fundaciónHermes
derechos de ciudadanía digital

El IoT

La Roomba, la tele con IA y Alexa te delatan

La lectura del estudio titulado In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homespone los pelos de punta. Publicado en octubre del año pasado, y encabezado por IMDEA Networks (de la red de Institutos Madrileño de Estudios Avanzados) y la Northeastern University, el informe pone a prueba 93 dispositivos IoT (internet of things) y su interacción con las aplicaciones móviles. Durante la presentación, uno de sus coautores, Vijay Prakash, de la NYU Tandon, declaró: "encontramos pruebas de que los dispositivos IoT desvelan información personal identificable, como la **dirección única de hardware, geolocalización o nombres de dispositivos en miles de hogares**. Cualquier indicador

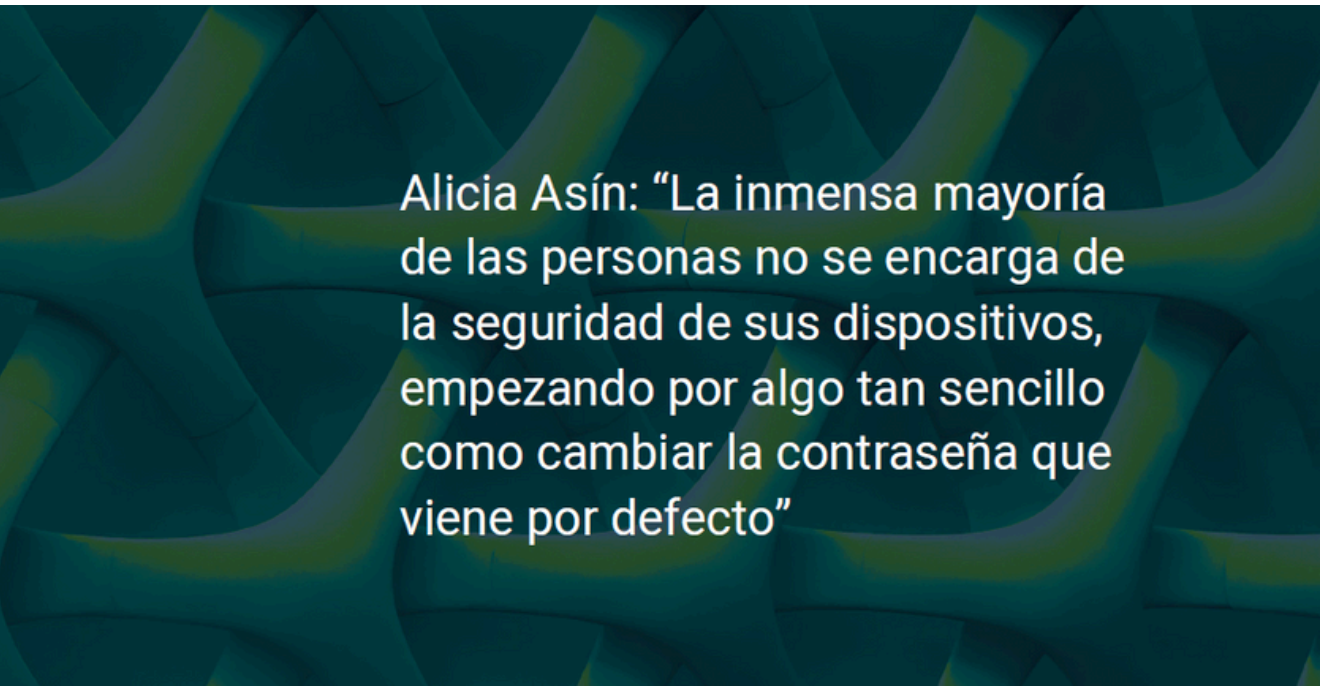
y metadato es útil para reconocer un domicilio, pero la combinación de tres hace que una casa sea única y fácilmente distinguible de manera global. A modo de comparación, si a un usuario web se le perfila utilizando la técnica más sencilla de fingerprinting, esta es tan única como 1 de cada 1.500 personas. Si se perfila un hogar inteligente con solo tres datos de estos dispositivos, este es tan único como 1 de cada 1,12 millones de hogares".

