Criptografía Liviana para Internet de las Cosas e Internet de las Cosas Industrial

Eterovic, Jorge; Cipriano, Marcelo; 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

{jorge.eterovic; marcelo.cipriano; edith.garcia}@usal.edu.ar
torreslu@ar.ibm.com

RESUMEN

El proyecto tiene por objetivo general el estudio y análisis de algoritmos criptográficos livianos como así también, los protocolos en los que sean incluidos en el contexto de IoT e IIoT en la llamada Industria 4.0.
Particularmente persigue estudiar y analizar:

- algoritmos criptográficos livianos y protocolos en IoT e IIoT, observando fortalezas y debilidades matemáticas y criptográficas.
- mecanismos de intercambio de claves, autenticación, resumen (hash) y protocolos en dispositivos IoT e IIoT.
- test y pruebas de seguridad para ser aplicados a algoritmos criptográficos.
- nuevos estándares criptográficos en el área de IoT e IIoT.
- ataques criptoanalíticos convencionales o recientes y su incidencia sobre los algoritmos.

Otros objetivos del proyecto, enmarcados en el ámbito de las actividades de Difusión y Transferencia, son:
- Explicar y difundir la existencia de nuevos algoritmos criptográficos, como así también sus características de seguridad, su ámbito de aplicación, los criterios de diseño y seguridad dentro de su ámbito de aplicación
- Transferir a la comunidad científica nacional o internacional, docentes e ingenieros del ámbito IT (Tecnologías de la Información, por sus siglas en inglés) y OT (Tecnologías de la Operación, por sus siglas en inglés) 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 la Industria 4.0.

La amplia variedad de dispositivos IoT en general, sus perfiles de hardware y software, como así también el tipo de aplicaciones, no existe al día de hoy una única primitiva criptográfica que pueda aplicarse por igual en todos ellos.
El estudio de cada una de las primitivas y algoritmos criptográficos propuestos por los diferentes autores resulta entonces, de gran importancia. Este es el objetivo que se persigue en el proyecto [9].

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

Desde el año 2015 un tercio de las calles de la Ciudad Autónoma de Buenos Aires cuenta con un Sistema de Telegestión que puede controlar individualmente las luminarias led que se están instalando, también conocidas como "luminarias inteligentes" [1]. Estos y otros dispositivos pertenecen a la llamada IoT, a un sub-campo conocido con el nombre de Smart Cities. Estos mecanismos ofrecen un uso racional de los recursos al poder configurarse para brindar servicio en determinados horarios o condiciones particulares. Ahorran energía y bajan los tiempos de mantenimiento. Son controlados remotamente y se conectan mediante una red de datos (inalámbrica usualmente). Se comunican entre sí y con el Centro de Control informando su estado de funcionamiento y su ubicación satelital exacta (mediante un receptor GPS), además de otros datos considerados relevantes.

1. Otros dispositivos como 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 [2] entre otras.
2. Estos y otros dispositivos pueden presentar vulnerabilidades susceptibles de ser explotadas. Es por ello que dotar a las comunicaciones de confidencialidad y/o autenticación mediante Criptografía Liviana o Ligera [3-4] ofrece solución a una parte del problema.
3. Este proyecto persigue el estudio y análisis de los algoritmos criptográficos que pueden ejecutarse sobre estos dispositivos IoT restringidos en recursos.

El crecimiento exponencial de la cantidad de dispositivos IoT que se ha observado en los últimos años[1] es un claro indicador de cómo esta tecnología está modificando nuestro mundo [5-6].
Sin embargo y de manera sorprendente la mayoría de los dispositivos IoT no presentan mecanismos de seguridad o los mismos son rudimentarios. Se resentiría de esa manera la confidencialidad, autenticación, integridad y privacidad de la información que procesan y transmiten.
La comunidad científica ha expuesto este problema en forma extensa y ha propuesto diferentes medidas y soluciones para reducir su incidencia [7-9].
Una dificultad persistente en estos dispositivos IoT está en la naturaleza misma de su diseño e implementación. Para cumplir con sus funciones, fueron diseñados restringidos en recursos de energía, memoria, capacidad de cómputo, entre otros.
La Criptografía Liviana o Ligera estudia cómo ofrecer confidencialidad, integridad, y autenticación mediante primitivas criptográficas que empleen la menor cantidad de recursos, sin que por ello se resienta la seguridad y la privacidad de información.
Hasta aquí se han expuesto los argumentos acerca de los riesgos que estos dispositivos IoT conllevan para los usuarios que no contemplen mecanismos de protección adecuados.
Sin embargo, cabe aplicar una mirada de mayor amplitud frente a esta situación: se observa cómo los dispositivos IoT han aumentado la llamada "*Superficie de Ataque*". Esta situación desnuda una vulnerabilidad de mayor escala al poner en riesgo infraestructuras de la red mundial y no a un usuario en particular, como si la vulnerabilidad individual de tal o cual dispositivo IoT pudiera "sumarse" a la de los demás equipos y escalar así hasta poner en riesgo activos críticos de objetivos impensados.
Tal escenario no es teórico. El ataque fue llevado a la práctica y ocurrió el 21 de Octubre de 2016. Y aunque no fue el primero de su tipo, sí fue el más grande registrado. Millones de dispositivos a lo largo del planeta -la mayoría de ellos de tecnología IoT- generaron un tráfico falso de alrededor de 620 Gbps apuntado contra un proveedor de servicio de DNS llamado Dyn. Este ataque Distribuido de Denegación de Servicio (DDoS) afectó un servicio esencial de la infraestructura misma de Internet.
Este exitoso ataque (que se repitió 3 veces a lo largo del día) dejó inaccesibles a plataformas y servicios de la talla de empresas como Amazon, BBC, CNN, Fox News, Github, HBO, Netflix, New York Times, PayPal, Spotify, Starbucks, Twitter, Visa, Wall Street Journal, entre otras, provocándoles pérdidas multimillonarias. Los equipos vulnerados (zombis) fueron explotados por medio de una BotNet y recibieron la orden de

