Ciberdefensa de Infraestructuras 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

La convergencia entre las redes corporativas, con gran cantidad de falencias de seguridad y las redes industriales, han dejado a estas últimas en total vulnerabilidad. Las redes industriales no sólo producen bienes transables, sino que también se encuentran en infraestructuras críticas de las naciones: plantas potabilizadoras, distribución de energía, y demás. En este proyecto se estudian algunas de las principales vulnerabilidades, se analizan y se desarrollan soluciones criptográficas basadas en el álgebra no conmutativa aptas para procesadores de 16 bits, lo que permitirá otorgarles seguridad criptográfica.

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

Contexto

Los proyectos del CAETI 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

Los sistemas de control industrial son sistemas y redes de mando y control diseñados para supervisar y actuar sobre los procesos industriales. Debido a sus características, y al nuevo panorama de interconexión de estos sistemas a las redes corporativas, los sistemas de control industrial se ven expuestos a amenazas cuya consideración se ha omitido en el pasado, resultando muy vulnerables, quedando aquellos expuestas a riesgos, que en muchas ocasiones cuentan con un análisis escaso o nulo, y que pueden suponer serias consecuencias para las actividades y las finanzas de las organizaciones [1].

Los sistemas industriales están presentes no sólo en las fábricas que producen bienes transables, sino también en plantas de potabilización de agua, producción y distribución de energía, transporte, telecomunicaciones, es decir, están presentes en las infraestructuras críticas de las naciones.

La confluencia entre la tecnología corporativa e industrial ha dejado a la seguridad en el medio de ambas [2]: la tecnología corporativa vigente posee debilidades estructurales en seguridad. Sin embargo, son muchos los esfuerzos puestos en el tema. En la tecnología industrial, la seguridad carece de prioridad. Sí lo es el proceso.

Hasta hace pocos años, era imposible plantear que un sistema industrial pueda ser infectado por un virus informático, hasta que en el año 2010 las plantas de desarrollo nuclear de Irán fueron atacadas por un virus informático llamado "*Stutnex*". Este ataque desconcertó a los analistas estratégicos de todo el mundo. Es un software dirigido específicamente para propagarse en los sistemas de software industrial. En particular, ataca los SCADA marca Siemens (entorno Windows), difundidos por todo el mundo. La comunidad internacional ya mostró su preocupación por su seguridad [3] y se está trabajando en soluciones [4], [5], [6].

El campo de la seguridad tiene amplia experiencia en el ámbito de la tecnología corporativa. En particular, los mecanismos de criptografía asimétrica o de clave pública y privada basan su seguridad en la elevada complejidad computacional requerida para solucionar el problema de la resolución del logaritmo discreto y la factorización entera dentro de grupos conmutativos [7]. Así, hoy por ejemplo, RSA con claves de 2048 bits se considera seguro [8]. Entonces, asegurar dispositivos con baja capacidad de cómputo (como son los "*PLCs*" o autómatas industriales) usando mecanismos de clave pública clásicos con claves cuya longitud se considere segura es prácticamente imposible, y deja a estos dispositivos vulnerables y en desventaja tecnológica frente a los computadores ordinarios actuales.

El desarrollo de algoritmia criptográfica de clave pública basada en estructuras algebraicas de anillos no conmutativos, permite que procesadores pequeños puedan procesar algoritmos criptográficos de clave pública seguros. En [9] se muestra un modelo basado en el protocolo de intercambio de claves Diffie-Hellman [10] mediante el uso de anillos no conmutativos y se mostró un ejemplo con matrices de 4x4 en Z_{256}. En [11] se presentó la aplicación de un desarrollo basado en el ejemplo presente en [9]: y se logra la generación de una clave de sesión común que permite, mediante un criptosistema simétrico AES, cifrar completamente una comunicación celular.

Esta línea criptográfica, no clásica, presenta otra ventaja interesante: es inmune a ataques cuánticos, lo cual hace que su estudio y desarrollo sea aún más atractivo.

Este proyecto pretende desarrollar soluciones criptográficas basadas en Algebra no Conmutativa e implementarlas en dispositivos industriales.

Líneas de Investigación, Desarrollo e Innovación

Se trabaja en dos ramas: matemática-criptografía y redes y hardware.

La rama matemática-criptográfica trabaja estudiando las estructuras de anillos no conmutativos y su posibilidad de aplicarlos criptográficamente. Se programan las variantes ideadas y se las pone a prueba en ambientes de simulación controlados.

