Aproximación a la Seguridad de las Comunicaciones en Internet de las Cosas

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; cipriano1.618}@gmail.com

RESUMEN.

Ya entrado el siglo XXI un sinnúmero de dispositivos y objetos almacenan, transmiten y reciben información con escasa o nula intervención de los seres humanos. Las Redes WSN[1] y dispositivos de tipo *RFID*[2] son ejemplo de ello.

Pare el público en general estos sistemas resultan ser "invisibles". Es decir que se ignora su existencia o se tiene una visión parcial o incompleta de los mismos.

Esta invisibilidad también incluye a las tecnicas de protección y seguridad de dichas comunicaciones, transporte y almacenamiento de datos personales, en los sistemas que así lo requieren.

Todos ellos tratan con información que en la mayoría de los casos es de índole personal y por ello surge la imperiosa necesidad que sea tratada de manera segura y confidencial[1,2]. Este es un objetivo a cumplir por empresas y organismos que emplean estas tecnologías.

Este proyecto persigue realizar un estudio y análisis de los protocolos de comunicaciones seguras que podrían ser usados en Internet de las Cosas[3]. En particular en los aspectos de privacidad y protección de datos personales usando Criptografía Ligera[3].

Palabras Clave:
Internet de las Cosas, Internet of Things Protocolos, Seguridad. RFID.

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 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] Wireless Sensor Network: Redes Inalámbricas de Sensores.
[2] Radio Frequency Identification: identificación por radiofrecuencia.
[3] Internet of Things: Internet de las Cosas.

1. INTRODUCCIÓN.

Aunque se emplee con más asiduidad día tras día y se tenga la sensación que siempre "ha estado ahí", la IoT fue dada a conocer al mundo no hace tantos años atrás. Fue en una presentación[4] para la empresa Procter & Gamble (P&G) hace 18 años, más precisamente en 1999.

Kevin Ashton[4] es miembro fundador del Laboratorio de Investigación Auto-ID Center del MIT[5] (hoy llamado Auto-ID Labs[5], junto a David Brock, Dr. Daniel Engels, Sanjay Sarma y Sunny Siu y patrocinado por las empresas Procter and Gamble, Gillette, the Uniform Code Council entre otras empresas fabricantes de nivel internacional) presentó las ventajas económicas del uso RFID[6].

Y de allí al concepto de "Internet de las Cosas" no hay mucho más que un paso. Se trata de la conectividad, mediante Internet, entre objetos para una gran diversidad de objetivos y formas

Este concepto revoluciona al mundo y aún no se ha visto casi nada de lo que vendrá. En el próximo mes de Octubre en Barcelona, España, se realizará la 2da edición del "IoT Solutions World Congress" [6] por ejemplo con usos medicinales, comerciales, científicos, hogareños y hasta militares[7].

La historia se inicia con las conocidas "etiquetas antirrobo" que se adhieren a libros, prendas y demás objetos en librerías y shoppings. Luego aparecieron otros objetos, como las llaves "computadas" de vehículos, los "tags" para abonar peajes y tarjetas para el pago electrónico de pasaje en transporte público (tarjetas SUBE, Monedero, etc.). Pero menos conocidos por su reciente aparición y no tan masiva difusión como son los pasaportes, licencias de conducir, documentos de Identidad y hasta incluso minúsculos chips subcutáneos[7], entre otros dispositivos y sistemas a implementar[8].

La consultora internacional McKinsey & Company tiene una visión de la IoT desde un punto de vista más global y no solamente técnico: "Connecting physical objects is creating new business models, improving processes, and can reduce costs and risks"[8] [9]. Sino que además augura que el impacto de IoT a escala mundial será de u$s $11{,}1 \times 10^{11}$ (más de once billones de dólares[9]) por año, para el año 2025[10].

Se espera que la IoT ingrese a casi todos los ámbitos de nuestras vidas y cambie la sociedad en la que vivimos. La mayoría de estos dispositivos manejarán información vital y sensible. Y de ahí la imperiosa necesidad de proteger su valiosa carga. Sin embargo no todos estos dispositivos tienen la capacidad para hacerlo por las capacidades limitadas de espacio, energía y recursos. Es por ello que el empleo de la Criptografía Ligera aplicada a la Internet de las Cosas se convierte en una solución [11,12].

Esta investigación se centrará en encontrar la mejor relación costo-beneficio-seguridad para las comunicaciones en Internet de las Cosas mediante el uso de Criptografía Ligera

Incluso las modificaciones de protocolos ya existentes, como el advenimiento de nuevos protocolos específicos exclusivos pensados para aplicaciones de IoT deben somerterse a exhaustivos análisis que permitan dotar de seguridad a esta tecnología. [13-15].