El impacto de esta investigación fue mucho más allá del mundo académico y alertó de la necesidad de que fabricantes, desarrolladores de software, operadores de plataformas IoT y móviles y reguladores tomasen **medidas para mejorar las garantías de privacidad de sus dispositivos**. El equipo del informe comunicó estos problemas a los proveedores de sistemas vulnerables y al equipo de Android de Google, lo que forzó a la compañía a mejorar la seguridad de estos productos. Pero como se sabe, basta que se cree un nuevo cortafuegos o se modernice la protección de un aparato digital, para que los hackers se pongan a trabajar en sortear las barreras.

Juguetes, relojes, robots de cocina, pulseras, pulsómetros, tensiómetros, robots aspiradores, altavoces, televisiones y vehículos son solo algunos ejemplos de objetos cuya conexión a Internet se ha normalizado en los últimos años, simplemente añadiéndoles el adjetivo 'inteligentes'.

El Comité Europeo de Protección de Datos define IoT a aquella infraestructura en la que múltiples sensores incorporados a dispositivos comunes y cotidianos registran, someten a tratamiento, almacenan y transfieren datos e interactúan con otros sistemas haciendo uso de sus capacidades de conexión en red. Estos objetos están asociados a identificadores únicos y tratan datos personales. Dicho de otro modo, **amplían la huella digital de la gente a la vez que datifican gran parte de los aspectos de su vida**. Si se considera la cada vez mayor capacidad digital para correlacionar, vincular y establecer relaciones causa-efecto, el perfil vital que se construye de una persona alcanza un gran nivel de exactitud y profundidad.

Alicia Asín, CEO de Libelium y miembro del Consejo Asesor de la Fundación Hermes destaca que al hablar de dispositivos de gran consumo (consumer IoT) se debe tener en cuenta que **la seguridad tiene que ser una responsabilidad compartida**: “La inmensa mayoría de las personas no se encarga de la seguridad de sus dispositivos, empezando por algo tan sencillo como cambiar la contraseña que viene por defecto porque no saben cómo hacerlo. Pero tampoco aparece en las instrucciones del dispositivo que esto sea lo primero que debes hacer”.



Los **ejemplos de violaciones a la privacidad** a causa de la IoT no son nuevos ni pequeños. Probablemente entre los más conocidos están los del fabricante de automóviles eléctricos Tesla, conocido por sus vehículos cada vez más autónomos. Hace ya casi una década, unos investigadores de la empresa de seguridad china Keen Lab lograron hackear de forma remota un Tesla Model S. Después de que el conductor del coche buscara algo en Internet (en este caso la gasolinera más cercana) los investigadores consiguieron tomar el control tanto del sistema multimedia como del ordenador de a bordo, llegando a abrir el techo solar, cambiar los intermitentes, mover el asiento y abrir las puertas sin usar la llave. También pudieron activar los limpiaparabrisas, plegar los espejos retrovisores y abrir el maletero mientras el vehículo estaba en movimiento. Por último,

mostraron que un operador a unos 20 km de distancia del automóvil podía manipular los frenos en movimiento. Informada Tesla de las vulnerabilidades de su modelo, la compañía de Elon Musk tardó 10 días en actualizar de forma remota el software y recompensar a los investigadores chinos.

Más allá de lo práctico

Uno puede pensar que Tesla aprendió la lección para siempre, pero resulta que no. En 2020, otro especialista en ciberseguridad, el belga Lennert Wouters, demostró que podía acceder en 90 segundos a un Model X. Primero, el experto interceptó la señal de la llave usando Bluetooth, ya que el Tesla se puede desbloquear también desde la app oficial. Luego, para que el coche arrancara, conectó un ordenador para capturar y descifrar señales a un puerto oculto en el salpicadero e indicó al software del vehículo que todo estaba en orden y que podía ponerse en marcha. Otra vez, Tesla, a rebufo de estos profesionales bienintencionados, que exponen las debilidades de su sistema, tuvo que reaccionar con celeridad y en menos de un mes actualizar las medidas de seguridad de todos sus modelos X.

90”

es lo que tardó Lennert Wouters en desbloquear un Tesla Model X

Tesla no es la única marca que tropieza varias veces con la misma piedra a la hora de no proteger adecuadamente los datos de sus conductores. Un reciente trabajo de la Fundación Mozilla, en el que se revisaron las prácticas de 25 grandes fabricantes de automóviles, desveló que **todos recopilan y analizan más datos personales de los necesarios y los utilizan con un fin distinto** al de operar el vehículo o gestionar la relación con el usuario. La mayoría comparte o vende la información y no da a los conductores la totalidad del control sobre sus datos. Más de la mitad incluso cedería todos esos parámetros a un Gobierno o autoridad policial si lo solicitan.

