J. Lopez, R. Roman, and P. Najera, "Los Desafíos de Seguridad en la Internet de los Objetos", *Revista SIC*, vol. 88, pp. 66-73, 2010.
NICS Lab. Publications: https://www.nics.uma.es/publications

LOS DESAFÍOS DE SEGURIDAD EN LA INTERNET DE LOS OBJETOS

Javier López (Catedrático de Universidad, jlm@lcc.uma.es), Rodrigo Román (Investigador Doctor, roman@lcc.uma.es), Pablo Nájera (Investigador, najera@lcc.uma.es)
Universidad de Málaga

RESUMEN: El paradigma de la Internet de los Objetos, donde todos aquellos objetos físicos que nos rodean tendrán la capacidad de generar y consumir información en el ámbito de un mundo virtual, se encuentra cada vez más cerca. Es ahora un buen momento para llamar la atención sobre sus principales desafíos de seguridad, partiendo de sus elementos más importantes (la tecnología RFID y las redes de sensores) hasta llegar a un punto de vista global. Una vez este paradigma pueda ser plenamente comprendido y protegido, podrá evolucionar hacia uno de los nuevos pilares del futuro. Los contenidos de este artículo nacen tanto de la experiencia profesional de sus autores como del estado del arte existente a nivel académico y a nivel legislativo e industrial.

INTERNET DE LOS OBJETOS, UNA NUEVA REALIDAD

Una Internet intrínsicamente diferente está emergiendo. Desde la ARPANET original que conectaba un restringido conjunto de universidades, hasta el Internet actual con más de mil millones de usuarios, esta red de redes ha revolucionado y agilizado nuestros modelos de comunicación a nivel global. Si bien la evolución que hemos vivido podría parecernos ya vertiginosa, la que está al llegar se prevé notablemente superior. Hasta el momento, el Internet que conocemos ha estado orientado desde y hacia las personas, donde prácticamente la totalidad de los 200.000 petabytes (1 petabyte = 1024 terabytes) de información que se estima contiene Internet ha sido generada por los seres humanos empleando algún mecanismo de entrada de datos. Sin embargo, en la inminente "Internet de los Objetos" ('Internet of Things' en su versión anglosajona) los actores capaces de generar y consumir información, interactuando entre ellos, serán los objetos que nos rodean: no sólo dispositivos eminentemente tecnológicos (como automóviles o frigoríficos), sino también objetos originalmente ajenos a este entorno (p. ej. prendas de ropa o alimentos perecederos), e incluso seres vivos (p.ej. plantaciones, bosques y ganado) pasan a ser elementos interconectados de la red de redes.

Esta incorporación de capacidades computacionales en todo tipo de objetos y seres vivos proporcionará un salto cualitativo y cuantitativo en diversas áreas. Es más, pocos serán los sectores que no se verán afectados y, a priori, beneficiados por la Internet de los Objetos. Por ejemplo, en el sector sanitario los pacientes podrán mejorar su calidad de vida siendo tratados de sus enfermedades en su propio hogar, gracias a avances en telemedicina, telecontrol, administración automática de medicinas, y otros. Los sistemas de medición eléctrica inteligentes favorecerán al sector de la energía, pudiendo conocer toda la información sobre el consumo en tiempo real y adaptando su funcionamiento a dicho consumo. La industria de las telecomunicaciones podrá explorar nuevas posibilidades comerciales en forma de nuevos servicios centrados en las necesidades específicas de los usuarios. Los coches podrán proporcionar, a través de una inteligencia colectiva, datos anónimos que permitirían una optimización del tráfico en las ciudades. Existen otras muchas aplicaciones que podrán aprovecharse de este nuevo paradigma: logística, alimentación, domótica, entretenimiento, etc.

FIGURA 1 AQUÍ

Para los organismos oficiales que gobiernan Europa, el rol que jugará la Internet de los Objetos en el futuro de la Unión Europea es claro. Tanto la ITU, organización responsable de la estandarización en el ámbito de telecomunicaciones, como el ISTAG, el grupo establecido por la Comisión Europea para ofrecer recomendaciones sobre cómo afrontar las nuevas tendencias en ICT, indican que la Internet de los Objetos "es una revolución tecnológica que representa el futuro de la computación y las comunicaciones", indicando que "no es ciencia ficción ni promoción industrial, sino que tiene su base en sólidos avances tecnológicos y visiones de ubicuidad de las redes que se están haciendo realidad religiosamente" [1]. Respondiendo a esta necesidad, las últimas ediciones del Programa Marco de Investigación y Desarrollo ya han financiado múltiples proyectos que abordan diferentes ángulos de esta problemática, y existe en compromiso de seguir financiando proyectos en este ámbito. Hay que puntualizar que Europa no es la única que está apostando por este paradigma. Por ejemplo, la “ciudad ubicua” de Songdo, inaugurada en agosto de 2009 en Corea del Sur y con una capacidad para 75.000 residentes y 300.000 trabajadores, es una inmensa plataforma de experimentación que permitirá a sus habitantes palpar de primera mano los beneficios del mundo interconectado que se avecina en la próxima década [2].

