Criptografía Liviana para aplicar en IoT e IIoT

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

Desde hace ya varios años existen algoritmos criptográficos que por sus características operativas, conforman la llamada Criptografía Liviana o Ligera. Tales algoritmos pueden emplearse en dispositivos con bajos recursos, como son los que pertenecen a la Internet de las Cosas (IoT) y la Internet Industrial de las Cosas (IIoT), también llamada Industria 4.0. Este proyecto persigue el estudio y análisis de tales algoritmos y los protocolos que los utilizan.
Además del abordaje matemático y algorítmico de la temática a investigar, el proyecto también se propone metas de Difusión y Transferencia de estas temáticas. No solamente orientadas al ámbito académico de las Tecnologías de la Información, también conocido como IT (Information Technology por sus siglas en inglés). Sino también y en la medida de lo posible, se alcance la difusión en el ámbito de la producción industrial y las empresas dedicadas a ello, donde las Tecnologías de las Operaciones u OT (Operation Technology) desarrollan sus actividades. Corazón de la llamada "Cuarta Revolución Industrial", cada vez más interconectada y con requerimientos de seguridad en aumento.
El proyecto desea contribuir con ambos mundos tecnológicos, cada vez más cercanos, cuyo horizonte a mediano plazo será seguramente, la convergencia en los llamados "Sistemas Ciber-Físicos".
La Criptografía Liviana [1] permite dotar de Confidencialidad, Integridad y Autenticación a dispositivos IoT, en los que la Criptografía convencional no puede aplicarse, por sus elevados requerimientos de recursos de procesamiento, cálculo, memoria, energía y demás.
Por otro lado, muchos fabricantes por razones que valdría la pena profundizar, pero que se escapan a los alcances del proyecto, no dotan de mecanismos de seguridad a sus diseños, dispositivos y equipos. Es un gran desafío a corto plazo, subsanar estas falencias que podrían poner el serio riesgo el mundo OT.

Palabras Clave:
Criptografía Ligera, Internet de las Cosas, Internet de las Cosas Industrial, IoT, IIoT.

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 (2021-2023).

1. INTRODUCCIÓN

Las llamadas "*Smart Cities*" o *Ciudades Inteligentes* son aquellas que adoptan sensores y dispositivos IoT para llevar adelante tareas de gestión, control y servicios que le son propias. Sin embargo, la novedad es que adicionalmente a las funcionalidades que de ellos se esperan, también se obtiene, entre otros:

- Uso racional de los recursos.
- Ahorro energético (importante factor a tener en cuenta en el contexto del cuidado del medio ambiente, la reducción de emisiones de CO2 y el cambio climático, claros desafíos de la humanidad para el siglo XXIl).
- Reducción en los tiempos de mantenimiento.
- Control a distancia e interconexión mediante una red de datos (inalámbrica usualmente).
- Comunicación interactiva entre sí y con el Centro de Comando y Control (C2).
- Información en tiempo real de los datos recabados y estado de funcionamiento.

Distintas ciudades argentinas han ingresado a la clase de las *Smart Cities,* desde hace ya varios años. Ellas han adoptado diferentes sistemas y equipos IoT. Por ejemplo, desde 2015 calles de la Ciudad Autónoma de Buenos Aires cuentan con un *Sistema de Telegestión* [1] que puede controlar individualmente el alumbrado público, a través de las llamadas "*luminarias inteligentes*" y desde 2016 las autopistas de la ciudad [2] cuentan con este tipo de iluminación, aprovechando todas las ventajas que de ellas se obtiene tal como fueron mencionadas anteriormente.

Los aportes no se agotan en las luminarias. Sensores de contaminación, ruido y tránsito, cámaras de seguridad con reconocimiento facial y lectura de patentes extienden las aplicaciones de IoT en nuestras ciudades, como Salta, Mendoza y Bahía Blanca [3] entre otras.

Pero por otro lado, estos y otros dispositivos IoT e IIoT presentan vulnerabilidades susceptibles de ser explotadas. Un aporte sustancial a la seguridad, entre otros, es la aplicación de confidencialidad y/o autenticación mediante *Criptografía Liviana o Ligera* [4-5].

Un análisis superficial del problema podría llevar a concluir que la inseguridad queda encerrada en el pequeño ámbito de las luminarias o los sensores antes mencionados. Y por lo tanto, es fácilmente de resolver. Por el contrario, el crecimiento exponencial de la cantidad de dispositivos IoT que se suman al ecosistema informático [6-7] y contribuye a aumentar el riesgo

El mundo IoT sorprende a los expertos en seguridad: la mayoría de tales dispositivos *no presentan mecanismos de seguridad o los mismos son rudimentarios.* Este grave problema ya fue expuesto en forma extensa [8-10], conjuntamente al reclamo por su pronta resolución.

