Unsafe exposure analysis of mobile in-app advertisements | Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks

By Michael C. GraceNorth Carolina State University, Raleigh, NC, USAView Profile

Abstract

In recent years, there has been explosive growth in smartphone sales, which is accompanied with the availability of a huge number of smartphone applications (or simply apps). End users or consumers are attracted by the many interesting features offered by these devices and the associated apps. The developers of these apps are also benefited by the prospect of financial compensation, either by selling their apps directly or by embedding one of the many ad libraries available on smartphone platforms. In this paper, we focus on potential privacy and security risks posed by these embedded or in-app advertisement libraries (henceforth "ad libraries," for brevity). To this end, we study the popular Android platform and collect 100,000 apps from the official Android Market in March-May, 2011. Among these apps, we identify 100 representative in-app ad libraries (embedded in 52.1% of them) and further develop a system called AdRisk to systematically identify potential risks. In particular, we first decouple the embedded ad libraries from host apps and then apply our system to statically examine the ad libraries, ranging from whether they will upload privacy-sensitive information to remote (ad) servers or whether they will download untrusted code from remote servers. Our results show that most existing ad libraries collect private information: some of them may be used for legitimate targeting purposes (i.e., the user's location) while others are hard to justify by invasively collecting the information such as the user's call logs, phone number, browser bookmarks, or even the list of installed apps on the phone. Moreover, additional ones go a step further by making use of an unsafe mechanism to directly fetch and run code from the Internet, which immediately leads to serious security risks. Our investigation indicates the symbiotic relationship between embedded ad libraries and host apps is one main reason behind these exposed risks. These results clearly show the need for better regulating the way ad libraries are integrated in Android apps.

Formats available

References

[1]

Android Permission Protection Levels. http://developer.android.com/reference/android/R.styleable.html#Android/ManifestPermission_protectionLevel.

[2]

Android Security and Permissions. http://developer.android.com/guide/topics/security/security.html.

[3]

Baksmali: A Disassembler for Android's Dex Format. http://code.google.com/p/smali/.

[4]

Dalvik. http://sites.google.com/site/io/dalvik-vm-internals/.
