Criptología liviana en internet de las cosas

Lightweight cryptography in internet of things

Investigador USAL:
Cipriano, Marcelo (marcelo.cipriano@usal.edu.ar); Eterovic, J.; García, Edith.

Alumno practicante USAL:
Mariscovetere, Juan María

Palabras clave: Seguridad de las Comunicaciones; Internet de las cosas; Criptografia Liviana.
Keywords: *Communications Security; Internet of Things; Lightweight Cryptography.*

Resumen:
Internet de las Cosas (IoT) se presenta como un cambio de paradigma que afectará positivamente a la sociedad. IoT permite que cualquier dispositivo se comunique con otros e intercambie información. Son notables las aplicaciones en medicina: marcapasos inteligentes o bombas de insulina, por ejemplo. Sin embargo, IoT no fue diseñada para ofrecer seguridad. Es decir, procurar la confidencialidad, integridad y disponibilidad de la información. Tales controles pueden ser técnicos, administrativos, organizacionales y metodológicos, entre otros. Algunos de ellos están basados en aspectos informáticos, electrónicos y hasta incluso matemáticos. Estos últimos son ofrecidos por la Criptografía: algoritmos de cifrado, funciones resumen, firma digital, entre otros.

A pesar de este cambio positivo, existe una gran cantidad de publicaciones que exponen las vulnerabilidades de estos dispositivos, dado que originalmente no se contempló la seguridad entre sus principios de diseño. Estas debilidades podrían ser explotadas maliciosamente. En principio, no parece que una tostadora IoT fuera peligrosa en sí misma, pero cambia radicalmente el asunto si se trata de un marcapasos implantado en un paciente. Y más aún si tal persona es un líder religioso o gobernante, entre otras personalidades destacadas de la sociedad. En rigor, también son vulnerables aquellos dispositivos empleados en la industria, como sensores o actuadores. Ellos podrían afectar procesos de fabricación, introduciendo inadvertidamente debilidades estructurales, las que incluso podrían poner en riesgo vidas humanas. Por ejemplo, introducir fallas en automóviles inteligentes que provoquen accidentes. Estos son apenas algunos ejemplos que permiten presentar la necesidad de ofrecer la mayor seguridad a estos dispositivos.

La Criptografía tradicional no puede implementarse en entornos con capacidades tan reducidas, propia de la naturaleza de IoT. Los procedimientos matemáticos que se llevan adelante son complejos y no pueden ser ejecutados en ellos. Recursos reducidos de memoria, poder de cálculo, energía, espacio, entre otros, fueron contemplados en los principios de diseño iniciales. Por ello, los aspectos de seguridad fueron relegados. Pero la situación actual ha vuelto insostenible esta ausencia de seguridad.

A principios de siglo, se ha podido observar la aparición de algoritmos de cifrado que, por sus propiedades matemáticas y criptológicas, sí pueden ejecutarse en contextos reducidos. Así nace la Criptografía Liviana o Ligera (*Lightweight Cryptography*). Con el advenimiento de la Revolución Industrial 4.0, también llamada Internet de las Cosas Industriales (IIoT), han cobrado una relevancia enorme los aspectos de seguridad. Desde la implementación de dispositivos Supervisory Control And Data Acquisition (SCADA), autos inteligentes, hasta las Infraestructuras Críticas (IICC), que permiten al mundo civilizado "girar", ya que todos necesitan ser protegidos.

Este proyecto indagó en la naturaleza y las propiedades de algunos algoritmos pertenecientes a la Criptografía Liviana. También estudió y analizó los protocolos de comunicaciones que involucran mecanismos criptográficos. Se llevó adelante un exhaustivo relevamiento de los principales algoritmos de cifrado utilizados por la IIoT. Se analizaron sus vulnerabilidades y los ataques conocidos que cada algoritmo presentaba, destacando las características criptográficas y resistencia a diferentes ataques genéricos. Incluso se mostraron ataques en los que algunos de dichos algoritmos habían sucumbido.

Por último, se alertó acerca de la mayor vulnerabilidad de toda la infraestructura de Internet ante ataques generados por dispositivos IoT distribuidos por todo el mundo: los ataques Distribuidos de Denegación de Servicio (DDoS). Más allá de las pérdidas económicas para las empresas y los usuarios derivadas de estos ataques, resulta aterrador pensar en la posibilidad de que alguien decida "apagar Internet" mediante el uso de nuestros propios equipos IoT. Sería una crisis de consecuencias impredecibles.

Abstract

Internet of things (IoT) presents itself as a paradigm shift that will positively affect society. It allows any device to communicate with others and exchange information. Medical applications such as smart pacemakers or insulin pumps are notable. However, IoT was not designed to offer security in the confidentiality, integrity and availability of information. Such controls can be technical, administrative, organizational and methodological. Some of them are based on computer, electronic and even mathematical aspects. The latter are offered by Cryptography: encryption algorithms, summary functions, digital signature, among others.

This change is positive but there are a large number of publications that expose the vulnerabilities of these devices, since security was not originally considered among its design principles. These weaknesses could be maliciously exploited. As an example an IoT toaster does not seem to be dangerous in itself, but it radically changes the matter if it is a pacemaker implanted in a patient. And even more so if this person is a religious leader or ruler, among other prominent personalities in society. Strictly speaking, devices used in industry, such as sensors or actuators, are also vulnerable. They could affect manufacturing processes, inadvertently introducing structural weaknesses, which could even put human lives at risk. Introducing faults in smart cars that caused accidents could be an example. These are just some examples that show the need to offer the most security to these devices.

Traditional Cryptography cannot be implemented in environments with such limited capabilities as those in the nature of IoT. The mathematical procedures that are carried out are complex and cannot be executed in them. Reduced memory resources, computing power, energy, space, among others, were considered in the design principles. For this reason the security aspects were relegated. But the current situation has made the lack of security unsustainable.

At the beginning of the century, the appearance of encryption algorithms that can be executed in reduced contexts due to their mathematical and cryptological properties has been observed. This is how Lightweight Cryptography was born. With the advent of the Industrial Revolution 4.0, also

called the Internet of Industrial Things (IIoT), security aspects have gained great relevance. From the implementation of Supervisory Control And Data Acquisition (SCADA) devices, smart cars, and even Critical Infrastructures (IICC), which allow the civilized world to "turn", since they all need to be protected.

This project investigated the nature and properties of algorithms belonging to Lightweight Cryptography. He also studied and analyzed communication protocols that involve cryptographic mechanisms. An exhaustive survey of the main encryption algorithms used by the IIoT was carried out. Known vulnerabilities and attacks that each algorithm presented were analyzed, highlighting the cryptographic characteristics and resistance to different generic attacks. Attacks were even shown in which some of these algorithms had succumbed.

Finally it was alerted about the greatest vulnerability of the entire Internet infrastructure to attacks generated by IoT devices distributed all over the world: Distributed Denial of Service attacks (DDoS). Beyond the economic losses for companies and users derived from these attacks, it is worrying to think about the possibility that someone decides to "turn off the Internet" by using our own IoT equipment. It would be a crisis with unpredictable consequences.