Executive Summary

Evaluation of Mobile Privacy and Security: Mobile App Privacy Score

Sponsor: Redmorph Inc.
Advisor: Timothy Libert
Team: Fan Yang, Jianlan Zhu

Carnegie Mellon University
MSIT-Privacy Engineering Capstone Project
November 2018

Nowadays, mobile applications suffer from tremendous user-privacy issues. With the popularity of mobile apps, users' data is shared between a large variety of entities. Problems like targeted advertising and information leakage are common privacy violations among mobile applications. What makes it even worse is that, according to research, few users have an idea of the complicated issues. Even users are aware of some of their personal data has been improperly used, they have no idea of how bad the situation is and no choice but to accept them.

Related studies have done plenty of work to identify privacy issues exist in current mobile applications. Researchers have taken many metrics like privacy policies, permission requested, code analysis, data transmission into consideration to evaluate mobile apps' privacy performance. But average users still have a difficult time understanding the issues because few studies have put forward a straightforward scoring system.

Our designed product, M.A.P.S, is a comprehensive scoring system, which evaluates mobile applications' privacy performance. We have incorporated four different metrics: Android system permissions, third-party connections, software security, and network connection security. For Android permissions and software security analysis, we've leveraged MobSF, an open source pentesting framework for Android applications, to detect critical issues. For network security, we specifically looked at the security of internet connection and the security of connected web servers of the application by using SSLLabs & VirusTotal platform. To analyze data sharing practice in the background, we adopted webXray to distinguish between 3rd-party connections and 1st party connections. For each metric, we deduct certain points for different issues based on their severity level from a full mark. Then translate the score into a letter grade, which makes evaluation more direct to users.

Together with a scoring system, our product also contains a designed UI prototype. The key ideas when we design the prototype is that it should be able to inform users about their mobile applications' privacy performance in a straightforward and pellucid way and educate people well on mobile privacy. Within our design, we also include an overview of our scoring mechanism to users.

In order to make our designed product more rational, we interviewed CMU privacy experts about our chosen metrics and scoring methodology. They suggested us to include apps' usage of third-party libraries and privacy policies of apps when calculating the privacy score. Also, they indicated that privacy score is subjective, the product should work better when taking users' preference into consideration.

We also conducted a user study for the designed prototype among CMU students. Their feedbacks include better UI design (be more attractive), providing more insight suggestions for users and removing unnecessary information for average users. We improved some features of our design based on their feedback.

As privacy problems become common these days, it is urgent for users as well as privacy assessment companies to have a good design of privacy evaluation system. M.A.P.S is a product/feature which provides a straightforward scoring mechanism for them and proven to be working well among average users. In the future, a massive user study on privacy preference is suggested, to incorporate users' preference into privacy evaluation. We strongly believe M.A.P.S will prove to be a very worthwhile and profitable design in this field.