Criptografía Ligera e Internet de las Cosas

Mg. Jorge Eterovic; Esp. Marcelo Cipriano; Lic. Edith García.

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; cipriano1.618; edithxgarcia}@gmail.com

RESUMEN

Es notorio el incremento de los usos y aplicaciones de la llamada Internet de las Cosas (IoT por sus siglas en inglés). La razón de ser de esta plétora de tecnologías concurrentes permite la conexión de objetos de distinta naturaleza e índole, a través de Internet.

La incidencia de su uso sobre la humanidad se vislumbra como un cambio de paradigma[1] al que ya la sociedad se está acostumbrando: no se sorprende ante la obtención de datos médicos en tiempo real por medio de dispositivos e-Health[1], el implante y uso de chips subcutáneos para la identificación y rastreo de personas, las zapatillas con GPS o las heladeras que hacen el pedido al supermercado de la mercadería faltante[2], entre otros aparatos. La tecnología IoT va penetrando en el entorno humano y todo hace pensar que esto recién es el principio.

Sin embargo de la mayoría de las personas ignora que por la propia naturaleza de estos dispositivos -que deben llevar adelante su tarea en contextos reducidos en tamaño, potencia de cómputo, consumo eléctrico, tamaño de las baterías, cantidad de memoria asignada, entre otras limitaciones- se detecta una reducción de la seguridad y privacidad de las comunicaciones y datos que se transmiten, procesan y almacenan. Incluso existen dispositivos que carecen completamente de ellas.

Es por ello que este proyecto propone llevar adelante el estudio de algoritmos pertenecientes a la llamada Criptografía Liviana [3], los que por su diseño pueden ser ejecutados en este tipo de dispositivos.

Palabras Clave:
Criptografía Ligera, RFID, Internet de las Cosas, Internet of Things.

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad Nacional del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndola 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, asociándolos 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 (Código VRID 1935 – Código Académico 100091) con una duración de 2 años (2019-2020).

[1] E-Salud: cuidados sanitarios apoyados en dispositivos TIC´s como pueden ser marcapasos, bombas de insulina, implantes cocleares, etc.

1. INTRODUCCIÓN

Aunque la llamada Internet de las Cosas aparece ante la sociedad como recién llegada al mundo, este concepto no es nuevo. El primer dispositivo conectado a internet fue una máquina expendedora de Coca Cola en la Universidad Carnegie Mellon, en el año 1982. Inocentemente comenzó como una manera de saber cuántas latas de producto aún tenía la máquina, si ya estaban frías o había que esperar para ir a comprarlas. Fue recién en 1999 que el término "Internet de las Cosas" fue propuesto por Kevin Ashton – que trabajaba en el Auto-ID Center del MIT pues allí le llevaban adelante investigaciones en los campos de nuevas tecnologías inalámbricas llamadas RFID[2] y WSN[3]- en una conferencia dictada en la empresa Procter & Gamble en 1999.

Enormes cantidades de información son recolectadas, procesadas y transmitidas, por estos dispositivos, a través de la Internet. Cabe preguntar acerca de los mecanismos de seguridad que tales equipos poseen. Dadas las limitaciones intrínsecas que estos aparatos tienen, existe la posibilidad que no se cuenten con los mecanismos de seguridad adecuados.

La sociedad debiera llevar adelante un extenso análisis en torno a la privacidad y seguridad de la información que se manipula en los entornos IoT[4], fuera de su control y al cuidado de empresas, gobiernos propios y terceros. Es lícito preguntar ¿qué hacen las empresas y organismos con la información que recolectan? ¿Cuál es el límite a partir del cual comienza a violarse la privacidad?

Los asistentes virtuales Siri, Alexia o diferentes Smarts TV son excelentes herramientas para personas con movilidad reducida. Nada haría presuponer en ello una amenaza, todo lo contrario. Hasta que alguien se percató que esos dispositivos inteligentes se mantienen en estado de escucha permanente a la espera de ser activados por la voz de sus propietarios. De esa manera fueron blanco de ataques, tal como quedó en evidencia en la presentación dada por Aaron Grattafiori y Josh Yavor en la conferencia Black Hat de 2013 en la que se mostró la manera de acceder al micrófono o la cámara incorporados a un smart tv para realizar espionaje o voyeurismo en el seno de un hogar cualquiera.

Frente a todo lo expuesto, pocos son los mecanismos viables para dotar de confidencialidad a las comunicaciones. Uno de ellos es el uso de algoritmos de cifrado que por su robustez y confiabilidad son una de las mejores alternativas.

En el contexto de la Criptografía Liviana[5] se pueden encontrar algoritmos de clave pública y clave privada, Block Ciphers[6-8] y Stream Ciphers[9-12] como así también algoritmos para la Gestión de Claves, Firma Digital y funciones Hash[13-15]. Es decir todo el conjunto de funcionalidades que la Criptografía convencional ofrece, pero capaces de correr en contextos reducidos como lo son los dispositivos IoT y sin que ello menoscabe su robustez y performance.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

La metodología a implementar es principalmente de tipo analítico y podría tener un correlato secundario de tipo experimental. Al aspecto analítico le corresponde el estudio de los algoritmos criptográficos, sus aspectos y propiedades matemáticas, como así también la propuesta de mejoras en la implementación de los mismos, aplicados a Internet de las Cosas.

