Criptografía Liviana para aplicar en dispositivos IoT

Mg. Jorge Eterovic; Esp. Marcelo Cipriano;

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@gmail.com – marcelo.cipriano@usal.edu.ar

RESUMEN

En los últimos tiempos se ha observado un notorio aumento en la cantidad y calidad de la conectividad de los dispositivos usados por las personas y hasta en aquellos que conectan dispositivos entre sí. Entre las múltiples razones de ello se encuentra lo que se ha dado en llamar *MtoM*[1] (o también *M2M*). Una de sus áreas es conocida por el nombre de "*Internet de las Cosas*"[2], la cual permite la conexión de objetos de distinta naturaleza e índole, a través de Internet. También las redes conocidas como *WSN*[3] y dispositivos *RFID*[4] se suman al ecosistema. La incidencia de estos factores sobre la humanidad se vislumbra como un cambio de paradigma.

Esta "nueva era" de la humanidad, en la que enormes cantidades de información son transmitidas y procesadas, conlleva un enorme desafío: la seguridad de la misma. Dados los perfiles de hardware y software de muchos de estos dispositivos, existe la posibilidad que no se cuenten con los mecanismos de seguridad adecuados.
Desde datos médicos en tiempo real obtenidos por dispositivos e-Health[5], chips subcutáneos para la identificación y rastreo de personas y zapatillas GPS[1] los dispositivos transmiten y reciben información que dejan expuesto al usuario a riesgos no sólo contra la confidencialidad de sus datos sino también al alcance de otros delitos.
Es por ello que este proyecto propone la realización de un estudio y análisis de algoritmos criptográficos -que podrían ser ejecutados en dispositivos con limitados recursos de hardware y software- haciendo uso de Criptografía Ligera[2].

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 de la y a sus investigadores para el desarollo de Proyectos y Programas de Investigación, nacionales e

[1] Machine to Machine: máquina a máquina. Se refiere la comunicación para el intercambio de información entre dos dispositivos distantes o remotos.
[2] Internet of Things: Internet de las Cosas.
[3] Wireless Sensor Network: Redes Inalámbricas de Sensores.
[4] Radio Frequency Identification: identificación por radiofrecuencia.
[5] E-Salud: cuidados sanitarios apoyados en dispositivos TIC´s como pueden ser marcapasos, bombas de insulina, implantes cocleares, etc.

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 (2017-2018).

1. INTRODUCCIÓN

La llamada *Internet de las Cosas* promete un cambio sin igual en la historia humana[3] que afectará directa o indirectamente a campos tan importantes, como son:

- Cuidados médicos.
- Manufactura de productos.
- Uso de la energía.
- Infraestructura urbana.
- Seguridad.
- Extracción de recursos naturales.
- Agricultura.
- Ventas.
- Vehículos.

A su vez, estos cambios se apoyan en tecnologías y dispositivos que están limitados en recursos, dada su naturaleza, como son entre otros:

- Espacio.
- Consumo de energía.
- Almacenamiento en Memoria.
- Capacidad de cómputo.

Existe además una tendencia a aumentar la cantidad de dispositivos que requieran conexiones a Internet. En particular datos relevados en el *Ericsson Mobility Report* del año 2015 prevee que 28.000.000.000[6] de teléfonos estarán conectados para el año 2021, más de la mitad de ellos con capacidades de IoT y M2M[4].
Dicha empresa, en el último reporte del año 2017 se informa que el tráfico de datos creció 65% interanual entre 2016 y 2017[5] y que 1.800.000.000 de dispositivos IoT obtendrán conectividad a través de teléfonos celulares para el año 2023.