> La mayoría de fabricantes de automóviles cedería datos a un Gobierno o autoridad policial si lo solicitan

Lo que demuestra el caso de los fabricantes de coches es que, por más precauciones que tome el proveedor final del equipo conectado a IoT, la complejidad de los actores que participan y datos que se obtienen con esta tecnología hace **muy difícil controlar que la información personal no se vea comprometida**. En la cadena aparecen fabricantes e integradores de dispositivos, desarrolladores de soluciones, proveedores de servicios en la nube, plataformas de datos, programadores de sistemas operativos, operadores de telecomunicaciones, redes sociales, sector publicidad, etc. Es verdad que el RGDP establece responsabilidades para estos actores en función de cómo intervengan en los tratamientos de datos personales, pero no siempre es fácil identificar perfectamente las obligaciones de cada uno de ellos.

Asín afirma: "Muchas veces los dispositivos tienen errores de diseño y son vulnerables. De hecho, California fue pionera en crear una guía de best practices para la industria, donde hablaban de security by design, es decir, cuáles son los estándares mínimos de ciberseguridad que deben cumplir los dispositivos de IoT. Sin embargo, es muy importante contar con la colaboración de los consumidores y los dueños".

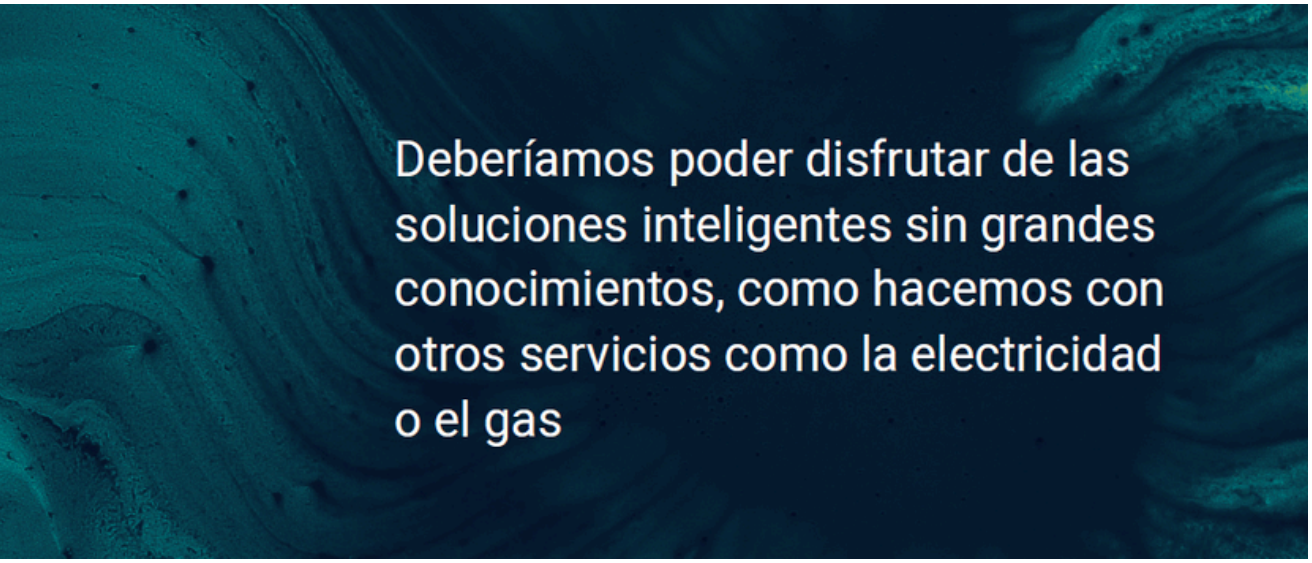
Datos inferidos

Añadido a esto, las categorías de datos personales tratados por dispositivos IoT son muy amplias: desde los básicos de contacto hasta la geolocalización, hábitos de uso de internet, intereses, registros fisiológicos como el ritmo cardiaco o la temperatura corporal, imágenes, voz, y un largo etcétera. En cuanto al **origen de la información**, a menudo los usuarios son conscientes del tratamiento de parámetros que ellos mismos facilitan o que son captados por aparatos inteligentes a través de sus sensores. Sin embargo, la obtención de evidencia personal derivada o inferida –es decir, aquella que se obtiene a través del procesamiento de los datos– es una práctica menos conocida para la mayoría de la gente.