En cuanto al aspecto experimental, se podrán llevar adelante pesquisas de laboratorio al aplicar el cifrado correspondiente a un determinado algoritmo y la observación de su comportamiento en ese entorno reducido de trabajo. Para tal fin podrían llevarse adelante mecanismos de virtualización y/o simulación de los equipos y ecosistema de software donde el algoritmo desempeñará sus funciones. Que podrían ser motivo de futuras líneas de investigación y trabajos netamente experimentales.

[2]RFID: Identificación por Radio Frecuencia (Radio Frequency IDentification).

[3] WSN: Wireless sensor network.

Asimismo cabe aclarar que los algoritmos criptográficos se encontrarán compartiendo hardware y software con otros algoritmos, constituyendo un "ecosistema" muy limitado y reducido, donde el comportamiento de los mismos podría recibir influencias negativas no previstas por sus creadores. Es por ello que podrían percibirse diferencias en el comportamiento esperado acerca de la velocidad y el desempeño, al ejecutarse en dispositivos de este tipo. Y es por ello que tal vez se requiera de la virtualización y/o simulación de los entornos y equipos donde el algoritmo podría desempeñarse.

Para llevar adelante el proyecto se proponen varias líneas de acción para conducir la investigación y el desarrollo del mismo:

- búsqueda de información y relevamiento de novedades acaecidas en el mundo de la Criptografía Liviana y su relación a Internet de las Cosas, dado que es un campo de investigación en constante ebullición, con la aparición de novedades a ritmo vertiginoso.
- análisis de los Protocolos de Comunicaciones en IoT que utilicen criptografía y ofrezcan algún tipo de seguridad.
- Relevamiento de los algoritmos criptográficos livianos más relevantes, tipo, modos de uso, longitud de la clave, mecanismos de cifrado, aplicaciones y usos.

3. RESULTADOS OBTENIDOS/ ESPERADOS

Este proyecto persigue como objetivo profundizar el estudio y análisis de algoritmos criptográficos pertenecientes a la llamada Criptografía Liviana que puedan ser usados en dispositivos de la Internet de las Cosas y que permiten asegurar la información, tanto en su transmisión como almacenamiento.

Se tratará de sugerir mejoras en los mismos, de manera que el comportamiento de la seguridad por medio de la criptografía sea más performante, sugiriendo mejoras en cuanto a la velocidad y robustez en las comunicaciones, lo que podrá conllevar como consecuencia una reducción en el consumo de la batería, espacio en memoria y demás indicadores de la Criptografía Ligera.

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 este proyecto que recién inicia se incorporarán próximamente una docente investigadora de larga experiencia y 2 alumnos que se encuentran promediando la carrera de Ingeniería en Informática. Esto redundará en un aumento del activo académico e investigativo representado por su cuerpo de docentes investigadores, como así también sembrando las bases para la investigación del futuro, a través de la participación de alumnos de la Facultad de Ingeniería.

5. BIBLIOGRAFÍA

[1] Manyika, J.; Chui, M.; Bughin, J.; Dobbs, R.; Bisson, P.; Marrs, A. "Disruptive technologies: Advances that will transform life, business, and the global economy". McKinsey Global Institute. 2013.

[2] http://tn.com.ar/tecno/f5/ces-2016-las-heladeras-del-futuro-conectadas-y-con-multiples-sensores_647274. Consultada el 28/2/19.

[3] ISO/IEC 29192. Information technogy - Security techniques - Lightweight Cryptography. 2012. https://www.iso.org.

[4] Puente García, M. "Iniciativas y mejores prácticas de seguridad para el IoT". Instituto Nacional de Ciberseguridad Español (INCIBE). 2017. https://www.incibe-cert.es/blog/ iniciativas-y-mejores-practicas-seguridad-el-iot. Consultada el 28/2/19.

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

[6] 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.
[7] 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.
[8] 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).
[9] Daniel J. Bernstein. "The Salsa20 family of stream ciphers" . URL:http://cr.yp.to/ papers.html# salsafamily. (2007).
[10] Babbage, S.; Dodd, M. "The MICKEY stream ciphers". In New Stream Cipher Designs. Pp. 191-209. Springer Berlin Heidelberg. (2008).
[11] 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).2
[12] De Canniere, C.; Preneel, B. "Trivium. New Stream Cipher Designs (pp. 244-266). Springer Berlin Heidelberg. (2008).
[13] Kavun, E. B., & Yalcin, T. "On the suitability of SHA-3 finalists for lightweight applications". The Third SHA-3 Candidate Conference. (2012).
[14] 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).
[15] 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).