Surveying developers on effects and awareness of modded apps

Luis A. Saavedra, Alastair R. Beresford, Hridoy S. Dutta, Alice Hutchings
Computer Laboratory, University of Cambridge
luis.saavedra@cl.cam.ac.uk, alastair.beresford@cl.cam.ac.uk

The Android operating system allows users to install apps directly from the Internet. Consequently, many third-party app markets have emerged, some of which offer *modded apps*: apps whose features and functionality have been altered by a third-party. We analysed over 146 thousand apps obtained from 13 of the most popular modded app markets and found that around 90% of them are altered in some way when compared to the official counterparts on Google Play. Modifications include games cheats, such as infinite coins or lives; premium features provided for free; and apps with modified advertising identifiers or excluded ads.

In iOS, usually considered a 'walled garden' free from sideloading, we have found around 90 modded app and sideloading markets and are studying them following a similar methodology. However, there is no existing dataset of Apple Store apps, so we have created our own.

We found the original Android app developers lose significant potential revenue due to: the provision of paid for apps for free (around 5% of the apps across all markets); the free availability of premium features that require payment in the official app; and modified advertising identifiers. While some modded apps have all trackers and ads removed (3%), in general, the installation of these apps is significantly more risky for the user than the official version: modded apps are ten times more likely to be marked as malicious and often request additional permissions.

However, there is a gap in the knowledge of these ecosystems of apps, and that is the awareness and effects noticed by the original developers. We are surveying the almost 30 thousand original developers of the Google Play apps we matched with the modded Android apps we found in the modded markets analysed in our study.[1] We contact them using their publicly-available developer emails, and give them a very brief summary of our findings, including the package names of their apps and in which markets we found them and when. In our survey we ask developers about their previous awareness of these modded versions of their apps and markets, whether they consented to these modded versions being hosted in third-party markets, and whether they used the available DMCA forms (in some markets) to try to take them down. We also asked about their perception of lost revenue and the available protections.

Preliminary results suggest the apps are not there with developer consent, and many have tried to remove them using DMCA forms with varied results; in the best case the current version is removed, but the next version still appears in the market in the future. The tools available, such as the Integrity API and obfuscation, appear to do little to deter motivated modders. Some developers integrate server-side validation and additional checks, potentially hindering the user experience.

[1] https://arxiv.org/abs/2402.19180