ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica
ISSN: 2007-5448
recibe@cucei.udg.mx
Universidad de Guadalajara
México

Martínez, Juan-Manuel; Mejía, Jezreel; Muñoz, Mirna; García, Yolanda-Meredith
La Seguridad en Internet de las Cosas: Analizando el Tráfico de Información en Aplicaciones para iOS
ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, vol. 6, núm. 1, 2017, Mayo-Octubre, pp. 77-96
Universidad de Guadalajara
México

Disponible en: https://www.redalyc.org/articulo.oa?id=512253717005

Cómo citar el artículo
Número completo
Más información del artículo
Página de la revista en redalyc.org

Sistema de Información Científica Redalyc
Red de Revistas Científicas de América Latina y el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Recibido 9 Sep 2016
Aceptado 15 Mar 2017
ReCIBE, Año 6 No. 1, Mayo 2017

La Seguridad en Internet de las Cosas: Analizando el Tráfico de Información en Aplicaciones para iOS

Security in the Internet of Things: Information Traffic Analysis for iOS Apps

Juan Martínez[1]
juan.martinez@cimat.mx

Jezreel Mejía[1]
jmejia@cimat.mx

Mirna Muñoz[1]
mirna.munoz@cimat.mx

Yolanda-Meredith García[1]
yolanda.garcia@cimat.mx

[1] Centro de Investigación en Matemáticas CIMAT, A.C., Zacatecas, México

Resumen: En los últimos años se ha observado un gran avance tecnológico y el servicio de Internet no es la excepción (en México el servicio doméstico básico es 180 veces más rápido que hace 15 años). Esto ha permitido conectar cada vez más dispositivos, surgiendo así el Internet de las cosas (IoT). De esta manera, el número de dispositivos conectados ha alcanzado una cifra aproximada de 20 mil millones, y se espera que para 2020 llegue a 50 mil millones. Esto ha generado grandes retos para mantener la seguridad y privacidad de la información ya que la mayoría de los dispositivos de IoT se centran en la conectividad y están incluyendo configuraciones por defecto donde la seguridad se ve gravemente afectada. Este artículo presenta los resultados del análisis de tráfico realizado a diversas aplicaciones para iOS, con el objetivo de informar lo fácil que puede ser capturar el tráfico, aunque se utilice el protocolo https y que aún existen muchas aplicaciones que transmiten información sin cifrar.

Palabras-clave: Internet de las cosas, IoT, Seguridad, Apple Watch, Análisis de tráfico.

Abstract: In recent years, a great technological advance has been observed and Internet service is not the exception (in Mexico, basic domestic service is 180 times faster than 15 years ago). This has allowed connecting more and more devices, thus arising the Internet of Things (IoT). In this way, the number of connected devices has reached around of 20 billion, and it is expected to reach 50 billion by 2020. This has generated major challenges for maintaining information security and privacy, because most IoT devices focus on connectivity and are including default settings where security is severely affected. This paper presents the results of the traffic analysis performed on various iOS apps, with the goal to inform how easy can be to capture traffic, even though using https protocol, and to show that there are still many applications that transmit information without encryption.

Keywords: Internet of Things, Security, Apple Watch, Traffic Analysis.

1. Introducción

En los últimos años se ha observado un gran avance tecnológico y el servicio de Internet no es la excepción (en México el servicio doméstico básico es 180 veces más rápido que hace 15 años). Esto ha permitido conectar cada vez más dispositivos, lo cual originó que la cantidad de dispositivos conectados a Internet superara al número de habitantes en el mundo (entre 2008 y 2009), dando como resultado el término “Internet de las cosas” (IoT, por sus siglas en inglés) (Figuerola, 2014).

(Figuerola, 2014; Rahman, Daud, & Mohamad, 2016) mencionan que para el año 2020 la cantidad de dispositivos conectados en total será de 50 mil millones, mientras que (Yu, Sekar, Seshan, Agarwal, & Xu, 2015) argumentan que, para el mismo año, habrá 25 mil millones de dispositivos sólo de IoT. Este gran incremento en el número de dispositivos conlleva un gran reto para la seguridad, ya que por lo general son productos novedosos que ofrecen una funcionalidad específica y muchos fabricantes descuidan las características de seguridad, debido a la competencia por llegar primero al mercado y que su producto sea fácil de usar (Yu et al., 2015).

Un estudio realizado por HP (Hewlett-Packard, 2015) revela que un 70% de los dispositivos de IoT no cifran sus comunicaciones, el 70% permiten a un atacante identificar las cuentas de usuario válidas, el 60% de los que tienen interfaz de usuario son vulnerables a distintos ataques como secuencias de comandos en sitios cruzados (XSS). Considerando que estos dispositivos recopilan una gran cantidad de información sensible para los usuarios, esto se vuelve un gran riesgo de seguridad (Rahman et al., 2016).

El objetivo de este trabajo es realizar una serie de análisis de tráfico en aplicaciones iOS que cuentan con versión para Apple Watch, para mostrar qué tan fácil es interceptar tráfico https y que, aunque las conexiones se hagan mediante este protocolo, no se debe transmitir información sensible de los usuarios sin cifrar.

Las siguientes secciones del documento están organizadas de la siguiente manera: en la sección 2 se presenta una breve contextualización acerca de IoT; la sección 3 muestra de manera sintetizada los resultados de una revisión sistemática acerca de la seguridad en IoT; la sección 4 muestra una clasificación de los dispositivos de IoT; la sección 5 presenta los resultados de las pruebas realizas y la sección 6 presenta las conclusiones.

2. Contextualización

El Internet de las cosas (IoT) se puede definir como una red altamente interconectada de entidades heterogéneas, tales como, etiquetas, sensores, dispositivos embebidos, dispositivos portátiles, etc., que interactúan y se comunican entre sí en tiempo real (Malina, Hajny, Fujdiak, & Hosek, 2016; Zhang & Green, 2015).

IoT revolucionará la manera en que las personas y las organizaciones interactúan con el mundo físico, la interacción con dispositivos domésticos, automóviles, plantas industriales, etc., sufrirá grandes modificaciones. También permitirá que muchos servicios como salud, educación y gestión de recursos, puedan ser mejorados para comodidad del cliente (Xu, Wendt, & Potkonjak, 2014).

