Chapter 6
Models of Privacy and Security Issues on Mobile Applications

Lili Nemec Zlatolas
University of Maribor, Slovenia

Marjan Heričko
University of Maribor, Slovenia

Tatjana Welzer
University of Maribor, Slovenia

Marko Hölbl
University of Maribor, Slovenia

ABSTRACT

The development of smart phones and other smart devices has led to the development of mobile applications, which are in use frequently by the users. It is also anticipated that the number of mobile applications will grow rapidly in the next years. This topic has, therefore, been researched highly in the past years. Mobile applications gather user data and that is why privacy and security in mobile applications is a very important research topic. In this chapter we give an overview of the current research on privacy and security issues of mobile applications.

INTRODUCTION

The aim of this Chapter is to present the current research topics in the field of privacy and security of mobile applications. Mobile technologies enable people to use mobile applications on their smart phones and smart devices constantly. The main operating systems used in the majority of mobile devices are Android with 70% market share and iOS with 23% market share ("Mobile/Tablet Operating System Market Share," 2016). Both most popular operating systems offer an app market for users with various mobile applications. Android users can download their mobile applications on Google Play Store and iOS users on Apple's App Store (Degirmenci, Guhr, & Breitner, 2013). The app markets are centralised systems that offer applications to users, which means that the users cannot download the applications from other websites like they can on desktop computers, unless they change their security settings on their mobile devices. The mobile device users have downloaded over 100 billion mobile applications from app markets in 2015 (Statista, 2016). Mobile applications are usually put on the app markets by the third-party developers and with different purposes of the applications. When an application is uploaded to the Google Play Store it is not checked and usually the application is then available for download

DOI: 10.4018/978-1-5225-2469-4.ch006

within a few hours. On the other hand, in Apple's Apps Store applications are checked and approved before they are put on the market ("iOS app approvals," 2016). Even though Apple checks applications on its market, researchers have found that Apple App Store enables developers of applications to download all the user's photos and calendars, meaning that being approved by the Apple App Store does not necessarily mean that the application respects the user's privacy (Weintraub, 2012). A German study compared users of Android and iPhones and discovered that Android users are more concerned that the applications could charge them with hidden costs and they more often mention security and privacy issues as important in comparison to iPhone users (Reinfelder, Benenson, & Gassmann, 2014). These results could either mean that the Android users do not trust their application market, because it is a more open system of applications upload, or that the users trust Apple more, because of Apple's general reputation of being more secure. Gilbert, Chun, Cox, and Jung (2011) proposed an automated security validation of mobile applications in application markets, but their proposal has not been implemented in practice in any app market. Therefore, applications on the app market could present a security problem and can be vulnerable. Implementing a better system of security and privacy checking in app markets would mean more security and privacy for users' data.

When users install a new mobile application from the app market, they are asked to read and confirm the terms of agreement of the application. Usually this means that users are requested to give their context information to applications or other third parties. Y. Liu (2014) argues that this way of getting users' consent is not the most adequate, because users usually just press continue without even reading which permissions they are giving the application. Users actually should have some control over what personal data they provide to third-party applications but, due to design and other restrictions, users just accept the terms of the application. A proposed solution by Y. Liu (2014) is the use of privacy by design concept with clearer and more user-friendly controls for privacy settings. Another group of researchers have conducted a study among 168 users using the Nokia N95 and, based on the research results, they presented a new business model for mobile platforms which would make mobile applications more privacy-friendly (Z. Liu, Bonazzi, & Pigneur, 2016). Another study showed that smartphone users are not much concerned about security when they install third-party applications to their smartphones (Mylonas, Kastania, & Gritzalis, 2013). The collaborators in the study trusted the application repositories and they disregarded security while adding applications to their smartphones.

Mobile applications are in use in many areas in people's lives as well as in corporate environments. The flow of data in mobile applications is enormous and there are numerous possibilities of the analysis and use of collected data by third-parties. It is important that data anonymity, confidentiality, integrity and authentication is provided for users of mobile applications. It is also important that protection of personal data is assured for the users of mobile applications. Research shows that users are often concerned about the privacy and security of their data, but some users would still not take any actions for protection (D'Ambrosio et al., 2016). On the other hand, Katell, Mishra, and Scaff (2016) have found that prompting users about permissions on data security and privacy might encourage users to take care of their privacy. Other possibilities to protect data also include biometric security measures when mobile applications are used and, in cases where personal authentications are required (Guerra-Casanova, Sánchez- Ávila, de Santos Sierra, & del Pozo, 2011). Such methods could provide better security for the applications that do not require personal authentication and collect sensitive information about the user.

In this Chapter a literature review is conducted to get a clear state-of-the-art on research in the field of privacy and security of mobile applications and what models were presented in considering this topic.