risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 18/12/2018
Aceitação/Acceptance: 28/02/2019

Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación

Jezreel Mejía

jmejia@cimat.mx

Centro de Investigación en Matemáticas, Unidad Zacatecas, Parque Quantum, Ciudad el Conocimiento Avenida Lassec, Andador Galileo Galilei, Manzana, 3 Lote 7, 98160. Zacatecas, México.

DOI: 10.17013/risti.31.82–93

Resumen: En los últimos años, la consolidación de Android, como el sistema operativo más utilizado en Smartphone lo convierte en blanco del mayor número de amenazas creciente; tendencia que se ha mantenido en los últimos años. De acuerdo al informe de 2016, Tendencias en Seguridad publicado por ESET, el número de vulnerabilidades móviles incrementa cada año desde 2013 y, a lo largo de 2015 la tasa de incremento dentro del ecosistema Android que ponen en riesgo la privacidad de su información, ha promediado de 200 nuevas muestras de malware por mes. Por lo tanto, en este artículo se presenta una aplicación (app) para la detección oportuna a potenciales aplicaciones maliciosas presentes en Smartphone, particularmente aquellos con sistema operativo Android, presentando un estudio de caso que ha permitido validar la app a través de la detección de aplicaciones maliciosas instaladas en un dispositivo móvil.

Palabras-clave: Smartphone, Android, Ciberseguridad, Hooking.

Detecting malicious applications on Smartphones with Android operating system through of an app

Abstract: In recent years, the Android operating system is the most used in Smartphones, which makes it the target of the greatest number of threats; trend that has remained in recent years. According to the 2016 report, Trends in Security published by ESET, the number of mobile vulnerabilities increases every year since 2013 and, throughout 2015, the rate of increase within the Android ecosystem that put the privacy of your information at risk, has averaged 200 new malware samples per month. Therefore, this article presents an application (app) for the timely detection of potential malicious applications present in smartphones, particularly those with Android operating system, presenting a case study that has allowed validating the app through the detection of malicious applications installed on a mobile device.

Keywords*:* Smartphone, Android, Cybersecurity, Hooking.

1. Introducción

El desarrollo, crecimiento y evolución de las Tecnologías de Información y Comunicación (TICs) ha creado nuevas formas para compartir, transferir y distribuir información por medios digitales (Cisco, 2017), (Sherman, 2019), (Dai, Miao, 2005); (Jin, et al., 2005), en este contexto, el panorama de la seguridad se ha vuelto más complejo al aumentar el número de amenazas y tipos de amenazas. En la última década, el uso de las tecnologías de la información en el ámbito personal, académico y empresarial ha aumentado de 30% a 70% (INEGI, 2014), lo que ha propiciado nuevas oportunidades de desarrollo tecnológico.

De acuerdo, al informe de 2016, ICT Realidad y cifras (Sanou, 2016) muestra que los Smartphone se han convertido en el medio masivo de comunicación más utilizado debido a su portabilidad y relativo bajo costo. Asimismo, al informe de 2016, Visión de la Ciberseguridad publicado por Norton (Symantec Corp., 2016), existe registro de alrededor de 594 millones de afectaciones por vulnerabilidades y amenazas informáticas que ponen en riesgo la privacidad de la información de estos dispositivos, debido a que su exposición en Internet es cada vez más frecuente.

El reporte de Gartner (Woods, 2016), muestra que Android se ha consolidado definitivamente como el sistema más utilizado en el segmento de usuarios de Smartphones con un 86,2% de las ventas en el segundo cuartil (Q2) del año 2016, seguido por iOS de Apple Inc., como la segunda plataforma preferida con el 12,9%, estadística que se ha mantenido desde Q1 de 2013. Además, de acuerdo al informe de 2016, Tendencias en Seguridad publicado por (ESET, 2016), el número de vulnerabilidades móviles ha aumentado cada año desde 2013 y, a lo largo de 2015 la tasa de creación de amenazas dentro del ecosistema Android creció con un promedio de 200 nuevas muestras de malware por mes, debido a la exposición de estos dispositivos en Internet.

De acuerdo a los informes mencionados, implican que la seguridad de los Smartphone es un asunto cada vez más importante. Sin embargo, la complejidad que conlleva analizar estos volúmenes de información generados, requiere de técnicas y herramientas sofisticadas para mejorar su seguridad (Ponemon, 2014).