El rápido crecimiento de IoT está creando grandes oportunidades de negocios. Los productos y servicios asociados a IoT generarán ingresos superiores a los $300 mil millones de dólares para 2020 (Singh & Singh, 2015).

A pesar de que se pronostica un acelerado crecimiento de IoT en todas las áreas, donde se encuentra más maduro es en el ámbito de los vestibles (wearables) ya que existe una gran cantidad de productos que se han estado comercializando y evolucionando desde hace varios años (Luque, 2016).

Son muchos los dispositivos vestibles que existen actualmente: lentes, gorras, relojes, bandas, ropa, zapatos, joyas, cinturones, cascos, etc.; sin embargo, los más utilizados son los que se usan en la muñeca (Luque, 2016), y según el estudio de IDC (International Data Corporation) de marzo de 2017, el Apple Watch es el tercer lugar de los vestibles más vendidos, es por ello que para realizar estas pruebas de concepto se eligió el Apple Watch.

3. Revisión Sistemática

Después de llevar a cabo la revisión sistemática de la literatura para identificar, evaluar, interpretar y sintetizar todas las investigaciones existentes y relevantes, se obtuvo el estado actual de la seguridad en IoT, siguiendo el método de Barbara Kitchenham (Kitchenham, 2004).
Como resultado del proceso de selección de estudios, se obtuvieron 31 estudios primarios, en la Figura. 1 se muestran las fuentes y cómo se fueron filtrando hasta obtener los primarios.

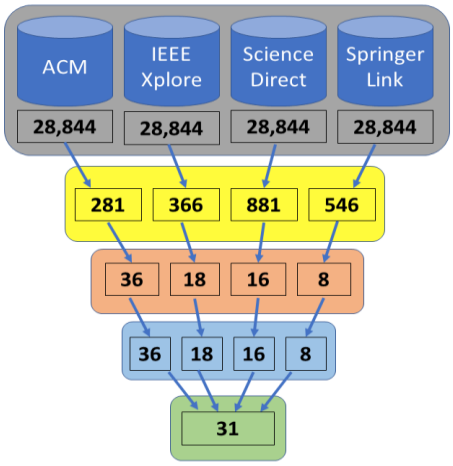

Figura 1. *Filtrado de resultados.*

El análisis de los estudios primarios permitió identificar que el principal problema de seguridad en IoT se encuentra en la fase de comunicación, convergiendo hacia temas de cifrado, de los cuales se detectaron: falta de un estándar de cifrado y descifrado, falta de algoritmos ligeros de cifrado que permitan implementarse en dispositivos con poca capacidad de procesamiento, fuga de información, pérdida de confidencialidad, comunicaciones no protegidas, rastreo de paquetes, etc., el total de estudios primarios seleccionados y el análisis completo, se pueden consultar en (Martínez, Mejía & Muñoz, 2016).

4. Clasificación de IoT

Como resultado de la revisión sistemática, en esta sección se realiza una clasificación de los dispositivos de IoT según su ámbito de aplicación. La cual se aprecia en la Tabla 1

Ámbito	Dispositivos
Vestibles	Relojes, lentes, bandas fitness y de salud, anillos, pulseras, ropa, cinturones, etc.
Domótica	Alarmas, cerraduras, cámaras, refrigeradores, televisores, manejo automático de luces, control de temperatura, automatización de cortinas, riego de macetas y jardines, etc.
Industriales	Variedad de sensores para monitorizar y controlar producción, monitorizar inventario, monitorizar estado físico y ubicación de los empleados, etc.
Automotriz	GPS, sensores en llantas para ahorrar combustible, seguros automáticos en puertas, encendido inteligente, estacionamiento automático, conducción automática, etc.
Ciudades inteligentes	Detectores de velocidad para monitorizar tráfico, sensores en las estructuras de los edificios para monitorizar su estado, cámaras de vigilancia, sensores para monitorizar el uso de bicicletas, estacionamientos inteligentes, sensores para medir la congestión de tráfico y redirigirlo en tiempo real para agilizarlo, vigilancia mediante drones, etc.

Tabla 1. *Clasificación de dispositivos IoT*

4.1 Tendencias

En general el IoT está generando grandes expectativas y se espera un crecimiento acelerado en los próximos años en todos los ámbitos (Yu, Sekar, Seshan, Agarwal, & Xu, 2015). Sin embargo, el ámbito de vestibles es el que ya está consolidado y con gran cantidad de productos comercializados, en el resto de los ámbitos muchos de los productos aún se encuentran como prototipos o se han implementado en proyectos aislados. Por ello para realizar las pruebas en este caso se seleccionó un dispositivo vestible, específicamente el Apple watch, ya que según (Luque, 2016) los dispositivos que se usan en la muñeca son los que tienen mayor demanda y en el último estudio realizado por IDC en marzo de 2017, el Apple watch aparece como el tercer vestible más vendido.

5. Pruebas realizadas

Una vez identificado que el mayor riesgo de seguridad se presenta durante la transmisión de la información y que el dispositivo para pruebas sería el Apple Watch, se procedió a realizar análisis de tráfico https para aplicaciones de iOS, ya que el reloj accede a las aplicaciones que necesitan conectarse a internet, a través de estar enlazado con un iPhone como receptor.

Se seleccionaron aplicaciones oficiales de las recomendadas por la misma App Store y con una valoración de 4+, todas de la categoría fitness y salud ya que Wristly Inc., en su informe del 2015 (Wristly, Inc., 2015) reporta que el principal uso que se le está dando al Apple Watch es el de monitorear la actividad física. Las aplicaciones seleccionadas fueron: Nike+ Run Club, Runkeeper, Runtastic, Strava y Pacer.

Para realizar las pruebas se utilizó una computadora con Windows 10, un iPhone y un Apple Watch, en la Figura 2 se muestran los dispositivos y herramientas utilizadas y el flujo de comunicación entre los mismos.

