Métrica basada en grupos de permisos para entender el impacto de las aplicaciones Android sobre la privacidad

Amador Aparicio[1], M. Mercedes Martínez-González[1], Valentín Cardeñoso[1,]
[1] Departamento de Informática, Universidad de Valladolid, 47071, Valladolid, Spain.
{amador,mercedes,valen}@infor.uva.es

The final, published version of this article is available online. Please check the final publication record for the latest revisions to this article.

[Aparicio, A., Martínez-González, M.M., Cardeñoso, V. (2022). Métrica basada en grupos de permisos para entender el impacto de las aplicaciones Android sobre la privacidad. 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), 1-5.

https://doi.org/10.23919/cisti54924.2022.9820147

Resumen. Android es el sistema operativo con mayor presencia en dispositivos móviles. El mecanismo de permisos se utiliza para conceder o restringir a las aplicaciones el acceso a los datos y recursos del dispositivo. Las aplicaciones solicitan permisos para acceder a ellos. Nuestra propuesta tiene como objetivo obtener una métrica basada en los permisos, fácil de utilizar para los propietarios de los dispositivos, que les proporcione una orientación sobre el riesgo para su privacidad que asumen cuando instalan una aplicación en su dispositivo. Como novedad relevante frente a propuestas anteriores, planteamos utilizar los grupos de permisos como uno de sus parámetros. Los grupos de permisos expresan conceptos más asequibles para cualquier tipo de usuario que los permisos individuales y son aquello sobre lo que en realidad los usuarios pueden actuar. Introducimos así el criterio de la usabilidad, lo que nos permite obtener una tecnología más humana.

Palabras clave: Android, privacidad, permisos, grupos de permisos, malware, métrica, riesgo.

1 Introducción

Acorde con el modelo de seguridad de Android [3][4], las aplicaciones deben solicitar permisos para acceder a los recursos del dispositivo del usuario [5]. En ocasiones las aplicaciones utilizan más permisos de los que realmente necesitan, lo cual puede derivar en riesgos para la privacidad de los usuarios. La privacidad es el derecho de una persona a la confidencialidad de su información privada y de su identidad [2]. Según expresa el Reglamento General de Protección de Datos (RGPD) y

recuerda la Agencia Española de Protección de Datos (AEPD) en su aclaración sobre el concepto de dato de carácter personal [1], se considera dato de carácter personal "toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente". En el mundo digital garantizar el derecho a la privacidad se traduce en la protección de los datos de carácter personal.

Los permisos en Android se organizan en grupos. Cada grupo recoge un conjunto de permisos relacionado con el acceso a algún dato o recurso del dispositivo: cámara, ubicación, micrófono, etc. Google proporciona indicaciones sobre qué permisos se deberían incluir en cada grupo [6], pero son los desarrolladores de aplicaciones quienes deciden qué permisos incluyen en cada grupo. Si la aplicación requiere acceder a esos datos o tener el control sobre recursos del dispositivo, se solicitará de manera explícita al usuario que conceda el permiso [7][8]. Cada vez que Google revisa la Interfaz de Programación de Aplicaciones (API) que utilizan los desarrolladores de las aplicaciones Android también revisa los permisos y los grupos de permisos que las aplicaciones pueden solicitar. De este modo, en sucesivas revisiones de la API han ido apareciendo nuevos grupos de permisos [9].

2 Problema

Aunque un alto porcentaje de los europeos manifiesta su preocupación por su privacidad en el uso de la tecnología[1] lo cierto es que muchos usuarios Android no son conscientes de la relación de los permisos con la seguridad y la privacidad [10]. Estos usuarios manifiestan no saber qué significan realmente estos permisos, a qué tipo de información accede una aplicación cuando se conceden. Es más, la mayoría de los usuarios ni siquiera se molestan en revisar la lista de permisos que pide una aplicación durante su instalación [11].