Un amplio conjunto de tecnologías participará en la consolidación de la Internet de los Objetos. El desarrollo de la infraestructura de redes de comunicación a través de redes de banda ultraancha y redes 3G y 4G será fundamental, así como la instauración de IPv6 que permitirá otorgar una dirección IP única a cada objeto que participe en la red. Las tecnologías que permitirán tanto la localización como la identificación de los objetos físicos serán también básicas en este contexto, Existen además tecnologías que pueden influenciar en el funcionamiento de la Internet de los Objetos, como la visión por computador, los sistemas biométricos, la robótica, y otros. Sin embargo, dentro de la conexión de los objetos a la infraestructura de los sistemas de información, dos son las tecnologías clave que han alcanzado ya la madurez y el calado suficiente en diversos sectores de la industria para acercar la Internet de los Objetos a la realidad. Estas tecnologías son la identificación por radiofrecuencia (RFID) y las redes de sensores inalámbricas.

RFID Y LA INTERNET DE LOS OBJETOS

De manera resumida, la tecnología RFID permite identificar de manera unívoca a un objeto y obtener información sobre él o su entorno gracias a los datos transmitidos de manera inalámbrica por una etiqueta RFID incorporada en el mismo [3]. En todo sistema RFID se emplean dos componentes básicos. Por una parte, la anteriormente mencionada etiqueta, que integra una cantidad limitada de memoria (de unos bytes a pocos megabits) para almacenar la información, un circuito integrado para manipular y procesar los datos, y una antena que se utiliza como medio de comunicación y como fuente de energía. Esa energía viene proporcionada por el otro elemento de la tecnología RFID, el lector RFID, que obtiene los datos de las etiquetas y las transmite a los servidores externos. La tecnología RFID es muy versátil, existiendo varias configuraciones de etiquetas (con batería incorporada, con sensores, con chips criptográficos,…) y permitiendo que el canal de comunicaciones tenga diferentes características en cuanto a distancia de lectura, velocidad y tolerancia a líquidos y metales.

FIGURA 2 AQUÍ

La tecnología RFID ha sido referenciada como la nueva generación de códigos de barras: permiten identificar a un objeto sin requerir contacto físico con el lector y carece en su mayor parte de elementos móviles y fuente de energía, igualando su tiempo de vida al del propio producto. Más allá, la tecnología RFID ofrece numerosas ventajas. No es necesaria una línea de visión directa entre lector y etiqueta. Los objetos pueden reconocerse a nivel individual (no sólo su tipo) y mantener un historial en la memoria incorporada. La comunicación puede realizarse a diferentes distancias (desde pocos centímetros a centenares de metros), y un lector puede interrogar a múltiples etiquetas de forma simultánea. Con el coste de céntimos de euro de muchas etiquetas EPC Gen2 y circuitos integrados de tan sólo 0.4 mm^2, se encuentran preparadas para su integración en todo tipo de objetos.

FIGURA 3 AQUÍ

No obstante, las prometedoras cualidades de la tecnología RFID la convierten en un arma de doble filo, principalmente debido a las amenazas a la privacidad e intimidad (p.ej. creación de perfiles sobre individuos, seguimientos no autorizados) y a la extremadamente baja capacidad de las etiquetas RFID. En términos de mecanismos de seguridad, los estándares en los que se basan las diferentes ramas de la tecnologías (p.ej. ISO/IEC 11784 – 11785, ISO 10536 – 15693, ISO 18000) proporcionan un cierto nivel de confidencialidad e integridad de los datos mediante la inclusión de mecanismos de seguridad básicos: protección a comandos de lectura mediante contraseña, direccionamiento de etiquetas mediante números aleatorios, comunicaciones enmascaradas entre lector y etiqueta, modo silencioso o protección en los comandos de escritura. Caso aparte se da en el estándar ISO 14443, orientado a sistemas de pago electrónico y documentación personal, en el que se incluyen mayores recursos criptográficos, con autenticación mediante desafío-respuesta y algoritmos triple-DES, AES o SHA-1. Tarjetas comerciales basadas en este último estándar como Mifare SmartMX llegan a incorporar coprocesadores con criptografía de clave pública con RSA y criptografía de curvas elípticas.

Por su parte, la investigación académica está dando un fuerte impulso a la definición de mecanismos que proporcionen un adecuado nivel de seguridad y privacidad dados los limitados recursos hardware disponibles en las etiquetas RFID. Las principales medidas aplicadas son: identificadores dinámicos y pseudónimos de etiqueta, esquemas de hashes encadenados para generar nuevos identificadores, protocolos de autenticación mutua ligeros e infraestructuras de gestión de claves. Con respecto a los esfuerzos específicos que abordan el problema de la privacidad, la protección de datos personales y la privacidad en las comunicaciones electrónicas cubiertos por las Directivas del Parlamento Europeo 95/46/CE y 2002/58 son aplicables a los sistemas basados en RFID, si bien en el año 2009 la Comisión Europea ha publicado la Recomendación C(2009) 3200 y el mandato M/436 para ahondar en las amenazas a la privacidad específicas de las aplicaciones RFID.