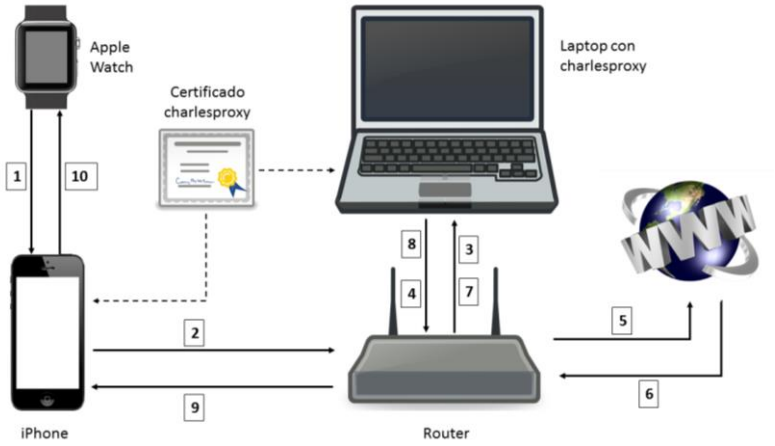

Figura 2. *Dispositivos utilizados y flujo de comunicación.*

En la computadora se instaló charlesproxy (XK72, 2017), esta herramienta cuenta con una versión de prueba la cual fue suficiente para las pruebas realizadas, aunque existen muchas herramientas similares como wireshark, ZAP de OWASP, fiddler, etc., se seleccionó ésta porque tiene lo necesario para cumplir el objetivo de estas pruebas, con una configuración muy sencilla y una interfaz intuitiva.

Una vez instalado el proxy en la computadora, es necesario configurar el puerto por medio del cual se van a recibir las conexiones. Para esto, solo se selecciona la opción Proxy del menú principal y luego Proxy Settings, en la ventana de configuración se escribe el puerto seleccionado, en este caso el puerto es 8181. La Figura 3 muestra un ejemplo.

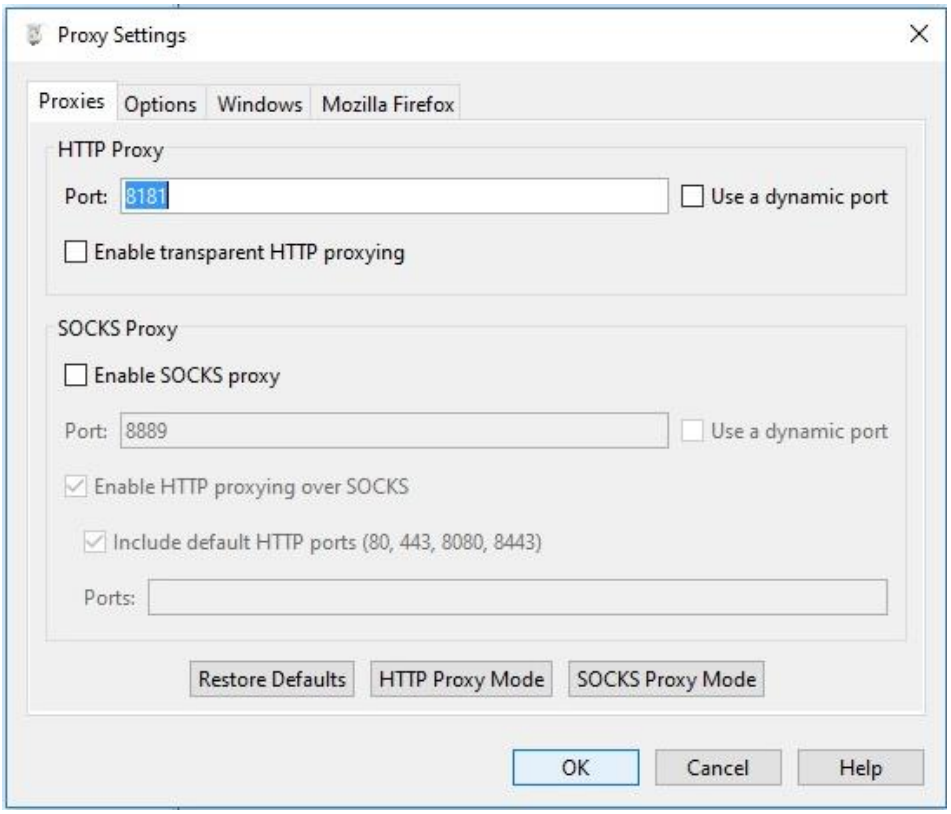

Figura 3. *Configuración de puerto.*

Enseguida se tiene que configurar el iPhone para que haga las peticiones a través del proxy, esto se hace en Configuración -> Wi-Fi, se selecciona la red a la que está conectada la computadora donde se instaló el proxy y se agrega un proxy http manualmente, en el servidor se pone la IP de la computadora donde se está ejecutando charlesproxy, y en puerto, el que se configuró previamente. La Figura 4 muestra un ejemplo.

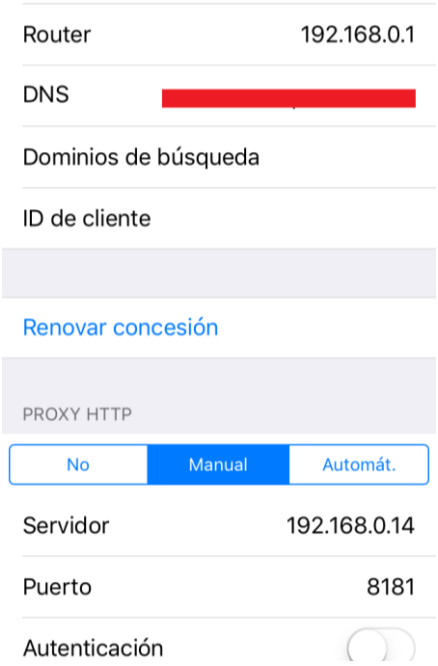

Figura 4. *Configuración de proxy manual en iPhone.*

Para realizar conexiones https es necesario instalar el certificado de charlesproxy en el iPhone, solo es necesario entrar a la página https://www.charlesproxy.com desde el iPhone con el navegador Safari (después de haber hecho la configuración anterior y teniendo en ejecución el proxy) y automáticamente aparecerá la pantalla para realizar la instalación. En la Figura 5 se muestra la pantalla antes y después de instalar el certificado.

