EL PELIGRO DEL INTERNET DE LAS COSAS

Alberto Vanegas Gallardo

Gracias al Internet de las cosas (IoT por sus siglas en inglés), hay refrigeradores que indican cuándo ha caducado la comida, vehículos autónomos que encuentran la ruta más corta y espejos interactivos que recomiendan la ropa apropiada para cada ocasión. Sin embargo, son poco conocidos los riesgos que conlleva el uso de estas tecnologías. De este tema trató la conferencia *El peligro del Internet de las cosas*, parte de las Pláticas de Seguridad Informática del Instituto de Ingeniería.

El pasado 31 de mayo, en el Salón de Seminarios Emilio Rosenblueth, el maestro Cuauhtémoc Vélez Martínez y los ingenieros Mauricio Velázquez Álvarez y Julio Alfonso de León Razo describieron qué implica el uso de objetos cotidianos conectados a Internet y las nuevas formas en que pueden ser vulnerados por cibercriminales en la red.

“El concepto del IoT, del inglés *Internet of Things*, surge en principios del S. XXI. No obstante, se empezó a hablar de él en 2011 y no fue sino hasta 2014 cuando se consideró una tecnología masiva”, señaló el Mtro. Cuauhtémoc Vélez, quien describió al IoT como un “conjunto de redes de interconexión de “cosas” que pasan a ser inteligentes si pueden identificarse, nombrarse y direccionarse”. En el entendido de que una “cosa” es el nodo de una red.

El objetivo del IoT es “lograr que todo artefacto, mediante el uso de sensores y red de datos, pueda conectarse en cualquier momento y lugar con otro dispositivo o persona. Todo ello para mantener un monitoreo y control total de los procesos que cada uno de estos artefactos realice”, agregó el maestro.

El Ing. Julio Alfonso de León hizo un comparativo entre el petróleo y la información. “Hoy en día, quien tenga la capacidad de procesar mayor cantidad de datos en un menor tiempo es quien va a tener mayor poder en el futuro, como antes era con el petróleo”.

Según los expositores, el IoT ha sido posible gracias al IPv6 (Internet Protocol version 6), que permite la asignación de direcciones a miles de millones de dispositivos; el desarrollo del Wi-Fi; el uso masivo de *smartphones* y perfeccionamiento de las comunicaciones entre ellos y otros dispositivos de comunicación; el uso eficiente de baterías de mayor duración y vida útil; y la disminución de costos en la electrónica involucrada (sensores actuadores), así como la miniaturización de los componentes.

Riesgos IoT

Si bien el objetivo del IoT es mejorar la calidad de vida, su uso conlleva un incremento en el uso de datos. “Ya no se habla de gigas, ni de teras ni de petas, se comenta que con el uso del Internet de las cosas se medirá en zettabytes (unidad de almacenamiento de información cuyo símbolo es el ZB y equivale a 10^{21} bytes)”, comentaron los expertos.

Entre los riesgos más destacables se encuentra la pérdida del dispositivo que controla a los demás. En este caso puede ser el *smartphone*, que dejaría sin funcionamiento ni configuración a los gadgets conectados a él, además de que la pérdida del teléfono mismo representa ya un problema, coincidieron los expositores.

Los hackeos. Dado que los dispositivos conectados no necesariamente cuentan con un programa antivirus, es posible que los delincuentes cibernéticos instalen un *malware* y puedan acceder a todo lo que esté conectado. Otro error es poner contraseñas muy fáciles que llegan a ser sencillas de “hackear” o de conseguir gracias a la ingeniería social.

“Si hackean nuestras cámaras, también están grabando nuestra intimidad”, agregó el ingeniero Julio de León, al explicar las formas de intromisión más comunes a la vida privada que pueden llevar a cabo los criminales.

El Big Data

“Es un término empleado para describir un gran volumen de datos que tomaría demasiado tiempo y sería muy costoso cargarlos a una base datos para su análisis” y “aplica a toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales”, comentaron los ponentes de la charla.

El maestro Vélez dijo que el aprovechamiento del IoT contempla necesariamente el uso del Big Data. “En el Big Data se manejan tres elementos involucrados: volumen, variedad y velocidad, aplicados a objetos tecnológicos diseñados para ser sencillos”, agregó. Algunos expertos dirán que el Big Data “apenas está comenzando”, mientras otros afirman que “a finales del 2019 IoT generará más de 500 ZettaBytes anuales”, comentó el Ing. Mauricio Velázquez.

Para reflexionar

Para recalcar los riesgos que implica el uso del IoT, los ponentes los separaron en cinco bloques: Tecnología móvil, complejidad IoT, vulnerabilidad en la privacidad, Big Data, Inteligencia Artificial.

“En realidad somos poco conscientes de la información que generamos. No sabemos el uso y el tratamiento que terceros le puedan dar a mi información”, aseguró el Ing. De León, “¿qué garantía tenemos de que la información generada por los dispositivos no será mal empleada?”, cuestionó.

Las recomendaciones que sugieren los académicos consisten en: Investigar las características de seguridad de los dispositivos IoT antes de adquirirlos, modificar las credenciales que vienen por omisión, deshabilitar los servicios que no sean utilizados, de ser posible, crear redes dentro de la red Wifi caseras, si no hay necesidad, no conectar dispositivos a la red, cualquier dispositivo conectado a IoT es susceptible de ser hackeado.