UNA APROXIMACIÓN A LA SEGURIDAD DE LAS COMUNICACIONES EN INTERNET DE LAS COSAS USANDO CRIPTOGRAFÍA LIGERA

Investigadores USAL:
Director Eterovic, Jorge (eterovic.jorgeesteban@usal.edu.ar); Cipriano, Marcelo;
López Pasarón, Cristian

Alumno Practicante USAL:
Rodríguez, Damián

Resumen

El desarrollo de la Internet de los Objetos o Internet de las Cosas dará lugar a un inmenso despliegue de millones de objetos inteligentes, que interactuarán entre sí y con Internet. El ritmo de avance de esta nueva tecnología es vertiginoso y ya se ha convertido en una realidad.

El objetivo de este proyecto es estudiar los protocolos de comunicaciones que podrían ser utilizados en Internet de las Cosas para garantizar seguridad en las comunicaciones electrónicas y protección de datos personales, usando criptografía ligera.

La manera en que los objetos inteligentes se pueden comunicar o recibir información es a través de sensores, que en algunos casos pueden visualizarse. Para la conexión de los objetos con los sistemas de información, existen dos tecnologías clave que ya se están implementando en diversos sectores de la industria, para acercar la Internet de las Cosas a la vida cotidiana. Estas tecnologías son: RFID (*Radio Frequency Identification*: Identificación por Radiofrecuencia) y WSN (*Wireless Sensor Network*: Redes Inalámbricas de Sensores). El uso de estas tecnologías trae asociados ciertos riesgos de seguridad y privacidad. La International Telecommunication Union (ITU), en su "Informe sobre la IoT" califica a la tecnología RFID como un "pivote que habilitará el Internet de las Cosas", y permitirá la conversión de los "objetos cotidianos" en "inteligentes".

Atento a estas recomendaciones, nuestro estudio se centra en la tecnología de comunicaciones RFID, y su evolución, la tecnología RFID UHF (*Ultra Hight Frequency*), que permite implementar soluciones de manera confiable y de bajo costo.

El análisis del estado del arte nos permite identificar que las soluciones criptográficas ligeras son las más adecuadas para estos dispositivos limitados, considerando que la mayoría de los chips RAIN (acrónimo derivado de *Radio frequency Identification*) RFID y UHF tienen una pequeña cantidad de memoria.

Hemos analizado las principales implementaciones tecnológicas de los protocolos de comunicaciones factibles de ser usadas en Internet de las Cosas. Los principales riesgos y vulnerabilidades identificados tienen relación con la interfaz web insegura; la autentificación y autorización insegura; los servicios de red inseguros; la ausencia de cifrado en las comunicaciones; la privacidad; la interfaz en la nube insegura; la interfaz móvil insegura; la configuración de seguridad insegura; el *firmware* y *software* inseguros y las debilidades en la seguridad física.

Palabras clave: Internet de las Cosas; criptografía ligera; seguridad en las comunicaciones

Abstract

The development of the Internet of Things will lead to an immense display of millions of intelligent objects that will interact with each other and with the Internet. The pace of advancement of this new technology is vertiginous and has already become a reality.

The objective of this project is to study the communication protocols that could be used in the Internet of Things to guarantee security in electronic communications and protection of personal data, using Light Cryptography.

The way in which intelligent objects can communicate or receive information is through sensors, which in some cases can be visualized. For the connection of objects with information systems, there are two key technologies that are already being implemented in various sectors of the industry to bring the Internet of Things closer to everyday life.

These technologies are: RFID (Radio Frequency IDentification: Identification by Radio Frequency) and WSN (Wireless Sensor Network). The use of these technologies brings associated security and privacy risks. The International Telecommunication Union (ITU), in its "Report on IoT" qualifies RFID technology as a "pivot that will enable the Internet of Things", allowing the conversion of "everyday objects" into "intelligent".

Paying attention to these recommendations, our study focuses on RFID communications technology, and its evolution, UHF RFID (Ultra Hight Frequency) technology, which allows reliable and low-cost solutions to be implemented. The analysis of the state of the art allows us to identify light cryptographic solutions as the most suitable for these limited devices, considering that most RAIN RFID UHF chips have a small amount of memory.

We have analyzed the main technological implementations of communication protocols that can be used in the Internet of Things. The main risks and vulnerabilities identified are related to the unsafe web interface; authentication and unsafe authorization; unsafe network services; absence of encryption in communications; privacy; unsafe cloud interface; unsafe mobile interface; unsafe security configuration; unsafe firmware and software and weaknesses in physical security.

Keywords: Internet of things; light cryptography; security in communications