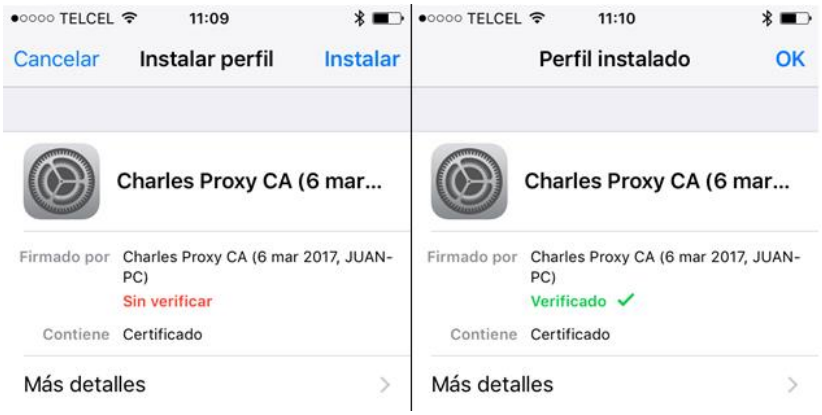

Figura 5. *Instalación de certificado en iPhone.*

Por último, para capturar el tráfico https en charlesproxy es necesario seleccionar la conexión, presionar el botón derecho del mouse y activar SSL Proxying como se muestra en la Figura 6.

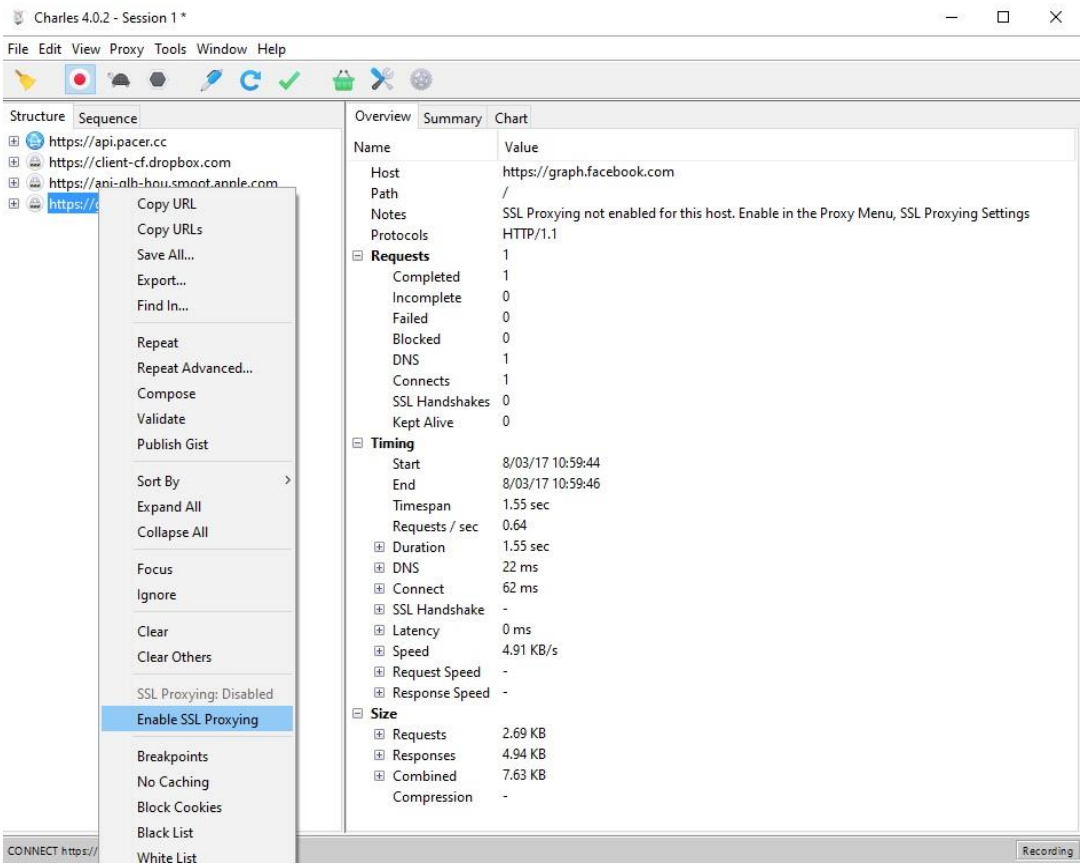

Figura 6. *Habilitar captura de tráfico HTTPS en charlesproxy.*

Las siguientes subsecciones muestran una pequeña descripción de cada aplicación seleccionada, así como los resultados obtenidos en las pruebas.

5.1 Nike+ Run Club

Es una aplicación desarrollada especialmente para apoyar a las personas que les gusta correr, utiliza seguimiento GPS para guardar toda la información de las sesiones de entrenamiento, se pueden establecer planes de entrenamiento personalizados, tiene conexión con redes sociales, consulta de estadísticas, entre muchas otras cosas. Tiene una valoración en la App Store de 4+ estrellas (Nike, Inc., 2017).

Al analizar el tráfico generado por esta aplicación se puede obtener información personal del usuario como: nombre, estatura, peso, fecha de nacimiento, correo electrónico, token de acceso, configuración y permisos concedidos a la aplicación, notificaciones, lista de amigos. En la Figura 7 se muestran algunos de estos datos.