Por lo tanto, para poder analizar la información generada por los Smartphones, es necesario contar con herramientas de análisis automático de datos (Moço, Lobato, 2014), (Maloof, 2006), (Spreitzenbarth, 2015), para examinar aplicaciones que representen brechas de seguridad; particularmente las de dispositivos con sistema operativo Android (ESET, 2014), (Martínez, 2015).

El objetivo de este artículo es presentar una aplicación (app) para la detección oportuna a potenciales aplicaciones maliciosas presentes en Smartphones, particularmente aquellos con sistema operativo Android. Para el desarrollo, de esta herramienta se ha utilizado técnicas de hooking y se ha realizado un estudio de caso para su validación.

El artículo está estructurado de la siguiente manera: la sección 2 presenta los conceptos generales relacionada a la seguridad; la sección 3 presenta la Herramienta para identificar aplicaciones potencialmente maliciosas; la sección 4 presenta un estudio de caso que se ha utilizado para validar la herramienta; finalmente, en la sección 5 se establecen las conclusiones.

2. Conceptos generales

En esa sección, se describirán los conceptos principales: Ciberseguridad, Seguridad, Seguridad de la Información, Hooking y amanezas principales en Smartphone con sistema operativo Android, con el objetivo de establecer la contextualización de terminología para el desarrollo de este artículo.

La ciberseguridad conforme a la norma ISO 27001, define Activo de Información como "el conocimiento o datos de valor para una organización", mientras que un Sistema de Información incluye aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.

La Seguridad de la Información, incluye métodos, procesos o técnicas para la protección de la información en formato digital de una organización o persona, incluyendo redes e infraestructura tecnológica. La principal diferencia entre Ciberseguridad y Seguridad de la Información (SI), es que esta la SI se encarga de las medidas adecuadas de protección de la información, de acuerdo a su importancia y criticidad, independientemente de su formato, medio de almacenamiento (físico o digital) y de transmisión.

Por otro lado, el término Hooking (Tinajero, 2017) abarca un conjunto de técnicas utilizadas para alterar o aumentar el comportamiento de un sistema operativo, sus aplicaciones o sus componentes, interceptando mediante un código llamado Hook, llamadas de función, mensajes o eventos. En el ámbito de la Ciberseguridad, Hooking ayuda a detectar comportamientos irregulares para así prevenir, por ejemplo, la ejecución de aplicaciones maliciosas.

Con respecto a las amenazas más relevantes para la plataforma Android, es el software malicioso desarrollado específicamente para la plataforma (Mendoza-López, 2015). Su cantidad, complejidad y diversidad crece de forma constante y exponencial, de tal forma que, nuevas familias de códigos maliciosos y sus variantes se desarrollan con distintos objetivos, entre los que se encuentran, por ejemplo: (a) troyanos que suscriben al usuario a servicios de mensajería SMS premium sin su consentimiento; (b) botnets que buscan convertir en zombi al dispositivo móvil mientras roban su información; (a) adware para el envío de publicidad no deseada y; (d) ransomware que cifra la información y solicita un pago como rescate para que el usuario pueda recuperar sus datos. (Mendoza-López, 2015).

De acuerdo con el reporte de 2016, Amenazas de Seguridad en Internet, publicado por Norton (Symantec Corp., 2016a), tan sólo en el año de 2015, se identificaron 528 nuevas vulnerabilidades móviles, 18 nuevas familias de malware para Android y 3,944 nuevas variantes de malware para el ecosistema Android.

3. Herramienta para identificar aplicaciones potencialmente maliciosas

3.1 Antecedentes de la Herramienta

Para establecer las bases de la herramienta propuesta se llevo a cabo una revisión sistemática (Mejía, et al., 2017). A partir del análisis de los resultados del proceso de Revisión Sistemática, y de las diferentes áreas de interés orientadas en la detección de aplicaciones maliciosas y de vulnerabilidades en Smartphones, se identifican los siguientes resultados.