En nuestra opinión esto tiene relación con el proceso de instalación. Cuando un usuario instala una aplicación, se le presenta una lista de los permisos a los que accederá la aplicación, pero no se le informa de modo claro y sencillo sobre el alcance del permiso, el tipo de datos al que accede y la razón de este acceso. Para conseguir esta información el usuario debería consultar la política de privacidad asociada a la aplicación, pero estas políticas suelen ser documentos largos, tediosos, en los cuales resulta complicado acceder a información específica sobre los permisos, esto es, difíciles de entender para muchos usuarios. Posteriormente, durante la ejecución de la aplicación la información que el usuario recibe no es mejor. El usuario únicamente recibe advertencias genéricas que le preguntan si quiere conceder un determinado permiso (en realidad es un grupo de permisos), con la indicación de que es necesario para que la

[1] European Commission - Press release.
Eurobarometer: Europeans show support for digital principles. Brussels, 6 December 2021. Disponible en
https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_21_6462/IP_21_6462_EN.pdf

aplicación funcione. Como consecuencia, no percibe un riesgo para su privacidad, aunque ésta puede verse comprometida de varios modos [12].

3 Objetivos

Nuestro objetivo es proporcionar a los usuarios de dispositivos Android una métrica basada en permisos, fácil de utilizar, que muestre el impacto sobre la privacidad de las aplicaciones que instalan. Nuestra hipótesis es que este tipo de métrica les ayudaría a entender mejor el impacto de las aplicaciones sobre su privacidad y en consecuencia tomar mejores decisiones.

Nuestras suposiciones de partida son:

1. Los permisos que han sido más explotados por el malware son más peligrosos para la privacidad del usuario.
2. La facilidad de uso de la métrica depende de la comprensión de los permisos que conceden. Para obtener una referencia fiable de esta comprensión, que es subjetiva, nos planteamos la necesidad de recabarla con algún instrumento como una encuesta.

4 Sistemas de permisos Android

A. Niveles de protección

El sistema operativo Android divide el sistema de permisos en varios niveles de protección (*protection levels*). Indican el nivel de riesgo de los permisos y las consecuencias de concederlo [7]. Es el sistema operativo quien gestiona los recursos asociados a los permisos. Si se concede el permiso, la aplicación podrá acceder a ellos, en otro caso no podrá.

- *Normal*: permiso con un riesgo mínimo para los recursos y datos del dispositivo. El sistema otorga automáticamente este tipo de permiso a una aplicación solicitante durante su instalación sin pedir la aprobación explícita del usuario.
- *Dangerous*: permiso de mayor riesgo, que daría a la aplicación solicitante acceso a datos privados del usuario o control sobre el dispositivo. Este tipo de permiso presenta un riesgo potencial, por lo que el sistema requiere la aprobación explícita del usuario.
- *Signature*: permiso que el sistema otorga solo si la aplicación que lo solicita es de un desarrollador que ya consiguió el permiso (dos aplicaciones son del mismo desarrollador si están firmadas con el mismo certificado). Estos permisos se conceden solo en el momento de la instalación.

B. Grupos de permisos

El grupo de permisos es una categorización lógica de los permisos de una aplicación. Es una facilidad que Android proporciona a los desarrolladores [6][13]. Se declara en el fichero `AndroidManifest.xml` usando elementos de tipo `<permission-group>`. Para declarar permisos se utilizan elementos de tipo `<permission>`. Los permisos se añaden a un grupo dando valor al atributo `android:permissionGroup`.

TABLA I. GRUPOS DE PERMISOS DE ANDROID.

Nivel API	Nombre del Grupo	Descripción
1	LOCATION	Permisos que permiten acceder a la localización del dispositivo.
4	STORAGE	Permisos relacionados con el almacenamiento.
17	ACTIVITY RECOGNITION	Permisos para el reconocimiento de actividad.
17	CALENDAR	Permisos relacionados con el calendario del usuario.
17	CAMERA	Permisos asociados con el acceso a la cámara o la captura de imágenes/videos desde el dispositivo.
17	MICROPHONE	Permisos asociados con el acceso al audio del micrófono.
23	CONTACTS	Permisos relacionados con contactos y perfiles en este dispositivo.
23	PHONE	Permisos asociados a las funciones de telefonía.
23	SENSORS	Permisos asociados con el acceso a sensores corporales o ambientales.
23	SMS	Permisos relacionados con los mensajes SMS del usuario.
28	CALL_LOG	Permisos asociados al registro de llamadas.
31	NEARBY DEVICES	Permisos para para descubrir y conectarse a dispositivos bluetooth cercanos.
	NOTIFICATIONS[2]	Permisos para la publicación de notificaciones.

