Criptografía Liviana y Ciberseguridad aplicados a Sistemas Ciberfísicos.

Cipriano, Marcelo; Eterovic, Jorge;García, Edith; Torres, Luis.

Instituto de Investigación en Ciencia y Tecnología
Dirección de Investigación Vicerrectorado de Investigación y Desarrollo.
Universidad del Salvador.
Lavalle 1854 – C1051AAB -Ciudad Autónoma de Buenos Aires - Argentina

{marcelo.cipriano; jorge.eterovic; edith.garcia}@usal.edu.ar
Luis.Antonio.Torres@kyndryl.com

RESUMEN

La fusión de las Tecnologías de la Información y Comunicación con la Automatización, Inteligencia Artificial, Robótica, Nanotecnología, Impresión 3D, Computación Cuántica, Biotecnología, entre otras disciplinas, está borrando notablemente las divisiones existentes entre lo digital, físico y biológico. En particular las esferas bien diferenciadas de la *Tecnología de la Información* y la *Tecnología de la Operación* (respectivamente *IT* y *OT* por sus siglas en inglés) ya se encuentran unificadas bajo una misma esfera.

Los llamados *Sistemas Ciberfísicos (CPS: cyber-physical system)*[1] son *mecanismos físicos controlados o monitorizado por equipos informáticos, integrados mediante una red de datos y de comunicaciones, siendo Internet la red más ampliamente empleada*.

Este nuevo conjunto de sistemas, agrupa prácticamente la totalidad de los equipos industriales modernos (*Industria 4.0),* como así también los recursos y sistemas de las *Ciudades Inteligentes (Smart-Cities), Cibermedicina (e-Health), Internet de las Cosas (Internet of Things)*[2–4], solamente por mencionar algunos de los más conocidos.

Esta revolución tecnológica no ha sido acompañada por una revolución equivalente, en la seguridad. Esta aún se encuentra algunos pasos por detrás. Y muy probablemente siempre sea así, tal como la seguridad de los sistemas informáticos ha demostrado en todos estos años. Pues aun habiendo transcurrido varias décadas de la llamada *Revolución Informática* y la *Era de Internet* no se ha logrado vencer la batalla de contra los ciberataques, la existencia de vulnerabilidades, el malware, las intrusiones de sistemas, robos de datos, ingeniería social y engaños, en su casi innumerable cantidad de situaciones. Factores que atentan contra la seguridad de la información, redes y demás. Sobre todo en una tendencia que se ha visto aumentar en los últimos años.

El proyecto persigue el estudio y análisis de las fortalezas y debilidades de los protocolos de comunicaciones de los Sistemas Ciberfísicos en general, como así también los mecanismos y algoritmos de seguridad criptográficos que en ellos se pueden implementar. En particular aquellos mecanismos de autenticación, confidencialidad e integridad de la información[5-7], ofrecidos por la llamada *Criptografía Liviana o Ligera (LiCrypt: Lightweigh Cryptography),* en la forma de algoritmos de cifrado, intercambio de claves, hash y firma digital.

Asimismo el proyecto también propone la difusión y promoción de estas temáticas en la comunidad científica y tecnológica local, en la que se aprecia un notable desconocimiento. Seguramente provocado por diferentes causas cuyo análisis y comprensión exceden los alcances del proyecto.

La persistente labor investigativa y de difusión que la Universidad del Salvador mantiene acerca de estas temáticas, contribuirá a sensibilizar sobre esta problemática, como así también acercar posibles soluciones. Tanto sea al interior del ámbito académico nacional, como del sector productivo e industrial del país.

Ademàs permitirà nutrir a la futura Diplomatura de Ciberseguridad en Entornos IT/OT (que se encuentra actualmente en evaluaciòn) con conocimientos actualizados y recursos humanos.

Palabras Clave:
Sistemas Ciberfísicos, Criptografía Liviana, Internet de las Cosas, CPS, LiCrypt, IoT.

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad Nacional del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndolas como un servicio a la comunidad, entendiendo que los nuevos conocimientos son la base de los cambios sociales y productivos. Con el impulso de las propias Unidades Académicas se han venido desarrollando acciones conducentes a concretar proyectos de investigación uni/multidisciplinarios, asociándose a la docencia de grado y postgrado y vinculando este accionar, para potenciarlo, con otras instituciones académicas del ámbito nacional e internacional.

