Análisis comparativo de Algoritmos Criptográficos Livianos para dispositivos RFID de bajo costo

Mg. Jorge Eterovic; Mg. Domingo Donadello; Esp. Marcelo Cipriano;
Lic. Mara Capuya; Esp. Pablo Pomar

Programa CyTMA2 / Departamento de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza
Florencio Varela 1903 (B1754JEC), San Justo, (5411) 4480-8900

eterovic@unlam.edu.ar; ddonadel@ing.unlam.edu.ar; cipriano1.618@gmail.com;
mcapuya@gmail.com; pablo_pomar@yahoo.com.ar

1. Resumen.

El desarrollo de la Internet de los objetos dará lugar a un inmenso despliegue de millones de objetos inteligentes que interactuarán entre sí y con Internet. El papel de la tecnología RFID será primordial en este escenario.

El ritmo de adopción del RFID es vertiginoso y ya se ha convertido en una realidad. Las etiquetas de bajo costo representan el mayor desafío en términos de seguridad y privacidad pero sus escasos recursos influyen sobre los métodos criptográficos existentes.

El objetivo de éste proyecto de investigación es realizar un análisis comparativo del comportamiento de los Algoritmos Criptográficos Livianos existentes para ser usados en dispositivos RFID de bajo costo.

Palabras Clave:

Criptografía Ligera, Algoritmos Criptográficos Livianos, RFID

2. Contexto.

La Universidad Nacional de La Matanza mantiene una política en la que se fomenta y promueve la investigación académica y la inclusión en ella de alumnos de grado, posgrado y maestría.

Es por ello que esta línea de investigación se en marca en el siguiente programa:

- Programa CyTMA2 (Programa de Investigación Científica, Desarrollo y Transferencia de Tecnologías e Innovaciones. UNLaM).

3. Introducción.

Cuando se habla sobre Internet de las Cosas, Internet of Things (IoT) por sus siglas en inglés), en realidad de lo que se está hablando es de la conectividad a través de Internet entre objetos. Pero Internet de las cosas va mucho más allá. Estas cosas van desde electrodomésticos controlados por un Smartphone hasta niveles más profesionales.

Con la Internet de las Cosas, todo lo real se convierte en virtual, lo que significa que cada persona y las cosas tienen una ubicación en Internet. Estas entidades virtuales pueden producir y consumir

servicios y colaborar entre sí con un objetivo en común.

La manera en que estos objetos pueden comunicar o recibir información es a través de sensores que en algunos casos, pueden visualizarse. Pero no siempre es posible notar su presencia. Dentro de la conexión de los objetos con los sistemas de información, dos son las tecnologías clave que ya se están insertando en diversos sectores de la industria para acercar la Internet de las Cosas a la realidad. Estas tecnologías son la identificación por radiofrecuencia (RFID) y las redes de sensores inalámbricas.

La International Telecommunication Union (ITU), en su "Informe sobre la Internet de las Cosas" califica a la tecnología RFID como un "pivote que habilitará el Internet de las Cosas", permitiendo la conversión de los "objetos cotidianos" en "inteligentes" [1]. Sin embargo, sin bases sólidas de seguridad, es posible que estos objetos sean pasibles de ataques. Estas amenazas podrían llegar a ser cada vez más perjudiciales que cualquiera de sus beneficios [2,3].

Las investigaciones sobre algoritmos criptográficos están avanzadas y cada día se generan nuevos algoritmos para las claves de autenticación. La investigación académica y la Asociación Internacional de Investigaciones en Criptografía (IACR-International Association for Cryptologic Research) [4], en particular, impulsaron la definición de distintos mecanismos que proporcionaron un nivel de seguridad y privacidad adecuados a las limitaciones del hardware de las etiquetas RFID.

Se trabaja continuamente sobre el área que dio en llamarse “Criptografía Ligera” [5] y se abordan los temas de privacidad, protección de datos personales y seguridad en las comunicaciones electrónicas sobre las amenazas específicas para las aplicaciones RFID.

La Criptografía Ligera o Liviana (LICRYPT - Lightweight Cryptography) es un nuevo campo de investigación que apunta a estudiar métodos criptográficos con el fin que puedan utilizarse en objetos inteligentes.

La LICRYPT está orientada a Hardware o Software, determinándose parámetros para evaluar y medir las implementaciones que apliquen a este tipo de criptografía. Por ejemplo para hardware se estudian el tamaño de los chips y el consumo de energía que se requiere. Para software, en cambio, se analizan la longitud del código, el uso y consumo de memoria Ram.

En LICRIPT se podrán encontrar: algoritmos de clave pública, clave privada, block ciphers y stream ciphers. Además funciones hash y mecanismos de autenticación, como pueden hallarse en la criptografía tradicional.

