

Criptografía Liviana y Ciberseguridad aplicadas a Sistemas Ciberfísicos.

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

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; sbianchi@usal.edu.ar

RESUMEN

Hasta hace poco tiempo, la *Tecnología de la Información* y la *Tecnología de la Operación* (respectivamente *IT* y *OT* por sus siglas en inglés) se encontraban bien diferenciadas. No compartían muchos criterios en común, pues el mundo de la información y el mundo físico, se encontraban separados por una brecha tecnológica. Sin embargo, con el advenimiento de los sistemas ciberfísicos, se transitó hacia una convergencia entre los universos *IT* y *OT*.

Por ejemplo, las otrora bien diferenciadas fronteras entre lo digital y lo físico, comienzan a desdibujarse. Surgen amplias "zonas grises" o intersecciones tecnológicas, que comienzan a dificultar el reconocimiento de los "lados" de cada frontera. Esta evolución es la que ha dado lugar, al nacimiento de los llamados *Sistemas Ciberfísicos* (*CPS: cyber-physical system*)[1]. Estos son *mecanismos físicos controlados o monitorizados por equipos informáticos, integrados mediante una red de datos y de comunicaciones, siendo Internet la red más ampliamente empleada.*

La mayoría de los equipos industriales modernos pertenecientes a la llamada *Industria 4.0*, pertenecen a esta categoría. Pero no de manera exclusiva. Es que también en ella, podemos hallar la *Cibermedicina (e-Health)*, la *Internet de las Cosas (Internet of Things)*[2–4], las *Ciudades Inteligentes (Smart-Cities)*, por mencionar algunos.

En todo crecimiento, se presentan crisis. Y eso mismo está ocurriendo en la actualidad. Esta importante evolución y convergencia de tecnologías, no ha podido responder con la misma

velocidad, a los desafíos que se le plantean de seguridad. Las diferentes técnicas que atentan contra los datos, la información y las comunicaciones, exclusivos del universo *IT*, se han potenciado con las vulnerabilidades propias del mundo *OT*, afectando negativamente, a este nuevo contexto de los *Sistemas Ciberfísicos*. Y lo que es peor aún, es una tendencia que va en aumento.

Este proyecto de investigación persigue el estudio y análisis de las técnicas y algoritmos de seguridad criptográficos, implementados en *CPS*. Haciendo especial énfasis en los mecanismos de confidencialidad, autenticación, e integridad de la información [5-7].

Por las características de diseño, construcción e implementación de los sistemas estudiados, los mecanismos criptográficos convencionales no pueden ser implementados. Los recursos disponibles en los dispositivos pertenecientes al mundo *CPS* se encuentran restringidos en recursos. Por ejemplo, procuran disminuir su consumo eléctrico y el espacio físico que ocupan. Ello conlleva a una reducción en la potencia de cómputo, capacidad de almacenamiento, y memoria *RAM*, entre otros.

La llamada *Criptografía Liviana o Ligera (LiCrypt: Lightweight Cryptography)*, una rama de la *Criptografía* es capaz de dar solución a estos inconvenientes. Y en ella se pueden encontrar todo tipo de recursos criptográficos, como ser algoritmos de cifrado, intercambio de claves, hash y firma digital.

Asimismo, el proyecto también persigue la promoción y difusión de estos temas. Sobre todo, en la comunidad científica y tecnológica vernácula, en la que se aprecia un cierto grado de desconocimiento de estas temáticas. La continua labor de investigación y difusión que desde la *Universidad del Salvador* se lleva adelante, respecto

a estas temáticas, seguramente contribuirá a sensibilizar sobre estas problemáticas, permitiendo tal vez, el arribo a posibles soluciones.

A consecuencia de estos esfuerzos, este año se comenzaría a dictar la *Diplomatura de Ciberseguridad en Entornos IT/OT*. La misma se nutrirá del importante capital humano y de conocimiento, producto de años de investigación y experimentación, llevados a cabo por el equipo de investigación.

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 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. Trámite SIGEVA 80020220200024US*.

1. INTRODUCCIÓN

En 2006, ante el *Parlamento Europeo*, *Jeremy Rifkin* expone las características de la llamada *Tercera Revolución Industrial* o *Industria 3.0* [8]. Se caracteriza por la integración de la Informática

y las *Tecnologías de la Información* con la *Automatización de Procesos Industriales*.

Una década después, en 2016, Klaus Schwab presenta las características de la llamada la *Cuarta Revolución Industrial* o *Industria 4.0* [9], ante el *Foro Económico Mundial* de ese año. Mucho más impactante que todas las anteriores revoluciones, esta vez a las Tecnologías de la Información y la *Automatización*, se le suman las diferentes tecnologías: *Comunicación, Inteligencia Artificial, Robótica, Nanotecnología, Impresión 3D, Computación Cuántica y Biotecnología* [10] entre otras.

Son estas fusiones las que comienzan a desdibujar las hasta no hace mucho, bien definidas 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*. Para ciertos asuntos, éstas prácticamente ya se encuentran unificadas.