La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación y a sus investigadores para el desarrollo de Proyectos y Programas de Investigación, nacionales e internacionales, como así también, apoyo y orientación de recursos para la investigación.

A ella pertenece el Instituto de Investigación en Ciencia y Tecnología (RR 576/12) en el cual se enmarca este proyecto con una duración de 2 años (2023-2025).

El mismo se encuentra aprobado por Disposición Decanal No 58/22 con el *Nro. Tràmite SIGEVA 80020220200024US*.

1. INTRODUCCIÓN

Thomas Kuhn ha expuesto la mecánica de ciertos cambios científicos cuyas características los convierten en verdaderas “revoluciones”. que mueven a la humanidad en su conjunto. Estas pueden afectar a su vez, otros campos del conocimiento, como por ejemplo, la Tecnología. Y es aquì donde se observa un nuevo y vertiginoso cambio de paradigma, llamado *“Revolución Industrial”*.

Jeremy Rifkin declaró ante el Parlamento Europeo en 2006, las características de la llamada *Tercera Revolución Industrial* o *Industria 3.0*[8]. *S*e distingue por la integración de la Informática y las *Tecnologías de la Información* con la *Automatización. de Procesos Industriales.*

En 2016, Klaus Schwab expone las características de la que dio en llamar la *Cuarta Revolución Industrial* o *Industria 4.0*[9], ante el Foro Económico Mundial de ese año. Esta vez la revolución sería mucho más impactante que todas las anteriores. A las Tecnologías de la Información y la *Automatización*, se le suman las diferntes tecnologìas: *Comunicación, Inteligencia Artificial, Robótica, Nanotecnología, Impresión 3D, Computa-ción Cuántica y Biotecnología,*[10] entre otras.

Esta fusión comienza a borrar las divisiones existentes entre lo digital, físico y biológico. Se difuminan las fronteras, otrora bien diferenciadas de la *Tecnología de la Información* y la *Tecnología de la Operación* (respectivamente *IT* y *OT* por sus siglas en inglés) las que prácticamente ya se encuentran unificadas.

Sin embargo, la Seguridad de la Información y de las Comunicaciones no han podido acompañar a la par, este desarrollo vertiginoso. Y probablemente jamás lo puedan hacer. Tal vez estén condicio-nadas a avanzar lo mejor que puedan, pero uno o varios pasos por detrás. Y justamente aquí, en esta persistente brecha, que se vislumbra infranquea-ble, es donde se fundamenta el problema.

Durante las revoluciones industriales anteriores, la seguridad se acotaba a la dimensiòn física; la máquina en cuestión, la planta o el producto.Pero la situación con los *Sistemas Ciberfísicos* de la *Industria 4.0,* es diferente. Se pueden mencionar, al menos 4 aspectos relevantes al momento de considerar los problemas de seguridad en estos sistemas[11]:

a) pueden ser víctima de ataques a distancia, llevados adelante a través de la red de datos y comunicaciones que los conecta.

b) algunas vulnerabilidades podrían ser explotadas sin que se requiera un conocimiento profundo o avanzado, al alcance de una cantidad mayor de atacantes.

c) la enorme superficie de ataque disponible, aumentando las posibilidades de éxito de los atacantes.

d) el alto impacto sufrido por las víctimas de los ataques, sean estos usuarios individuales y/u organismos empresariales, gubernamentales, etc.

En cuanto a este último punto, se pueden destacar, a su vez:

a) comprometer la información que se procesa y transmite, afectando su privacidad y seguridad[12–13]

b) secuestrar el/los dispositivos del sistema a cambio de un rescate llamado *“Ransom of Things*” (RoT).

c) conformar redes zombis que tomen el control parcial o total de los dispositivos y con ellos llevar

adelante ataques masivos a organismos, empresas y gobiernos.

d) afectar el funcionamiento de una o varias *Infraestructuras Criticas* de una nación, como por ejemplo la interrupción del suministro eléctrico, introducir defectos en las plantas potabilizadoras de agua o de tratamientos de desechos, etc.

Este último escenario, no solamente es posible, sino que algunas naciones ya han considerado medidas: a partir del 14 de Junio de 2016 la *Organización del Tratado del Norte (OTAN)* considera a los ciberataques como "*ataques armados convencionales*". Es decir que si cualquiera de sus miembros fue víctima de un ciberataque adjudicado a alguna potenci extranjera, solicitarà ejecutar el *Artículo 5* del tratado. Este artículo indica la *respuesta armada de la parcialidad o totalidad de sus países miembros[*14].

