Title:	How much does a zero-permission Android app know about us?
Year:	2019
Author:	Antonios Dimitriadis, George Drosatos, Pavlos S. Efraimidis
Abstract:	Android devices contain a vast amount of personal data of theirowners. These data are stored on the device and are protected bythe Android permission scheme. Android apps can obtain access tospecific data items by requesting the appropriate permissions fromthe user. However, in Android, the access to certain assets is grantedby default to the installed apps. For example, any Android app hasthe right to get the device's network operator, which may be usedto infer information about user's country and nationality. Similarly,any app has access to the clipboard which may occasionally containvery sensitive information, like a password. Consequently, a honestbut curious Android app may leverage the implicit access rights toaccumulate such unguarded information pieces and gradually builda detailed profile of the user. The device owner has no immediateway to control this flow of information and, even worse, may noteven be aware that this type personal data flow can take place. Inthis work, we examine the issue of default access rights of Androidapps and discuss the potential threat against user privacy. We assessthe user awareness and present a prototype zero-permission appthat collects user data.