




SEGURIDAD EN EL INTERNET DE LAS COSAS

—

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

SEGURIDAD EN EL INTERNET DE LAS COSAS

El término "Internet de las cosas" (Internet of things, en adelante IoT) es una expresión en auge que hace referencia a objetos comunes que con el avance de la tecnología se están interconectando a Internet. El término IoT se introdujo cuando el número de dispositivos fue mayor que el número de personas conectadas a Internet, entre 2008 y 2009. Hoy en día es habitual que la mayor parte de ciudadanos dispongan de un smartphone, una tablet o un equipo portátil. Esto hace que se tenga acceso permanente a Internet sin importar el lugar donde se encuentre el usuario. Asimismo, casi un 70% de los hogares españoles¹ disponen de Internet. Según el informe del ONTSI, en el tercer trimestre de 2013 los dispositivos que más han aumentado son las tablets (28,5 % de los hogares), las televisiones (78,6 %) y los ordenadores portátiles (62,5 %). Como se ha comentado anteriormente, el término IoT va mucho más allá, y engloba objetos comunes que hasta ahora no disponían de conectividad. Con esta evolución, algunos elementos como neveras, hornos, lavadoras, coches, relojes, televisores y un largo etcétera disponen ya de conexión a Internet. La conectividad de estos elementos permite, entre otras muchas cosas, controlar el objeto de forma remota a través de otro dispositivo o una aplicación a través de Internet. Además permite recibir información externa como puede ser el caso de una nevera que informa en tiempo real de la climatología en cualquier ciudad, o que se pueda consultar a través de una pantalla incorporada en la misma la caducidad de los productos, consultar el correo electrónico o leer las últimas noticias. Son algunas funciones de las que dispone este tipo de dispositivo, además de las funcionalidades habituales de cada uno. Hasta ahora Internet era una herramienta de trabajo, de consulta de información y de comunicación. Mediante esta nueva forma de interacción, hacemos que Internet sea una parte necesaria en las tareas comunes y cotidianas de la vida. Además del término IoT también se llega a denominar este fenómeno como "Internet del Todo" (Internet of Everything). La tendencia es que siga evolucionando y aumentando exponencialmente. Un ejemplo de la expansión de esta unión de la tecnología con la vida real es la domótica. Durante el boom inmobiliario las casas de nuevas construcción empezaron a disponer de este tipo de sistema, que venía preinstalado en el domicilio. La domótica permite que muchas familias en su vida diaria realicen de forma remota y/o automática acciones como encender la calefacción, abrir y cerrar persianas, encender y apagar las luces, controlar el acceso al domicilio, y un largo etcétera. Hoy en día los estudios indican que hay numerosos hogares utilizando este sistema interconectado también a Internet, y se espera que sigan en aumento. Algunos de los dispositivos más conocidos que están liderando la expansión de IoT son los llamados wearables. Son pequeños dispositivos que una persona



puede llevar puestos y que pueden capturar información de ciertas actividades que realiza. Además, pueden proporcionar otro tipo de información al usuario como puede ser la hora, el tiempo o incluso las notificaciones que se reciben en él mismo o en un teléfono móvil enlazado. Un ejemplo claro de un dispositivo wearable son los relojes que disponen GPS que geoposiciona al usuario, además de disponer de acelerómetro, pulsómetro, etc. Algunos de estos relojes además de sincronizar la actividad con otros dispositivos o redes sociales, son capaces de recibir correos, mensajes, e incluso llamadas, por lo que en la mayoría de ocasiones la información es almacenada en la nube. Otros ejemplos de wearables son gafas (como es el caso de las famosas Google Glass), sensores incorporados en la ropa o zapatillas (como es el caso de las Nike+), localizadores incorporados en llaves, y se espera que en un futuro no muy lejano haya biosensores destinados a medir variables médicas como glucosa o colesterol. Internet ha sido y sigue siendo una revolución y su llegada a dispositivos de uso cotidiano IoT va a generar grandes cambios y, si cabe, generar más necesidad de disponer de estos tipos de dispositivos y, en consecuencia, de mayor conectividad a Internet. De esta forma, el tráfico que circulará por la red va a aumentar exponencialmente en los próximos años con la expansión de IoT y... ¿quién sabe qué será lo siguiente? Según el IBSG de Cisco, en un estudio de 2011², calcularon que en 2020 habrá 50.000 millones de dispositivos conectados a Internet, a una media de 6,58 dispositivos conectados por persona.


Riesgos asociados En este apartado vamos a analizar los riesgos asociados a la evolución de IoT. Los riesgos varían en función de la criticidad del dispositivo ya sea por la función que realizan o por la dependencia que se tenga del mismo. En cualquier caso, vamos a analizar algunos de los riesgos más comunes y las áreas que pueden verse afectadas ante la materialización de una amenaza. Más adelante nos centraremos en riesgos que pueden ser propios de determinados dispositivos. La materialización de las amenazas a las que están expuestos nuestros dispositivos puede afectar a la accesibilidad del dispositivo, a la integridad de la información que contiene y a la identidad del usuario que la posee ya que puede provocar una suplantación de identidad. Y no nos quedamos ahí, ya que la disponibilidad quizá sea uno de los aspectos que más problemas puede generar, principalmente si hablamos por ejemplo de entornos industriales donde una parada del servicio debido a un ataque de denegación de servicio (DoS) entre otros, puede provocar grandes pérdidas. Otro factor a tener en cuenta y directamente relacionado con la información es la confidencialidad de los datos, que se debe garantizar tanto a la información almacenada en el dispositivo como a la transmitida en las comunicaciones que éste realice, más si son a través de Internet. Todos estos factores son considerados riesgos asociados a IoT. Para determinar el nivel riesgo que produce la materialización de estas amenazas vamos a concretar algunas situaciones que se pueden producir en determinados dispositivos.