A pesar de los desafíos de seguridad existentes, el ritmo de adopción del RFID es vertiginoso y se ha convertido ya en una realidad en el mundo industrial. En 2008 se vendieron 2.200 millones de etiquetas RFID en el mundo, un tercio de ellas en Europa. Además, la Comisión Europea prevé que el uso de esta tecnología se multiplique por cinco durante la próxima década. Pero donde el papel de la tecnología RFID será primordial es en la futura Internet de los objetos. La ITU, en su "Informe sobre la Internet

de los Objetos" [1] califica a la tecnología RFID como un "pivote que habilitará el Internet de los Objetos", permitiendo la conversión de los "objetos cotidianos" en "inteligentes". Si bien los primeros escenarios con objetos inteligentes aún limitan su interacción y comunicación a la propia red de la aplicación, a medida que éstos se vayan integrando dentro de Internet su funcionalidad podrá aprovecharse a un nivel global.

WSN Y LA INTERNET DE LOS OBJETOS

Metafóricamente hablando, una red de sensores puede considerarse como la “piel” de un sistema computacional, la cual es capaz de percibir las características físicas del entorno [4]. En vez de “células”, las redes de sensores están compuestas de una serie de dispositivos conocidos como nodos sensores o simplemente nodos, los cuales normalmente están limitados en términos de velocidad de procesamiento (hasta 32MHz) y memoria (hasta 256KB). Su principal tarea es la de “sentir”, es decir, obtener información del entorno a través de medidores de temperatura, humedad, radiación, y otros. Además, los nodos pueden “pensar” (almacenar y procesar la información utilizando sus microcontroladores) y “hablar” (enviar y recibir información a través de un canal de comunicación, normalmente inalámbrico). Mediante el uso de estas capacidades, los nodos de una red de sensores pueden colaborar para adquirir información del mundo físico y proporcionarla a las entidades del mundo digital de forma directa o a través de un sistema ‘front-end’ conocido como estación base.

FIGURA 4 AQUÍ

Respecto a la seguridad de las redes de sensores, éstas tienen una mayor capacidad de lo que en un principio podría suponerse. Primitivas criptográficas como el estándar AES-128 pueden implementarse por software sin imponer una sobrecarga excesiva sobre los nodos, e incluso es posible ejecutar sistemas de criptografía asimétrica basados en curvas elípticas en menos de dos segundos. La naturaleza distribuida de las redes de sensores no es tampoco obstáculo para el desarrollo de mecanismos de distribución de claves: estándares actuales como ZigBee y WirelessHART™ utilizan una clave simétrica maestra para autenticar un nodo y proceder a la negociación de un clave de sesión, y existen otros mecanismos más avanzados basados en estrategias estadísticas y matemáticas que se encuentran en estudio. La protección del canal de comunicaciones no se basa sólo en el uso de las primitivas de seguridad, sino que se utilizan otras técnicas como ‘frequency hopping’ y ‘channel blacklisting’ para controlar la frecuencia del canal inalámbrico y aumentar la robustez del canal ante posibles ataques de denegación de servicio (p.ej. ‘jamming’).

Existen otros elementos y mecanismos de seguridad que, aunque no están estandarizados aún, se encuentran lo suficientemente avanzados como para ser utilizados. Un ejemplo es la sincronización segura de los relojes de los nodos. Esta tarea es vital para asegurar el correcto funcionamiento de una red, ya que es necesario conocer en la mayoría de los casos cuando un dato determinado fue obtenido. Igualmente, el mantenimiento de los nodos es una tarea importante, así que existen protocolos de diseminación de código que protegen el proceso de actualización de los programas y su configuración utilizando mecanismos sencillos. Finalmente, también son significativas la detección de intrusiones y la autoconfiguración de la red. Ambas suelen tener en la misma base: la identificación de anomalías. Precisamente, existen varias

técnicas que permiten descubrir este tipo de situaciones sin malgastar los recursos de la red.

La capacidad de funcionar con unos mínimos de seguridad no es la única ventaja de las redes de sensores. Las ventajas más importantes son: autonomía, gracias al uso de baterías y/o fuentes de energía renovables; adaptabilidad, mediante el uso de mecanismos de autoconfiguración; y bajo coste, debido al ahorro en términos de coste de los nodos y del cableado. Estas ventajas han permitido el desarrollo de estándares anteriormente mencionados (ZigBee, WirelessHART™ e ISA100.11a) y la existencia de aplicaciones tales como la domótica y la obtención de datos en sistemas SCADA. Sin embargo, El potencial de todas estas aplicaciones se aumentaría hasta límites insospechados en el momento en el que las redes de sensores pasasen a formar parte integral de la Internet de los Objetos. Los beneficios van más allá del simple acceso remoto: diversos sistemas computacionales pueden colaborar entre sí en base a la información recibida para proporcionar un servicio.