---

[4] Tecnólogo y científico británico.

[5] Massachusetts Institute of Technology: una de las principales universidades de Estados Unidos y del mundo, se enfoca principalmente en investigación, disciplinas científicas y educación tecnológica.

[6] Radio Frequency Identification: en español identi-ficación por radiofrecuencia.

[7] Más propio de la Ciencia Ficción que de la realidad. Sin embargo ya es una "vieja" tecnología del año 2004, registrada por la empresa VeryChip que logró la autorización de la FDA, la Administración de Alimentos y Medicamentos de Estados Unidos, para el registro de datos médicos en seres humanos.

[8] La conexión de objetos físicos está creando nuevos modelos de negocio, mejorando procesos y puede reducir costos y riesgos.

[9] "11.1 trillons of dollars" según el informe, equivalen a 11.100.000.000.000 de dólares en nuestra forma de expresar cantidades.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO.

Se realizará un relevamiento, estudio y análisis exhaustivo de los principales protocolos de comunicaciones que podrían ser usados en IoT.

Se realizará un análisis de riesgos para determinar el grado de exposición en los aspectos de privacidad, protección de datos personales y seguridad en las comunicaciones electrónicas.

Se definirán indicadores utilizando las experiencias publicadas en trabajos internacionales para evaluar comporta-mientos y permitir comparaciones.

Se volcarán los resultados obtenidos en una tabla comparativa sobre el comportamiento de algoritmos usando los protocolos de comunicaciones estudiados.

Finalmente se redactará un informe final con los resultados obtenidos.

3. RESULTADOS OBTENIDOS/ ESPERADOS.

El objetivo de este proyecto es realizar un análisis comparativo, de acuerdo a criterios de aplicabilidad y seguridad, de 3 Algoritmos Criptográficos Livianos para dispositivos RFID de bajo costo.

Se realizará un relevamiento exhaustivo de los principales algoritmos criptográficos ligeros existes y determinará cuáles se podrían utilizar para dispositivos RFID de bajo costo.

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

Se simulará el funcionamiento de los algoritmos seleccionados y se realizará una tabla comparativa sobre el comportamiento de los algoritmos estudiados.

Finalmente se redactará un informe final y se presentarán en diferentes congresos los resultados obtenidos de esta investigación, para difusión y conocimiento de la comunidad científica.

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.

Dado que este proyecto recién inicia se espera que en breve se sumen a él alumnos de las carrera de Ingeniería en Informática y Licenciatura en Sistemas de Información.

5. BIBLIOGRAFÍA.

[1] Román R., Nájera P., López J. “Los Desafíos De Seguridad En La Internet De Los Objetos” University of Malaga, España. 2010.

[2] Heer, T.; Garcia-Morchon, O.; Hummen, R.; Keoh, S.L.; Kumar, S.S.; Wehrle, K. “Security challenges in the IP-based internet of things”. Wirel. Pers. Commun. 61, 527– 542. 2011.

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

[4] http://www.rfidjournal.com/articles/view ?4986. Consultada el 1-3-17.

[5] https://autoidlabs.org/. Consultada el 1-3-17.

[6] http://www.iotsworldcongress.com Consultada el 1-3-17.

[7] Radio frequency identification ready to deliver, Armed forces communications and electronics association 2005. http: //www.afcea.org .

[8] http://www.lanacion.com.ar/1892969-club-tigre-chips-bajo-la-piel-una-tecnologia-de-identificacion-practica-o-invasiva. Consultada el 1-3-17.

[9]http://www.mckinsey.com/global-themes/ internet-of-things. con-sultada el 1-3-17.

[10] Manyika, J.: Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; The Internet of Things:Mapping the Vaule Beyond the Hype.Executive Summary. McKinsey Global Institute.2015.

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

[12] Bhattasali Tapalina. "LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment". University of Calcutta. 2013.

[13] Garcia-Morchon, O.; Keoh, S.; Kumar, S.; Hummen, R.; Struik, R. "Security Considerations in the IP-based Internet of Things". IETF Internet Draft draft-garcia-core-security-04; The Internet Engineering Task Force (IETF): Fremont, CA, USA, 2012.

[14] Cirani S., Ferrari G., Veltri L. "Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview". Algorithms 2013, 6, 197-226;

[15] Garcia-Morchon, O.; Keoh, S.; Kumar, S.; Hummen, R.; Struik, R. "Security Considerations in the IP-based Internet of Things". IETF Internet Draft draft-garcia-core-security-04; The Internet Engineering Task Force (IETF): Fremont, CA, USA, 2012.