GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 4, April (2024)

ANALYSIS OF DANGEROUS PERMISSION TYPES THE MOBILE APPLICATIONS

Yangiboev Navruz Zufar ugli
Student of Tashkent University of Information
Technology named after Muhammad al-Khorazmi
e-mail: navrozy99@gmail.com
Phone: +99890-288-19-99

ABSTRACT

The research paper explores the risks associated with different types of permissions requested by mobile apps and comprehensively analyzes their implications. Also, by examining the various permissions required by mobile apps, the study sheds light on the security vulnerabilities and privacy issues faced by users. Through systematic assessment and categorization, the study identifies different levels of risk associated with different permission types, providing valuable insights for both developers and users. The research also aims to improve understanding of mobile app security practices and empower users to make informed decisions about app permissions. Ultimately, the article serves as an important resource for stakeholders seeking to mitigate risks and protect user privacy in the rapidly evolving mobile technology environment.

Keywords: Mobile applications, permissions, security, analysis, risks, features, vulnerabilities, security.

INTRODUCTION

In an age where mobile technology dominates, the proliferation of mobile apps has taken our interactions with digital services to a new level. However, this convenience comes with its own risks, especially the permissions requested by these apps. This research paper explores the multifaceted landscape of mobile app permissions, with the goal of explaining the risks associated with different permission types and their impact on user privacy and security.

To provide advanced features and personalized experiences, mobile apps often require access to various device functions and user data. [1] However, this access can raise serious concerns about user privacy, data security, and misuse of sensitive information. Understanding the risks posed by different types of permissions is critical for developers, regulators, and users to effectively manage the complexities of mobile app security.

Permissions for mobile apps were introduced in Android 3.0 and were designed to help apps be more dynamic and automatic in their functionality. Permissions are introduced to help apps retrieve certain data from a user's device and use that data to help perform transactions and services in the background to benefit the user and update their accounts in turn [2].

Permissions inform the user that the application is requesting access to certain information that may be dangerous to personal information [3]. If an application compromises the requested information, the user may refuse to install or run it, and the application will be terminated. This ensures the protection of user data and information.

This study aims to identify risks associated with mobile app permissions that may affect user privacy. Google helps users identify dangerous permissions lists that may affect user privacy.

However, the technical requirements for these permissions are difficult for the average user to understand, and it doesn't make sense to check this list every time a user installs a new app. One possible solution is to develop a mobile application that has the ability to scan all the application code of all the applications on the mobile phone, providing a detailed and systematic report on the specific risks or concerns that are inherited in the permissions of these applications in a simple way. is to understand. by a normal user. This increases the awareness of mobile users and allows them to determine whether or not an app affects their privacy. If yes, what is the impact? Such a review helps users evaluate and analyze whether the application is safe to use or not and helps them make an informed decision whether to install the application or not, thereby allowing mobile phone applications provides an effective and long-term solution to associated risks. Previous research conducted as part of this study also provides important information about a specific mobile application called Sparrow, which was developed to examine the device for risks related to permissions granted to other applications.

Initial stages

Mobile applications use complex technologies that can be difficult for end users to understand. Malicious Android app developers use this feature to collect user data and track their activities. This section provides an overview of the concept of permissions, explores the functions a developer can perform on a device, and reviews the permission steps seen in different Android versions.

In the past, app developers were able to gain unauthorized access to a device's hardware or other app data without the user's knowledge. Such intrusions include activating the device's camera and surreptitiously tracking the user. As a result, the concept of permissions emerged as a means of regulating and controlling access and operations that occur outside the scope of an application.

In turn, this means that the purpose of enabling mobile applications is to increase the dynamism and automation of application performance. For example, if the device does not have the necessary permissions to access the microphone, the functionality of the recording software may be broken. As a result, a permissions procedure was introduced to address the interpersonal dynamics between developers and users.

Developer options on a specific device.

Exceeding the fixed mobile app permissions has led to serious security breaches for several users, which means it could cause ongoing problems for mobile phone users. Doherty states that Android permissions have the ability to facilitate a variety of activities such as spying, information and data theft, data breaches, user tracking, and illegal acquisition of personal information and passwords [4].

Chen (2) notes that communication applications often require read and write privileges for personal data and contact information, adding that they pose a number of additional risks for users who are unaware of these requirements. also provides. If the program contains malicious code that accesses personal information such as passwords, logins, and email addresses, these

rights may have harmful consequences for the user. Such information can lead to impersonation, financial loss, and personal data breaches. [5]

Tracking is another dangerous permission granted by mobile apps. These programs pose a potential threat to users because they allow attackers to track their location and whereabouts, thus affecting their privacy and, in some cases, their personal security [5].

Another important aspect is that the read phone status and identity permissions are often misused and not well understood by users. This license often applies to telecommunications and allows a mobile user to initiate calls while simultaneously managing games or other functions. The functionality allows the user's mobile device to prioritize phone calls over all other applications and processes. Additionally, this authorization gives the app access to the device ID, device apps, and user settings. This type of identification information may include an individual's identification card number, name, and address [6]. This is because the network allows for the unique identification of each device, making it easier to identify the owner of a particular phone, as they are under the manufacturer's control.

Using mobile permissions allows Android developers to track users, delete data, gain unauthorized access to private and personal information (such as passwords and email), financial theft, and loss of user funds. allows you to engage in activities such as the use of In addition, the gadget has the ability to listen and track the user, as well as track the whereabouts of the user. Therefore, it is important to develop a competent approach to inform users about the potential risks associated with the application [5].

