ABSTRACT

With the development of versatile platforms for mobile computing environments, growth of high-speed communication channels, and decreasing costs, smartphones are becoming ever popular and, expanding its user-base. These gadgets are utilized for storing and organizing a large amount of personal and sensitive data like messages, contacts, pictures, recorded videos, emails, GPS location and have turned out to be an essential part in our day to day life. At the same time, various data privacy threats and security issues in mobile devices are posing challenges for both users and the developers of mobile operating systems. One of the primary reasons for the increasing popularity of smartphone is their functional expandability by installing third-party applications (Apps). After Android, iOS is the most broadly used mobile operating system which is designed, developed and promoted by Apple Inc. In recent years, the incredible growth in the number of iOS users has led to an increase in the number of downloads of the third-party apps. Consequently, the menace because of the apps that are potentially risky to user’s privacy has increased. As smartphone and mobile devices store a lot of user’s personal sensitive and crucial data, they have become an ideal target for data privacy threats and security issues in the entire mobile ecosystem.

Privacy concerns are principally about leakage of user’s crucial data like text messages, email information, downloaded documents, location coordinates, pre-recorded audios, and videos. Permission-based resource access is one of the approaches adopted by the developers of the mobile operating system to restrict accessibility. However, research studies have identified that current permission access declaration control mechanism, is insufficient to protect end-users data. It is difficult to distinguish between an over-privileged, malicious and a legitimate app simply based on permission-usage. Machine learning approaches utilized to detect malicious apps have offered promising outcomes for the Android platform due to availability of large labeled app data set and vast permission set. Conversely, there has been minimal work in extending the malware recognition work and protection of end-users privacy for the iOS platform which is a closed-source platform when compared with its peer Android.

The aim of the thesis is, to model user’s information privacy leaks by iOS apps (after installation and during their usage) and design privacy-enhancing techniques, to preserve the privacy of users. To attain the set objectives, three frameworks have been proposed out of which iABC (iOS Application analyzer and Behaviour Classifier) and iABC-AL (iOS Application
analyzer and Behaviour Classifier using Active Learning) intend to classify iOS apps (after installation and during usage) by using concepts of reverse engineering, network penetration testing and active learning approaches. iShield framework has also been proposed that incorporates privacy-preserving techniques for various data elements. The proposed frameworks intend to preserve end user’s privacy by protecting their private and sensitive data. The research work emphasizes protection of user’s data and confinement of malicious iOS apps. The work discussed in the thesis is valuable for developers of mobile apps, mobile Operating system designers and manufactures of mobile devices.

**Keywords:** Information privacy; iOS apps; Reverse Engineering; Static analysis; Dynamic analysis; Privacy preservation