ACCESO DE APLICACIONES A LA PANTALLA EN DISPOSITIVOS ANDROID

I. INTRODUCCIÓN

En esta nota técnica se lleva a cabo un análisis de los mecanismos que existen en el ecosistema ANDROID para que las aplicaciones puedan acceder a la pantalla de los dispositivos. Como se detallará posteriormente, se solicita el permiso cuando se produce el acceso por parte de la aplicación a la pantalla sin informar correctamente al interesado, éste no puede comprobar si el acceso está activado ni se puede revocar el permiso.

Este es un documento orientado a usuarios y desarrolladores, a los usuarios para que conozcan las implicaciones y carencias de dicho mecanismo de permisos, así como la problemática de aceptar los cuadros de diálogo de las aplicaciones, a los desarrolladores para que adopten las medidas de transparencia y responsabilidad a la hora de diseñar apps que accedan a la pantalla.

II. ESTUDIO DE PERMISOS EN EL ACCESO A LA PANTALLA

En 2014 se libera la versión de Android 5.0 Lollipop que incorpora la versión de su API 21[1]. A través del API android.media.projection[2] se proporcionan métodos que posibilitan realizar la captura y uso compartido de la pantalla del dispositivo móvil[3].

Esta funcionalidad permite que una APP pueda acceder a la pantalla para realizar grabaciones o envío de la pantalla a otros dispositivos. Esta API no permite la captura del audio del dispositivo ni acceder al contenido de una ventana que esté marcada como segura[4].

A partir de Android 6.0 los permisos ya no son solicitados al instalar una APP, sino que es en tiempo de ejecución[5], cuando por primera se va a acceder a un recurso por parte de la APP cuando se pide permiso al usuario. Sin embargo, las Apps que quieran capturar o compartir la pantalla no necesitan de ningún permiso para ello. A través de un Intent[6] la aplicación puede solicitar el inicio de la grabación o difusión de la pantalla, mostrándole un simple cuadro de diálogo al usuario, que no constituye un permiso de la aplicación.

---

[1] https://developer.android.com/about/versions/android-5.0?hl=es-419
[2] https://developer.android.com/reference/android/media/projection/package-summary.html?hl=es-419
[3] https://developer.android.com/reference/android/media/projection/MediaProjectionManager#createScreenCaptureIntent()
[4] https://developer.android.com/reference/android/view/Display#FLAG_SECURE
[5] https://developer.android.com/training/permissions/requesting?hl=es-419
[6] https://developer.android.com/reference/android/content/Intent

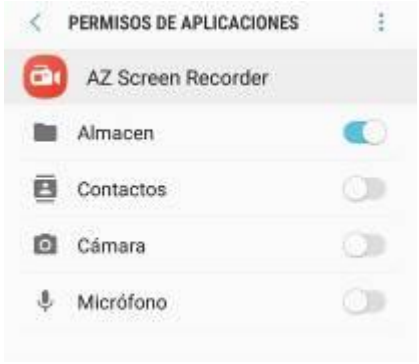

Figura 2

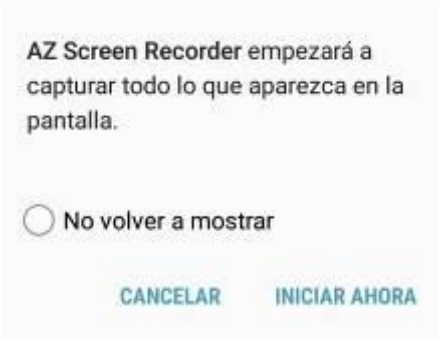

Figura 1

Como ejemplo, la aplicación AZ SCREEN RECORDER[7], disponible en Google Play Store, al ejecutarse solicita los permisos de almacén, contactos, cámara y micrófono. Si únicamente se acepta el de almacén para que se puedan grabar los ficheros como se muestra en la figura 1, al iniciar la grabación, la aplicación muestra el cuadro informativo de la figura 2, que debe ser aceptado por el usuario.

Se comprueba que la aplicación es capaz de capturar la pantalla de un dispositivo móvil, figura 3.