Entre las técnicas utilizadas se encuentran: 1) Hooking, que se basa en la inyección de código, para la detección y tratamiento de aplicaciones maliciosas (Tinajero-Manjarez et al., 2017); 2) Máquinas de Soporte Vectorial (Support Vector Machines, por sus siglas en inglés SVM), utilizadas para clasificar aplicaciones desconocidas como maliciosas o benignas y en la detección de actividad de los usuarios, mencionadas en (Kaghyan & Sarukhanyan, 2013) y (Spreitzenbarth et al., 2015); 3) Redes Neuronales para localización en interiores y exteriores, aplicado a tráfico y demografía, descritas en (Su et al., 2014), (Huang et al., 2014), (Paul & George, 2015), (Mugagga & Winberg, 2015), (Mugagga & Winberg, 2015), (Carlos E. Galván-Tejada et al., 2015), y (Dou et al., 2015); 4) K-Means y Local Outlier Factor (por sus siglas en inglés LOF) para detección de anomalías, utilizado en dominios como: medicina, detección de intrusos y fraude, abordadas en (Karim et al., 2014) y (Pasillas D. & Ratté, 2016); 5) Árboles de Decisión, Redes Bayesianas y Regresión, en cómputo forense y para la localización y detección de actividad utilizado en la detección de acoso escolar o bullying, analizadas en (Moço & Lobato-Correira, 2014) y (Garcia-Ceja et al., 2014), y; 6) Big Data y Autómatas Celulares para localización en interiores/exteriores y demografía, cubierta en (Tosi et al., 2014), (Asri et al., 2015), y análisis de comportamiento humano en entornos sociales (Human Social Behavior, por sus siglas en inglés HSB), estudiado en (More & Lingam, 2015) y (Dou et al., 2015).

De igual forma, se observó que los sensores de Smartphones son utilizados, principalmente, para: 1) la detección de la actividad del usuario, por medio del giroscopio y el acelerómetro, como se menciona en (Paul & George, 2015), (Moço & Lobato-Correira, 2014), (Carlos E. Galván-Tejada et al., 2015) y (Garcia-Ceja et al., 2015); 2) la localización en interiores y exteriores con ayuda de, por ejemplo el campo magnético de la tierra, utilizando sensores de orientación, micrófono e iluminación, estudiada en (Carlos E. Galván-Tejada et al., 2015) autenticación, cubierta en (Haque et al., 2013).

Por otro lado, los tipos de dato más utilizados para el análisis de comportamiento de un Smartphone son: 1) datos crudos, utilizados en (Tuttle et al., 2010), (Su et al., 2014), (Tosi et al., 2014), (Pasillas D. & Ratté, 2016) y (Garcia-Ceja et al., 2014), y; 2) logs de información, como se muestra en (Asri et al., 2015), (Mestry et al., 2015), (More & Lingam, 2015), (Mugagga & Winberg, 2015), (Moço & Lobato-Correira, 2014); mientras que, las principales vulnerabilidades detectadas son: 1) la infección por malware, analizada en (Karim et al., 2014); 2) el acceso o disposición indebida de la información y comportamiento sospechoso, cubiertos en (Pasillas D. & Ratté, 2016) y (Haque et al., 2013), y; 3) la aplicación de código malicioso, estudiado en (Chen et al., 2015).

Con respecto a herramientas se encontraron las siguientes: 1) ARES – Adaptable Reverse Engineering System, presentada en (Tuttle et al., 2010), una herramienta para Sistemas Móviles Forenses que asiste en el análisis de los datos recuperados en las investigaciones de actividad de Smartphones, por ejemplo: Logs de llamadas, email, mensajes de texto, eventos de calendarios, entre otros; 2) Log Analysis, mostrada en (Catanese & Fiumara, 2010), otra herramienta de Cómputo Forense que, utilizando técnicas de clustering, representa de manera gráfica el resultado de un análisis de la información, haciendo uso del formato GraphML (basado en lenguaje de marcas XML); 3) Demographic-Vis, cubierta en (Dou et al., 2015), el cual analiza información demográfica, en base al contenido generado por el usuario a través de una encuesta

para determinar características sociales, económicas y de comportamiento, por medio de técnicas como SVM y Redes Bayesianas, y; 4) Xposed framework (Barolli & Enokido, 2018), herramienta enfocada en la detección de aplicaciones maliciosas.

3.2. Desarrollo de la herramienta

De acuerdo a los resultados de la revisión sistemática la herramienta propuesta debe otorgar funcionalidades con respecto a:

- Detectar oportunamente aplicaciones potencialmente maliciosas mediante la ponderación de los permisos concedidos estática y dinámicamente a una aplicación, mediante la suma de los pesos asignados a cada uno de los permisos clasificados como peligrosos.
- Prevenir la disposición indebida de información sensible de usuario.
- Notificar al usuario de cualquier riesgo potencial mediante semaforización: (1) aplicación no maliciosa – negra; (2) aplicación sospechosa – amarilla; y (3) aplicación potencialmente maliciosa – roja.

