Introduction to Android Permissions

All permissions that an app requires are granted at the time it is installed. Before installation, the user is shown the list of permissions that the app requests. The user must then choose whether to grant all of the requested permissions, and install the app, or deny the permissions and cancel the installation. There is no way to install an application while specifically denying some of the permissions it has requested. Similarly, there is no way to block access to sensitive resources after an app has been installed. A user's only recourse against an app that requests permissions that a user doesn't want to grant is to uninstall the app or never install it in the first place.

The Android operating system enforces that an application does not overstep its permissions by checking that an app has the necessary permission before allowing it to perform any potentially dangerous action. If an application attempts to do anything for which it does not have permission, the action will be blocked. There is also no way for an application to request additional permissions after it has been installed. If an updated version of an app requires more permissions than the older version, the user must approve the new set of requested permissions.

While this model ensures that an app cannot perform any inappropriate actions, the burden is largely placed on the user to decide exactly what is appropriate for an application. A user must decide, without ever having run an app, exactly what actions that app is allowed to perform. Making the decision even more difficult is the fact that individual permissions may only pose a risk when combined with certain other permissions. For example, access to contacts or location alone may not be harmful unless an app also has a permission that would allow it to get that data off of the device, such as access to the internet.

Deciding whether to install a new app that requests a long list of permissions is a daunting process for any user. It is very difficult to be 100% safe without refusing to install any new app,

but doing so would rob the user of all of the exciting and innovative apps that have been one of the main factors in Android's growing popularity. In most cases, applications have legitimate uses for requesting the permissions that they do. Mapping apps require the device's location, multiplayer games need access to the Internet, and social network apps may use the contacts list to automatically find friends on the same network. In other cases, apps ask users to knowingly exchange some personal information for free access to an app or service that might otherwise cost money. For example, many apps integrate advertising services that download location-based ads from a central server.

So is a new app safe to install? Answering the following questions may help you decide:

· Are there any obvious red flags? The most direct way for an application to cost a user money is by placing phone calls or sending text messages. Any application that requests these permissions without having a very obvious reason for doing so should be considered suspicious.

· Do you trust the application creator? The more you trust a company not to intentionally perform any malicious activity on your device and to handle your private data in a responsible manner, the more you should feel more comfortable installing their apps. Similarly, if a company is unknown to you or if you have reason to doubt their intentions, you should be wary of their apps.

· Are the requested permissions consistent with the app's advertised functionality? An app requesting permissions that appear to be unnecessary for its described functionality is a signal that it may be performing some undesirable behavior. However, in many cases apps request permissions to perform legitimate but non-obvious functionality. There is a lot of grey area here, but be on the lookout for extreme cases, such as a game requesting access to the camera or a wallpaper app wanting to read contacts.

· Would you be comfortable if the app collected or leaked your private data? Every user has a different tolerance for risk when it comes to having their personal data exposed. If you are comfortable with an app sharing the information to which it requests access, even if there is no apparent reason for it to do so, then feel free to install it.

Check out and compare permissions with our Android Permissions Stats Tracker

Mobilesecurity