¿Qué es IoT?

Hoy en día, la computación y la comunicación pueden estar integrados hasta en los objetos más mundanos como las bombillas, utensilios de cocina, juguetes para los niños, duchas, cepillos de dientes, etc. Esta tecnología revolucionaria se llama Internet of Things (IoT) y crea numerosas oportunidades, pero también una gran cantidad de nuevos desafíos respecto a su integridad.

Grandes mentes como Alan Turing y Nikola Tesla, ya predijeron de forma sorprendente esta revolución en diferentes entrevistas:

En 1926, Nikola Tesla en una entrevista a la revista Colliers anticipó el crecimiento de la conectividad global y la miniaturización tecnológica [1]:

> *"Cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro, que de hecho ya lo es, con todas las cosas siendo partículas de un todo real y rítmico... y los instrumentos que usaremos para ellos serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo"*

Esta visión de la tecnología del futuro también la compartió Alan Turing (considerado por muchos el padre de la informática). En 1950 en su artículo *Computing Machinery and Intelligence*[2] publicado en el Oxford Mind Journal, hizo referencia a la necesidad futura de dotar de inteligencia y capacidades de comunicación a los dispositivos mediante sensores:

> *"...también se puede sostener que es mejor proporcionar la máquina con los mejores órganos sensores que el dinero pueda comprar, y después enseñarla a entender y hablar inglés. Este proceso seguirá el proceso normal de aprendizaje de un niño"*

Esta revolución está aquí para quedarse dado que se estima que en los 3 próximos años la cantidad de dispositivos inteligentes se dispare y se sitúe entre los 20 y los 50 billones. Por ello es de gran importancia hacer frente a los desafíos que genera esta tecnología. [3]

Uno de los principales problemas de estos dispositivos es la "ciberconfianza". El botón para aceptar los términos y condiciones que casi nunca es opcional no ayuda a afianzar la confianza en estos dispositivos. Además, los componentes de terceras partes como el hardware y el

software integrado en el dispositivo, tampoco ayudan a generar esta confianza por parte de los usuarios ya que actúan como una caja negra cuando estos los utilizan. Los usuarios no saben a dónde se dirigen ni como se procesan sus datos. ¿Se está haciendo un uso adecuado de mis datos? ¿Tengo realmente privacidad? ¿Están seguros mis datos? [3]

Dado que no existe una definición universal para IoT, la creación de un estándar de seguridad es difícil y más aún desarrollar un método para medir la seguridad de estos dispositivos. Por ello, la creación de una certificación para aumentar la "ciberconfianza" en los dispositivos IoT es uno de los mayores retos a los que se enfrenta esta disruptiva tecnología. [3]

Conforme aumenta la cantidad y diversidad de estos dispositivos, tanto las empresas públicas como privadas del sector continúan explorando nuevos paradigmas y áreas en los que integrarlos. Las capacidades de seguridad de estos dispositivos aumentan a la par que el campo del IoT evoluciona y ya se pueden discernir algunas tendencias en el ámbito de la seguridad. [4]

Inicialmente, para solventar los nuevos problemas de seguridad bastaba con adaptar los modelos ya existentes, aun así, según el IoT evoluciona, se van necesitando nuevos modelos para solventar los nuevos problemas que se van generando. Un ejemplo de estos nuevos modelos son las funciones físicamente imposibles de clonar. Estas funciones se utilizan para autenticar un dispositivo y no son más que elementos de hardware que trabajan en una sola dirección como por ejemplo, el uso de huellas dactilares. Estas, son fáciles de evaluar pero muy difíciles de predecir[4].

¿Podemos confiar en que nuestros dispositivos inteligentes no nos traicionarán? ¿Podemos confiar en que nuestras camas inteligentes, electrodomésticos inteligentes y relojes mantengan el nivel de seguridad que esperamos?

A medida que los dispositivos online aumentan a niveles asombrosos, se plantean serias preguntas sobre el nivel de "ciberconfianza" que esperamos en nuestro moderno estilo de vida. Vivimos en la era de la información y sin duda la polémica sobre la privacidad y seguridad de los datos no ha hecho más que empezar.

Referencias

1. Nikola Tesla Predicted the Smartphone in 1926, acceso el 09 de Octubre del 2019, https://kottke.org/18/04/nikola-tesla-predicted-the-smartphone-in-1926

2. Computing Machinery and Intelligence, acceso el 09 de Octubre del 2019, https://en.wikipedia.org/wiki/Computing_Machinery_and_Intelligence

3. Jeffrey Voas, Rick Kuhn, Constantinos Kolias, Angelos Stavrou, Georgios Kambourakis, <<Cibertrust in the IoT Age>>, IEE Computer Society, vol 57 nº 7 (2018): 13-15

4. Rodrigo Román-Castro, Javer López, Stefanos Gritzalis, <<Evolution and Trends in IoT Security>>, IEE Computer Society, vol 57 nº 7 (2018): 16-19