Más seguridad en IoT

Juan Ignacio de Arcos
Director Técnico Programa Ejecutivo Big Data & Business
EOI Escuela de Organización Industrial

CIFRAS como 212.000 millones (IDC), 50.000 millones (Cisco), 26.000 millones (Gartner)… son proyectadas por distintos estudios de mercado de cuál será la evolución de la implantación de sensores en el mundo para el año 2020. Estos constituyen el elemento clave en el denominado Internet de las Cosas (IoT) y los encontraremos en variados ámbitos de negocio, el entorno doméstico o en nuestro propio cuerpo. El caso es que todos apuntan a cifras fabulosas de decenas de miles de millones. No sospecho que se equivoquen aunque no sea fácil predecir las implicaciones que tendrá en el ámbito económico y privado.

IoT no es nuevo. Los sensores ya forman parte de nuestra vida diaria: en los electrodomésticos del hogar, en todo tipo de vehículos de transporte, en el control de los edificios y obra pública o en las cadenas de producción industrial. Los hay activos y pasivos, aunque los más interesantes son aquellos que son capaces de generar una señal por sí solos, es decir, los activos. El problema de no haberse extendido de forma masiva probablemente radique en dos factores: su precio unitario escasamente competitivo y sus dificultades de interconexión. Sin embargo en los últimos años se ha producido un descenso importante en el precio, la conectividad se ha ampliado con la incorporación nuevos protocolos de comunicación y, además, la funcionalidad que ofrecen en dichos dispositivos se ha incrementado notablemente.

No obstante, la información que es capaz de almacenar un sensor es realmente escasa: el fabricante ha de balancear distancia (o lo que es lo mismo, potencia de la señal) con duración de su batería. Difícil elección. Además, está la frecuencia de envío de la señal, que dependerá de la criticidad de dicha información para la toma de decisiones, en el más amplio sentido.

Hasta ahora, esto no nos ha preocupado en excesivo. Pero en ese teórico futuro que nos vaticinan los analistas, nos vamos a ver rodeados en nuestro ambiente profesional y personal por estos dispositivos dispuestos a entregar su información de forma periódica para ser convenientemente digerida en servidores, casi con toda seguridad ubicados en la nube y, por tanto, sirviéndose de internet.

Y esto implica un serio problema: la reducida capacidad de almacenamiento no permite protocolos de seguridad sofisticados que impidan accesos no deseados, por no hablar ya de antivirus. Esto deviene en miles de millones de puntos débiles o brechas potencialmente accesibles por hackers o agentes inteligentes (los recientemente rebautizados bots), ya que desencriptar su exiguo código de protección será relativamente sencillo.

Misha Dohler, IEEE Fellow*, presenta un panorama inquietante. Nos dice que IoT es como el cambio climático: tenemos que actuar hoy para evitar un desastre a largo plazo, pero no sabemos cómo. No tenemos constancia de ataques masivos (aunque sí puntuales) a sensores, quizá porque aún no hay suficientes incentivos para hacerlo.Y como medida de protección, no parece probable que ahora nos dediquemos a comprobar la integridad de todos los dispositivos ya implantados, entre otras cosas, porque adolecen de una interfaz de usuario que permita su control y eventual desconexión.

Pensemos en el caso de Marie Moe**, investigadora en seguridad. Ella vive en primera persona esta inquietud. Le implantaron un marcapasos en 2012 con una interfaz wireless que facilita el ajuste de la frecuencia del dispositivo en remoto. Asimismo permite enviar información del paciente y su estado a la empresa fabricante. A ella le atemoriza la posibilidad de que un hacker pueda interactuar y desconfigurar su marcapasos o, peor aún, apagarlo, con fatales consecuencias. Desde 2008 está demostrado que esto es posible, aunque a distancias muy próximas al paciente. Hacerlo a mayores distancias es cuestión de tiempo.

Ya hay sensores que generan paquetes de datos que viajan por internet en donde el control por una entidad ajena puede generar problemas importantes: señales de tráfico, control de frenos en autos, sistemas automáticos en centrales nucleares…millones de eventos disparados automáticamente a raíz de la señal de un sensor con importantes implicaciones en nuestro confort o supervivencia.

Es necesario, pues, trabajar desde entidades públicas y privadas en nuevas políticas de protección de aquella información que podamos considerar sensible a estos efectos. El concepto de ciberseguridad se nos ha quedado corto y hemos de ampliarlo al mundo de IoT. En definitiva, más seguridad. ■

(*) Edición UK de Wired (mayo 2016). (**) https://www.wired.com/2016/03/go-ahead-hackers-break-heart/