A través de la llamada a esta API, cualquier aplicación en la que el usuario acepte su cuadro de diálogo podrá grabar las aplicaciones que se muestren en la pantalla del dispositivo. Durante el desarrollo de una aplicación se puede activar el parámetro FLAG_SECURE[8] para algunas Actividades[9] (pantallas de la aplicación), lo que permite que la región de la pantalla que ocupe esta aplicación aparezca en negro en la grabación.

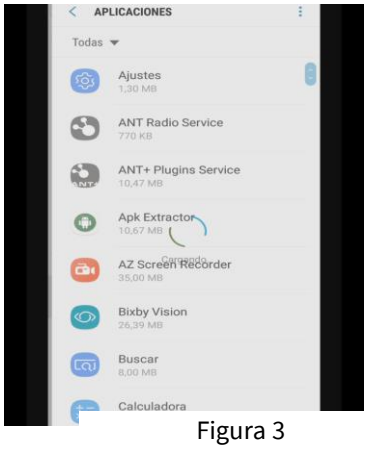

Figura 3

Figura 4

Figura 5

Pero FLAG_SECURE también presenta una serie de problemas, como permitir la captura de las ventanas hijo, el autocompletado o el teclado virtual[10] a pesar de tener activado este flag de seguridad. En la figura 4 se muestra una prueba de concepto de esta circunstancia[11].

[7] https://play.google.com/store/apps/details?id=com.hecorat.screenrecorder.free
[8] https://developer.android.com/reference/android/view/WindowManager.LayoutParams#FLAG_SECURE
[9] https://developer.android.com/guide/components/activities.html?hl=es

[10] https://commonsware.com/blog/2016/06/06/psa-flag-secure-window-leaks.html
[11] https://github.com/commonsguy/cwac-security/blob/master/docs/FLAGSECURE.md

Además, desde la versión 7 de Android hasta la 8.1 existió la vulnerabilidad CVE-2018-9524[12] que posibilitaba que se sobrepusiera un cuadro de diálogo sobre otro. Así un atacante podría mostrar un texto diferente sobre el cuadro informativo de inicio de captura de pantalla, de tal manera que el usuario no supiera que se va a capturar la pantalla del dispositivo[13]. La única pista que quedaría para el usuario sería que en la barra de tareas del dispositivo se seguirá mostrando el icono de "cast", como se muestra en la figura 5.

En noviembre de 2018 AOSP liberó un parche que mitiga esta vulnerabilidad[14]. La actualización del dispositivo, si es que el fabricante la implementa, es la única solución existente para evitar que se sobreponga el cuadro de dialogo.

III. CONCLUSIONES Y CONSEJOS

La aceptación por el usuario de la grabación de la pantalla no cumple con las condiciones del consentimiento si previamente no se ha informado claramente al interesado de los propósitos de dicho tratamiento de acuerdo con el artículo 13 del RGPD. De igual forma, no cumplirá con los principios de trasparencia que la grabación de la pantalla se produzca sin que el usuario sea consciente de en qué momentos se está ejecutando la misma, independientemente de que se haya concedido el consentimiento en un momento dado.

Los desarrolladores de aplicaciones, si utilizan la grabación de la pantalla, han de asegurarse de que se recoge de forma apropiada el consentimiento de los usuarios con posterioridad a cumplir los requisitos de información que señalan la normativa y que se ofrece una forma fácil de retirar dicho consentimiento. Además, han de proporcionar mecanismos para que el usuario sea plenamente consciente de cuándo se están realizando dichas grabaciones.

Los usuarios no han de aceptar aquellas aplicaciones que soliciten el acceso al contenido de la pantalla sin que se les haya informado apropiadamente del propósito de dichas grabaciones, las comunicaciones de dicha información a terceros, los periodos de conservación y resto de requisitos establecidos en el artículo 13 del RGPD. En caso contrario, no han de permitir el acceso al contenido de su pantalla y nunca activar la opción "No volver a mostrar" el aviso de inicio de acceso a la misma. A su vez, los usuarios han de mantener sus dispositivos al día con las últimas actualizaciones de seguridad.

[12] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9524
[13] https://labs.mwrinfosecurity.com/advisories/screencapture-via-ui-overlays-in-mediaprojection/
[14] https://source.android.com/security/bulletin/2018-11-01