Para el desarrollo de esta herramienta se llevo a cabo la siguiente tecnología:

- Android Studio, API 18+ como IDE de desarrollo.
- Xposed framework API (XposedBridge) 5.4 (jar), marco de trabajo para desarrollo de los módulos que cambian el comportamiento del sistema Android y sus respectivas aplicaciones.
- Smartphone con sistema operativo Android v4.0 API 18+.
- KingRootV5.0.5.397172 (apk), software para obtener privilegios de superusario.
- Xposed Installer 2.6.1 (apk), gestor de los módulos desarrollados con el Xposed framework.

La aplicación propuesta, está conformado por una interfaz de usuario, habituales para una app de Android, con objetos View y ViewGroup para desplegar los elementos gráficos, tales como: aplicaciones, servicios, permisos, etc. La Figura 1, muestra un ejemplo de la vista principal de la aplicación.

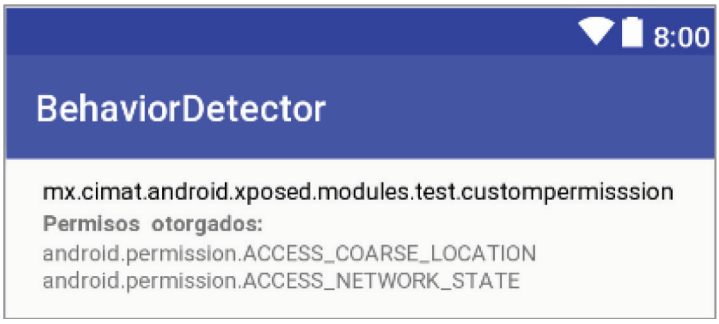

Figura 1 – Vista principal de la aplicación “BehaviorDetector”

La arquitectura de la aplicación propuesta, la cual es llamada BehaviorDetector, y los elementos que la conforman está divida en 3 paquetes principales (Figura 2):

- ***base,*** representa las clases, interfaces y entidades que implementa la funcionalidad principal mediante el uso del framework de Xposed, p.e: la clase hook, que es la encargada de realizar las llamadas a la API de Xposed
- ***hooks,*** donde se definen las clases que implementan tanto la funcionalidad estática como dinámica de la aplicación propuesta; y
- ***clase monitor,*** encargada de administrar los llamados a la funcionalidad estática y dinámica de la aplicación

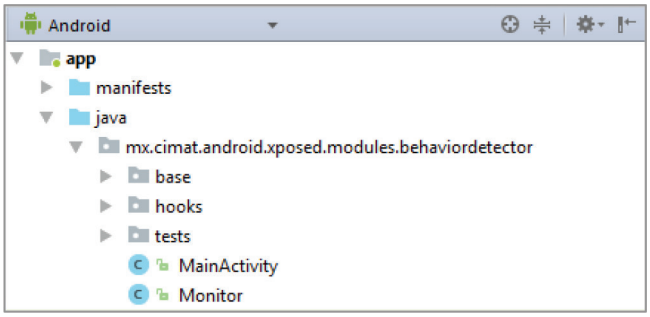

Figura 2 – Paquetes principales de la aplicación "BehaviorDetector "

Cuando se ejecuta instala la apk, se debe habilitar la aplicación con el gestor de módulos del Xposed Installer. Una vez iniciada la aplicación, el programa captura todos los paquetes que se cargan al iniciar el sistema operativo y, mediante la ponderación de los permisos estáticos que tienen definidos en sus manifiestos, determina si es una aplicación o proceso potencialmente peligroso o que ponga en riesgo la integridad del dispositivo, listándolo en la pantalla principal de la aplicación con su correspondiente semáforo.

4. Estudio de Caso

Para validar la herramienta, se realizó el análisis de un grupo de aplicaciones que, de manera nativa, forman parte del sistema operativo Android, versión 4.0 o superior, así como una aplicación personalizada que dinámicamente cambia los permisos solicitados, tanto de manera estática como en tiempo ejecución. El conjunto de permisos sobre los que se evaluó el riesgo potencial de cada aplicación, pertenece al que Android tiene clasificado como riesgosos, es decir, aquellos que podrían afectar la privacidad del usuario o el funcionamiento normal del dispositivo. El sistema operativo solicita al usuario que otorgue explícitamente esos permisos:

- En tiempo de ejecución (para Android 6.0 API 23 o posteriores). El usuario puede revocar los permisos en cualquier momento.
- Al instalar o actualizar la app (para Android 5.1 API 22 o anteriores). La única manera de revocar los permisos, es desinstalando la app.
- También, pueden aplicar permisos en los escenarios siguientes:
  - Cuando una llamada ingresa al sistema, para evitar que la app ejecute determinadas funciones.