- **Posicionamiento GPS.** Como hemos comentado anteriormente, los wearables son dispositivos que un usuario lleva puestos. Por lo general, estos van conectados a Internet por lo que pueden ser fácilmente geoposicionados en todo momento (algunos incluso incluyen módulos GPS dedicados a ello).

Esto hace que la localización del usuario quede registrada en algún sitio web y, en función de la configuración de privacidad pueda estar al alcance de cualquiera. Esta situación se produce también al usar un smartphone si no sabemos qué aplicaciones tienen acceso a la localización. Para ampliar información sobre este riesgo, en CSIRT-CV hemos realizado una campaña sobre el uso seguro de los dispositivos wearables⁵.

- Robo de información. Como se ha comentando, en los dispositivos que conectamos a Internet cada vez almacenamos más información. En muchos casos, y dada la nueva mentalidad de la nube (o cloud), podemos acceder a esa información desde otros dispositivos a través de Internet, desde aplicaciones móviles o desde entornos web donde para acceder disponemos de un usuario y una contraseña. En caso de que un tercero pudiera acceder, dispondría de información que podría vulnerar nuestra privacidad. En cualquier caso el robo de información puede no producirse debido a una debilidad en el acceso, ya que como los dispositivos wearables son cada vez más pequeños, la facilidad de perderlos también es un riesgo que puede facilitar a cualquier persona acceso directo a nuestra información. El uso de aplicaciones en dispositivos conectados a Internet puede hacer pública cierta información, como es el caso de las aplicaciones de salud y vida sana que pueden publicar la posición GPS, las calorías quemadas durante la carrera, la edad, la altura, el peso, los kilómetros recorridos,... y todo ello en ¡tiempo real!

- Control y uso malintencionado de los dispositivos. Otro de los riesgos al que nos enfrentamos en esta nueva era son los ataques que pueden llegar a tomar el control de los dispositivos que utilizamos. Dispositivos que después de un ataque aprovechando una posible vulnerabilidad son controlados por terceros de forma remota. Vamos a imaginarnos por un momento que un atacante consiguiese controlar nuestro frigorífico, nuestro horno, nuestra lavadora, o incluso como ya ha ocurrido⁶, nuestro coche. El uso no legítimo de alguno de estos dispositivos puede afectar a la seguridad e integridad física de sus usuarios. Los riesgos que se han mencionado en este apartado del informe no son aspectos tan remotos o lejanos como pueden parecer, ya que la probabilidad de que se materialicen es considerablemente alta si no se aplican las salvaguardas adecuadas. Aunque quizá pensemos que estas situaciones ocurren en entornos personales y de ámbito reducido, debemos tener en cuenta, como ya hemos mencionado también, que IoT ha llegado también a los entornos profesionales e industriales. En estos entornos además de los dispositivos que podemos encontrar y utilizar en cualquier hogar, hay Infraestructuras Críticas monitorizadas en tiempo real por sistemas complejos, llamados sistemas SCADA (Supervisory Control And Data Acquisition; Supervisión, Control y Adquisición de Datos) ampliamente utilizados. Los sistemas SCADA, como parte de IoT, están integrando los sensores de las redes con Internet de modo que estos puedan ser monitorizados y controlados de forma remota. En algunos sistemas SCADA incluso se gestionan flujos de datos recibidos de subestaciones (UTR, Unidades Terminales Remotas) como es el caso de sistemas de control de tráfico, sistemas de transporte o sistemas de distribución de agua entre otros. De esta forma recolectan y gestionan información recibida por sensores y la transmiten al sistema central. Asimismo se está extendiendo también el uso de redes de sensores inalámbricas (Wireless Sensor Networks, en adelante WSNs). Estos son dispositivos que transmiten los datos al sistema



SCADA de forma inalámbrica. Por tanto es evidente el riesgo que corren estas infraestructuras al utilizar sensores inalámbricos para el intercambio de información y control de los sistemas, que aumenta considerablemente si está conectado a Internet. Es obvio que la seguridad en los sistemas SCADA es un aspecto que debe estar en constante mantenimiento y control ya que detrás de estas redes hay Infraestructuras Críticas como sistemas de energía, de transporte, de agua, de salud, etcétera, que afectar a seres humanos. Para finalizar este apartado, la comunicación inalámbrica sea quizá uno de los riesgos a los que más expuestos nos encontremos puesto que en redes domésticas lo más generalizado es disponer de una red Wifi y, si esta red es insegura se convierte en una puerta de acceso a nuestra red y por tanto a todos nuestros dispositivos conectados a ésta (como pueden ser el horno, la lavadora, la calefacción,...). Por tanto debemos asegurarnos que los accesos a la misma sean legítimos.