Internet de las Cosas: 50 Mil Millones de Puntos Inseguros

Ponciano Jorge Escamilla-Ambrosio
Moisés Salinas-Rosales
Raúl Acosta-Bermejo
Instituto Politécnico Nacional,
Centro de Investigación en Computación,
Av. Juan de Dios Bátiz, Esq. Miguel Othón de Mendizábal,
Gustavo A. Madero, México, D.F.
pescamilla@cic.ipn.mx; msalinasr@mail.cic.ipn.mx; racosta@cic.ipn.mx

Abraham Rodríguez-Mota
Instituto Politécnico Nacional,
Escuela Superior de Ingeniería Mecánica y Eléctrica Zacatenco
Av. Luis Enrique Erro S/N,
Gustavo A. Madero, Zacatenco, México, D.F.
armesimez@gmail.com

Resumen: El Internet de las cosas (IoT, por su acrónimo en inglés) representa la evolución radical del Internet actual a una red interconectada de 'objetos inteligentes' que colectan información del medio ambiente (sensado) e interactúan con el mundo físico (actuación, comando y control) y utilizan el Internet para proveer servicios de transferencia, análisis, aplicaciones y comunicación de la información. Se estima que actualmente existen alrededor de 18 mil millones de dispositivos conectados a Internet. Más aún, existen predicciones de que para el 2020 existirán un poco más de 50 mil millones de dispositivos o "cosas" conectados a Internet. El IoT es un habilitador de aplicaciones tales como ciudades inteligentes, control de tráfico inteligente, sistemas de salud inteligente, distribución de energía inteligente y muchos otros sistemas a los que les podemos añadir la palabra "inteligente". Estos sistemas sin duda persiguen mejorar nuestra calidad de vida. Sin embargo, como en muchos casos anteriores, todo avance tecnológico conlleva beneficios, responsabilidades y riesgos. En este caso, el inmenso número de dispositivos, produciendo, comunicando y procesando información, conforman un hoyo negro en términos de seguridad. En este contexto, existen muchas preguntas abiertas. ¿Podría alguien "hackear" mi auto y controlarlo de manera remota? ¿Podría mi administrador de insulina automático recibir un comando remoto de administrarme toda la insulina que pueda? ¿Podría alguien en todo momento saber mi localización, la de mi esposa, mis hijos y hasta la de mi perro? Y ¿podría alguien ganar acceso al control de mi casa y encerrarme o dejarme fuera de ella? En este trabajo se da respuesta a algunas de estas preguntas, se dan algunos ejemplos de vulnerabilidades que han sido explotadas en este tipo de dispositivos, así como algunos controles de seguridad y líneas de investigación abiertas en el área.

PALABRAS CLAVE: Internet de las cosas (IoT), ciberseguridad, código malicioso, robo de información, privacidad.

1 INTRODUCCIÓN

El Internet de las Cosas (IoT, por sus siglas en inglés) representa la evolución radical del Internet actual a una red interconectada de 'objetos inteligentes' que no solamente colectan información del medio ambiente (sensado) e interactúan con el mundo físico (actuación, comando y control), sino que también utilizan el Internet para proveer servicios de transferencia, análisis, aplicaciones y comunicación de la información [1]. Se estima que actualmente existen alrededor de 18 mil millones de dispositivos conectados a Internet, superando por mucho el número de habitantes en el planeta (estimada en 7 mil millones en 2011 [2]). Más aún, la empresa CISCO predice que para el 2020 existirán un poco más de 50 mil millones de dispositivos o "cosas" conectados a Internet, ver Figura 1.

Figura 1. Predicción del número de objetos conectados a Internet (adaptado de [3]).

El IoT es un habilitador de aplicaciones tales como ciudades inteligentes, control de tráfico inteligente, sistemas de salud inteligente, distribución de energía inteligente y muchos otros sistemas a los que les podemos añadir la palabra "inteligente". Estos sistemas sin duda persiguen mejorar nuestra calidad de vida. Sin embargo, como en muchos casos anteriores, todo avance tecnológico conlleva beneficios, responsabilidades y riesgos. En este caso, el inmenso número de dispositivos, produciendo, comunicando y procesando información, conforman un hoyo negro en términos de seguridad. En este contexto, existen muchas preguntas abiertas. ¿Podría alguien "hackear" mi auto y controlarlo de manera remota? ¿Podría mi administrador de insulina automático recibir un comando remoto de administrarme toda la insulina que pueda? ¿Podría alguien en todo momento saber mi

localización, la de mi esposa, mis hijos y hasta la de mi perro? Y ¿podría alguien ganar acceso al control de mi casa y encerrarme o dejarme fuera de ella?