FIGURA 5 AQUÍ

Esta integración no es sólo una conjetura, sino un hecho respaldado por varias compañías Internacionales. Claros ejemplos son la estrategia “Un Planeta Inteligente” de IBM [5], que considera a los sensores como pilares en temas de gestión de agua inteligente y ciudades inteligentes, y el proyecto CeNSE de HP Labs, orientado a desplegar una red de pequeños sensores a nivel mundial para crear un “sistema nervioso central para la Tierra”. Asimismo, las tecnologías que permitirán la integración se encuentran en un proceso de desarrollo efervescente. Por un lado, el estándar 6LowPAN, definido por el IETF, permite que se transmitan paquetes de IPv6 a través de redes de capacidad limitada. Por otro lado, la conexión de la información producida por una red de sensores con servicios web basados en SOAP y REST, mecanismos de mensajería (correos electrónicos, SMS), y redes sociales (Twitter) y blogs (Wordpress), es ya una realidad.

SEGURIDAD EN LA INTERNET DE LOS OBJETOS

Existen varios desafíos que deben ser tenidos en cuenta para conseguir que la Internet de los Objetos se convierta finalmente en parte integral de nuestras vidas, desde la creación de estándares de comunicación y adquisición de datos hasta detalles menos tecnológicos como el reciclaje de los objetos. Entre estos desafíos, uno de los más importantes consiste en mantener la seguridad y la privacidad de todas las entidades (usuarios, datos, servicios…) asociadas a la Internet de los Objetos. La necesidad de considerar la seguridad y la privacidad desde la primera fase del diseño ha sido contemplada por la Comisión Europea en su estudio “Internet of Things - An action plan for Europe” [6], encargando a la Agencia Europea de la Seguridad de las Redes y de la Información (ENISA) el estudio de los riesgos de seguridad inherentes a este nuevo paradigma. Aunque este estudio se hará público a finales del año 2010, es posible exponer aquí un resumen de los diversos problemas de seguridad actualmente reconocidos, obtenidos tanto de estudios realizados por nuestro grupo de investigación como de análisis realizados por diversas entidades y universidades.

Como inicio de este resumen, es necesario mencionar la integración de los mecanismos de seguridad y la aceptación de los usuarios [7]. Es esencial contemplar la seguridad de la Internet de los Objetos de forma global, no como un conjunto de problemas inconexos

asociados a unas tecnologías específicas. De no hacerse así, podríamos encontrarnos con una situación en la que todas las tecnologías cumplen con unos requisitos de seguridad mínimos de forma separada, pero en el momento de su integración se generasen nuevos requisitos que no han sido considerados anteriormente. Así, los mecanismos de seguridad definidos en las secciones anteriores son necesarios, pero no suficientes. En cuanto a los usuarios, la Internet de los Objetos tiene que ser capaz de cumplir sus expectativas sin defraudar a su confianza. No sólo la Internet de los Objetos tiene que ser útil, sino que los usuarios tienen que tener la percepción de que ellos tienen el control sobre aquello que los afecta, por ejemplo a través de mecanismos de seguridad con una usabilidad adecuada. Si el usuario percibe que está siendo controlado por el sistema, o tiene una falsa percepción de seguridad que es traicionada por la vulneración de lo que considera sus derechos, las ventajas de la Internet de los Objetos serán básicamente rechazadas de plano.

La privacidad de los datos es uno de los aspectos más problemáticos de la Internet de los Objetos. La información asociada a un usuario particular no sólo consistirá en sus datos personales, sino que además estará compuesta de toda aquella información generada por los objetos que lo rodean. Por ejemplo, un entorno de hogar inteligente podría guardar todas las preferencias del usuario, como por ejemplo sus hábitos alimenticios (como, cuando, y donde toma café). Cabe entonces preguntarse quién es el dueño de estos datos, y como puede el usuario estar seguro de que esos datos están convenientemente protegidos y no se utilizarán para identificarlo sin su permiso. Además, hay que tener en cuenta la existencia de casos en los que parte de la información relacionada con un usuario en particular pueda ser compartida para permitir la provisión de un servicio. Por ejemplo, una persona debería proporcionar de forma automática los datos médicos necesarios (p.ej. historial, alergias) a la ambulancia y al personal médico que le atendiese en caso de urgencia. Más allá de los usuarios particulares, la privacidad de los datos afecta también al mundo empresarial. Una empresa que utilice mecanismos de la Internet de los Objetos generará un gran caudal de información procedente de todos sus elementos (recursos humanos, procesos productivos,…). Esa información debe ser confidencial, controlada dentro del ámbito de la empresa y accesible únicamente cuando se considere necesario.

FIGURA 6 AQUÍ

Otro aspecto a tener en cuenta es la protección de los elementos que componen la Internet de los Objetos mediante el uso de mecanismos de seguridad. Bajo nuestra percepción, esta seguridad debe abordarse desde dos puntos de vista: el acceso a los objetos y las interacciones entre objetos. Comentaremos en éste párrafo el primer punto de vista, el acceso a los objetos. Ya que los usuarios (humanos o no humanos) son capaces de conectarse remotamente a los servicios proporcionados por lo objetos, es necesario proteger este canal de información para asegurar la confidencialidad e integridad de los datos. Además, el acceso de la comunidad Internet a los objetos haría crecer exponencialmente el número de potenciales usuarios maliciosos o no autorizados que tratarían de manipularlos. Es entonces necesario crear mecanismos que puedan tanto autenticar a los usuarios y a los objetos como verificar si se dispone de los permisos necesarios para acceder a los servicios. Dada la naturaleza altamente distribuida de la Internet de los Objetos, sería también valioso disponer de una infraestructura de diagnóstico de problemas, permitiendo la trazabilidad del funcionamiento de los objetos e incluso una posible detección de intrusiones. Finalmente, habría que asegurar la disponibilidad de los servicios considerados

esenciales, incluyendo mecanismos de replicación que permitiesen acceder a un determinado tipo de servicio cuando sea necesario.

