Android Applications Privacy Risk Assessment

Abstract:
During the last few years, software security especially at the operating system level has been significantly improved for consumer electronics devices. However, few would argue that very little attention has been paid to software intrusiveness when it comes to preserve end-user’s privacy and security. In fact, this situation is in contrast to the security incidents leading to data leakages that are constantly on the rise. Furthermore, software developers in majority fail to offer strong warranties regarding the software they implement, meaning that they often do not bear any responsibility for software insecurities and misconfigurations. So, a major open question is whether end-users are in position to become informed and cope with the various forms of software intrusiveness threatening their private sphere as a consequence of security incident. This is especially important when using their mobile devices as they provide a fine grained access to private data sources. Note that nowadays mobile devices provide end-users equivalent or even more advanced services than the ones provided by PCs, as they incorporate a variety of sensors e.g., GPS, accelerometer, etc. that can be accessed through operating system services. In this way, mobile apps that get access to end-users’ data might invade their privacy and anonymity as a trade-off for offering the app free of charge. Moreover, end-users do not usually notice this, as in most cases such applications get access to this information “silently”. In this direction, end-users and even organizations lack the appropriate tools for accomplishing software privacy risk assessment. For instance, current risk management methodologies (e.g., CRAMM) are basically not considering software “features” in their risk models. While beneficial, these approaches in their current form can be used only for assessing a possible impact in terms of cost, as they do not assess software intrusiveness. So, there is not a way both for end-users and for organizations to use a risk assessment methodology in order to assess mobile applications intrusiveness before application “employment”. In this chapter, we study Android apps’ features that can be used to assess their intrusiveness to end-user’s private sphere, so end-users can be informed about possible privacy exposure in the direction of a mobile apps risk assessment methodology. To do so, we introduce a practical and an easily employable approach that does not require access to the apps’ original source code. We evaluate our approach using both goodware and malware.

URI:
Authors:
GENEIATAKIS Dimitrios
MEZENIDIS Charalabos
KOUNELIS Ioannis
STERI Gary
NAI FOVINO Igor

Publication Year:
2017

Science Areas:

  Information Society [1]

Keywords:

  ICT [2]
  security [3]

Publisher:
Taylor & Francis

ISBN:
978-1-138-03357-3 (print); 978-1-315-30582-0 (pdf)


Links