ACCESS TO APPLICATIONS ON THE SCREEN FOR ANDROID DEVICES

INTRODUCTION

This technical note analyses the mechanisms that exist on the ANDROID ecosystem for apps to be able to access the device's screen. As will be detailed below, permission is requested when the app accesses the screen without providing proper information to the data subject, he can't check if the permission was granted neither withdraw the permission granted previously.

This document is addressed to users and developers, to users so that they can understand the implications and shortfalls of these permissions, as well as the problems with accepting the dialogue boxes on apps, and to developers so that they adapt the measures of transparency and accountability when designing apps that access the screen.

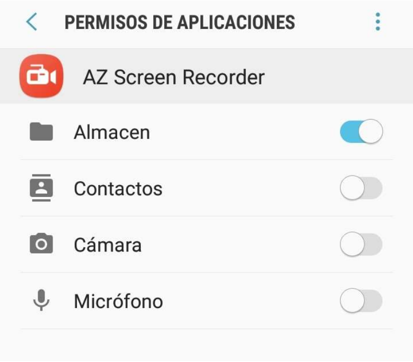
STUDY OF PERMISSIONS FOR ACCESSING SCREEN

In 2014 the Android 5.0 Lollipop version was released, which incorporated the version of its API 21.[1] Via the API android.media.projection[2], methods are provided that make the capture and shared use of the mobile screen possible.[3]

This function lets an app access the screen to record or send the screen shot to other devices. This API does not permit the capture of audio on the device or access to the content of a window that is marked as secure.[4]

Starting with Android 6.0, permissions are no longer requested when installing an app, but instead the user is asked for permission at run time,[5] when the app is about to access a resource for the first time. However, the apps that want to capture or share the screen do not need any permission to do so. Via an intent,[6] the app can request to start recording or broadcasting the screen, displaying a simple dialogue box to the user, which does not represent permission for the app.

[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

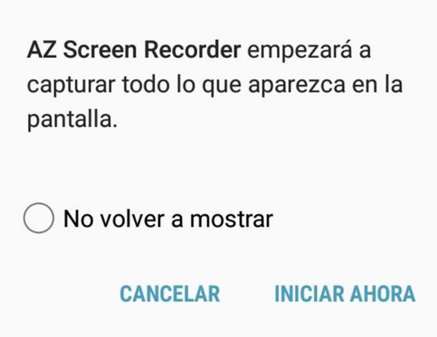


PERMISOS DE APLICACIONES

AZ Screen Recorder

- Almacen ●
- Contactos ○
- Cámara ○
- Micrófono ○

Figure 2



AZ Screen Recorder empezará a capturar todo lo que aparezca en la pantalla.

○ No volver a mostrar

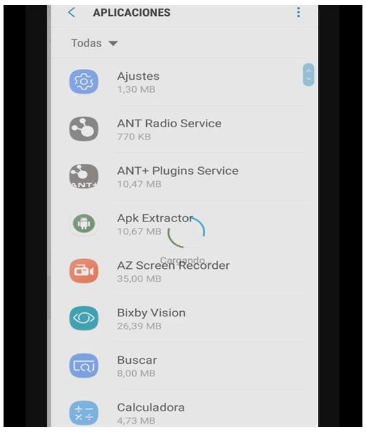
CANCELAR INICIAR AHORA

Figure 1

For example, the app AZ SCREEN RECORDER, available on the Google Play Store,[7] requests permissions for storage, contacts, camera and microphone when it is run. If only the storage request is accepted so that the files can be recorded as shown in Figure 1, when recording starts, the application displays the textbox shown in Figure 2, which must be accepted by the user.

It checks that the app is able to capture the screen of a mobile device, as shown in Figure 3.

Via the call to this API, any app for which the user accepts this dialogue box will be able to record the apps that are displayed on the device's screen. When developing an app, the FLAG_SECURE[8]parameter can be activated for some activities[9] (app screens), which lets the region of the screen occupied by this app appear as black during recording.



APLICACIONES

Todas

- Ajustes 1,30 MB
- ANT Radio Service 770 KB
- ANT+ Plugins Service 10,47 MB
- Apk Extractor 10,67 MB
- AZ Screen Recorder 35,00 MB
- Bixby Vision 26,39 MB
- Buscar 8,00 MB
- Calculadora 4,73 MB

Figure 3

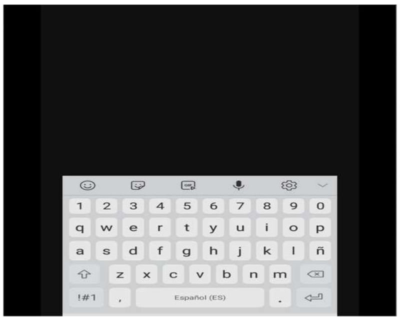


Figure 4

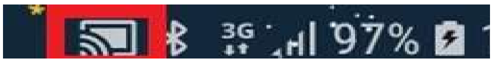


Figure 5

However, FLAG_SECURE also has a series of problems, like permitting the capture of child windows, autocomplete and the virtual keyboard, despite having this security flag[10] activated. Figure 4 shows a concept test for this circumstance.[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

Further, vulnerability CVE-2018-9524[12] existed in Android versions 7 to 8.1, which made it possible to overlay a dialogue box over another one. Thus, an attacker could display a different text over the info box on starting screen capture, so that the user would not know that the device's screen was going to be captured.[13] The only clue that the user would have would be on the device's task bar, which would continue to display the "cast" icon, as shown in Figure 5.

In November 2018, AOSP released a patch to mitigate this vulnerability.[14] The device update, if the manufacturer implements it, is the only solution existing to prevent the dialogue box overlay.

CONCLUSIONS AND ADVISE

Acceptance by the user to record the screen does not comply with the consent permissions if they have not been previously clearly informed of the purposes for this processing, pursuant to article 13 of the GDPR. Likewise, it does not comply with the principles of transparency when the screen recording takes place without users being aware when it this is being done, regardless of the fact that they have granted consent at some point.

App developers, if they use screen recording, must assure they gather user consent after providing the information required by GDPR and provide a easy method to withdraw such consent. More the over, they must provide mechanisms for the user to be fully aware in the moment they are doing such screen recordings.

Users should not accept those applications asking for screen access without providing the right information about the purpose of such access, the disclosure of the recording to a third party, retention periods, and the rest of requirements pursuant to GDPR article 13.

Otherwise, they should not grant screen access and in any case do not tick the option "Don´t show again" in the warning message before the first access. Users should also keep their devices up to date with the last security updates.

[11] https://github.com/commonsguy/cwac-security/blob/master/docs/FLAGSECURE.md
[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