Los distintos sensores, aplicaciones y componentes del IoT transmiten, reciben, procesan y almacenan información. Mucha de esa información es información privada, por ejemplo, en un sistema de salud inteligente podría ser información referente a enfermedades o del estado de salud de pacientes. Adicionalmente, dichos dispositivos pueden estar conectados a sistemas de información en la nube, disponibles todo el tiempo y en cualquier lugar. Lo anterior hace un requerimiento esencial para la adopción del IoT el identificar y analizar las distintas características de seguridad, privacidad, vulnerabilidades, amenazas y medidas de prevención, detección y tratamiento.

En este trabajo se da respuesta a alguna de las preguntas planteadas arriba, se dan algunos ejemplos de vulnerabilidades que han sido explotadas en este tipo de dispositivos, así como algunos controles de seguridad y líneas de investigación abiertas en el área. El resto del presente trabajo se organiza de la siguiente manera. En la Sección 2 se presentan algunos ejemplos de vulnerabilidades y ataques en el IoT que han llamado la atención de la gente al haber hecho eco en distintos medios. En la Sección 3 se describen los principales requerimientos y retos de seguridad en el IoT. Las principales vulnerabilidades de seguridad en el IoT se presentan en la Sección 4. Finalmente, en la Sección 5 se presentan las conclusiones de este trabajo.

2 EJEMPLOS DE VULNERABILIDADES Y ATAQUES EN EL IOT

En esta sección se presentan algunos ejemplos recientes de vulnerabilidades de seguridad y explotación por hackers de éstas en dispositivos y aplicaciones del IoT.

1) *Hackeo remoto de la computadora de automóviles.* En julio de este año los hackers Charlie Miller y Chris Valasek hicieron público un video donde muestran como de manera remota, vía Internet, tomaron control de la computadora de un vehículo Jeep Cherokee cuando éste estaba en movimiento [4-Wired_072115]. La toma del control de la computadora lo realizaron explotando una vulnerabilidad de día-zero en el sistema de información y entretenimiento Uconnect [5-Uconnect]. Entre las acciones que pudieron realizar incluyen: cambiar la velocidad del vehículo, controlar los frenos del vehículo, controlar la dirección del vehículo, controlar el radio del vehículo, activar/desactivar los limpiadores, controlar la transmisión del vehículo, entre otras. Como consecuencia de lo anterior, Fiat Chrysler decidió retirar 1.4 millón de vehículos afectados en Estados Unidos con el fin de realizar un parche en el software y solucionar el problema de seguridad puesto en evidencia por los hackers [4-Wired_072115].
2) *Hackeo de semáforos de control de tráfico*. Desde aproximadamente hace un año el investigador argentino Cesar Cerrudo ha estado investigando la posibilidad de acceder al control de los semáforos de distintas ciudades. En particular se ha

reportado que en las ciudades de Washington DC, San Francisco y New York el investigador pudo ganar acceso a los sistemas de control de tráfico y cambiar las luces de rojo a verde y de verde a rojo de los semáforos [6-New York Times]. Lo anterior fue posible debido a que se encontró que la información que fluye por los sensores de tráfico no se encripta y este hoyo de seguridad pudo ser explotado.