La información de los usuarios se puede ver comprometida severamente, como así también el dispositivo en sí mismo.

Es evidente el nivel de gravedad de esta situación. Pero aún no se ha visto el panorama completo. Está en ciernes un aspecto más grave aún, un punto débil que ya ha sido explotado y nada impediría que se repita en un futuro cercano. O peor aún, que escale su efecto nocivo.

Los dispositivos IoT e IIoT amplían (incluso a un ritmo exponencial) la llamada "*Superficie de Ataque*". Esta situación pone en riesgo a la propia interconexión mundial de las redes. Y ya ocurrió pues el 21 de Octubre de 2016, millones de dispositivos en todo el planeta, la mayoría de ellos IoT, produjeron un ataque *Denegación de Servicio Distribuido (DDoS)* direccionado contra un proveedor de servicio de *DNS*. Este ataque afectó un servicio crítico de la propia Internet. No fue el primero de tu tipo, pero si el mayor registrado hasta el presente.

Este exitoso ataque afectó a empresas como *Amazon, BBC, CNN, Fox News, Github, HBO, Netflix, New York Times, PayPal, Spotify, Starbucks, Twitter, Visa, Wall Street Journal,* entre otras.

El responsable del ataque fue un malware del tipo *Botnet*. Luego de infectar los equipos y propagarse en la red, ordenó el ataque. Las pérdidas ascendieron a cientos de millones de dólares.

Los algoritmos livianos *Block Ciphers* [12-14] o *Stream Ciphers* [14-18] pueden contribuir a mitigar los problemas de confidencialidad. Asimismo pueden utilizarse también algoritmos para la *Gestión de Claves, Firma Digital* y funciones *Hash* [19-21]. Y por supuesto, esto sin por ello reducir la fortaleza criptográfica que de ellos se espera.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

La comunidad científica ya cuenta con muchos algoritmos criptográficos livianos. Algunos de ellos fueron creados por investigadores de universidades. Otros fueron desarrollados por empresas que requerían que sus equipos adquieran mecanismos de seguridad. Una parte del proyecto se destina al relevamiento, estudio y análisis de estos últimos algoritmos, sobre todo los que fueron ideados para dispositivos IIoT.

Además, se destina esfuerzos al análisis de los protocolos de comunicaciones en IoT que utilicen criptografía y la búsqueda de sus puntos débiles o vulnerables.

Finalmente, el proyecto sigue de cerca la última etapa del concurso del *NIST* [22] que pretende establecer el estándar criptográfico de cifrado autenticado de Criptografía Liviana para dispositivos IoT. Se espera que en breve se conozca al algoritmo finalista, que mediante el proceso de estandarización correspondiente, ofrezca sus servicios.

Por supuesto, apenas eso ocurra, el equipo procederá a su estudio, análisis y difusión del mismo, tal como se ha informado anteriormente.

3. RESULTADOS OBTENIDOS/ ESPERADOS

Estudios previos llevados adelante por el mismo equipo de investigadores del presente proyecto, ha llevado adelante un profundo relevamiento de muchos de los algoritmos empleados en IoT e IIoT, para detectar que la mayoría de ellos poseen vulnerabilidades que han permitido debilitar o romper la seguridad que ofrecían [23-24].

Por lo tanto, es recomendable el seguimiento de los algoritmos criptográficos, estudio y análisis de los mismos, dado que en cualquier momento pudiera detectarse un ataque. Y lo que se consideraba altamente seguro, deja de serlo.

El seguimiento y difusión de tales resultados, debe considerarse en gran medida, una tarea permanente.

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*. A ellos se suma una alumna para hacer su pasantía. Ella se encuentra promediando la carrera de *Ingeniería en Informática*, en nuestra Facultad.

Se espera que en el presente año el equipo pueda crecer con la incorporación de más docentes investigadores y alumnos. Incluso poder tener alumnos que quieran llevar adelante su Proyecto de Promoción y Síntesis, en el área de la Criptología.

La incorporación de docentes y alumnos redundará en un aumento del activo académico e investigativo para la unidad académica, como así también sembrando las bases para la investigación del futuro, a través de la participación de alumnos, para beneficio de nuestra universidad.

5. REFERENCIAS

[1] Shancang Li , Lida Xu, Securing the Internet of Things. Syngress Media,U.S. Rockland, MA, United States. 2017.