La rama de redes y hardware estudiará los protocolos de comunicaciones intervinientes, presentará las principales vulnerabilidades documentadas, realizará

pruebas de las diferentes soluciones criptográficas y otras, y analizará y medirá su alcance.

Resultados y Objetivos

Mientras que la rama matemática-criptográfica enfoca sus objetivos en el diseño y en las mejoras de algoritmos criptográficos actuando a modo de criptógrafos, la rama de Redes y Hardware trabajan buscando y analizando las debilidades de las redes actuando a modo de criptoanalistas, cubriéndose así los objetivos globales de la criptografía.

La semilla del proyecto fue el Trabajo Final Integrador de la Especialización en Criptografía y Seguridad Teleinformática de Kamlofsky [12] que generó un trabajo posterior [13]. Ambos tratan acerca de cómo pueden explotarse vulnerabilidades descubiertas en el chip MF1ICS50 presente en cientos de millones de tarjetas utilizadas generalmente para el pago de tarifas del transporte público usadas en gran parte del mundo, siendo el transporte público una de las infraestructuras críticas de las naciones.

Dado que el proyecto está en sus inicios, los resultados son limitados: se logró desarrollar y poner en marcha el protocolo propuesto en el trabajo de Hecht [9]. El mismo, se implementará en una red industrial y se analizará su efecto. Se espera, además, lograr diseñar una mejora de dicho protocolo que permita un funcionamiento con menores tiempos de procesamiento.

El objetivo final esperado es el desarrollo de soluciones de Seguridad que puedan implementarse en las redes industriales: en SCADA y en PLCs.

El problema en cuestión es crítico, y el desarrollo de soluciones (al menos parciales), podrán aliviar esta situación. Las soluciones obtenidas pueden ser transferidas 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. Pedro Hecht.

El equipo se completa con los siguientes alumnos de la UAI: Juan Pedernera y Oscar Hidalgo Izzi.

- Juan Pedernera es alumno del tercer año de la carrera de Ingeniería en Sistemas, posee experiencias en Seguridad de Redes. 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 es alumno de la Licenciatura en Matemática, próximo a termina. Su participación en el proyecto le permitirá adquirir los conocimientos para el armado de su Tesis de grado.

Durante el año 2015 se espera incorporar un alumno de la Maestría en Sistemas Informáticos encargado de modelar la integración e implementación de la solución en la red industrial. Se espera que su trabajo contribuya a la confección de su tesis.

Referencias

[1] Sánchez, Pablo. *Sistema de Gestión de la Ciberseguridad Industrial*. Universidad de Oviedo. (2013). [Fecha de consulta: 11 Febrero 2015]. Disponible en: <http://dspace.sheol.uniovi.es/dspace/bitstream/10651/17741/1/TFM%20-%20PABLO%20SANCHEZ.pdf>.

[2] Carrasco, Óscar Navarro, y Antonio Villalón Puerta. *Una visión global de la ciberseguridad de los sistemas de control.* Revista SIC: ciberseguridad, seguridad de la

información y privacidad 106 pp. 52-55, (2013).

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

[4] Paulo Simoes, Tiago Cruz, Jorge Proença and Edmundo Monteiro. *Honeypots especializados para Redes de Control Industrial*. VII CIBSI. Panamá. (2013).

[5] Arias, Diego. *Seguridad en Redes Industriales*. Trabajo Final, Universidad de Buenos Aires, (2013).

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

[7] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography.* CRC press, (1996).

[8] Aura, Tuomas. *Cryptographically generated addresses (CGA).* Microsoft Reaserch, (2005). [Fecha de consulta: 11 Febrero 2015]. Disponible en: <http://tools.ietf.org/html/rfc3972>.

[9] Hecht, Juan Pedro. *Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos*. V CIBSI, Montevideo, (2009).

[10] Diffie W., Hellman M.E *New directions in cryptography*, IEEE Transactions on information theory, 22, 644-654, (1976).

[11] Ron Helguera, B. *Implementación de un Protocolo de Intercambio de Claves Diffie-Hellman Empleando Anillos No Conmutativos.* Trabajo Final, Universidad de Buenos Aires, (2013).

[12] Kamlofsky, Jorge. *El Quiebre de la Seguridad de Mifare Classic.* Trabajo Final Integrador, Escuela Superior Técnica, (2013).

[13] Kamlofsky, Jorge. *Selective Attacks to Mifare Classic Cards*. VII CIBSI, Panamá, (2013).