3) *Hackeo de inodoro inteligente*. En agosto del 2013 se reportó que el inodoro inteligente Satis que fabrica la compañía japonesa Lixil fue hackeado de manera inalámbrica [7-Extremetech]. En este caso los hackers utilizaron una vulnerabilidad de puerta trasera. El inodoro inteligente es vulnerable a través de la comunicación Bluetooth, embebida en el dispositivo. Los hackers pudieron de manera remota abrir o cerrar la tapa del inodoro, descargar el inodoro, y también activar la función de bidé incorporada en el dispositivo.
4) *Dispositivos de consumo conectados a Internet utilizados como una red de robots (thingbots)*. En enero de 2014 la compañía Proofpoint reportó que uno de sus investigadores encontró una red de robots o botnet, de más de 100,000 televisiones inteligentes, enrutadores y otros dispositivos de consumo, incluido al menos un refrigerador, todos conectados a Internet, participaron en el envío de 750,000 correos electrónicos maliciosos durante un período de dos semanas [8-Proofpoint], [13]. La red de robots, renombrada como 'thingnet', fue creada explotando las contraseñas de administración por defecto, que no habían sido cambiadas, y otros errores de configuración. Los atacantes también fueron capaces de controlar dispositivos que ejecutaban versiones anteriores del sistema operativo Linux aprovechando errores de software crítico.
5) *Hackeo de sistemas de automatización y entretenimiento para casas*. El investigador David Jacoby de Kapersky Lab ha demostrado y presentado en diferentes conferencias y seminarios como es relativamente fácil comprometer la seguridad de distintos aparatos domésticos, tales como: televisiones inteligentes, consolas de juego, sistemas de almacenamiento, receptores de señal satelital, enrutadores e impresoras [9]. En este caso las vulnerabilidades explotadas incluyen la utilización de los nombres de usuario y claves de acceso instaladas por default por el fabricante, la falta de encriptación de la información en los sistemas de almacenamiento, la no actualización del firmware, entre otras [14].
6) *Stuxnet*. Este ataque por un gusano de computadora, aunque no se realizó directamente contra un dispositivo del IoT, representa lo que podría suceder en el llamado Industrial IoT (IIoT, por su acrónimo en inglés). Stuxnet fue utilizado en 2010 para atacar la planta nuclear de Bushehr, en Irán [10]. Específicamente, lo que Stuxnet realizo es reprogramar un controlador lógicos programable particular con el fin de sabotear las centrifugadoras de enriquecimiento de uranio. Hasta la fecha

Stuxnet se sigue considerando como la pieza de software malicioso más sofisticada que se haya concebido y que marcó un hito en la ciberseguridad.

Los casos anteriores junto con el creciente número de cosas o dispositivos conectados a Internet, así como los avances en la capacidad de procesamiento y conectividad de estos dispositivos, hacen pensar que los escenarios anteriores sean cada vez más factible y frecuentes. En las siguientes secciones se describen en términos generales los requerimientos y retos de seguridad de los dispositivos del IoT. También se presentan las vulnerabilidades de seguridad identificadas en estos dispositivos.

3 REQURIMIENTOS Y RETOS DE SEGURIDAD

Como se deduce de los escenarios presentados en la introducción, en el IoT existen tanto requerimientos como retos de seguridad que deben ser atendidos. A continuación se presenta un resumen de éstos.

3.1 Requerimientos de seguridad

Los requerimientos de seguridad del IoT son similares a los requerimientos de los sistemas de comunicación y procesamiento de información tradicionales [11-Hossain et al, 2015], [12-Islam et al, 2015]:

1) Confidencialidad. La confidencialidad en el IoT garantiza la inaccesibilidad de la información para usuarios, incluyendo otros objetos, no autorizados. Adicionalmente, un mensaje confidencial debe resistir revelar su contenido a cualquier intruso.
2) Integridad. La integridad significa que cualquier dato recibido en el IoT no ha sido alterado o modificado en tránsito por algún adversario. Un adversario podría cambiar la información y poner en peligro la integridad de la información en el IoT. También, la integridad de la información almacenada y su contenido no deben de ser comprometidos.
3) Disponibilidad. La disponibilidad garantiza la supervivencia de los servicios del IoT a usuarios autorizados (objetos o personas) cuando sea necesario a pesar de los ataques a dichos servicios. Además, garantiza que se tenga la capacidad de proporcionar un nivel mínimo de servicios en presencia de una pérdida de energía y/o falla.
4) No-repudiación. Un nodo u objeto en el IoT no puede negar el envío de un mensaje que ha enviado previamente.
5) Autenticación. La autenticación permite a un dispositivo u objeto del IoT garantizar la identidad de otros objetos con los que se comunica (por ejemplo, un receptor comprueba si los datos que ha recibido procedían de la fuente correcta o no). La autenticación también es necesaria para asegurar que solamente usuarios válidos obtengan acceso a los dispositivos y redes del IoT para llevar a cabo las tareas administrativas: control remoto y/o reprogramación de los dispositivos y redes del IoT.

