MobSec Final Project Proposal
APK Dangers

Unveiling the Hidden Vulnerabilities of Play Store Apps

Michael Agee | Henry Post

Intro

The Google Play Store, having millions of applications across diverse categories, serves as a gateway for Android users to access a vast digital landscape. However, this immense app ecosystem harbors a discrete vulnerability: the potential for security flaws that threaten user privacy, data integrity, and even device functionality. This paper investigates a selection of Play Store apps and scans them for vulnerabilities, exploring their nature, impact, and potential mitigation strategies.

Scope

Our investigation stems from a growing concern about the rising number of security incidents linked to Play Store apps. We aim to shed light on the possible risks associated with Play Store apps and contribute to the ongoing discussion around user protection and app security best practices.

Methodology

We will determine this by random sampling of 10 APKs. We will use “apktool” and “jadx” for decompiling APKs, we will use “apkurlgrep” to find URLs within APKs, we will use “Snyk” to do SAST (Static AppSec Testing) scanning, and we will use “gitLeaks” for secrets scanning.

Key Areas

Types of vulnerabilities

Examining common vulnerabilities like insecure coding practices, permission overreach, and lack of encryption.

Impact on users

Assessing the potential harm caused by vulnerabilities, including data theft, financial losses, and identity compromise.

Root causes

Identifying the underlying factors contributing to app vulnerabilities, such as developer oversight, inadequate testing, and outdated libraries.

Mitigation strategies

Exploring potential solutions, including improved developer education, stricter app review processes, and user awareness campaign

References

[1] *Android Applications Pentesting*. Hacktricks. (n.d.). https://book.hacktricks.xyz/mobile-pentesting/android-app-pentesting/
[2] *GitLeaks.* GitLeaks. (n.d.). https://github.com/gitleaks/gitleaks
[3] *apkurlgrep.* apkurlgrep. (n.d.). https://github.com/ndelphit/apkurlgrep