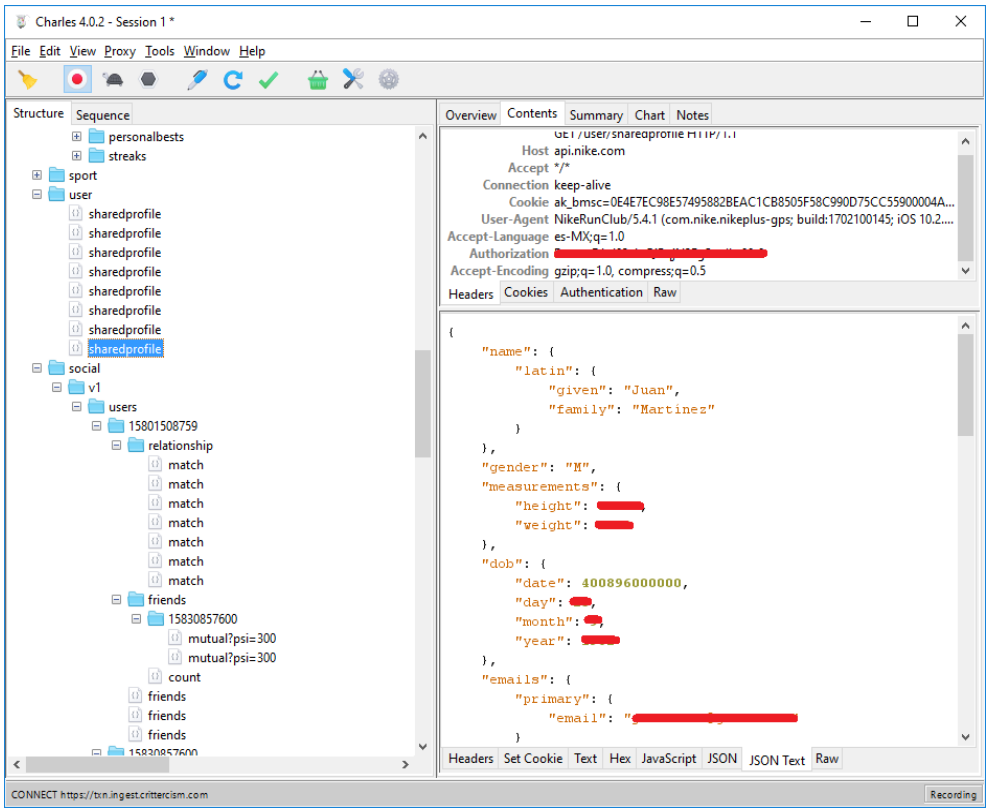

Figura 7. *Datos de perfil en Nike Run Club.*

5.2 Runkeeper

Es una aplicación que sirve para registrar la actividad física mientras se practican diferentes deportes como: caminar, correr, andar en bicicleta, etc., muestra estadísticas de ritmo, distancia, tiempo y calorías quemadas, cuenta con planes detallados que ayudan a cumplir objetivos, tiene conexión con redes sociales para compartir información con los amigos, etc. Tiene valoración en la App Store de 4+ estrellas (Runkeeper, LLC, 2017).

Algunos de los datos que se lograron obtener durante las pruebas de esta aplicación fueron: nombre del usuario, token de acceso, peso, estatura, correo electrónico, configuración y permisos otorgados a la aplicación, registros de actividad (calorías quemadas, kilómetros recorridos, tiempo invertido, etc.), lista de amigos (si el amigo inició sesión con Facebook, se puede obtener su id de usuario en Facebook), además si se vincula la cuenta de Twitter con esta aplicación, también se puede ver el usuario, el token de acceso y el token secreto de Twitter. La Figura 8 muestra un poco de esta información.

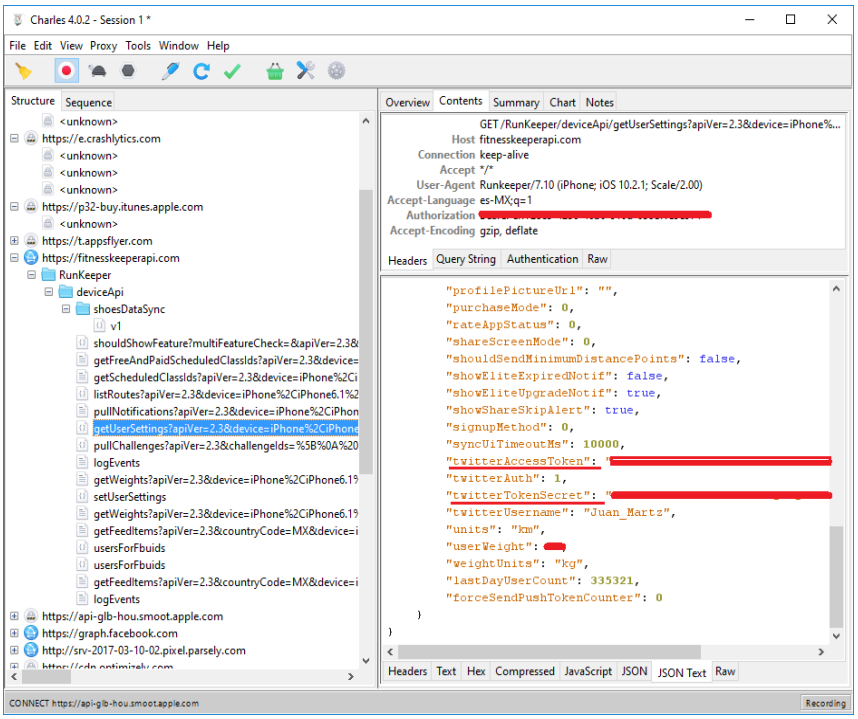

Figura 8. *Datos capturados de aplicación Runkeeper.*

5.3 Runtastic

Es una aplicación para hacer ejercicio y registrar actividades deportivas (correr, caminar, ciclismo, etc.) vía GPS, muestra estadísticas, se puede establecer el objetivo anual y motiva al usuario a alcanzarlo, cuenta con una clasificación que muestra quien ha corrido más en un periodo determinado, se pueden compartir los logros en Facebook y Twitter, y muchas cosas más. Tiene valoración en la App Store de 4+ estrellas (Runtastic, 2017).

Algunos de los datos que se lograron obtener durante las pruebas fueron: nombre del usuario, token de acceso, peso, estatura, correo electrónico, configuración de la aplicación, registros de actividad (calorías quemadas, distancia, coordenadas de latitud y longitud, etc.). La Figura 9 muestra un poco de información de perfil y de configuración.