6) Actualidad de la información. Actualidad de la información significa asegurar la actualidad de cada mensaje. Es decir, que se garantice que los datos son recientes y no se han reproducido mensajes antiguos.
7) Autorización. Es asegurar que sólo los dispositivos y los usuarios autorizados puedan obtener acceso a los servicios de red o a los recursos del IoT.
8) Control de acceso. Es el acto de asegurar que un nodo del IoT que ha sido autenticado tenga acceso solamente a lo que tiene autorizado y a nada más.
9) Resiliencia. Es la garantía de que a pesar de que algunos dispositivos del IoT estén comprometidos, un esquema de seguridad debe continuar protegido contra ataques.
10) Anonimato. El anonimato oculta el origen de los datos. Este servicio de seguridad ayuda a la confidencialidad y la privacidad de los datos.

3.2 Retos de seguridad

Los requerimientos de seguridad en el IoT no pueden ser atendidos por las técnicas de seguridad tradicionales. El IoT impone nuevos retos para el desarrollo de técnicas novedosas que atiendan estos retos, que incluyen [11-Hossain et al, 2015], [12-Islam et al, 2015]:

1) Capacidad de cómputo limitada. Los objetos y dispositivos del IoT generalmente tienen procesadores embebidos que no son muy potentes en términos de su velocidad. Además, estos dispositivos no están diseñados para realizar operaciones costosas computacionalmente hablando. Es decir, que simplemente actúan como un sensor o actuador. Por lo tanto, encontrar una solución de seguridad que reduzca al mínimo el consumo de recursos y, por lo tanto, maximice la seguridad no es una tarea trivial.
2) Memoria disponible limitada. En comparación con un sistema tradicional digital (por ejemplo: PC, laptop, etc.), los objetos y dispositivos del IoT están construidos con memoria RAM y Flash limitada. Usan sistema operativo en tiempo real (RTOS, por su acrónimo en inglés) o alguna versión ligera de un sistema operativo de propósito general (GPO, por su acrónimo en inglés), por ejemplo Linux. También pueden ejecutar software de sistema y servicios propietarios. Por lo tanto, los sistemas de seguridad deben ser eficientes en el uso de memoria. Sin embargo, los algoritmos de seguridad tradicionales no se diseñaron específicamente para ser eficientes en el uso de la memoria, ya que los sistemas digitales tradicionales utilizan una memoria RAM amplia y disco duro de alta capacidad de almacenamiento. Por lo tanto, los algoritmos de seguridad convencionales no pueden utilizarse directamente en los dispositivos del IoT.
3) Energía disponible limitada. Un objeto inteligente en el IoT generalmente incluye una batería como medio de suministro de energía para los sensores y los actuadores de abordo (por ejemplo, sensor de temperatura, acelerómetro, GPS, etc.). Los objetos inteligentes administran el uso de energía mediante la activación del modo de ahorro de energía cuando no hay una lectura del sensor que deba ser informada.

Adicionalmente, el procesador de abordo funciona a baja velocidad si no hay nada importante que se vaya a procesar. Por lo tanto, la restricción energética, propia de los objetos inteligentes en el IoT, hace que sea difícil encontrar una solución de seguridad que minimice el uso de energía.