Una de las principales causas de los problemas de seguridad radica en que por su diseño, tamaño y demás características propias, los Sistemas Ciberfísicos (incluìdos los dispositivos IoT, entre otros) no suelen disponer de robustos mecanismos de defensa y protección. Las conexiones, datos, información, comandos que procesan y transmiten carecen mayoritariamente de confidencialidad, autenticación, integridad, no repudio y hasta disponibilidad.

En la actualidad existen muchas vulnerabilidades explotadas por Malware y Redes Botnets[15], entre otros.

Es por ello que el gobierno de Estados Unidos vislumbró los peligros de permitir que la Internet de las Cosas quede sin seguridad. pues la mayoría de tales dispositivos no se ve alcanzado por ningún estándar, naceional o internacional y cada fabricante ofrece los servicios a su criterio.

Fue así que en abril de 2017 a través de *National Institute of Standards and Technology (NIST: Instituto Nacional de Estándares y Tecnología en inglés)* Estados Unidos llama a concurso internacional en busca del mejor algoritmo de cifrado-autenticado de criptografía liviana para ambos perfiles: para ser usado indistintamente en hardware y software (profile 1) y sólo en hardware (profile 2). Los ganadores del certamen se convertirán en los primeros estándares para aplicar en *Internet de las Cosas*. Al menos para aquellos productos que sean comercializados en ese país.

Es probable que los estándares que NIST emita, se conviertan también en estándares de facto para el resto del mundo, como ocurrió oportunamente con DES y luego con AES, dos algoritmos de cifrado por bloque.

Es por todo lo expuesto que se manifiesta la relevancia del estudio de la seguridad de los *Sistemas Ciberfísicos* en general como así también los protocolos y algoritmos criptográficos que se adopten para proteger las comunicaciones e información en el contexto de la *Industria 4.0.*

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Se persigue el estudio y análisis de:

a) algoritmos criptográficos livianos y protocolos de seguridad, observando fortalezas y debilidades matemáticas y criptográficas[16-17].

b) mecanismos de intercambio de claves, autenticación, resumen (hash) y seguridad[18–19].

c) test y pruebas de seguridad para ser aplicados a algoritmos criptográficos.

d) el o los nuevos estándares criptográficos en el campo de la *Criptografía Liviana o Ligera (LiCrypt).*

e) los ataques criptoanalíticos convencionales/recientes y su incidencia sobre los algoritmos y protocolos[20–22].

Asimismo y por la relevancia, alcance del tema y escaso conocimiento del mismo por gran parte de la comunidad industrial de nuestro paìs, tambièn se persiguen las siguientes lìneas de difusiòn y concientizaciòn:

1) Explicar y difundir la existencia de nuevos algoritmos y estándares criptográficos, como así también sus características de seguridad y su ámbito de aplicación.

2) Transferir a la comunidad académica, científica nacional o internacional, docentes e ingenieros del ámbito IT y OT, la información y resultados obtenidos. En procura de lograr un nexo entre la investigación científico/aca-démica y el mundo de la producción en el marco de Industria 4.0.

3. RESULTADOS OBTENIDOS/ ESPERADOS

Se persigue, tal como se ha indicado, no sòlamente el alcance de conocimientos teòricos y analìticos en el àrea de la Criptologìa. Ademàs se persigue la concientizaciòn de la problemàtica de la ciberseguridad en el entorno industrial, la difusiòn de estàndares de seguridad, protocolos y algoritmos criptogràficos.
Tambièn este proyecto permitirà nutrir a la *Diplomatura en Ciberseguridad en Entornos IT y OT* que fue diseñada y presentada a las autoridades de la Universidad del Salvador. Actualmente la misma se encuentra en el proceso de evaluaciòn a la espera de su aprobaciòn. Cuyos docentes conforman, en su gran mayorìa, el equipo de investigadores de este proyecto.

4. FORMACIÓN DE RECURSOS HUMANOS

El equipo de investigadores pertenece al cuerpo docente de *Tecnologías Aplicadas* en la *Facultad de Ingeniería*, el área de la *Seguridad Informática*, de la *Universidad del Salvador.*
Se espera que en el presente año el equipo pueda crecer con la incorporación de más docentes investigadores y alumnos. Ya que redundará en un aumento del activo académico e investigativo representado por su cuerpo de docentes participantes, como así también sembrando las bases para la investigación del futuro, a través de la participación de alumnos de la Facultad de Ingeniería.
Se espera, ademàs, que cuando la diplomatura en Ciberseguridad IT/OT sea aprobada y ofrecilda a la comunidad, posibilite el ingreso de docentes y alumnos al proyecto.

