Data security and privacy in mobile applications

Ghimpu Lucian Eduard[1]

[1]*Faculty of Mathematics and Computer Science, Babeș-Bolyai University, Cluj-Napoca*

Abstract

In the last few years, the mobile device market has grown exponentially, the main reasons being the fast developing speed of the technology and the shift of interest from desktop computers to portable devices. The amount of data that these devices processes at any given time is massive, among which private and confidential data. The thesis proposes to explore some of the security issues that can appear in the lifecycle of a mobile application and how can these issues be fixed or prevented. We will analyze how the data is processed from its source, the user, and how it's handled throughout all the parts of the application.

The theoretical part consists of 4 chapters. The first chapter, Authentication and identity verification, explore some of the most secure and well known authentication mechanism and how can they be integrated into a mobile app. The second chapter, Permissions, gives an overview of the permission system used in most mobile operating systems and the importance of such systems. The third chapter, Communication Channels, presents secure ways of transmitting data from the client (the mobile application) to a secure server or other parties. The last chapter, Data Persistence, analyzes how can the private data be stored in a secure way making use of techniques such as cryptography.

The practical part is composed of 5 chapters that cover each part of the lifecycle of a mobile app, from the planning phase to the testing one. This part covers some of the latest technologies and techniques to create a robust and secure mobile app.

The thesis ends with a Conclusion chapter in which there are provided a summary and some future development ideas. This work is the result of my own activity. I have neither given nor received unauthorized assistance on this work.