Con frecuencia, estos datos son compartidos o vendidos a un tercero. Hace cuatro años las autoridades europeas previeron que para 2025 **un 80 % de los elementos sensibles de cualquier ciudadano será procesado por algún dispositivo inteligente**, frente al 20 % de 2018.

“Esta es la eterna reflexión”, plantea Asín: “Si el dispositivo es seguro, si eres tú el culpable de no asegurarlo lo suficiente, o si el dispositivo te dice en su política de privacidad todo lo que va a suceder. Somos nosotros los responsables finales de que estos dispositivos infieran más cosas de nuestra vida de las que somos conscientes”.

Está claro que la creciente implementación de tratamientos basados en IoT precisa de modelos de desarrollo que incorporen los requisitos normativos, estándares y mecanismos de certificación que garanticen el máximo nivel de protección de los derechos y libertades. Además, del mismo modo que una persona puede disfrutar de otros servicios como la luz eléctrica o el gas natural sin disponer de amplios conocimientos en dichas materias, debería poder utilizar soluciones inteligentes con la confianza de que no van a ser una amenaza para su privacidad.

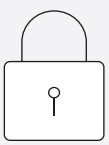


“Existen propuestas donde se plantea que se creen etiquetas similares a las del Nutriscore; etiquetas totalmente visuales, fácilmente identificables y entendibles por cualquiera, que detallen si esto recopila datos, si recopila voz, imagen, si se procesan en el dispositivo o en la nube y si se borran… Esto se podría hacer y sería mucho más sencillo para que las **políticas de privacidad** sean más inclusivas de lo que son ahora”, reclama Asín. “Creo que no va a haber una auténtica libertad por parte de los consumidores para poder decidir mientras no exista información generalizada del impacto que todos estos datos puedan tener”, añade.

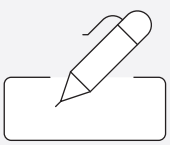
Responsabilidad de industria y consumidores

Siempre existe el riesgo de que algunos fabricantes dejen de lado importantes aspectos para la seguridad en su prisa por lanzar productos al mercado. Y si esos peligros se pasan por alto en el proceso de desarrollo, una vez puestos en marcha, existe la amenaza de que las actualizaciones de seguridad sean insuficientes.

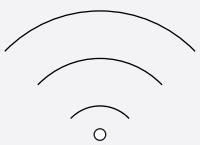
Los usuarios, para proteger su propia intimidad, están obligados al menos a cambiar las contraseñas y las credenciales de inicio de sesión de los dispositivos IoT, utilizando una clave larga (al menos 12 caracteres), que contenga una combinación de letras mayúsculas y minúsculas, además de símbolos y números. También es más seguro cambiar el nombre que viene de fábrica del router y utilizar un método de cifrado seguro para la configuración del aparato (por ejemplo, WPA2 o posterior). Y si el router da la opción, no está de más crear una red inalámbrica para invitados ante la duda de que sus equipos estén infectados.



Clave de al menos 12 caracteres



Cambiar el nombre de fábrica del router



Red inalámbrica para los invitados

Alicia hace hincapié en la **responsabilidad de la industria** por facilitar información sobre la activación de los mecanismos de seguridad, pero también en la responsabilidad de los consumidores, para que “nos informemos y seamos conscientes de que esto es algo que tenemos que hacer”, ya que “las personas son responsables de leer las políticas de privacidad de los dispositivos que están instalando en sus casas”.

Lo más importante, sin embargo, es asegurarse de que el vendedor de un dispositivo IoT proporciona las actualizaciones para aplicarlas cada vez que estén disponibles. Estas mejoras del software son una parte fundamental para la seguridad de los aparatos inteligentes. Para los hackers es mucho más fácil vulnerar los sistemas antiguos.

Por último, hay que **evitar el manejo de estos sistemas** a través de un móvil cuando se está fuera de casa; en una cafetería, un centro comercial o un aeropuerto. Es muy cool y moderno (sobre todo hacerlo delante de otros), pero muy peligroso para la privacidad.