4) Movilidad. La movilidad es uno de los principales atributos de los objetos y dispositivos en el IoT, donde los dispositivos se pueden conectar a una red local próxima sin configuración previa. Esta característica de movilidad plantea la necesidad de desarrollar algoritmos de seguridad que se adapten a está movilidad de los objetos y dispositivos en el IoT.
5) Escalabilidad. El número dispositivos en el IoT está creciendo día a día y más dispositivos se conectan a la red mundial de información, Internet. Los sistemas de seguridad actual no están diseñados con la propiedad de escalabilidad; por lo tanto, estos sistemas no son adecuados para aplicarse en los dispositivos del IoT.
6) Multitud de estándares de comunicación. En general, los dispositivos están conectados a las redes locales y globales a través de una amplia gama de enlaces inalámbricos, como Zigbee, Z-Wave, Bluetooth, Bluetooth de bajo consumo de energía, WiFi, GSM, WiMax y 3G/4G, entre otros. Las características del canal de comunicación inalámbrico de estas redes hacen que los esquemas de seguridad diseñados para canales de comunicación con redes cableadas sean inapropiados. Por lo tanto, es difícil diseñar protocolos de seguridad que sean aplicables tanto en redes cableadas como en redes inalámbricas por igual.
7) Multiplicidad de dispositivos. Los dispositivos en el IoT son muy diversos, van desde las computadoras personales (PCs) totalmente equipadas hasta la gama baja de etiquetas de identificación por radiofrecuencia (RFID, por su acrónimo en inglés). Este tipo de dispositivos varían en términos de su capacidad de su cómputo, potencia de alimentación, memoria y el software incorporado. Por lo tanto, el reto consiste en diseñar un esquema de seguridad que puede albergarse incluso en el más sencillo de estos objetos o dispositivos del IoT.
8) Topología dinámica de red. Los objetos y dispositivos en el IoT pueden unirse o abandonar una red en cualquier momento desde cualquier lugar. Esta característica de los objetos y dispositivos en el IoT de dinámicamente conectarse y desconectarse tanto temporal como espacialmente requiere la existencia de una topología dinámica de red. Los esquemas de seguridad existentes para los sistemas digitales tradicionales no consideran este tipo de red en donde pueden existir cambios repentinos de topología. Por lo tanto, un modelo de seguridad tradicional no es directamente aplicable en los objetos y dispositivos inteligentes del IoT.
9) Red Multi-protocolo. Los objetos y dispositivos del IoT podrían utilizar un protocolo de red propietario (por ejemplo, diferente al protocolo IP) para la comunicación con redes locales. Al mismo tiempo, podrían comunicarse con un proveedor de servicios a través

de redes IP. Estas características hacen que los protocolos de comunicación tradicionales no sean adecuados para sistemas de seguridad en dispositivos del IoT.

10) Actualización dinámica de protocolos de seguridad. Para mitigar las vulnerabilidades potenciales, es necesario seguir protocolos de seguridad actualizados al día. Por lo tanto, las actualizaciones continuas de los protocolos de seguridad en los dispositivos del IoT son necesarias. Sin embargo, diseñar un mecanismo dinámico para la instalación de parches de seguridad es una tarea difícil.
11) Encapsulado de sensores y dispositivos a prueba de ser manipulados o abiertos. Una característica que generalmente no es tomada en cuenta de manera apropiada es la seguridad física de los objetos y dispositivos del IoT. Un atacante puede manipular físicamente los dispositivos y tal vez podría extraer secretos criptográficos, modificar los programas residentes en el dispositivo, o sustituir a los nodos con nodos maliciosos. Embalaje resistente a las manipulaciones y a la apertura es una forma de defenderse de estos ataques, pero el diseño y construcción de este tipo de embalaje es difícil de realizar en la práctica.

4 VULNERABILIDADES DE SEGURIDAD

Debido a la multitud de requerimientos de seguridad mencionadas en la sección anterior, combinado con los retos de seguridad, hacen que encontrar una combinación adecuada de técnicas, protocolos y esquemas de seguridad para el IoT sea mucho más difícil, comparado con los sistemas digitales típicos. Los parámetros que hacen que las tareas de seguridad sea más compleja pueden representarse en un eje 3-D (véase la Figura 3). La complejidad de las soluciones de seguridad requeridas cambia con la variación de los parámetros en cualquier dimensión. Es decir, es necesario considerar las especificaciones de los dispositivos, las redes utilizadas y las aplicaciones objetivo, al mismo tiempo, para atender las cuestiones de seguridad y las contramedidas requeridas en el IoT.

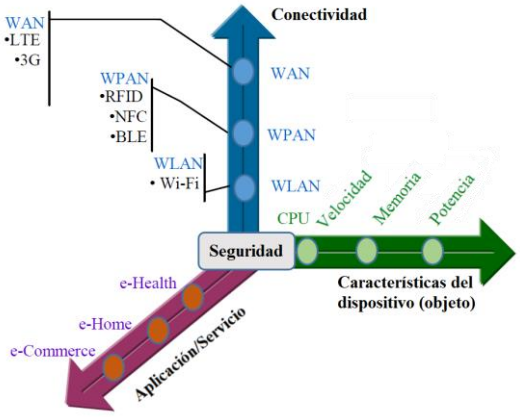

Figura 2. La seguridad en el IoT como un problema complejo en tres dimensiones (adaptado de [11]).