Todos los permisos de tipo *dangerous* (aquellos sobre los que el usuario puede actuar una vez ha instalado la aplicación) deben estar asignados a algún grupo. En las sucesivas revisiones de las API que utilizan los desarrolladores de aplicaciones, Android ha incorporado progresivamente nuevos grupos de permisos. En la Tabla 1 se muestra el nivel de API en el que aparece el grupo de permisos, el nombre del grupo y su descripción[3].

[2] Este grupo de permisos estará disponible en la versión 12L de Android. https://developer.android.com/reference/android/Manifest.permission_group#NOTIFICATIONS

[3] En la fecha de redacción de este artículo, la versión actual del nivel de API es la 31.

5 Estado del arte

Yang Wang, Jun Zheng, Chen Sun, S. Mukkamala realizaron una evaluación cuantitativa de los riesgos de seguridad de los permisos Android [14]. Usaron dos conjuntos de datos con 27274 aplicaciones benignas de Google Play[4] y 1260 muestras de *malware* Android. Sus resultados demuestran que es más probable que el *malware* solicite más permisos que las aplicaciones benignas, y también que solicite más permisos peligrosos. Un resultado de este trabajo es un *ranking* de los permisos más utilizados por las aplicaciones benignas y el *malware*, que ellos utilizan para cuantificar el riesgo de las aplicaciones, de modo que aquellas que requieren más permisos utilizados por *malware* se consideran más peligrosas.

Chen, Kuan-Lin, Yang y Chung-Huang [19] crean una aplicación que obtiene un valor del riesgo para los datos presentes en un dispositivo. Calculan este valor a partir de los permisos concedidos a las aplicaciones instaladas en el dispositivo y las opciones de configuración del dispositivo [6][14]. En el artículo se indica que es una evaluación del impacto sobre la privacidad (EIP). Sin embargo, su procedimiento no se ajusta a lo previsto en las evaluaciones de impacto sobre la privacidad [21][22].

A. Khatoon y P. Corcoran [15] destacan las dificultades del usuario para comprender qué impacto tienen las diferentes restricciones del dispositivo en su seguridad y privacidad. Su premisa es que cuantos más permisos se conceden, mayor es el impacto sobre la privacidad. En este artículo aparece una asignación de permisos a grupos de permisos, aunque para el cálculo del valor no se utiliza. Tampoco muestran cuál es el criterio de agrupación de los permisos en grupos de permisos, ni los grupos de permisos están actualizados.

Iman M. Almomani y A. Khayer [16] obtienen una lista de permisos para el nivel 30 de la API de Android que incluye 168 permisos definidos por los desarrolladores del sistema operativo Android, que abarcan desde la API 1 (2008) al nivel de API 30 (2020). Categorizan los 168 permisos en los grupos de permisos propuestos por Google [13]. Pero no aportan una métrica basada en permisos. El trabajo es de interés porque categorizan los permisos en los grupos de permisos Android. Los grupos de permisos utilizados no están actualizados desde que se publicó la API 31.

Aguilar, R [23] habla del abuso del permiso de accesibilidad que permite tomar el control total del dispositivo. Activar el servicio de accesibilidad, *protection level signature*,

En [17][18] utilizan los permisos de Android para diferenciar de manera rápida y efectiva aplicaciones benignas y *malware*. Analizan los permisos de un conjunto de aplicaciones. Proporcionan un *ranking* de permisos utilizados por las aplicaciones benignas y el *malware*.

En [14][15][17][19] se aportan métricas. Detectamos que no se utilizan los grupos de permisos propuestos por Android en las métricas. Asimismo, la lista de permisos Android y los grupos de permisos no está actualizada a la última versión del nivel de API. Estas métricas tienen en común apoyarse en la idea de que los permisos más

---

[4] https://play.google.com/store/apps?hl=es&gl=US

explotados por el *malware* son más peligrosos. En [16] no aportan métricas, pero nos interesa la categorización de los permisos Android y los grupos de permisos. No obstante, debido a actualizaciones de la API Android posteriores a su publicación, están incompletos.