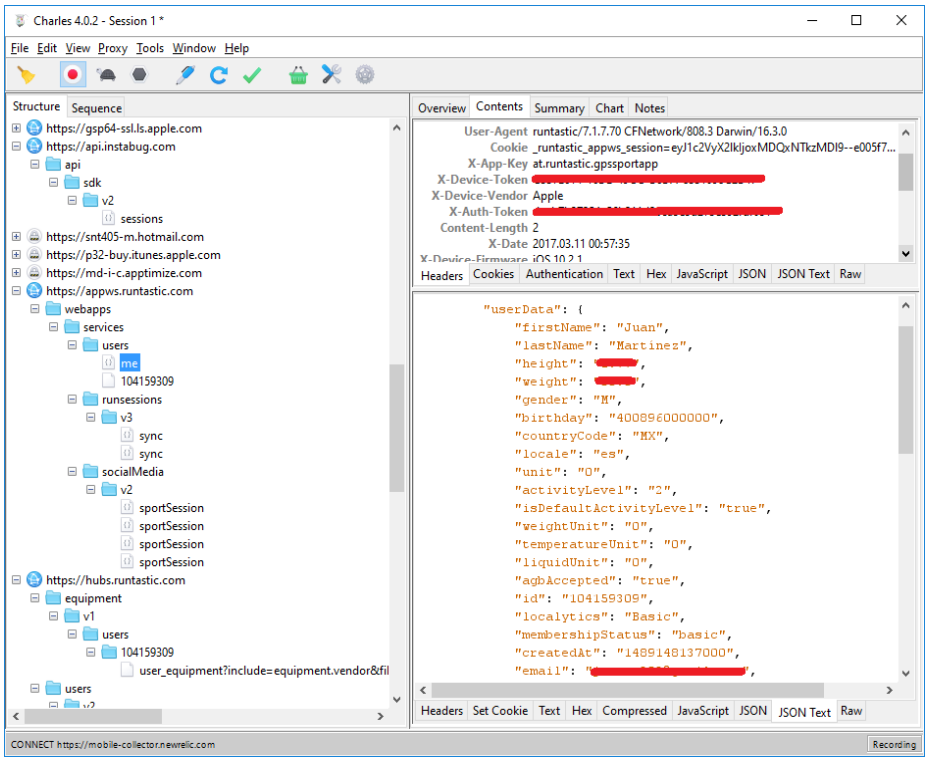

Figura 9. *Datos obtenidos de aplicación Runtastic.*

5.4 Strava

Esta aplicación monitorea carreras y vueltas en bicicleta con GPS, permite compartir actividades en Facebook y Twitter, comparte fotos en Instagram, cuenta con tabla de posiciones para competir contra amigos, guarda historial de actividades, sugiere lugares populares que los usuarios usan para correr o entrenar, entre muchas cosas más. Tiene valoración en la App Store de 4+ estrellas (Strava, Inc., 2017).

El análisis del tráfico generado por esta aplicación permitió obtener algunos datos, entre los cuales están: nombre del usuario, token de acceso, correo electrónico, configuración de la aplicación, registros de actividad (fecha, distancia, duración, etc.), lista de amigos (si el amigo inició sesión con Facebook, se puede obtener su id de usuario en Facebook). La Figura 10 muestra un poco de esta información.

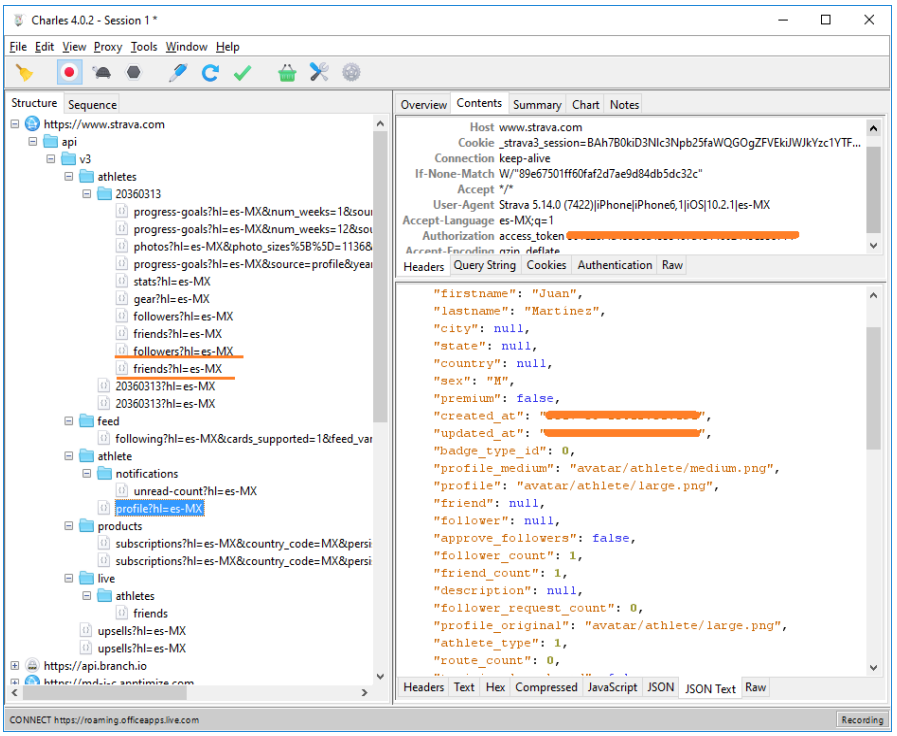

Figura 10. *Datos obtenidos de aplicación Strava.*

5.5 Pacer

Aplicación diseñada para ayudar a llevar un control sobre tres de las principales mediciones de salud: actividad diaria, peso corporal y presión arterial; cuenta pasos, calorías quemadas y kilómetros recorridos en segundo plano, también cuenta con la opción para registrar actividad (caminar o correr) por medio de GPS, cuenta con un objetivo diario de pasos, guarda historial diario, permite crear o unirse a grupos, entre muchas otras cosas. Tiene valoración en la App Store de 4+ estrellas (Pacer Health, Inc., 2017).

Algunos de los datos de los usuarios a los que permitió tener acceso el análisis de tráfico de esta aplicación son: dispositivo desde el que se conecta, id del dispositivo, llave de autenticación, token de acceso, id de usuario, nombre, domicilio, año de nacimiento, grupos a los que pertenece, además la aplicación recomienda grupos de los cuales, sin formar parte de ellos, se puede obtener información como nombre del propietario y su domicilio incluso con coordenadas de latitud y longitud. En la Figura 11 se muestran algunos de estos datos.