Las vulnerabilidades de seguridad en el IoT pueden plantearse desde tres aspectos [11]:

1) Seguridad de los dispositivos finales (end device security). Estas incluyen: inseguridad debido a la categoría y capacidad del dispositivo, seguridad del software y el firmware y seguridad en el almacenamiento.
2) Seguridad en las comunicaciones. Aquí se incluye: seguridad en conectividad múltiple, seguridad en servicios de red y seguridad criptográfica.
3) Seguridad en los servicios. Se incluyen: seguridad de servicios nativos, seguridad de servicios en la nube y seguridad de servicios entre pares.

4.1 Taxonomía de ataques

Un atacante puede fraguar diferentes tipos de amenazas a la seguridad y comprometer los dispositivos y objetos del IoT. Algunas amenazas son tangibles, algunas son predecibles, y muchas son difíciles de predecir. Las amenazas existentes en el IoT pueden clasificarse según [12] basándose en tres propiedades principales a saber: ataques a la información, ataques basados en las propiedades del objeto o dispositivo y ataques basados en las propiedades de la red.

1) Ataques a la información. La información que se encuentra en tránsito podría ser manipulada o analizada por un atacante con el fin de alterar dicha información o eliminarla. Entre este tipo de ataques se encuentran: *a) Interrupción de servicio*. Un adversario realiza un ataque de denegación de servicio con el fin de causar que el enlace de comunicación se vea interrumpido o no disponible. *b) Intercepción*. Es cuando un adversario captura (escucha) la información en tránsito amenazando la privacidad y

confidencialidad de la información. *c) Modificación*. Un adversario que obtiene acceso no autorizado a la información puede alterarla o modificarla con el fin de crear confusión y engañar a los usuarios. *d) Fabricación*. En este caso el adversario cambia mensajes inyectando información falsa amenazando la autenticidad de la información y confundir a los usuarios. *e) Reenvío*. En este caso un adversario reenvía información existente amenazando la actualidad (freshness) de la información creando confusión y engañando a los usuarios.

2) Ataques basados en las propiedades del objeto o dispositivo del IoT. En esta clasificación caen tres tipos de ataques: *a) Usuario comprometido*. Un adversario compromete los dispositivos y red del usuario siendo atacado por engaño o robo; este ataque puede revelar información sensitiva como claves de acceso, llaves de cifrado y datos sensibles del usuario. *b) Hardware comprometido*. Un adversario manipula físicamente el hardware del objeto o dispositivo del IoT con el fin de extraer el código a bordo del dispositivo, las llaves de cifrado o la información almacenada; también un atacante podría reprogramar el dispositivo comprometido con código malicioso. *c) Software comprometido*. En este caso el atacante explota las vulnerabilidades del software, por ejemplo, el sistema operativo, el firmware y las aplicaciones, con el fin de provocar un malfuncionamiento o forzar algún estado disfuncional del dispositivo (por ejemplo, desbordamiento de memoria y agotamiento de recursos).
3) Ataques basados en las propiedades de la red. En esta categoría caen dos formas de ataque: *a) Protocolo estándar comprometido*. Un atacante no utiliza los protocolos estándar (aplicaciones y protocolos de res) para actuar de manera maliciosa con el fin de amenazar la disponibilidad, privacidad, integridad y autenticidad de la información. *b) Ataque a la pila del protocolo de red*. Considerando la pila de protocolo de red para el IoT propuesta por la 'Internet Engineering Task Force (IETF)', ésta tiene diferentes tipos de vulnerabilidades en cada capa que un adversario podría explotar para realizar actividades maliciosas.

5 CONCLUSIONES

Recientemente se está hablando mucho sobre las implicaciones potenciales de la seguridad y privacidad en la era del IoT, y con mucha razón. Estas cuestiones se presentan como resultado de la recopilación de datos sensitivos realizada por sensores colocados en todos lados. No es difícil predecir un escenario e imaginar un sistema de información en una ciudad inteligente que sabe dónde vive cada individuo, sabe cuándo está en casa y puede predecir cuándo saldrá a la calle, sabe cuándo y con qué frecuencia ve TV o usa la lavadora, sabe cuándo y con qué frecuencia un individuo usa su coche y puede predecir en que camino conduce o que autobús va a tomar en la mañana. La información colectada puede servir por ejemplo, para determinar el comportamiento de consumo de los individuos. Se podría crear un modelos predictivos individualizado del el uso de energía, de agua y uso de

transporte. Más preocupante es el saber que además está información podría ser obtenida por un atacante que ingrese ilegítimamente a un sistema de automatización del hogar por la puerta trasera dejada en una cafetera o refrigerador conectados a internet.