6 Metodología

La metodología propuesta tendrá una parte de elaboración de la métrica y otra de validación de la métrica.

A. Elaboración de la métrica

1. Se obtiene un conjunto con todos los permisos de Google [20], su nivel de API y su *protection level*.
2. Se eliminan del conjunto aquellos permisos que el usuario no puede gestionar. Sólo se mantienen los permisos cuyo *protection level* sea *normal* o *dangerous*. Son los permisos que el usuario puede gestionar.
3. Se obtiene un *ranking* con la frecuencia de los permisos más utilizados por aplicaciones benignas y el *malware*. Se añade al conjunto de permisos del paso 2 la frecuencia de cada permiso obtenida del *ranking* de permisos. Sabremos qué permisos y grupos de permisos son más utilizados.
4. Se marcan los permisos con un *protectión level normal* y *dangerous* que son explotados por el *malware*. Estos permisos tendrán un impacto más alto sobre la privacidad del usuario.
5. Para los permisos con *protection level normal* y *dangerous*, se obtienen los datos a los que accede cada permiso. Ayudará a determinar el impacto de los permisos y grupos de permisos sobre la privacidad del usuario. Aquellos permisos con una frecuencia más alta que accedan a datos personales presentarán un mayor riesgo para la privacidad del usuario.
6. Se obtienen los grupos de permisos actualizados y se clasifican los permisos obtenidos en el paso 2 en un grupo de permisos acorde con la propuesta de Google [20]. De este modo se dispone de una clasificación de referencia que indica en qué grupo debería estar cada permiso. La usaremos para comparar la asignación de permisos a grupos de cada aplicación con esta clasificación de referencia.
7. Se define la primera versión de la métrica utilizando los parámetros anteriores. Para cada permiso: nivel de API, *protection level*, peligrosidad o riesgo. Para la app: distancia de la clasificación de permisos en grupos encontrada respecto al estándar de referencia obtenido en el paso 8.

B. Validación de la métrica

1. Se selecciona un repositorio de aplicaciones. Existen diversos repositorios: Google Play[5], Tacyt[6] o apkpure[7].
2. Se selecciona un conjunto de aplicaciones del repositorio. Se utilizarán como caso de estudio para la validación.
3. Se analizan los permisos de cada aplicación y se clasifican en función de los parámetros utilizados en la métrica.
4. Se aplica la métrica propuesta a las aplicaciones seleccionadas.
5. Se elaboran y realizan encuestas para obtener una aproximación cuantitativa de la percepción que tienen los usuarios sobre el impacto en la privacidad de cada uno de los grupos de permisos propuestos por Android.
6. Estas encuestas se pasan a los usuarios antes de pedirles que utilicen la métrica.
7. Se pide a los usuarios que prueben la métrica sobre el conjunto de aplicaciones seleccionadas y que vuelvan a rellenar una encuesta.
8. Se analizan y comparan los resultados proporcionados por la métrica y las encuestas.
9. Se proponen modificaciones a la métrica y/o a las encuestas en función de los resultados obtenidos.

7 Resultados esperados

- Métrica sencilla y fácil de entender para medir el impacto sobre la privacidad de aplicaciones Android.
- Encuestas para validar la hipótesis de que la métrica ayudará a los usuarios a entender mejor el impacto sobre su privacidad.
- Resultados de la validación sobre un caso de estudio.
- Una clasificación actualizada de los permisos Android dentro de cada grupo de permisos.

[5] https://play.google.com/store/apps?hl=es&gl=US
[6] https://tacyt.elevenpaths.com/login
[7] https://m.apkpure.com/es/

Referencias

[1] Agencia Española de Protección de Datos. (2019). Informe jurídico del reglamento general de protección de datos de interés legitimo. https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf

[2] *IEC 60050 - International Electrotechnical Vocabulary - Details for IEV number 871–04-23: «privacy»*. (s. f.). International Electrotechnical Commission. Recuperado 11 de febrero de 2022, de https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=871-04-23

[3] Mayrhofer, R., Stoep, J.V., Brubaker, C., & Kralevich, N. (2021). The Android Platform Security Model. ACM Transactions on Privacy and Security (TOPS), 24, 1 - 35.

