CRIPTOGRAFÍA LIVIANA PARA INTERNET DE LAS COSAS E INTERNET DE LAS COSAS INDUSTRIAL

LIGHTWEIGHT CRYPTOGRAPHY FOR THE INTERNET OF THINGS AND THE INDUSTRIAL INTERNET OF THINGS

Investigadores USAL:
Cipriano, Marcelo José (marcelo.ciprirano@usal.edu.ar); Eterovic, Jorge Esteban; García, Edith Noemí; Torres, Luis Antonio

Alumna practicante USAL:
Lomoro, Agostina

Palabras clave: internet industrial de las cosas, criptografía, criptografía liviana
Keywords: *industrial internet of things, cryptography, lightweight cryptography*

Resumen

La llamada cuarta revolución industrial o industria 4.0 se sustenta en los sistemas ciberfísicos. Esto permite que se lleven adelante procesos de fabricación con flexibilidad y adaptabilidad de sus medios de producción, con un notable mejoramiento en el uso de los recursos materiales, energéticos, humanos, temporales, etc. Uno de sus soportes es la internet industrial de las cosas. Este concepto es un subcampo de otro mayor llamado internet de las cosas (IoT: *Internet of Things*). Esto es la interconexión de sensores y dispositivos a través de redes de datos. Cualquier dispositivo o sensor puede ser una "cosa" interconectada con otras de su misma naturaleza o con su sistema de comando y control, recopilando e intercambiando datos, procesando información y recibiendo instrucciones. Cuando IoT nació en 1999, no se consideraba que la seguridad fuera un factor preponderante. Por la propia naturaleza de estos dispositivos, su tamaño, los recursos de memoria y energía que utilizan, no es posible implementar en ellos mecanismos de seguridad de los datos, de la información ni del canal de comunicación que establecen entre sí o con el usuario al cual sirven. Hasta ahora se han identificado al menos 3 tipos de peligros, producto de la vulnerabilidad de estos dispositivos:1) La producción de la fábrica donde ofrecen sus servicios; 2) La confidencialidad y la integridad de la información de los usuarios finales; 3) Terceras personas, empresas, organizaciones o gobiernos que pueden ser utilizados para fines maliciosos. La criptografía liviana o ligera, aunque no nace para dar respuesta a la falta de confidencialidad, autenticación, integridad y no repudio de la IoT o IIoT, sí puede usarse para tal fin. Nacida como un subcampo de la criptografía, hoy puede encontrarse una enorme cantidad de algoritmos, los que podrían ser empleados en estos dispositivos. El proyecto permite el estudio, análisis, campo de aplicación, fortalezas y debilidades de algoritmos de cifrado, intercambio de claves, autenticación, resumen (*hash*) y protocolos de seguridad, cuyas características les permiten proteger dispositivos IIoT. Tales algoritmos no

solamente son creados por el mundo de las tecnologías de la operación (OT), sino también en el de las tecnologías de la información (IT). Ambos mundos conciliados, aliados y aunando esfuerzos para enfrentar los riesgos de seguridad. Por ejemplo los algoritmos presentados en el concurso internacional propuesto por el NIST en procura de hallar el nuevo estándar para IoT.

Abstract

The so-called Fourth Industrial Revolution or Industry 4.0 is based on cyber-physical systems. This allows manufacturing processes to be carried out with flexibility and adaptability of their means of production. With a notable improvement in the use of material resources, energy, human and temporary resources, etc. One of its bases is the Industrial Internet of Things. This concept is a branch of a larger one called the Internet of Things (IoT: internet of Things). This is the interconnection of sensors and devices through data networks. Any device or sensor can be a "thing" interconnected with others of the same nature or with its command and control system, collecting and exchanging data, processing information and receiving instructions. When IoT was born in 1999, security was not considered to be an overriding factor. Due to the very nature of these devices, their size, the memory and energy resources they use, it is not possible to implement security mechanisms for the data in them, nor security mechanisms in the information and communication channel that they establish with each other or with the user they serve. So far, at least 3 types of hazards have been identified, as a result of the vulnerability of these devices:- the production of the factory where they offer their services.- the confidentiality and integrity of the information of the end users- third parties, companies, organizations or governments as they can be used for malicious purposes. Light Cryptography, although it doesn't solve the problem of lack of confidentiality, authentication, integrity and nonrepudiation of the IoT or IIoT, can be used for this purpose. Born as a branch of Cryptography, today a huge number of algorithms can be found and used in these devices. The project allows the study, analysis, field of application, strengths and weaknesses of encryption algorithms, key exchange, authentication, summary (hash) and security protocols, whose characteristics allows them to protect IIoT devices. Such algorithms are not only created by the world of Operation Technologies (OT), but also in that of Information Technology (IT). Both worlds have reconciled, allied and joined forces to face security risks. For example, the algorithms presented in the international competition proposed by NIST in an attempt to find the new standard for IoT.