LITERATURE ANALYSIS

So, the following three studies talk about the developments of the authors who conducted scientific work on the topic of the current scientific article. Pelet [8] says that the Android system permission model includes three main areas that contain risks. Ayed [9] found that users need a way to know when applications are using their personal data; research solves this problem. According to Felt [10], an application's permission request does not specify whether the permission instructions involve inadvertent access to more sensitive information. Felt proposed an automated method to fill this gap, which supports this study on mobile app consent risk.

As noted by Pelet [8], the Android system permission scheme allows some applications to access certain system addresses while blocking others. The Android system's permission model includes three categories: normal, dangerous, and signed or system. Any application that asks for normal permissions will get them without harming users. They perform wallpaper setting, ringtones and other functions.

However, users must approve dangerous permissions during installation [9]. Signature or system rights are granted after the application has been reviewed for eligibility. These rights are granted only to applications signed by the developer who developed and launched them [11]. Because they can access and modify sensitive phone data, these rights are the most dangerous and vulnerable.

According to Pelet [8], permissions for Android phone applications are one of the biggest threats to mobile phone consumers. Pelet said that while permissions have a predefined range

of access levels, determining whether an app has hidden permissions can make consumers more vulnerable and less secure.

As Ayed [9] pointed out, rogue programs can request permission to act on user data and devices. Ayed said that while the permission model requires users to accept permissions before installing an app, they are not aware of how their data is being used. Apps can use the granted permissions to capture user data or keystrokes, which poses a major security risk.

According to Felt et al., app permission requests do not indicate in the permission guidelines that passwords, personal information, and other sensitive information on a mobile device can be inadvertently accessed. [10] Spyware programs pose a serious threat to consumers' data and information.

METHODOLOGY

Mobile users' understanding of mobile app permissions and privacy was assessed using an online survey distributed on social media. The questionnaire contains 10 multiple-choice questions. The identity of the participants remained anonymous. The responses were studied and their relationships were examined for an interesting experiment.

Specifically, the study involved 100 participants, 53% of whom were women and 47% were men. 98% of the participants are between 18-40 years old, which shows that they are mature enough to know what is good and what is bad. 64% indicate they have a bachelor's degree, so they've probably heard about permissions and privacy.

Surprisingly, 56% of respondents do not check app permissions before installing. If responsible and educated people are like that, imagine young and illiterate people. These numbers highlight the need for increased awareness of app authorization risks.

According to the report, only 42% of users will try another app if their initial choice requires important permissions. The quiz tested participants' understanding of parental controls over children's app downloads on the Google Play Store. 26% of people used it, 63% knew about it but didn't use it, and 11% had never heard of it.

Only 32 percent of participants installed apps outside of the Google Play Store. A survey released showed that 53% of users do not know that most apps installed outside of the Google Play store are dangerous and have vital access to personal data without their consent. 65% of participants know that they usually install apps with unsafe permissions that can access or modify their contacts or photos. 65% of participants want the results of this study.

CONCLUSION

Mobile app permissions is a relatively new security topic that requires extensive research to identify many of the issues. Research suggests ways to make permissions more straightforward for mobile apps, allowing users to make informed decisions about whether to install an app by reviewing the permissions requested by mobile apps before granting them access to the areas they're looking for. The result of this study showed that the participants were over 18 years old and about 64% of them had at least a bachelor's degree, which means that they are responsible and educated users. However, more than 50% of them do not read the permissions before installing the app. This raises concerns about the safety of young and

less educated users. For the reasons mentioned above, it is necessary to develop an easy solution to this problem.

Dangerous permissions are divided into read, write and spy permissions. To support this classification, Sparrow is designed to help users identify dangerous apps. Sparrow does not require the user to remember what dangerous permissions are, nor does it require the user to have technical knowledge about permissions. The benefits of the Sparrow app include:

1) No permission is required for operation;
2) Does not require technical knowledge;
3) Easy to use;
4) available for free in the Google Play store;

The study also offers recommendations and best practices for what to do if a user needs to use an app with unsafe permissions.

REFERENCES

1. Mass, F. (2017) Coming off a Slow 2016, Smartphone Shipment Volume Expected to Recover in 2017 and Gain Momentum into 2018, According to IDC. (IDC) Worldwide Quarterly Mobile Phone Tracker.
2. Chen, L., McGrew, D. and Mitchell C. (2016) Security Standardisation Research. Springer International, New York.
3. https://doi.org/10.1007/978-3-319-49100-4
4. Carrascosa, I.P., Kalutarage, H.K. and Huang, Y. (2017) Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. Springer International Publishing, Cham.
5. https://doi.org/10.1007/978-3-319-59439-2
6. Doherty, J. (2016) Wireless and Mobile Device Security. Jones & Bartlett Learning, Burlington.
7. Elenkov, N. (2015) Android Security Internals: An In-Depth Guide to Android's Security Architecture. No Starch Press, San Francisco.
8. Six, J. (2012) Application Security for the Android Platform. O'Reilly Media, Sebastopol.
9. Android Developer (2017) Request App Permissions
10. https://developer.android.com/guide/topics/permissions/requesting.html
11. Pelet, J.-E. (2016) Mobile Platforms, Design, and Apps for Social Commerce. Advances in E-Business Research Series, IGI Global, New York.
12. Ayed, A.B. (2015) A Literature Review on Android Permission System. International Journal of Advanced Research in Computer Engineering & Technology, 4, 1520-1523.
13. Felt, A.P., Ha, E., Egelman, S. and Haney, A. (2012) Android Permissions: User Attention, Comprehension, and Behavior. Computer Science Department, University of California, Oakland, 1-14.
14. https://doi.org/10.1145/2335356.2335360