Comparing the security impact of Online generated apps and apps developed using IDEs

Joy Idialu
j2idialu@uwaterloo.ca
University of Waterloo
Waterloo, Ontario, Canada

Amirreza Shamsolhodaei
amirreza.shamsolhodaei@uwaterloo.ca
University of Waterloo
Waterloo, Ontario, Canada

1 Introduction

With the wide adoption of mobile devices by a large population of the world, specifically Android devices, there is an increased demand for mobile apps; for business and personal use. Businesses' demand for mobile apps stem from their need to use these mobile apps as a means to provide services to their clients and for the day-to-day running of their business operations. Whereas people use mobile apps for their personal activities. With this increase in demand for mobile apps, there are multiple solutions for individuals and companies to develop their own apps and make their services available in different formats; one solution could be to pay developers with sufficient technical skills and knowledge to build the app from the scratch, another option is the use of a simple tool to build the desired app. Online App generator (OAG) is one of the solutions provided where people use available and inter-connected UI elements that represent application components to build the app that they require. Online app generators have been on the rise as they involve little to no coding and no developing experience. OAGs also reduce the cost of developing apps, this is due to the fact that the need for hiring developers with high salaries is removed from the costs, as well as the cost of provisioning more infrastructure than is needed for running the apps. The cost of maintenance which could involve adding more features is drastically reduced. OAGs also reduce the development time which could have been longer if the apps were built from scratch. These factors encourage individuals and even companies to try out and eventually adopt these tools.

Oltrogge et al. [1] set out to determine the security implication of apps developed by Online App Generators and compare them with the primary way of producing applications which is developing an app by programming in Integrated Development Environments (IDEs) such as Android studio.

2 Threat Model

Android apps are allowed to engage in inter-component communication. However, there are apps that export their components to get accessed by other apps. If these apps have insufficient security protection and they are generated without complying to industry standards and best practices in terms of permission enforcement, they may grant an attacker app access to their sensitive data or methods. This would lead to issues that we are set to uncover when we compare apps developed with OAGs and apps developed using an IDE.

In our work, we want to compare the security features of apps developed by developers using Android studio and apps generated by Online app generators.

Looking at the results of [1], it could be said OAG apps hardly adhere to security best practices and these apps that have monolithic or module-dependent boilerplate code raise security concerns and points of failures such as creating over-privileged apps that if not considered carefully, might produce security issues. These issues could lead to attacks such as reconfiguration attacks, ad revenue theft, changing app-specific data, etc. It also pointed out that apps generated by OAGs do not prevent man-in-the-middle attacks due to flaws with certificate signatures.

By creating apps in both of these methods, we want to determine what security vulnerabilities they exhibit, for example to check if they use more permissions than required.

3 Methodology

In this project, we propose reproducing the results of the study done by [1]. which identified certain vulnerabilities introduced by OAGs. We focus our study on analyzing apps generated by 5 out of the 12 Freeware OAGs identified by [1]. Freeware OAGs are app generators that require no monetary payment as they are free to use. We plan on building some sample apps on Android studio and comparing their respective apps generated using OAGs.

From our study, we hope to discover certain added or missing features in Online generated apps when compared with Android studio apps and the security impact of such features. We also plan on identifying vulnerabilities identified by [1]. and other known security vulnerabilities in the Android ecosystem.

We plan on manually analyzing both apps, however if we are within the time limit of this project, we will further analyze the apps using the static analysis and dynamic analysis conducted by [1].

References

[1] Marten Oltrogge, Erik Derr, Christian Stransky, Yasemin Acar, Sascha Fahl, Christian Rossow, Giancarlo Pellegrino, Sven Bugiel, and Michael Backes. 2018. The Rise of the Citizen Developer: Assessing the Security Impact of Online App Generators. In *2018 IEEE Symposium on Security and Privacy (SP)*. 634–647. https://doi.org/10.1109/SP.2018.00005