La comunidad científica, a la actualidad, aún no tiene un criterio determinado para clasificar a un algoritmo criptográfico como ligero. Lo que sí está claro es que las técnicas criptográficas involucradas tienen que usar la mínima cantidad de recursos posibles de los objetos en los que se las aplicará.

4. Líneas de Investigación, Desarrollo e Innovación.

Muchos son los avances a nivel de criptografía que se están realizando, pero no todos los algoritmos livianos son eficientes a la hora de implementarlos en la seguridad de los RFID de bajo costo.

La presunción que es posible evaluar el desempeño general de un algoritmo perteneciente a LICRIPT funcionando

sobre una determinada plataforma móvil [6,7,8].

El mismo podrá ser un teléfono celular en particular, una tablet, un dron, lentes como el google glass o equivalentes con capacidad de comunicaciones, o cualquier otro tipo de dispositivo inteligente y portable, para el cual querrá hacer que ejecute un algoritmo determinado. Tal equipo será simulado a través de una virtualización.

De esa manera obtener las métricas que permitan determinar la performance del mismo y emitir un juicio acerca de su comportamiento.

Esta línea de investigación propone evaluar la posibilidad de determinar el funcionamiento performático de un algoritmo criptográfico [9-16] ejecutado en distintos perfiles de HW/SW. Luego, poder evaluar su comportamiento para ser aplicados en dispositivos RFID de bajo costo.

5. Resultados y Objetivos.

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.

Se desarrollará un capítulo específico de "Criptografía Ligera" en la materia electiva Criptografía y "Aplicaciones de Criptografía Ligera" en la materia Auditoria y Seguridad informática de la carrera de Ingeniería en Informática del DIIT.

6. Formación de Recursos Humanos.

La Lic. Mara Capuya se suma al equipo de investigadores como alumna de la Maestría en Informática de la UNLaM. Tanto la Lic. Capuya como el Esp. Pablo Pomar se encuentran desarrollando su trabajo de tesis de posgrado de la Maestría en Informática. Ambos están siendo tutoreados por el Mag. Jorge Eterovic, director del proyecto de investigación y por el Esp. Marcelo Cipriano.

Asimismo parte del equipo de investigación dictan la asignatura electiva Criptografía en el 5to. Año de la carrera de Ingeniería Informática de la UNLaM, invitarán a sus alumnos a participar de la investigación. Dado que es un proyecto nuevo, aún no se ha logrado la incorporación de ningún alumno.

7. Referencias

[1] Instituto Nacional de Tecnologías de la Comunicaciòn y Agencia Española de Protecciòn de Datos.: Guìa sobre seguridad y privacidad de la tecnologìa RFID. Spain. 2010. www.inteco.es

[2] Román R., Nájera P., López J. "Securing the Internet of Things". University of Malaga, Spain. 2011.

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

[4] International Association for Cryptologic Research. 2015. http://www.iacr.org/events/

[5] Bhattasali Tapalina. “LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment”. Research Scholar, University of Calcutta. 2013.

[6] 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.

[7] 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.

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

[9] Suzaki,T. Minematsu K., Morioka S., Kobayashi E. “TWINE: A Lightweight, Versatile Block Cipher”. NEC Corporation, Japan. 2014.

[10] Bogdanov A., Knudsen L., Leander G. et al. “PRESENT: An Ultra weight Block Cipher”. Springer-Verlag Berlin Heidelberg 2007 HES 2007, LNCS 4727, pp. 450–466. 2007.

[11] Wentao Z. , Zhenzhen B., Dongdai L., Rijmen V., Yang B.,Verbauwhede I.. “RECTANGLE: A Bit-slice Ultra-Lightweight Block Cipher Suitable for Multiple Platforms”. China, Bélgica. 2015.

[12] Beaulieu R., Shors D y otros. “The SIMON and SPECK Families of Lightweight Block Ciphers”. Cryptology ePrint Archive: Report 2013/404. 2013.

[13] Mouha N., Mennink B., y otros. “Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers”. Department of Electrical Engineering, Leuven and iMinds, Bélgica. 2013.

[14] Hongjun W., Tao H. “JAMBU Lightweight Authenticated Encryption Mode and AES-JAMBU (v1)” Division of Mathematical Sciences Nanyang Technological University, Singapur. 2014.

[15] Engels D., Fan X., Gong G., Hu , H , Smith M. “Hummingbird: Ultra Lightweight Cryptography for Resource-Constrained Devices.” 1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC’2010). Tenerife, Canary Islands, Spain, 2010.

[16] ISO/IEC 29192-2:2012. Information technology - Security techniques - Lightweight cryptography - Part 2: Block ciphers. 2012.