- Cuando comienza una actividad, para evitar que las apps inicien actividades de otras apps.
- Cuando se envían y reciben transmisiones, para controlar los receptores y transmisores.
- Cuando se inicia o vincula un servicio.

Los permisos riesgosos abarcan áreas en las cuales una app requiere datos o recursos que incluyen información privada del usuario, o bien que podrían afectar los datos almacenados del usuario o el funcionamiento de otras apps. Por ejemplo, la capacidad de leer los contactos del usuario, se considera es un permiso riesgoso.

Todos los permisos riesgosos del sistema Android pertenecen a grupos de permisos. Si el dispositivo tiene Android 6.0 (nivel de API 23) instalado, el siguiente comportamiento del sistema tiene lugar cuando una app solicita un permiso riesgoso:

- Si una app solicita un permiso riesgoso incluido en su manifiesto y no tiene permisos actualmente en el grupo de permisos, el sistema muestra un cuadro de diálogo al usuario en el que se describe el grupo de permisos al cual la app desea acceder. En el cuadro de diálogo no se describe el permiso específico dentro de ese grupo. Por ejemplo, si una app solicita el permiso READ_CONTACTS, en el cuadro de diálogo del sistema se indica únicamente que la app necesita acceso a los contactos del dispositivo. Si el usuario brinda la aprobación, el sistema otorga a la app solamente el permiso que solicitó
- Si una app solicita un permiso riesgoso incluido en su manifiesto y ya tiene otro permiso riesgoso en el mismo grupo de permisos, el sistema lo otorga de inmediato sin interacción con el usuario. Por ejemplo, si a una app ya se le otorgó el permiso READ_CONTACTS y luego esta solicita el permiso WRITE_CONTACTS, el sistema lo otorga de inmediato.

Cualquier permiso puede pertenecer a un grupo de permisos. Sin embargo, el grupo de un permiso solo afecta la experiencia del usuario si es riesgoso. Se puede ignorar el grupo de permisos para los permisos normales. Por lo que se realizaron pruebas en Aplicaciones personalizadas y nativas.

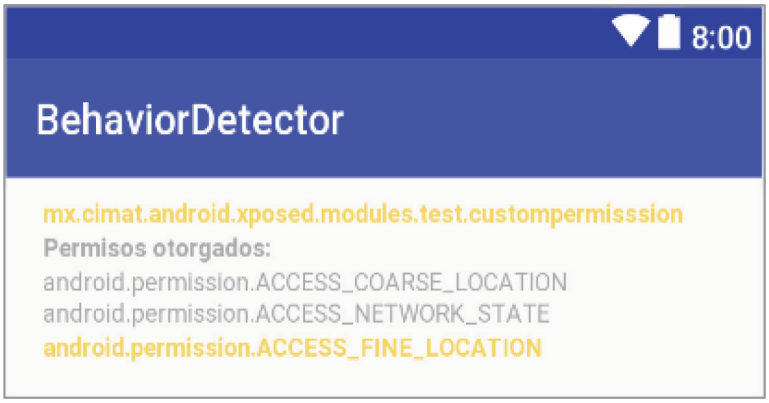

Figura 3 – Detección de una aplicación “sospechosa”.

Aplicación personalizada: Se realizaron varias pruebas durante el desarrollo del módulo con el objetivo de probar la efectividad de la detección de aplicaciones potencialmente maliciosas, por la solicitud de permisos riesgosos en tiempo de ejecución. Se probó usando una aplicación que usa permisos similares a los utilizados por aplicaciones maliciosas. El resultado obtenido, muestra que, conforme se van incrementando los permisos riesgosos, el semáforo para esa aplicación cambia, dependiendo de los permisos solicitados. En las Figura 3 y Figura 4, se muestra como el módulo desarrollado por la aplicación propuesta, alerta al usuario la ejecución de aplicaciones potencialmente maliciosas.

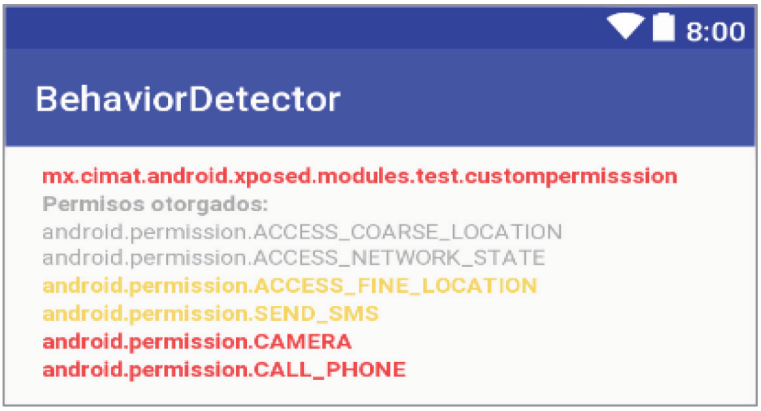

Figura 4 – Detección de una aplicación “potencialmente maliciosa”.