Si partimos de la premisa de que todo lo que se conecta a Internet es potencialmente hackable, con el Internet de las cosas existirán 50 mil millones de cosas potencialmente hackables. Es por lo anterior que se hace necesaria una revisión de los requerimientos de seguridad, así como de los retos que representa establecer controles de seguridad en los objetos y dispositivos del IoT. En ese sentido el presente trabajo ha realizado esta revisión, pero hay mucho trabajo por hacer, particularmente en el diseño y desarrollo de protocolos y esquemas de seguridad que satisfagan los requerimientos y retos encontrados.

6 AGRADECIMIENTOS

Los autores agradecen el apoyo de CONACYT bajo el proyecto número 216747 y del Instituto Politécnico Nacional bajo el proyecto número SIP-20150617.

REFERENCIAS

[1] Escamilla-Ambrosio PJ, Salinas-Rosales M, Acosta-Bermejo R. Internet de las cosas: estado actual, retos y perspectivas. **Memorias 1er Congreso Iberoamericano de Instrumentación y Ciencias Aplicadas - SOMI XXVIII Congreso de Instrumentación**. Sn. Francisco de Campeche, Campeche, México, 28-31 de octubre, 2013.

[2] Centro de Noticias ONU. La población mundial alcanza hoy 7.000 millones. Available at: http://www.un.org/spanish/News/story.asp?newsID=22135#.UiZRHRvTvNI. (Accesed on: August 23, 2015).

[3] CISCO: Connections counter: The Internet of everything in motion, Available at: http://newsroom.cisco.com/feature-content?articleId=1208342 (Accessed on: August 24, 2015).

[4] Wired_072115 Wired magazine: Hackers remotely kill a jeep on the highway – with me in it. Available at: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Accessed on: August 15, 2015).

[5] Uconnect. Available at: http://www.driveuconnect.com/ (Accessed on: August 23, 2015).

[6] New York Times: Traffic hacking: Caution light is on. Available at: http://bits.blogs.nytimes.com/2015/06/10/traffic-hacking-caution-light-is-on/?_r=2 (Accessed on: August 23, 2015).

[7] Extremetech: Smart toilet's bidet hacked via Bluetooth, gives new meaning to 'backdoor vulnerability'. Available at: http://www.extremetech.com/extreme/163119-smart-toilets-bidet-hacked-via-bluetooth-gives-new-meaning-to-backdoor-vulnerability (Accessed on: August 20, 2015).

[8] Proofpoint: Your fridge is full of SPAM: Proof of nn IoT-driven attack. Available at: https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM (Accessed on: August 15, 2015).

[9] David Jacoby on Hacking His Home. Available at https://threatpost.com/david-jacoby-on-hacking-his-home/108517/ (Accessed on: August 28, 2015).

[10] Hagerott M. Stuxnet and the vital role of critical infrastructure operators and engineers. International Journal of Critical Infrastructure Protection, 2014; 7: 244-246.

[11-Hossain et al, 2015] Hossain M, Fotouhi M, & Hasan R. Towards an analysis of security issues, challenges, and open problems in the Internet of things. **Proceedings of the IEEE 11th World Congress on Services (IEEE SERVICES 2015)**. New York, USA, June 27-July 2, 2015.

[12] Islam SMR, Kwak D, Kabir MDH, Hossain M, Kwak KS. The Internet of things for health care: A comprehensive survey. IEEE Access 2015; 3: 678-708.

[13] Ars technical: Is your refrigerator really part of a massive spam-sending botnet? Available at: http://arstechnica.com/security/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet/ (Accessed on: August 16, 2015).

[14] IEEE Spectrum: Vulnerable "smart" devices make an Internet of insecure things. Available at: http://spectrum.ieee.org/riskfactor/computing/networks/vulnerable-smart-devices-make-an-internet-of-insecure-things/?utm_source=techalert&utm_medium=email&utm_campaign=090414 (Accessed on: August 20, 2015).