Respecto al segundo punto de vista, el de las interacciones entre objetos, éste se encuentra inherentemente relacionado con el funcionamiento seguro de los servicios. Ya que la base de la Internet de los Objetos es una infraestructura distribuida, dinámica, y heterogénea, es necesario combinar diversas tecnologías, protocolos, y modos de acceso para poder proporcionar un servicio de forma satisfactoria. Esto implica, en términos de seguridad, que los objetos y las infraestructuras subyacentes deben ser capaces de manejar diversos mecanismos de identificación y seguridad de la forma más transparente y escalable posible. Aunque es cierto que pueden existir "islas" (p.ej. un hogar digital o la sede de una empresa) en los que las interacciones entre los objetos están más controladas, existen servicios como la distribución de mercancías que utilizarán varios elementos localizados en diversos puntos del globo. Así, lograr una armonía en las interacciones seguras entre objetos es uno de los retos más interesantes de la Internet de los Objetos [8].

Finalmente, hay que considerar también la infraestructura de red, es decir, la estrategia para interconectar los elementos de la Internet de los Objetos con la infraestructura de Internet. Esta claro que si los objetos tienen una dirección IP y son capaces de manejar la pila de protocolos TCP/IP (p.ej. a través de 6LoWPAN [9]), su integración dentro de Internet será total. Sin embargo, es posible que existan casos en los que este tipo de integración no sea deseable, debido a varios factores. Un objeto cuyos recursos sean limitados puede no ser capaz de incluir los protocolos de seguridad estándares utilizados en Internet (p.ej WS-SecureConversation). Incluso si esto fuera posible, todavía existirían otros detalles a resolver como la inclusión de mecanismos distribuidos para controlar el acceso a los usuarios externos y el filtrado de ataques tales como DoS. Además, el protocolo IP puede no estar optimizado para resolver problemas en entornos específicos, como por ejemplo en redes de sensores que implementen el protocolo ISA100.11a. En estos casos, puede ser necesario usar otros tipos de integración que aislasen a la red de los objetos como si fuese una LAN, como la estrategia de integración "Front-End" (los objetos son inalcanzables de forma directa y solo interactúan a través de un servidor) o la estrategia de integración "Gateway" (un servidor ejerce de traductor entre Internet y la red local de objetos).

AVANCES LEGISLATIVOS Y TECNOLÓGICOS

La Internet de los Objetos requiere de avances en todos los frentes, tanto legislativos como tecnológicos, para convertirse en una realidad. Bien es cierto que algunas de las ventajas de este nuevo paradigma se encuentran disponibles actualmente en forma de algunas aplicaciones, y que los mecanismos de seguridad existentes pueden garantizar la seguridad de dichas aplicaciones. Por ejemplo, es posible considerar a los objetos como miembros de una red independiente de Internet que funciona con sus propios mecanismos de seguridad, y que proporcionan sus servicios a través de un servidor central protegido mediante mecanismos estándar como TLS/SSL, IPsec, y otros. No obstante, alcanzar el verdadero potencial de este nuevo paradigma significa estudiar a fondo los nuevos desafíos de seguridad que pueden surgir y desarrollar soluciones que tengan en cuenta sus características.

Actualmente, no existe ninguna legislación específica que considere la seguridad de la Internet de los Objetos como un todo. No obstante, sí existen estándares y normativas,

principalmente en desarrollo, que persiguen definir y/o regular a algunos de sus elementos [10]. Por ejemplo, los grupos de trabajo SG17 del Sector de Normalización de las Telecomunicaciones de la UIT (ITU-T) y JTC1/SC6 de la Organización Internacional para la Estandarización (ISO/IEC) están desarrollando estándares para la creación de una infraestructura de redes de sensores segura: el X.usnsec y el ISO/IEC 29180, respectivamente. Además, el grupo de trabajo TC M2M del Instituto Europeo de Normas de Telecomunicaciones (ETSI) está preparando interfaces que definan como pueden interoperar los futuros sistemas de interconexión entre máquinas (Machine-to-Machine). Es de suponer que los planes futuros de la Unión Europea en materia de la Internet de los Objetos (que parten de su estudio “Internet of Things - An action plan for Europe”, mencionado anteriormente en este mismo artículo) fomentarán la creación de nuevos estándares que aúnen las diversas tecnologías desde un punto de vista global.