[4] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M.S., Conti, M., & Rajarajan, M. (2015). Android Security: A Survey of Issues, *Malware* Penetration, and Defenses. IEEE Communications Surveys & Tutorials, 17, 998-1022

[5] Stach, C. (2013). How to Assure Privacy on Android Phones and Devices? 2013 IEEE 14th International Conference on Mobile Data Management, 1, 350-352.

[6] Android Open Source Project, AndroidManifest.xml. (s. f.). Recuperado 11 de febrero de 2022, de https://github.com/aosp-mirror/platform_frameworks_base/blob/master/core/res/AndroidManifest.xml

[7] Manifest.permission_element |. (s. f.). Android Developers. Recuperado 26 de enero de 2022, de https://developer.android.com/guide/topics/manifest/permission-element

[8] Li, L., Bartel, A., Klein, J., Traon, Y.L., Arzt, S., Rasthofer, S., Bodden, E., Octeau, D., & Mcdaniel, P. (2014). I know what leaked in your pocket: uncovering privacy leaks on Android Apps with Static Taint Analysis. ArXiv, abs/1404.7431.

[9] Kim, J., Yoon, Y., & Yi, K. (2012). Static Analyzer for Detecting Privacy Leaks in Android Applications.

[10] Peruma, A.S., Palmerino, J., & Krutz, D.E. (2018). Investigating User Perception and Comprehension of Android Permission Models. 2018 IEEE/ACM 5th International Conference on Mobile Software Engineering and Systems (MOBILESoft), 56-66.

[11] Khatoon, A., & Corcoran, P.M. (2017). Android permission system and user privacy — A review of concept and approaches. 2017 IEEE 7th International Conference on Consumer Electronics - Berlin (ICCE-Berlin), 153-158.

[12] Stevens, R., Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012). Investigating User Privacy in Android Ad Libraries.

[13] Manifest.permission_group |. (s. f.). Android Developers. Recuperado 27 de julio de 2021, de https://developer.android.com/reference/android/Manifest.permission_group

[14] Yang Wang, Jun Zheng, Chen Sun, S. Mukkamala (2013, 15 julio). Quantitative Security Risk Assessment of Android Permissions and Appli. SpringerLink. Recuperado 27 de enero de 2022, de https://link.springer.com/chapter/10.1007/978-3-642-39256-6_15?error=cookies_not_supported&code=1fbae5d4-7eb3-4f4b-bb02-8217f9ca6b96

[15] Khatoon, A., & Corcoran, P.M. (2017). Android permission system and user privacy — A review of concept and approaches. 2017 IEEE 7th International Conference on Consumer Electronics - Berlin (ICCE-Berlin), 153-158.

[16] Almomani, I.M., & Khayer, A.A. (2020). A Comprehensive Analysis of the Android Permissions System. IEEE Access, 8, 216671-216688.

[17] M. S. Saleem, J. Misic, V. Mišić, V.B. (2022). Android *Malware* Detection using Feature *Ranking* of Permissions.

[18] M. Upadhayay, A. Sharma, G. Garg and A. Arora, "RPNDroid: Android *Malware* Detection using Ranked Permissions and Network Traffic," 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021, pp. 19-24, doi: 10.1109/WorldS451998.2021.9513992.

[19] Chen, Kuan-Lin, Yang, Chung-Huang (2016). Design and Implementation of Privacy Impact Assessment for Android Mobile Devices.

[20] Manifest.permission |. (s. f.). Android Developers. Recuperado 27 de agosto de 2021, de https://developer.android.com/reference/android/Manifest.permission

[21] Tecnología de la información. Técnicas de seguridad. Directrices para la evaluación del impacto de la privacidad (ISO/IEC 29134:2017) (Ratificada por la Asociación Española de Normalización en mayo de 2020.) (UNE-EN ISO/IEC 29134:2020). (2020). Norma Española UNE-EN ISO.

[22] Agencia Española de Protección de Datos. (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

[23] Aguilar, R. (2022, 26 febrero). Así de fácil es que el malware controle tu Android: el permiso de moda que se lo permite. Xataka Android. Recuperado 28 de febrero de 2022, de https://www.xatakandroid.com/sistema-operativo/asi-facil-que-malware-controle-tu-android-permiso-moda-que-se-permite