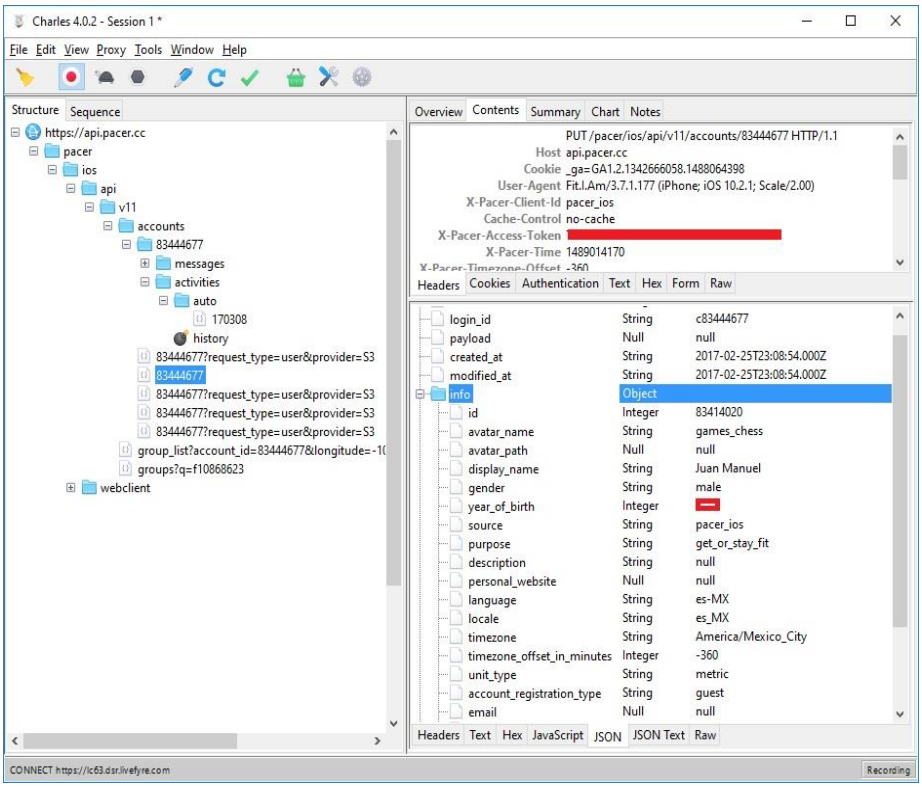

Figura 11. *Datos de usuario en aplicación Pacer.*

5.6 Comparación de resultados obtenidos

A continuación, en la Tabla 2, se presenta de manera sintetizada una comparativa entre las aplicaciones, tomando como base la información que se pudo obtener de cada una de ellas a través del análisis del tráfico https.

Datos filtrados	Nike+ Run Club	Runkeeper	Runtastic	Strava	Pacer
Nombre	✓	✓	✓	✓	✓
Estatura	✓	✓	✓		
Peso	✓	✓	✓		
Fecha de nacimiento	✓				✓
Correo electrónico	✓	✓	✓	✓	
Token de acceso	✓	✓	✓	✓	✓
Configuración	✓	✓	✓	✓	
Permisos concedidos	✓	✓			
Notificaciones	✓				
Amigos	✓	✓		✓	
Registros de actividad		✓	✓	✓	
ID de Facebook de amigos		✓		✓	
Usuario de Twitter		✓			
Token de acceso a Twitter		✓			
Token secreto de Twitter		✓			
Coordenadas de lugares de entrenamiento			✓		
Domicilio del usuario					✓
Grupos a los que pertenece					✓

Tabla 2. *Comparativa entre aplicaciones.*

Como se puede observar, estas aplicaciones transmiten una cantidad considerable de información sin cifrar que, aunque la mayoría de ésta pudiera parecer no muy comprometedora, el simple hecho de que alguien pueda acceder a los hábitos de una persona y conocer dónde vive, lugares dónde ejercitarse, cuanto tiempo en promedio dura su rutina de ejercicio, etc., es un gran riesgo, porque estos datos podrían ser útiles para delincuentes.

6. Conclusiones

En este trabajo se presentaron de manera sintetizada los resultados de una revisión sistemática de literatura para conocer el estado actual de la seguridad en IoT, una vez identificado el problema de seguridad en IoT el cual es la transmisión de información sin cifrar, se decide realizar el análisis de tráfico a diversas aplicaciones oficiales de la App Store. El resultado obtenido mostró que las peticiones son solicitadas por medio del protocolo https, sin embargo, transmiten mucha información sin cifrado que es susceptible a ser interceptada ya que actualmente existe una gran variedad de aplicaciones diseñadas para capturar tráfico https.

Cabe resaltar que estas pruebas fueron realizadas únicamente para analizar el tráfico que trasmiten las aplicaciones y dar a conocer a los usuarios la información que puede ser vulnerable en caso de que se conecten a redes desconocidas e instalen certificados de procedencia dudosa. Como trabajo futuro se analizarán otras herramientas que permitan realizar pruebas

similares, pero que sean totalmente transparentes para el usuario del Apple Watch.

Referencias:

Figuerola, N. (2014). Seguridad en Internet de las cosas Estado del Arte. PMQuality. Recuperado de http://www.csirtcv.gva.es/sites/all/files/downloads/[CSIRT-CV] Informe-Internet_de_las_Cosas.pdf

Hewlett-Packard. (2015). Internet of Things Research Study 2015 Report, 6. Recuperado de http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(TR/SE-0401), 28. http://doi.org/10.1.1.122.3308

Luque, J. (2016). Dispositivos y tecnologías wearables. ACTA - Autores Científico Técnicos Y Académicos, (RD 041).

Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. Computer Networks, 102, 83–95. http://doi.org/10.1016/j.comnet.2016.03.011

Martinez, J., Mejia, J., & Munoz, M. (2016). Security analysis of the Internet of Things: A systematic literature review. 2016 International Conference On Software Process Improvement (CIMPS). http://dx.doi.org/10.1109/cimps.2016.7802809

Nike, Inc. (2017). Nike+ Run Club (Versión 5.4.1) [Aplicación Móvil]. Descargado de https://itunes.apple.com/mx/

Pacer Health, Inc. (2017). Pacer (Versión 3.7.1) [Aplicación Móvil]. Descargado de https://itunes.apple.com/mx/

Rahman, A. F. A., Daud, M., & Mohamad, M. Z. (2016). Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework. Proceedings of the International Conference on Internet of Things and Cloud Computing - ICC '16, 1–5. http://doi.org/10.1145/2896387.2906198

Runkeeper, LLC. (2017). Runkeeper (Versión 7.10). [Aplicación Móvil]. Descargado de https://itunes.apple.com/mx/

Runtastic. (2017). Runtastic (Versión 7.1.7). [Aplicación Móvil]. Descargado de https://itunes.apple.com/mx/

Singh, S., & Singh, N. (2015). Internet of Things(IoT): Security Challenges, Business Opportunities & Reference Architecture for E-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1577–1581). IEEE. http://doi.org/10.1109/ICGCIoT.2015.7380718