[2] Autor no informado. “Buenos Aires, una ciudad con iluminación inteligente”. Portal de información y trámites de la Ciudad Autónoma de Buenos Aires. Mayo, 2015. https://www.buenosaires.gob.ar/ noticias/buenos-aires-una-ciudad-con-iluminación-inteligente

[3] Autor no informado. Portal CONSTRUAR, Periódico Digital de la Construcción, propiedad de Gómez Nieto Consultores Asociados https://www.construar.com.ar/2016/01/las-autopistas-de-buenos-aires-estrenan-iluminacion-inteligente/

[4] Mármol, H. “Cuáles son y qué hacen las ciudades argentinas que quieren parecerse a Japón” Portal del Diario Clarín, Septiembre 2019. https://www.clarin.com/tecnologia/smart-cities-hacen-ciudades-argentinas-quieren-parecerse-japon_0_i0n7KiJ5K.html.

[5] ISO/IEC 29192. Information Technology - Security Techniques - Lightweight Cryptography. 2012.

[6] Panasenko, S.; Smagin, S. “Lightweight Cryptography: Underlying Principles and Approaches”. International Journal of Computer

Theory and Engineering, Vol. 3, No. 4, August 2011.

[7] Manyika, J.; Chui, M.; Bughin, J.; Dobbs, R.; Bisson, P.; Marrs, A. “Disruptive tech-nologies: Advances that will transform life, business, and the global economy”. McKinsey Global Institute. 2013.

[8]Evans, D. "Internet of Things La próxima evolución de Internet lo está cambiando todo". Cisco IBSG. 2012.

[9] Román R., Nájera P., López J. “Los Desafíos De Seguridad En La Internet De Los Objetos” University.

[10] Fei Hu, Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. Taylor & Francis Inc. Portland, United States. 2016.

[11] Masanobu Katagi; Shiho Moriai, Lightweight Cryptography for the Internet of Things; Sony Corporation; 2016.

[12] Satoh, A.; Morioka, S. “Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES”. Conference: Information Security, 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003, Proceedings.

[13] Beaulieu, R.; Shors, R.; Smith, J.; Treatman-Clark, S.; WeeksWeeks, B.; Wingers. L. ”The SIMON and SPECK Families of Lightweight Block Ciphers." Cryptology EPrint Archive. International Association for Cryptologic Research, 19 June 2013.

[14] Dworkin, M. "NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication." NIST Computer Security Resource Center. National Institute of Standards and Technology, Spring (2005).

[15] Daniel J. Bernstein. “The Salsa20 family of stream ciphers” . URL:http://cr.yp.to/ papers.html# salsafamily. (2007).

[16] Babbage, S.; Dodd, M. “The MICKEY stream ciphers”. In New Stream Cipher Designs. Pp. 191-209. Springer Berlin Heidelberg. (2008).

[17] Hell, M.; Johansson, T.; Meier, W. “Grain: a stream cipher for constrained environments”. International Journal of Wireless and Mobile Computing, 2, pp. 86-93 (2007).

[18] De Canniere, C.; Preneel, B. “Trivium. New Stream Cipher Designs (pp. 244-266). Springer Berlin Heidelberg. (2008).

[19] Kavun, E. B., & Yalcin, T. “On the suitability of SHA-3 finalists for lightweight applications”. The Third SHA-3 Candidate Conference. (2012).

[20] Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., & Yoshida, H. “A lightweight 256-bit hash function for hardware and low-end devices: Lesamnta-LW”. International Conference on Information Security and Cryptology. Pp. 151-168. Springer Berlin Heidelberg (2010).

[21] Guo, J.; Peyrin, T.; Poschmann, A. “The PHOTON family of lightweight hash functions”. Advances in Cryptology–CRYPTO 2011 (pp. 222-239). Springer Berlin Heidelberg (2011).

[22]https://csrc.nist.gov/projects/lightweight-cryp-tography

[23] Eterovic, J.; Cipriano, M.; García, E.; Torres, L. Criptografía Ligera en Internet de las Cosas para la Industria. Congreso Argentino de Ciencias de la Computación. CACIC 2019. Libro de Actas. Pág. 1228-1240. UniRío. ISBN 978-987-688-377-1. 2019.

[24] Eterovic, J. Cipriano, M. García, E. Torres, L. Lightweight Cryptography in IIoT The Internet of Things in the Industrial field. Computer Science Cacic 2019. Revised Selected Papers. Springer. ISBN 978-3-030-48324-1.