En el ámbito tecnológico, tampoco existen grandes avances en materia de seguridad en la Internet de los Objetos, pero si podemos encontrar señales que nos indican el camino a seguir. En términos de privacidad, se tiene la certeza de que los usuarios deberían de ser capaces de manejar y controlar la información que producen. Eso indica que la información, por sí misma, debe conocer los elementos (físicos o virtuales) con los que está relacionada. Por ejemplo, el historial médico de un paciente debe conocer la identidad de ese paciente y la forma en la que elementos externos pueden acceder a sus datos de forma ubícua. Esta necesidad de privacidad, y la ubicuidad en el acceso a la información a cargo de varios actores (humanos o no humanos), plantean varios retos en términos de identificación, autorización y control de acceso, entre otros. Un serie de posibles puntos de partida para comenzar a abordar este problema pueden ser los diversos mecanismos de federación de identidad (Shibboleth, Liberty Alliance,…), así como dar importancia a la aplicación de políticas de seguridad.

Con respecto a los protocolos utilizados en la Internet de los Objetos, es de suponer que los mecanismos de creación de canales de comunicación seguros tendrán que considerar la heterogeneidad de los sistemas que conectan. Este hecho se hace patente ante las limitaciones del protocolo de IPv6 optimizado para sistemas de objetos, 6LoWPAN, el cual no considera la implementación de IPsec por cuestiones de diseño. Asimismo, en términos de estrategias de integración entre redes, también hay que considerar las necesidades de las aplicaciones. Por ejemplo, en las infraestructuras de información críticas los elementos de un sistema SCADA que obtienen información de un entorno industrial (remotas) deben estar completamente protegidos ante cualquier tipo de acceso indebido. Así, uno de nuestros estudios revela que estas remotas deberían delegar su función como elementos de la Internet de los Objetos a un sistema que actuase como interfaz en caso de que fuera necesario.

La necesidad de innovación en el área de la seguridad en la Internet de los Objetos se traduce en la existencia de diversos proyectos de investigación a nivel nacional y a nivel europeo que la consideran como un tema esencial. Por ejemplo, dentro del Séptimo Programa Marco (FP7), existen proyectos centrados en un tipo de tecnología específica pero con un enfoque parcialmente orientado a Internet [11]: los proyectos AWISSENET y SENSEI buscan la creación de un marco de trabajo donde objetos tales como nodos sensores puedan colaborar de una forma segura, mientras que proyectos como CASAGRAS estudian la integración segura de los sistemas RFID. A un nivel más general, redes de excelencia como EMANICS analizan no sólo los retos de seguridad de la Internet de los Objetos, sino también los retos de seguridad de la Internet del Futuro. Dentro de esta visión generalista también se engloban proyectos Españoles

como SPRINT [12], en el que nuestro grupo de investigación persigue desarrollar una plataforma de servicios de seguridad específicos para la Internet de los Objetos tales como conectividad segura, administración de identidad y privacidad, y otros.

CONCLUSIONES

Las principales tecnologías que permitirán la existencia de la Internet de los Objetos están finalmente alcanzando su madurez, y a día de hoy es posible soñar con un futuro donde lo real y lo virtual podrán convivir de forma transparente. Sin embargo, si este paradigma nace sin la seguridad como parte de su diseño inicial estará condenado al olvido o relegado a un papel marginal, creando un mercado considerable pero insignificante en comparación con lo que podría haber sido. Es por esa razón por la que hay que estudiar y desarrollar ahora mecanismos de seguridad y privacidad (cifrado de datos, identificación, control de acceso, análisis de información, mecanismos de interoperabilidad, etc) que permitan proteger este futuro y convertirlo en una realidad.

AGRADECIMIENTOS

Las imágenes de la figura 1: “All Lined Up” (de Ian Muttoo), “Distribution centre” (de Nick Saltmarsh), “Flower Growing” (de ‘marcusrg’) y “Outer London traffic” (de ‘nikoretro’), se encuentran bajo una licencia Creative Commons Reconocimiento 2.0 Genérica, http://creativecommons.org/licenses/by/2.0/deed.

BIBLIOGRAFÍA

[1] Informe sobre la Internet de los Objetos: http://www.itu.int/osg/spu/publications/internetofthings
[2] Ciudad de Songdo: http://www.songdo.com
[3] RFID Journal: http://www.rfidjournal.com
[4] Redes de Sensores: http://wsn.oversigma.com
[5] A Smarter Planet: http://www-05.ibm.com/innovation/es/index.html?ca=innovation_es&me=w&met=hp
[6] IoT - An action plan for Europe: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/952
[7] Christoph P. Mayer . “Security and Privacy Challenges in the Internet of Things”. GSN09 Workshop
[8] Joris Claessens, Microsoft. “Trust, Security, Privacy, and Identity perspective”. FIA Madrid 2008
[9] IPv6 over Low power WPAN: http://www.ietf.org/dyn/wg/charter/6lowpan-charter.html
[10] August Nilssen, Standards Norway. “Security and Privacy Standardisation in Internet of Things”
[11] http://www.future-internet.eu/activities/fp7-projects.html
[12] Proyecto SPRINT: http://www.isac.uma.es/SPRINT
[13] Proyecto Natal, Microsoft. http://www.xbox.com/projectnatal

CUADRO: PREDICCIONES

1. Como ya se ha enunciado en anteriores ediciones de esta revista, el concepto de “perímetro” dejará de existir en la mayoría de los casos, ya que cualquier objeto tendrá la capacidad de proporcionar y acceder a servicios a través de Internet. Las soluciones de seguridad deberán evolucionar para funcionar de una forma completamente distribuida y tolerante a fallos e intrusiones.
2. Las Interfaces de usuario experimentarán una revolución, en la que los usuarios interactuarán con los objetos que lo rodean de múltiples formas (un ejemplo serían gestos usando sistemas como los del proyecto Natal de Microsoft [13]). Esto también transformará las interfaces de los mecanismos de seguridad, haciéndolos más usables y más intuitivos. Así, aumentará la aceptación de los usuarios y su confianza en la Internet de los Objetos.

