procesadores, así como también de las telecomunicaciones logró que los sistemas informáticos actuales se encuentren presentes en una cantidad enorme de lugares facilitando mejoras en productos y servicios. Su interconexión creciente a través de internet ha llegado incluso hasta el ámbito doméstico [1]. Surgen a diario, nuevas vulnerabilidades y ataques, gracias a la profesionalización del malware. Se requieren estrategias

[1] Centro de Altos Estudios en Tecnología Informática, dependiente de la Facultad de Tecnología informática de la UAI.

claras y concisas de seguridad que minimicen riesgos con un esquema de defensa en profundidad [2].

El caso de los Sistemas de Control Industrial (ICS de sus siglas en inglés) es distinto. Los ICS son redes de tele-mando y tele-control de procesos compuestos por autómatas industriales (los "PLCs") interconectados entre sí y cada uno de ellos a sensores (caudalímetros, sensores de nivel, de temperatura, etc.) y/o a actuadores (motores, válvulas, etc.). Se diseñaron para supervisar y actuar sobre procesos industriales.

Los ICS son muy robustos. Hoy están presentes en plantas de potabilización de agua, producción y distribución de energía, transporte, telecomunicaciones, es decir, están en infraestructuras críticas de naciones. Los SCADA (por sus siglas en inglés: Supervisory Control and Data Acquisition) se idearon para controlar sistemas industriales, conectando PC y redes de autómatas industriales; conformando la interfaz hombre máquina.

Con el tiempo surgió la necesidad de vincularlos a la red corporativa e incluso a internet. Y esta tendencia es creciente. Su interconexión dejó a los ICS expuestos a amenazas y riesgos, 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]. En la tecnología industrial, la seguridad carece de prioridad. Sí lo es el proceso. El aislamiento de los procesos de producción industrial, le dio a los ICS una ilusoria sensación de seguridad por ocultamiento, durante muchos años [6, 7].

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 preocupación por la seguridad [8 – 10], y se encuentra trabajando en soluciones [11 – 14].

En el ámbito de las tecnologías corporativas se tiene experiencia en Seguridad. Las recomendaciones de las normas ISO27000 ayudan a proteger la seguridad de los activos informáticos [15]. 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 [16, 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 criptográficas basadas en Algebra no Conmutativa integrándolas con esquemas simétricos compactos para ser implementadas en las redes industriales.

Líneas de Investigación, Desarrollo e Innovación

El equipo de investigación trabaja en dos ramas: matemática-criptografía y redes y hardware.

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

Resultados y Objetivos

La rama matemática-criptográfica ha logrado implementar el protocolo presentado en [16] y ha llegado a una mejora en tiempos de ejecución usando cuaterniones [17].

La rama de Redes y Hardware analizó ataques a infraestructuras críticas publicados en [19] y ha propuesto un enfoque para disminuir los efectos de ciber ataques [20].

Se encuentra en proceso la instalación en laboratorio de una red industrial y un sistema SCADA. Con ello, se pretende replicar algunos ataques y probar las soluciones propuestas.

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 industrial del mundo. Con el avance de este proyecto pueden obtenerse soluciones transferibles a la industria.

Formación de Recursos Humanos

El proyecto está dirigido por el Lic. Jorge Kamlofsky y la Dra. Samira Abdel Masih. Integran el proyecto el PhD. Hugo Colombo, el Lic. Daniel Veiga y el Dr. Juan Pedro Hecht.

El equipo se completa con los siguientes alumnos de la UAI: Juan Pedernera, Matías Sliafertas, Federico Arrieta, Oscar Hidalgo Izzi, Oscar Morales y Pablo Oviedo.

- Juan Pedernera, Matías Sliafertas y Federico Arrieta son alumnos que se encuentran promediando la carrera de Ingeniería en Sistemas. Juan Pedernera y Matías poseen experiencias en Seguridad de Redes. Federico Arrieta posee buen manejo en varios lenguajes de programación. Su participación en el proyecto le permitirá adquirir capacidades formales en investigación en redes industriales, para realizar su Trabajo Final de carrera.
- Oscar Hidalgo Izzi, Oscar Morales y Pablo Oviedo son alumnos de la Licenciatura en Matemática, próximos a concluir. Su participación en el proyecto le permitirá adquirir los conocimientos para el armado de sus Tesis de grado, las cuales se basan en los fundamentos

matemáticos de la algoritmia criptográfica que se desarrolla en el proyecto.

Referencias

[1] Gustafson, S., and Sheth, A. *Web of Things*. Computing Now 7.3, 2014.

[2] Jara H y Pacheco F. *Ethical Hacking 2.0*. Usershop, 2012.

[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] 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.

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

[8] 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.

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

[10] 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.

[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., Proença, J. and Monteiro, E. *Honeypots especializados para Redes de Control Industrial*. VII CIBSI. Panamá, 2013.

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

[14] 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.

[15] 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].

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

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

[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] Security Incidents Organization, *RISI: The Repository of Industrial Incidents* [En línea], (2015). Disponible en: <http:// www.risidata.Com / Database> [Consulta: 14/08/2015].

[20] 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.