Los permisos detectados, normalmente serían utilizados en Android para realizar cualquier tipo de trabajo malicioso. Este conjunto de permisos representa un subconjunto

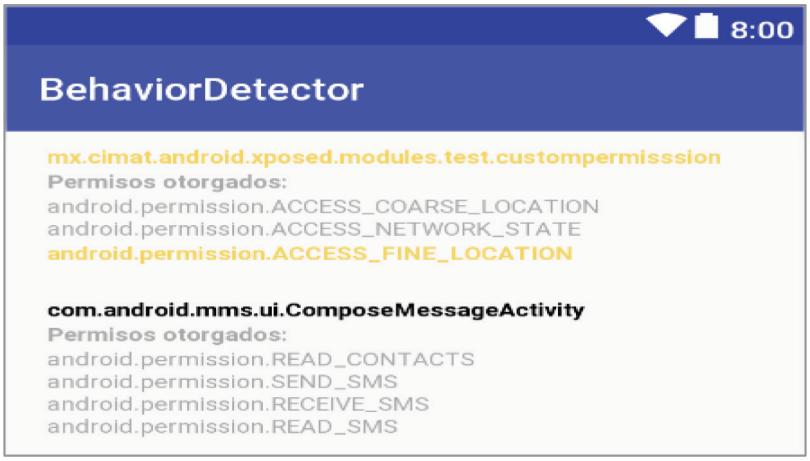

Figura 5 – Detección de una aplicación nativa “no maliciosa”.

de los permisos riesgosos utilizados para acceder a información privada y un medio de comunicación con el mundo exterior.

Aplicaciones nativas: También se probó este enfoque de detección con aplicaciones nativas que se cargan al inicio del sistema operativo. La Figura 5, muestra un ejemplo del análisis realizado durante el arranque des sistema operativo, donde se encuentra una aplicación no maliciosa.

Al observar los resultados obtenidos al utilizar la herramienta propuesta se pude observar que: (1) se detectan aplicaciones con permisos potencialmente riesgos declarados estáticamente; (2) se detectan las aplicaciones que solicitan permisos riesgosos de forma dinámica o en tiempo de ejecución; y (3) se notifica al usuario sobre las aplicaciones o servicios potencialmente riesgosas que estén instalados o en ejecución.

6. Conclusiones.

El creciente uso de las Tecnologías de Información ha revolucionado a tal grado de evolucionar en nuevos dispositivos como son los Smartphone, los cuales se encuentran conectados a internet, lo que ha permitido nuevas formas de transmitir información. Sin embargo, esto mismo ha generado que la seguridad en estos dispositivos sea mas complejo, ya que se han vuelto el medio masivo de comunicación portátil mas utilizado. En este contexto, Android como el sistema operativo más utilizado actualmente en Smartphone lo ha convertido en blanco del mayor número de amenazas creciente. En este contexto, analizar la información generada por estos dispositivos, es necesario contar con herramientas de análisis automático de datos. Por lo tanto, la herramienta desarrollada ha permitido detectar de manera oportuna aplicaciones personalizadas o nativas que son maliciosas. Al observar los resultados obtenidos se pude observar que el uso de la herramienta es viable para ayudar a usuarios con un nivel de habilidad y conocimiento mayor al básico del sistema operativo Android.

Agradecimientos

Al alumno Ricardo E. Melchor Velásquez quien ha desarrollado la herramienta presentada en este artículo como parte de su tesis para obtención del grado de Maestro en Ingeniería de Software ofrecida en el Centro de Investigación en Matemáticas.

Referencias

Asri, H., Mousannif, H., Al Moatassime, H., & Noel, T. (2015). Big data in healthcare: Challenges and opportunities. In: 2015 International Conference on Cloud Technologies and Applications (CloudTech) (pp. 1–7). IEEE. Doi: 10.1109/CloudTech.2015.7337020.

Barolli, L., & Enokido, T. (2018). Innovative Mobile and Internet Services in Ubiquitous Computing. In: 11th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2017) (Vol. 612, pp. 952–958). Torino, Italia: Springer. Doi: 10.1007/978-3-319-61542-4.