Esta demanda de conectividad será satisfecha con la nueva tecnología 5G[7]. Estos dispositivos móviles intercambiarán información con objetos de la vida cotidiana: desde zapatillas con GPS, marcapasos, heladeras que elaboran listas de compras y demás[6]. La lista no deja de crecer año a año. Estos dispositivos y otros que se sumarán a los existentes, comparten la imperiosa necesidad de asegurar la información que procesan y transmiten. Pero por su propia naturaleza, tienen limitaciones de Hardware y Sofware que impiden el uso de mecanismos criptográficos tradicionales. La Criptografía Ligera o Liviana estudia algoritmos que por sus propiedades matemáticas pueden ejecutarse en plataformas o dispositivos de recursos limitados, como lo son los antes mencionados.
Existen algoritmos livianas de clave privada tipo Block Ciphers[8], Stream Ciphers[9] y de clave pública[10] como así también Gestión de Claves, Firma Digital y funciones Hash. Por ejemplo los Block Ciphers creados por la agencia gubernamentalNSA[11], llamados SIMON y SPECK[7,8] de uso público.

2.LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Algoritmos como Simon y Speck, junto con el resto de ellos, deben ser capaces de demostrar su robustez al ser sometidos a ataques criptoanalíticos[12]. Es por ello que este proyecto

[6] Asumiendo una población mundial de alrededor de 7.000.000.000 personas, este valor indica una media de 4 teléfonos por persona en el planeta.

[7] 5G: es la llamada 5ta generación de Tecnologías de Telefonía Móvil. Su antecesora, la tecnología 4G aún no del todo difundida en nuestro país.

[8] Algoritmo de Cifrado por Bloques: algoritmos que dividen el mensaje a cifrar en bloques de n bits y luego proceden al cifrado del bloque.

[9] Algoritmo de Cifrado en Cadena o Flujo: algoritmos que generan largas secuencias seudoaleatorias de bits, los cuales uno a uno pueden ser operados con cada bit del mensaje a cifrar.

[10] Algoritmos que utiliza 2 claves, una de ellas es pública y sirve para cifrar el mensaje. La otra permanece secreta y se usa para descifrar el mensaje. También son llamados Algoritmos Asimétricos, por el uso que se hace de sus claves.

[11] National Security Agency: Agencia de Seguridad Nacional. Organismo gubernamental de Estados Unidos.

[12] Criptoanálisis: parte de la Criptología que se encarga de analizar, estudiar y desarrollar ataques para el

persigue la profundización en el estudio de las propiedades criptológicas y matemáticas que posibiliten hallar sus vulnerabilidades o debilidades.

3.RESULTADOS OBTENIDOS/ ESPERADOS

El objetivo de este proyecto es abordar y profundizar en el conocimiento de las propiedades criptológicas y de seguridad de Algoritmos Criptográficos Livianos que puedan emplearse en Internet de las Cosas[9] u otros dispositivos semejantes, que así lo requieran por sus limitaciones.

Se realizará un relevamiento, estudio y análisis exhaustivo de los principales algoritmos, que podrían ser usados en IoT, poniendo énfasis en los del tipo Stream Ciphers, pues son los que por sus características podrían emplearse con mayor asiduidad en los dispositivos de IoT y RFID.

Se definirán indicadores utilizando otras experiencias internacionales para avaluar comportamientos y permitir comparaciones.

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 fines del año 2017 el alumno *Leonardo Parisi* se ha sumado como colaborador al equipo de investigación. Se espera que en breve más alumnos se incorporen como él.

5. BIBLIOGRAFÍA

[1] http://www.lanacion.com.ar/1753934-las-zapatillas-con-gps-dan-un-primer-paso-buscando-nuevos-mercados. Consultada el 1-3-2017.

[2] ISO/IEC 29192. Information tech-nogy - Security techniques - Lightweight Cryptography. 2012. https://www.iso.org.

[3] 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.

[4] https://www.ericsson.com/mx/news/2015-11-17-emr-es_254740126_c. Consultada el 1-3-2017.

[5] https://www.ericsson.com/en/mobility-report/reports/november-2017. Consultada el 3-2-2018.

[6] http://tn.com.ar/tecno/f5/ces-2016-las-heladeras-del-futuro-conectadas-y-con-multiples-sensores_647274

[7] http://www.nsa.gov/. Consultada el 1-3-2017.

[8] http://eprint.iacr.org/2013/404.pdf

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

descubrimiento de los mensajes cifrados o las claves que fueron empleadas.