How Mobile Applications Undermine User Privacy

Minh Nguyen

April 13, 2022

Abstract

Technological advancement has brought the age of smartphones and the development of thousands of mobile applications performing various tasks. However, some mobile applications installed in smartphones often gather user information from the devices without the user's consent or knowledge. Collecting user information poses privacy challenges, where users' data may be used to conduct targeted marketing, brute-force attacks, and social engineering attacks. This paper analyzes the contribution of mobile applications to users' privacy violations, their impact, and mitigative measures stakeholders can take to minimize it.

Introduction

Mobile devices are becoming more popular due to their ease of use, flexibility, and availability at low costs. According to Statista (2022), there are more than 2.5 million mobile applications in the Google Play Store in 2022. Advancements in mobile technology allow mobile phones to offer great user experience by incorporating hardware and software features that provide various services to end-users. Mobile applications extend the usability of smartphones by providing entertainment, communication, information, and entrepreneurship opportunities. The massive number of applications in the Play Store and App Store today indicates the exponentially growing reliance on mobile applications for everyday activities. It also shows the need for applications to offer highly personalized services to stand out in an overcrowded marketplace.

This paper presents an in-depth analysis of privacy challenges in mobile devices brought by mobile applications. It also discusses some remedies that can mitigate this challenge and make mobile devices safer to use.

Technical analysis

Developers primarily incorporate channels of collecting information from users in their applications. For instance, this information can be used to understand how users interact with the app, the challenges they are experiencing, and what fascinates them most about the application. The challenge that arises here is that the information collected may be beyond what is needed, bordering on leakage of sensitive user data. Additionally, some developers who use third-party libraries to collect data may expose the collected information to adversaries (Liu et al., 2019) [6]. It is also challenging to track down background operations that applications undertake to determine if they leak information since most are complex, use various libraries, and interact with different systems and networks (Castelluccia et al., 2017) [1]. Consequently, personally identifiable information collected from the applications may be leaked to developers, analytics companies, and third parties.

Mobile phones are more susceptible to data leaks due to their inability to incorporate robust anti-malware systems than desktop computers. According to Kim et al. (2015) [4], the anti-malware tools built for mobile devices are limited due to smaller mobile memory to accommodate them and the reliance on cellular batteries that provide less power. Additionally, most malicious applications masquerade as popular applications, then request for more permissions than are required. Users, therefore, mistake them for the original ones, downloading and installing them on their devices. Mobile devices are also hard to insecure due to their small size, making them easy to steal. Additionally, the ease of installing applications makes them more susceptible to malware.

Mobile phones contain more sensitive data captured by users through sensors than desktop and laptop computers. Mobile devices have cameras, GPS, microphones, fingerprint sensors, and accelerometers primarily used to increase their usability. However, installed applications can use these systems to gather information about the user for illegal purposes (Castelluccia et al., 2017) [1]. Additionally, most users consider their devices very personal; therefore, they store a lot of personally identifiable information and carry them around. For instance, it is possible to gather information such as a person's religion, health status, and supermarket preferences by monitoring their mobile phone's location. Malicious applications may, therefore, easily track them to gather information about the user using the sensors on the mobile devices.

Although the various app marketplaces have put restrictions to vet and restrict various applications' availability, the availability of third-party app stores leads to an increased threat. App stores and play stores provide security by scanning the apps to prevent viruses and fake applications (Castelluccia et al., 2017) [1]. For instance, Android devices can easily access unavailable applications in the Google Play Store by side-loading (Suleman et al., 2021) [9]. Similarly, iOS devices allow the installation of unverified applications through jailbreaking. Installing unvetted applications poses a risk to users as they may contain malicious bits of code that fetch information from the devices. This

risk escalates since the applications available in the third-party stores include modified applications for popular apps offering enhanced services such as free movie streaming, making them popular among users. Additionally, the usage of some of these applications often requires altering permissions and security settings, making the devices vulnerable to attacks.

Applications often collect more information than they indicate in their privacy policies. Most people assume that the permissions requested by applications upon their installations are the only pieces of information collected. However, studies show that some applications collect data beyond what they indicate in their privacy policies (Hayes et al., 2020) [3]. The value of big data may cause mobile developers to gather more information than they are willing to disclose, then trade it off to third-party companies. Apart from collecting data from users, Hayes et al. (2020) [3] established that apps like Instagram, Seamless, and Spotify gather information from other applications, then share it with third-party providers. Consequently, these applications end up with more details than the users consciously gave them. Trading information with third parties increases the risk of data mishandling and exposure to unwarranted parties.

Analysis and Discussion

Users' privacy is of great concern to developers, users, and manufacturers of various devices. Developers are required to include a privacy policy to help users understand what information applications need from them and how the applications use that information. However, even though mobile applications are expected to display their privacy policies, most users do not read them (Kimmons, 2021) [5]. Additionally, the privacy policies are mostly lengthy and contain jargon, making it hard for users to understand the implications of installing particular applications. Consequently, most users are unaware of what information is collected and how it can be used or shared. Therefore, some applications may contain information they do not require without users' consent. Thus, the privacy policy does not guarantee the protection of users' data by the application.