3. Las necesidades de miniaturización, así como de minimización de costes para permitir que la tecnología pueda ser integrada en todo tipo de objetos cotidianos dejará como contrapartida unos recursos hardware dedicados a la seguridad limitados, lo que motivará el avance de la criptografía ligera con la necesidad de algoritmos de seguridad robustos pero minimalistas.
4. Existirán estándares específicos que consideren como un elemento primordial el tema de la seguridad en las tecnologías que forman la Internet de los Objetos, como RFID y las redes de sensores. Uno de los mayores desafíos que surgirá en ese momento será precisamente la interacción entre estos estándares.
5. Se desarrollarán extensiones y nuevas versiones de los diversos mecanismos de seguridad que se utilizan en Internet (p.ej. TLS/SSL, Kerberos, Web Services Security), y éstas tendrán en cuenta de forma explícita características tales como la movilidad de los objetos.
6. Debido a la gran cantidad de información generada por la nueva Internet de los Objetos, aparecerán nuevas técnicas y servicios específicos encargados de filtrar esa información en búsqueda de posibles problemas de seguridad. Esas técnicas deberán cumplir una serie de requisitos principalmente relacionados con la privacidad.
7. El ciclo actual de desarrollo y adopción de "parches" para cubrir problemas de seguridad sufrirá un cambio radical. La razón es simple: un usuario no tendrá un solo dispositivo conectado a Internet, sino decenas de ellos que interactuarán entre sí para ofrecer un servicio de forma distribuida. Esto también afectará al desarrollo del software, donde las buenas prácticas y las herramientas automáticas de programación segura cobrarán una mayor importancia.
8. La proliferación de objetos cotidianos inteligentes e interconectados unido a la cantidad de información sobre los individuos que estos generarán de forma irremediable creará una importante alarma social por las consecuentes amenazas a la privacidad y la pérdida de anonimato. Los innegables beneficios y nuevos servicios generados por la Internet de los Objetos propiciarán su aceptación y la reformulación del concepto de privacidad, pero exigirá continuos avances tecnológicos y legales para la protección de la información personal.
9. Debido a la información transmitida por bienes de lujo, objetos personales e inmuebles a través de la red, surgirán nuevas formas de delincuencia que explotarán estos datos para reconocer posibles víctimas, crear perfiles y patrones. Será necesario el desarrollo de sistemas de gestión de identidades junto a identidades virtuales de objetos e individuos para mitigar tales amenazas, así como técnicas avanzadas de control de acceso y administración de privilegios.
10. Finalmente, la robustez del paradigma de la Internet de los Objetos se pondrá a prueba cuando se intente explotar de forma ilícita los servicios del nuevo mundo virtual (véase la recomendación anterior) a una gran escala. El resultado de esta batalla determinará la supervivencia del paradigma, relegándolo al ostracismo o convirtiéndolo en el pilar de una nueva sociedad tecnológica.