Catanese, S. A., & Fiumara, G. (2010). A visual tool for forensic analysis of mobile phone traffic. In: MiFor '10 Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence (pp. 71–76). New York, NY. USA: ACM. Doi: 10.1145/1877972.1877992.

Cisco. (2017) ¿Qué es un firewall? Retrieved from: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-afirewall.html.

Chen, Y., Lee, H., Jeng, A. B., & Wei, T. (2015). DroidCIA: A Novel Detection Method of Code Injection Attacks on HTML5-Based Mobile Apps. In: 2015 IEEE Trustcom/BigDataSE/ISPA (pp. 1014–1021). IEEE. Doi: 10.1109/Trustcom.2015.477.

Dai J., Miao H. (2005). D_DIPS: An Intrusion Prevention System for Database Security. In: Qing S., Mao W., López J., Wang G. (eds). Information and Communications Security. ICICS 2005. Lecture Notes in Computer Science, (vol 3783). Berlin, Heidelberg: Springer.

Dou, W., Cho, I., ElTayeby, O., Choo, J., Wang, X., & Ribarsky, W. (2015). DemographicVis: Analyzing demographic information based on user generated content. In: 2015 IEEE Conference on Visual Analytics Science and Technology (VAST) (pp. 57–64). IEEE. Doi: 10.1109/VAST.2015.7347631.

ESET LLC. (2014). Guía de seguridad para smartphones: ¿Cómo configurar tu Android de la forma más segura?. Buenos Aires, Argentina. Retrieved from: http://www.welivesecurity.com/wp-content/uploads/2014/06/guia_seguridad_android_eset.pdf.

ESET LLC. (2016). Trends 2016 (in) Security Everywhere. Retrieved from: http://www.welivesecurity.com/wp-content/uploads/2016/01/eset-trends-2016-insecurity-everywhere.pdf.

Galván-Tejada, C. E., García-Vázquez, J. P., Galván-Tejada, J. I., Delgado-Contreras, J. R., & Brena, R. F. (2015). Infrastructure-Less Indoor Localization Using the Microphone, Magnetometer and Light Sensor of a Smartphone. Sensors (Basel), 15(8), 20355–20372. Doi: 10.3390/s150820355.

García-Ceja, E., Brena, R., & Galván-Tejada, C. E. (2014). Contextualized hand gesture recognition with smartphones. In: 2014 Mexican Conference on Pattern Recognition (MCPR) (pp. 122–131). Springer. Doi: 10.1007/978-3-319-07491-7_13.

Haque, M. M., Zawoad, S., & Hasan, R. (2013). Secure techniques and methods for authenticating visually impaired mobile phone users. In: 2013 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 735–740). IEEE. Doi: 10.1109/THS.2013.6699095.

Huang, C., Ying, J. J., Tseng, V. S., & Zhou, Z. (2014). Location semantics prediction for living analytics by mining smartphone data. In: 2014 International Conference on Data Science and Advanced Analytics (DSAA) (pp. 527–533). IEEE. Doi: 10.1109/DSAA.2014.7058122.

INEGI. (2014). Estadísticas sobre la disponibilidad y uso de tecnología de información y comunicaciones en los hogares, 2013. Aguascalientes, Ags. México. Retrieved from: http://www3.inegi.org.mx/sistemas/biblioteca/ficha.aspx?upc=702825062378.

Jin H., Yang Z., Sun J., Tu X., & Han Z. (2005) CIPS: Coordinated Intrusion Prevention System. In: Kim C. (eds). Information Networking: Convergence in Broadband and Mobile Networking. ICOIN 2005. Lecture Notes in Computer Science, (vol 3391). Springer, Berlin, Heidelberg: springer.

Kaghyan, S., & Sarukhanyan, H. (2013). Accelerometer and GPS sensor combination based system for human activity recognition. In: Ninth International Conference on Computer Science and Information Technologies (CSIT) Revised Selected Papers (pp. 1–9). IEEE. Doi: 10.1109/CSITechnol.2013.6710352.

Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: review, future trends, and issues. Journal of Zhejiang University SCIENCE C, 15(11), 943–983. Doi: 10.1631/jzus.C1300242.

Maloof, M. A. (2006). Machine Learning and Data Mining for computer security: Methods and applications. Advanced Information and Knowledge Processing. Washington, DC. USA: Springer.

Martínez Retenaga, A. (2015). Situación del Malware para Android. Madrid, España. Retrieved from: https://www.certsi.es/guias-y-estudios/estudios/android-malware-situation.