[1] No hay cifras exactas, pero se presume que en 2020 se habrán instalado en hogares, empresas, industrias y ciudades alrededor del mundo entre 30 y 50 mil millones de dispositivos IoT.

realizar peticiones maliciosas al servicio DNS al que apuntaban.
La autenticación de usuarios y equipos, el uso de una VPN que permita constituir un túnel cifrando las comunicaciones desde y hacia estos dispositivos, como así también la correcta administración de contraseñas, hubieran podido evitar el ataque.
El mundo no puede permitirse conservar un nivel de riesgo semejante que pueda afectar globalmente a Internet, afectando las bases mismas de su funcionamiento.
La Criptografía Liviana ofrece una variedad de algoritmos de clave pública y clave privada, Block Ciphers [11-13] y Stream Ciphers [14-17] como así también algoritmos para la Gestión de Claves, Firma Digital y funciones Hash [18-20]. Lo mismo que puede ofrecer una criptografía convencional pero con la posibilidad de correr sobre los dispositivos Internet de las Cosas (IoT) y dispositivos Internet de las Cosas Industrial (IIoT) y sin sufrir por ello una pérdida de robustez y performance.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Ya se cuenta con una gran cantidad de algoritmos criptográficos que han sido creados para satisfacer las necesidades de IoT. Una parte de ellos fueron desarrollados por empresas que requerían dotar de seguridad dispositivos de su creación. Siguiendo con la línea de investigación propuesta para el proyecto se ha llevado adelante un relevamiento de tales algoritmos, en particular aquellos que se han propuesto para aplicaciones de la llamada Internet de las Cosas Industrial.
Otra línea de investigación busca analizar los protocolos de comunicaciones que se utilizan en los dispositivos IoT que empleen algún tipo de criptografía y mecanismo de seguridad. Se persigue la búsqueda de debilidades y vulnerabilidades de los mismos, a fin de poder realizar las propuestas correspondientes que minimicen o eliminen las mismas.
Por último, el equipo de investigadores sigue de cerca las vicisitudes y etapas por las que transcurre el concurso que en este momento mantiene el NIST [21] el cual persigue la búsqueda del nuevo estándar criptográfico de cifrado autenticado de Criptografía Liviana para dispositivos reducidos en recursos. Se han revisado los algoritmos más prometedores (de acuerdo al criterio vertido del propio NIST) y se está a la espera del algoritmo finalista. Una vez acaecido este acontecimiento, se podrá analizar y estudiar en profundidad el algoritmo y sus propiedades criptográficas.

3. RESULTADOS OBTENIDOS/ ESPERADOS

Se ha hallado que muchos de los algoritmos existentes para ser usados en dispositivos de la llamada Internet de las Cosas Industrial poseen vulnerabilidades que han permitido debilitar o romper la seguridad que ofrecían [22-23].
Es por ello que el continuo relevamiento, estudio, análisis y evaluación de los algoritmos criptográficos empleados en IoT y en IIoT es de suma importancia para que las fábricas, instalaciones industriales e infraestructuras críticas, preserven la seguridad en la realización de sus tareas y operaciones.

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.
El año pasado se incorporaron al mismo dos docentes investigadores y algunos alumnos que se encuentran promediando la carrera de Ingeniería en Informática.
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.

5. REFERENCIAS

[1] 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-luminacion-inteligente
[2] 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.

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

[4] Panasenko, S.; Smagin, S. "Lightweight Cryptography: Underlying Principles and Approaches". International Journal of Computer Theory and Engineering, Vol. 3, No. 4, August 2011.

[5] 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.

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

[7] Román R., Nájera P., López J. "Los Desafíos De Seguridad En La Internet De Los Objetos" University.

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

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

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

[11] 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.

[12] 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.

[13] 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).

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

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

[16] 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).

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

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

[19] 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).

[20] 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).

[21]https://csrc.nist.gov/projects/lightweight-cryptography (consultada el 13/03/20).

[22] 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.

[23] 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.