5. REFERENCIAS

[1] Lee, E. Cyber Physical Systems: Design Challenges. EECS Department University of California, Berkeley Technical Report No. UCB/EECS-2008-8 January 23, 2008. https://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html

[2]Bono, S. Green, M. Stubblefield, A. Juels, A. Rubin, A. Szydlo, M. Security analysis of a cryptographically-enabled RFID device. In Proceedings of the 14th Conference on USENIX Security Symposium - Volume 14, SSYM'05, pages 1–1, USA, 2005.

[3]Courtois, N. Nohl, K. O'Neil, S. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards. Cryptology ePrint Archive, Report 2008/166, 2008. http://eprint.iacr.org/2008/166.

[4]Dubrova, E. Hell, M. Espresso: A stream cipher for 5g wireless communication systems. Cryptography and Communications, 9(2):273–289, 2017.

[5]Wang, M. Lin, D. Related Key chosen IV Attack on Stream Cipher Espresso Variant. IEEE International Conference on Computational Science and Engineering (CSE) 2017.

[6]Golic, J. Cryptanalytic attacks on MIFARE classic protocol. In Ed Dawson, editor, Topics in Cryptology – CT-RSA 2013, volume 7779 of Lecture Notes in Computer Science, pages 239–258. Springer, Heidelberg, February / March 2013.

[7]Jovanovic, P., Luykx, A., and Mennink, B. (2014). Beyond 2 c/2 security in sponge-based authenticated encryption modes. In Sarkar, P. and Iwata, T., editors, Advances in Cryptology – ASIACRYPT. 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014.

[8]Rifkin, J. The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World. Palgrave Macmillan New York, 2011.

[9]Schwab, K. The Fourth Industrial Revolution. What It Means and How to Respond. Foreing. Affares. World Economic Forum. 2016.

[10]Hermann, M. Pentek, T. Otto, B. "Design Principles for Industrie 4.0 Scenarios," 49th Hawaii International Conference on System Sciences (HICSS), pp. 3928-3937. Hawaii, 2016.

[11]Garcia, F. van Rossum, P. Verdult, R. Schreur, R. Dismantling SecureMemory, CryptoMemory and CryptoRF. In Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10, pages 250–259, New York, NY, USA, 2010. ACM.

[12]Li, R. Li, H. Li, C. Sun, B. A low data complexity attack on the GMR-2 cipher used in the satellite phones. Pages 485–501.

[13]B. Driessen, R. Hund, C. Willems, C. Paar, and T. Holz. Don't trust satellite phones: A security analysis of two smatphone standards. In 2012 IEEE Symposium on Security and Privacy, pages 128–142, May 2012.

[14]Organización del Tratado del Atlántico Norte (OTAN). Texto completo del tratado actualizado. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

[15]Graham, Robert. Mirai and IoT botnet Analysis. RSA Conference 2017. San Francisco. 2017.

[16]Lu, Y. Vaudenay, S. Faster correlation attack on Bluetooth keystream generator E0. In Matthew Franklin, editor, Advances in Cryptology – CRYPTO 2004, volume 3152 of Lecture Notes in Computer Science, pages 407–425. Springer, Heidelberg, August 2004.

[17]Borghoff, J. Knudsen, L. Leander, G. Matusiewicz, K. Cryptanalysis of C2. In Halevi [Hal09], pages 250–266.

[18]Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: On the security of the keyed sponge construction. In: Symmetric Key Encryption Workshop (SKEW). February 2011.

[19]Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Duplexing the sponge: single-pass authenticated encryption and other applications. Cryptology ePrint Archive, Report 2011/499. 2011.

[20]Garcia, F. de Koning Gans, G. Verdult, R. Wirelessly lockpicking a smart card reader. International Journal of Information Security, 13(5):403–420, 2014.

[21]Nohl, K. Evans, D. Starbug, S. Plötz, H. Reverseengineering a cryptographic RFID tag. In USENIX security symposium, volume 28, 2008.

[22]Verdult, R. Garcia, F. Ege, B. Dismantling Megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In Supplement to the 22nd USENIX Security Symposium (USENIX Security 13), pages 703–718. USENIX Association, August 2013.