Pero surge un grave problema: la *Seguridad de la Información y de las Comunicaciones* no ha podido acompañar a la par de su avance, este desarrollo vertiginoso. Y lo que es peor, tal vez jamás lo pueda hacer. En esta brecha, que podría ser infranqueable, radican o se originan un sinnúmero de amenazas. La situación de seguridad en los *Sistemas Ciberfísicos* de la *Industria 4.0*, es diferente a las revoluciones industriales anteriores. En ellas, la seguridad se acotaba a la dimensión física; la máquina en cuestión, la planta o el producto. Pero en la situación actual, se pueden mencionar, al menos 4 aspectos relevantes al momento de considerar los problemas de seguridad en estos sistemas[11]:

- a) Se pueden realizar ataques a distancia, llevados adelante a través de la red de datos y comunicaciones que los conectan.
- b) Se podrían explotar ciertas vulnerabilidades, sin que se requiera un conocimiento profundo o avanzado por parte del atacante. Este punto aumentaría la presión sobre las vulnerabilidades, al incrementarse la cantidad de actores maliciosos potenciales.
- c) Se expande la superficie de ataque, al aumentar la cantidad de posibles dispositivos objetivo. Factor que aumentaría las posibilidades de éxito de los atacantes.
- d) El incremento del impacto sufrido por las víctimas de los ataques, sin distinción entre usuarios individuales y/u organismos empresariales, gubernamentales, etc.

Considerando este último punto, a su vez, se puede observar :

a) El compromiso sobre la privacidad y seguridad de la información que se procesa y transmite [12–13].

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

c) Que se tome el control parcial o total de los dispositivos para la conformación de redes zombis o botnets [15] y con ellos, se puede llevar adelante ataques masivos a organismos, empresas y gobiernos.

d) Que se afecte seriamente, el funcionamiento de una o varias *Infraestructuras Críticas* de una nación. Por ejemplo, la interrupción del suministro eléctrico, introducción de defectos en las plantas potabilizadoras de agua o de tratamientos de desechos, etc.

En cuanto a este último asunto, el mencionado ciberataque puede ser considerado un ataque equivalente a uno convencional. Es que a partir del 14 de Junio de 2016 la *Organización del Tratado del Atlántico Norte (OTAN)* considera a los ciberataques como “*ataques armados convencionales*”. Y si es considerado un ataque de esas características, entonces cualquier país miembro, que se considere víctima de un ataque adjudicado a alguna potencia extranjera, podría solicitar la ejecución del *Artículo 5*. Esto es la *respuesta armada de la parcialidad o totalidad de sus países miembros* [14].

Una de las principales causas de estas vulnerabilidades y las consecuencias de su explotación por parte de actores maliciosos de cualquier índole (individuos, grupos criminales, activistas políticos, etc.) radica en su diseño y fabricación. Los *Sistemas Ciberfísicos* (los dispositivos IoT incluidos) no suelen disponer de mecanismos robustos de defensa y protección. Es decir que se carece de *confidencialidad, autenticación, integridad, no repudio* y hasta *disponibilidad*, con las obvias y graves consecuencias que estas ausencias provocan.

En reconocimiento a todos estos serios problemas, es que en abril de 2017 el *National Institute of Standards and Technology (NIST: Instituto Nacional de Estándares y Tecnología* en inglés) perteneciente al gobierno de *Estados Unidos*; llamó a concurso internacional en busca del mejor algoritmo de *Cifrado Autenticado* de criptografía liviana. Los ganadores del certamen se convierten en los primeros estándares para aplicar en *IoT*, para aquellos productos que sean comercializados en ese país.

Es por este estado de cosas 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

El proyecto 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 paradigmas 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].

También se procura llevar adelante las siguientes líneas de difusión y concientización:

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/académica y el mundo de la producción, en el marco de *Industria*.

3. RESULTADOS OBTENIDOS/ ESPERADOS

Se esperan alcanzar resultados acerca de los conocimientos teóricos y analíticos en el área de la *Criptología*. Asimismo, se persigue concientizar acerca de la problemática en ciberseguridad, en el entorno industrial, la difusión de estándares de seguridad, protocolos y algoritmos criptográficos.

Finalmente se espera que el proyecto permita nutrir a la *Diplomatura en Ciberseguridad en Entornos IT y OT*, diseñada y presentada a las autoridades de la *Universidad del Salvador*. La misma ha superado su proceso de evaluación y se espera la pronta aprobación, para que, durante este año, comience su dictado. Los docentes que estarán al frente de la misma, son en su mayoría, docentes investigadores de este proyecto.

4. FORMACIÓN DE RECURSOS HUMANOS

El equipo de investigadores pertenece al cuerpo docente de *Ciencias Básicas y Tecnologías Aplicadas* en la *Facultad de Ingeniería*, de la *Universidad del Salvador*.

Desde las distintas cátedras, se invita a los alumnos a participar del proyecto. Como así también se procura la incorporación de docentes investigadores. Esto 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, además, que cuando la *Diplomatura en Ciberseguridad IT/OT* sea aprobada y presentada a la comunidad, fomente 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*. Foreign Affairs. 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 smartphone 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.