It is crucial to note that data collection is almost inevitable for the proper running of most mobile applications. Mobile apps such as dating platforms require sensitive information such as a user's location and sexual orientation to find suitable matches (Brandtzaeg et al., 2018) [7]. They also have to expose this sensitive information to other users to enable matching. Similarly, payment apps need users' credit card and bank information to allow transactions. While these applications only require this information to function within the expected limits, they can easily jeopardize users' information if they misuse their data. For instance, payment apps may expose a person's shopping preferences to third parties who may use them to perform targeted marketing. However, it is worth

noting that most applications' functioning is dependent on the data they collect from the user. Therefore, depriving them of this data reduces their effectiveness.

There is a growing concern about how privacy regulations are applied globally in mobile applications. The lack of uniformity in privacy regulations leads to increased distrust among the internationally used applications, as users are unsure how their data is handled. For instance, in Europe, there are more strict regulations on how user data is collected and used compared to the United States (Brandtzaeg et al., 2018) [7]. Failure to regulate how companies collect, use, and share personal information uniformly undermines privacy in the regions that have not embraced these measures. Additionally, countries with more stringent standards often express their concerns or restrict the usage of applications they consider unsafe. For instance, the United States has expressed its concerns over China's companies such as Huawei and mobile apps such as TikTok and restricted their use in the country (Williams and Center, 2020) [10]. Therefore, the lack of global standard regulations pokes holes in the integrity of mobile applications, raising concerns over their safety.

Several interventions can help in reducing privacy leakages in mobile apps today. These measures apply to developers, governments, and final users of these apps. One of the most effective ways of improving privacy in mobile apps is restricting their access to users' data. The less the mobile applications collect from users, the lower the risk of misuse of that data. According to Castelluccia et al. (2017) [1], apps need to be restricted to the data they can collect from the user to ensure that they only collect the information they require. The legal regulations should be tightened to scrutinize why applications require special permissions before authorizing their operation. Minimizing the information available to mobile apps ensures the protection of sensitive data from malicious applications that are likely to use it for ill purposes.

The end-users play a pivotal role in promoting their privacy. As noted earlier, most users grant permissions to apps without reading their privacy policies. Therefore, it is ineffective to implore users to read these policies before or during the installation process. Balebako et al. (2011) suggest soft paternalism, where users are made aware of the impacts of their decisions [8]. For instance, nudging users when they are about to grant particular permissions to apps may help them make wiser decisions. Additionally, alerting users when an application attempts to collect data from the phone may help users remain aware of the applications' information. Nudges improve decision-making by informing users of the pros and cons of granting particular permissions to apps and helping them keep track of the apps' data.

Another approach to minimizing user privacy violations is applying more stringent regulations on sensitive data applications. As earlier established, dating apps, transactions, and fitness apps require sensitive information for their operations. These applications should be put in a special category, where their operations are closely monitored to prevent mishandling of sensitive information. According to Castelluccia et al. (2017) [1], when users provide information

to these applications, there needs to be a controller who ensures that users have consented to the use of information for the intended purpose. Applications that process children's data should be equally scrutinized. Monitoring apps that handle sensitive data minimizes the risk of exposing users' data to unauthorized parties by promoting its authorized use.

Implementing app tracking transparency is an effective way of preventing mobile apps from gathering unnecessary information from users. Since most mobile apps tend to track more information from the user than they need, mobile operating systems should be designed in such a way that they allow users to deny them permission to do so. For instance, Apple's App Tracking Transparency enables users to authorize or deny apps' permission to track them (DeGiulio et al., 2021) [2]. This feature protects users who opt-out of tracking from fingerprinting and any other method that apps use to collect information from users. In their study, DeGiulio et al. (2021) [2] report that about 96.1 percent of respondents opted out of tracking. Therefore, implementing this option in all mobile devices would significantly improve privacy and allow users to control the amount of information apps can collect from their devices.

Conclusion

Mobile applications significantly contribute to the violation of users' privacy. It is essential to protect users' information in the most effective way possible. This paper has discussed how mobile apps compromise users' security and measures that can be taken to reduce privacy violations.

References

[1] Castelluccia. "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR". In: (2017).

[2] DeGiulio. "Ask App Not to Track": The Effect of Opt-In Tracking Authorization on Mobile Privacy. In International Workshop on Emerging Technologies for Authorization and Authentication". In: (Oct. 2021).

[3] Hayes. "An effective approach to mobile device management: Security and privacy issues associated with mobile applications". In: (2020).

[4] Kim. "Analyzing user awareness of privacy data leak in mobile applications". In: (2015).

[5] Kimmons. "Safeguarding student privacy in an age of analytics". In: (2021).

[6] Liu. "Privacy risk analysis and mitigation of analytics libraries in the Android ecosystem". In: (2019).

[7] Brandtzaeg Petter. “Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. Social Science Computer Review”. In: (2018).

[8] Balebako Rebecca. “Nudging users towards privacy on mobile devices”. In: (Jan. 2011).

[9] Suleman. “Combating Against Potentially Harmful Mobile Apps”. In: (June 2021).

[10] Williams. “Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security.” In: (2020).