Strava, Inc. (2017). Strava (Versión 5.14.0). [Aplicación Móvil]. Descargado de https://itunes.apple.com/mx/

Xu, T., Wendt, J. B., & Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 417–423). IEEE. http://doi.org/10.1109/ICCAD.2014.7001385

Wristly, Inc. (2015). The State of the Apple Watch (pp. 9-10). Recuperado de http://fortune.com/2015/09/08/apple-watch-satisfaction-survey/

XK72, L. (2017). Charles Web Debugging Proxy • HTTP Monitor / HTTP Proxy / HTTPS & SSL Proxy / Reverse Proxy. Charlesproxy.com. Recuperado de https://www.charlesproxy.com/

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices. Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV, 1–7. http://doi.org/10.1145/2834050.2834095

Zhang, C., & Green, R. (2015). Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network. In Proceedings of the 18th Symposium on Communications & Networking (pp. 8–15). Recuperado de http://dl.acm.org/citation.cfm?id=2872550.2872552

Notas biográficas:

Juan Manuel Martínez Martínez es Licenciado en Informática, egresado del Instituto Tecnológico Superior Zacatecas Norte (ITSZN) en el año 2005. Cuenta con dos años de experiencia como docente en nivel medio superior, siete años como Jefe de Oficina de Servicios Escolares y un año como responsable de Centro de Cómputo dentro del mismo subsistema educativo. Está certificado en Kanban Trainning y en Microsoft Office. Actualmente estudia la Maestría en Ingeniería del Software en el Centro de Investigación en Matemáticas (CIMAT) Unidad Zacatecas. Entre sus temas de interés se encuentran: modelos y estándares de calidad, seguridad en tecnologías de información, metodologías para realizar pruebas de

penetración, desarrollo de aplicaciones web y móviles, y aseguramiento de la calidad del software.

Jezreel Mejía Miranda es doctor en Informática por la Universidad Politécnica de Madrid (UPM), España, donde se le concedió la nota máxima, Cum Laude, y mención de "Doctorado Europeo". Realizó una estancia de investigación para obtener el doctorado europeo en la Universidad Fernando Pessoa en Oporto, Portugal. Previamente, en el Instituto Tecnológico de Orizaba, Veracruz, cursó la maestría en Ciencias de la Computación y la licenciatura en Informática. Es miembro del grupo de investigación Cátedra de Mejora de Procesos Software en el Espacio Iberoamericano (MPSEI), donde participa en proyectos internacionales de investigación con entidades educativas y de gobierno (Instituto Tecnológico de Orizaba; Instituto Regional de Zacatecas; Facultad de Informática de la UPM) y de vinculación con la industria (clúster de empresas de desarrollo de software en Zacatecas). Asimismo, es miembro del comité científico de diversos congresos internacionales como: CISTI (2009-2013), CERMA (2009-2013), del Coloquio de Investigación Multidisciplinaria del Instituto Tecnológico de Orizaba (2011) y del Infonor Chile 2012 y de la revista internacional RISTI (2010-2013). Ha publicado diversos artículos técnicos en temas relacionados con la gestión de proyectos, entornos multi-modelo, modelos y estándares de calidad y temas relacionados en entornos outsourcing. También ha participado en proyectos de la empresa multinacional everis consulting. Actualmente, el Dr. Jezreel Mejía Miranda es investigador del Centro de Investigación en Matemáticas, A.C. (Cimat), Unidad Zacatecas, en el área de Ingeniería de Software. También forma parte del equipo oficial de traducción al español del libro CMMI-DEV v1.2 y 1.3, versiones reconocidas por el prestigioso Software Engineering Institute (SEI) de la Carnegie Mellon University. Como investigador, sus áreas de interés son: entornos multi-modelo, gestión de proyectos software, modelos y estándares de calidad (CMMI, ISO, TSP, PSP, etc.), metodologías ágiles, métricas, mejora de procesos en entornos outsourcing y entornos de desarrollo tradicional. Cuenta con certificación en CMMI e ISO 20000.

Mirna Ariadna Muñoz Mata, Doctor en Informática por la Universidad Politécnica de Madrid, en Madrid España, con mención de “Doctorado Europeo”. Ha realizado una estancia posdoctoral en la Universidad Carlos III de Madrid, España. Actualmente es investigador del Centro de Investigación en Matemáticas (CIMAT) - Unidad Zacatecas en el área de Ingeniería de Software y es miembro del grupo de investigación Cátedra de Mejora de Procesos Software en el Espacio Iberoamericano (MPSEI), donde participa en proyectos internacionales de investigación con entidades educativas y de gobierno y de vinculación con la industria. Ha participado en

proyectos con la empresa everis consulting. Ha participado en el equipo de traducción oficial al español reconocida por el SEI del libro CMMI-DEV v1.2 y 1.3. Es miembro del comité científico de diversos congresos. Ha publicado diversos artículos técnicos en temas relacionados con la gestión de proyectos, implementación de mejora de procesos software, entornos multi-modelo y modelos y estándares de calidad. Es autora del libro Metodología Multimodelo para Implementar Mejoras de Procesos Software.

Yolanda Meredith García Molina es Licenciada en Informática, egresada del Instituto Tecnológico Superior Zacatecas Norte (ITSZN) en 2005, mismo año en que ingresó a laborar al ITSZN y colabora como docente e imparte materias afines a las Ciencias Computacionales e Ingeniería de Software en las carreras de: Ingeniería en Sistemas Computacionales, Ingeniería Informática, Ingeniería Electromecánica e Ingeniería en Gestión Empresarial, a su vez participó en proyectos de la institución como Estudio de Factibilidad para apertura de una nueva carrera, Acreditación de la carrera de Ingeniería en Sistemas Computacionales y fungió como secretaria de Academia de Informática y Sistemas. Está certificada en Kanban Trainning así como en Microsoft Project 2007.Actualmente estudia la Maestría en Ingeniería del Software en el Centro de Investigación en Matemáticas (CIMAT) Unidad Zacatecas. Sus temas de interés son: modelos de calidad, gestión de proyectos de desarrollo de software, desarrollo de software, seguridad informática y arquitectura de software, ha desarrollado algunos sistemas de software.

Esta obra está bajo una licencia de Creative Commons Reconocimiento-NoComercial-CompartirIgual 2.5 México.