IMÁGENES

Figura 1. Ejemplo de los sectores beneficiados por la Internet de los Objetos

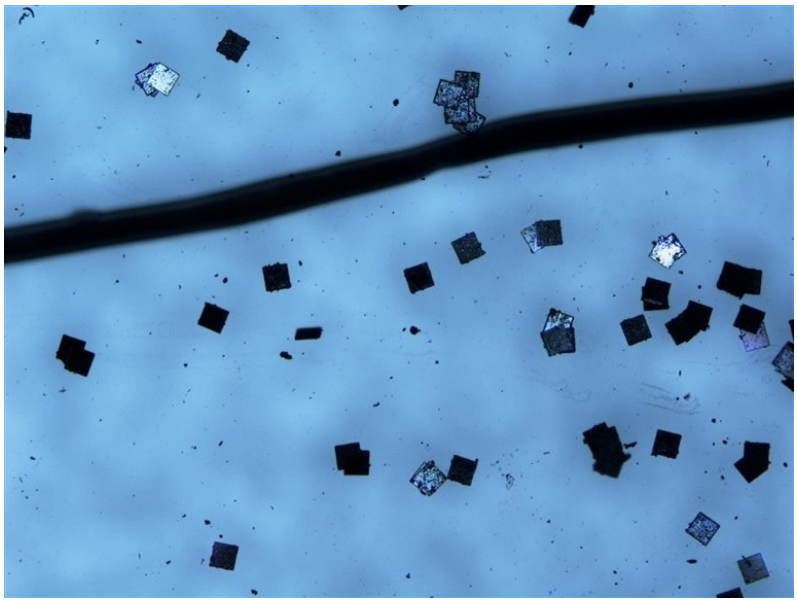

Figura 2. RFID Hitachi mu-chips junto a un cabello humano

Figura 3. Etiquetas RFID utilizadas en el etiquetado de bienes de consumo

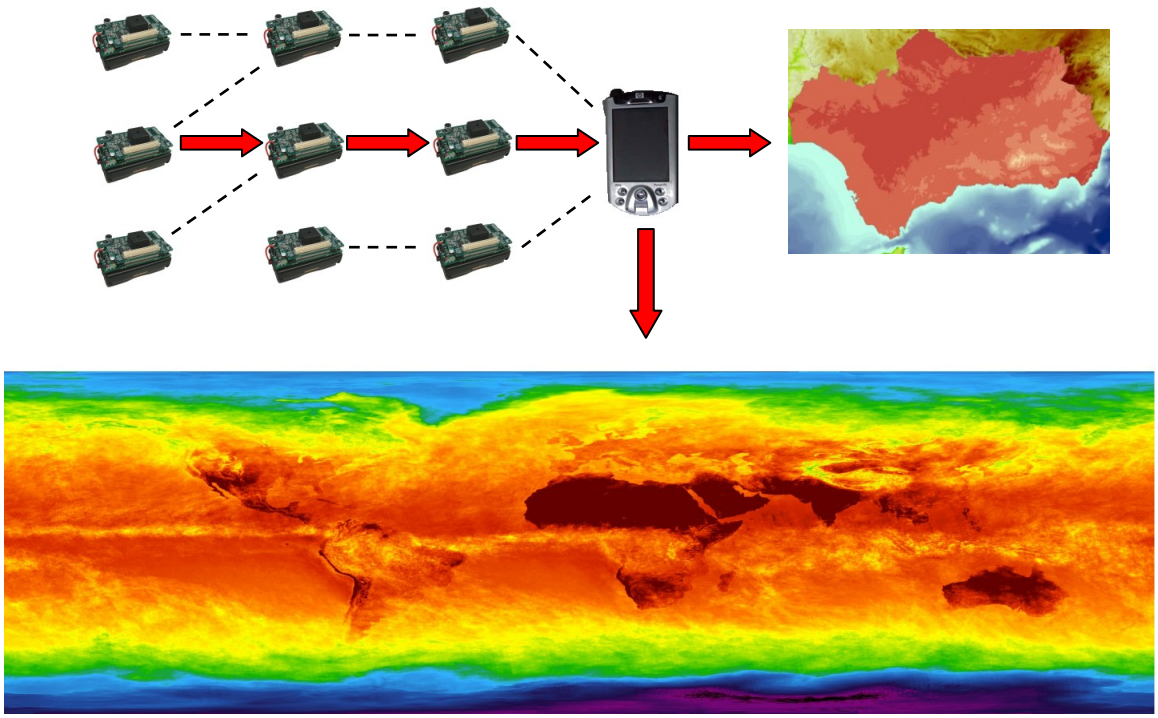

Figura 4. Ejemplo de una red de sensores inalámbricas

Figura 5. Diferentes sensores inalámbricos de ámbito académico

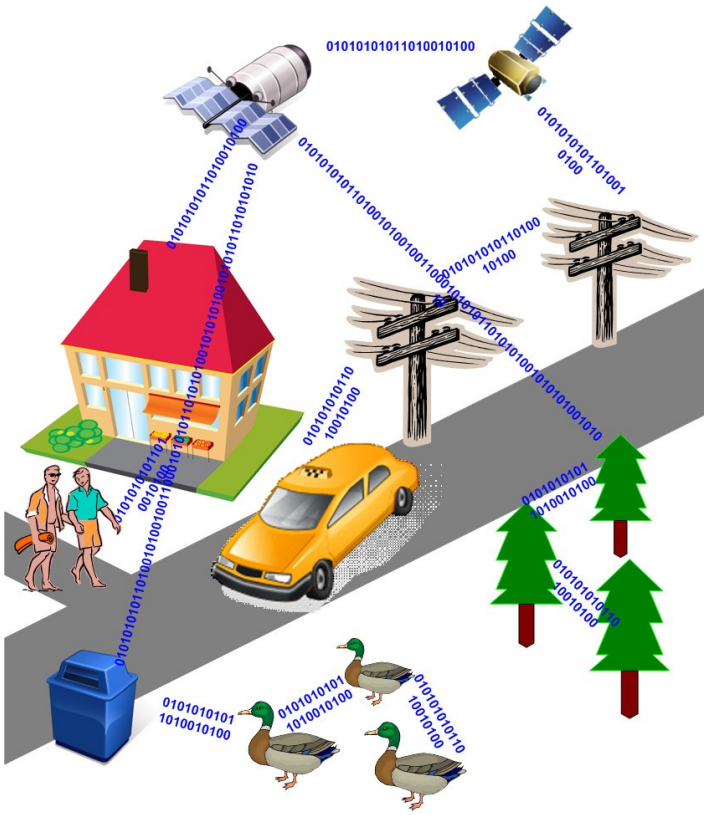

Figura 6. Una visión particular de la Internet de los Objetos