Mendoza-López, M. Á. (2015). Herramientas de detección - Investigación, desarrollo y acción. Coordinación de Seguridad de La Información UNAM-CERT, (23), 34. Retrieved from: http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/23_RevistaSeguridad-HerramientasDeDeteccion.pdf.

Mejía-Miranda, J., Melchor-Velásquez, R.E., & Muñoz-Mata, M.A. (2017). Vulnerability detection in smartphones: A systematic literature review. In: 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), (pp. 1-7). doi: 10.23919/CISTI.2017.7975914.

Mestry, M., Mehta, J., Mishra, A., & Gawande, K. (2015). Identifying associations between smartphone usage and mental health during depression, anxiety and stress. In: 2015 International Conference on Communication, Information & Computing Technology (ICCICT). IEEE. Doi: 10.1109/ICCICT.2015.7045656.

Moço, N. F., & Lobato-Correira, P. (2014). Mobile forensics: A smartphone-based activity logger. In: 2014 21st International Conference on Telecommunications, ICT 2014 (pp. 462–466). IEEE. Doi: 10.1109/ICT.2014.6845159.

More, J. S., & Lingam, C. (2015). Reality Mining based on Social Network Analysis. In: 2015 International Conference on Communication, Information & Computing Technology (ICCICT). Mumbai, India: IEEE. Doi: 10.1109/ICCICT.2015.7045752.

Mugagga, P. K. B., & Winberg, S. (2015). Sound Source Localisation on Android Smartphones. In: AFRICON 2015. Doi: 10.1109/AFRCON.2015.7331970.

Pasillas D., J. R., & Ratté, S. (2016). An unsupervised approach for combining scores of outlier detection techniques, based on similarity measures. In: CLEI 2016 - The Latin American Computing Conference (pp. 61–77). Valparaíso, Chile: Electronic Notes in Theoretical Computer Science. Doi: 10.1016/j.entcs.2016.12.005.

Paul, P., & George, T. (2015). An Effective Approach for Human Activity Recognition on Smartphone. In: 2015 IEEE International Conference on Engineering and Technology (ICETECH). IEEE. Doi: 10.1109/ICETECH.2015.7275024.

Ponemon Institute LLC. (2014). Enhancing Cybersecurity with Big Data: Challenges & Opportunities. Retrieved from: https://blogs.microsoft.com/microsoftsecure/2014/11/19/new-report-enhancing-cybersecurity-with-big-data/.

Spreitzenbarth, M., Schreck, T., Echtler, F., Arp, D., & Hoffmann, J. (2015). Mobile-Sandbox: combining static and dynamic analysis with machine-learning techniques. International Journal of Information Security, 14(2), 141–153. Doi: 10.1007/s10207-014-0250-0

Sanou, B. (2016). ICT Facts and Figures 2016. Geneva, Switzerland. Retrieved from: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Sherman, F. (2019). The Differences Between a Firewall and an Intrusion Detection System. Small Business - Chron.com. Retrieved from: http://smallbusiness.chron.com/differences-between-firewall-intrusion-detection-system-62856.html

Su, X., Tong, H., & Ji, P. (2014). Activity Recognition with Smartphone Sensors. Tsinghua Science and Technology, 19(3), 235–249. Doi: 10.1109/TST.2014.6838194

Symantec Corp. (2016a). Internet Security Threat Report. Mountain View, CA. Retrieved from: https://www.symantec.com/security-center/threat-report

Symantec Corp. (2016b). Norton Cybersecurity Insights Report. Mountain View, CA. Retrieved from: http://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt

Tinajero-Manjarez, G., Escamilla-Ambrosio, P. J., & Rodríguez-Mota, A. (2017). Analysis and Detection of Malware in Smartphones with Android Operating System Using Hooking Techniques. In: Conference'17, July 2017, Washington, DC, USA (p. 6). Washington, DC. USA.

Tosi, D., Marzorati, S., & Pulvirenti, C. (2014). Vehicular Traffic Predictions from Cellular Network Data – A real world case study. In: 2014 International Conference on Connected Vehicles and Expo (ICCVE) (pp. 485–491). Doi: 10.1109/ICCVE.2014.7297594

Tuttle, J., Walls, R. J., Learned-Miller, E., & Niel-Levine, B. (2010). Reverse engineering for mobile systems forensics with Ares. In: Proceedings of the 2010 ACM Workshop on Insider Threats - Insider Threats '10, (pp. 21–28). Doi: 10.1145/1866886.1866892

Woods V., (2016). Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016. Egham, UK.