Research on security classification and evaluation methods of application programs

*Yi Liu, Jianping Hong**
(Guangdong Yuemi Technical Service Co., LTD., Guangzhou 510000, China)

Abstract: In the existing research of Application security detection, mainly through the "APP self-check" function of the "risk self-check" option group of the National Anti-Fraud Center APP(Application), the installed application in the mobile terminal and the stored application installation self-check. The standard of application detection is limited to whether there are suspected fraud and malicious programs, which leads to the lack of comprehensive security detection. To solve the above problems, this paper proposes a security detection method for application programs, including: running at least one target application; Detect whether there is malicious behavior in the target application program. If the malicious behavior occurs when the target application program is running, add the target application program to the first detection list; Detect the permission information of the target application program, if there is an unauthorized behavior, the target application program is added to the second detection list; Detect all third party SDKS of the target application for the existence of third party advertising SDKS, and if so, add the target application to the third detection list; Determine the risk level of the target application according to the first test list, the second test list and the third test list. This method solves the technical problem that the security detection of the application program is not comprehensive.

Key words: Application program; Security; detection

Introduction

With the popularization and development of mobile intelligent terminals, applications play an increasingly important role in people's lives. Using smart phones for entertainment, social interaction, office work and even consumption has become a daily behavior of users. After more than ten years of development and evolution, the two major mobile intelligent platforms -- Android and iOS have become the most widely used mobile intelligent systems. Since the advent of the first Android device and the announcement of iOS to open up the app market and support third-party applications, applications have faced a large number of security threats. The main security challenges include application analysis and cracking, malicious program issues, and application vulnerabilities and security issues. If the security of the application is not guaranteed, users will face the threat of privacy and sensitive data leakage, and even property damage. In addition, for application developers and manufacturers, they also face threats such as copyright infringement, leakage of key business logic, and loss of benefits. At present, it is mainly through the "APP self-check" function of the "Risk self-check" option group in the APP(Application) of the National Anti-Fraud Center to self-check the installed applications in the mobile terminal and the stored applications. Its standards for detecting applications are only limited to whether there are suspected fraud and malicious programs, which leads to insufficient security detection defects.

To solve the above problems, this paper proposes a security detection method for application programs, including: running at least one target application; Detect whether there is malicious behavior in the target application program. If the malicious behavior occurs when the target application program is running, add the target application program to the first detection list; Detect the permission information of the target application program, if there is an unauthorized behavior, the target application program is added to the second detection list; Detect all third party SDKS of the target application for the existence of third party advertising SDKS, and if so, add the target application to the third detection list; Determine the risk level of the target application according to the first test list, the second test list and the third test list. This method solves the technical problem that the security detection of the application program is not comprehensive.

1. Literature review

1.1 Research background and significance

With the popularization and development of mobile intelligent terminal, more and more researches begin to shift from the traditional computer platform to the research of mobile intelligent terminal platform. On the one hand, the popularity of mobile intelligent terminal benefits from the convenience brought to users, on the other hand, it also largely depends on various applications running on the system.

Today's mobile intelligent system has a more perfect ecosystem, and the system provides a very convenient development environment, process and tools to help developers develop a variety of featule-rich third-party applications, and deploy them to run on the mobile intelligent system, which can meet various needs of users. The application of mobile intelligent terminal can not only provide basic call and SMS functions, but also send and receive emails, consult information, browse documents, mobile office, even shopping, online payment and so on. Because of this, mobile intelligent terminals currently carry more sensitive user data and personal privacy, and its security issues have also received great attention. If the security of applications is not guaranteed, on the one hand, users will face serious privacy and sensitive data leakage, and even property losses. On the other hand, developers and manufacturers developing these applications are also facing copyright infringement. Key business logic leakage, and even damage to interests and other issues. Considering that Android and iOS are the two mobile intelligent operating systems with the largest number of users and the most widely used in today's market, both in

China and in other parts of the world, the combined market share of the two has exceeded 99%, not only that, The Android operating system has surpassed Microsoft's Windows operating system in 2017, becoming the most widely used operating system in the world (regardless of desktop platform or), and the current market share is about 3 times that of iOS. Therefore, our research focuses on the application security of these two mobile intelligence platforms, especially Android.

1.2 Research status at home and abroad

Many scholars and researchers have published relevant studies on the threats and challenges faced by application security -- application vulnerabilities and security problems. Although these research contents and results can solve the corresponding problems to a certain extent, there are still various shortcomings. In addition, there are still gaps in the research on some specific problems, and more complex technical difficulties need to be solved, which are elaborated as follows:

2. Security detection methods of application programs

2.1 Overview

The security detection method of application program is characterized in that it includes: running at least one target application program; Detect whether malicious behavior occurs in the target application program, and add the target application program to the first detection list if malicious behavior occurs during the running of the target application program; Detect the permission information of the target application program, if there is an unauthorized behavior, the target application program is added to the second detection list; Detect all third party SDKS of the target application for the existence of third party advertising SDKS, and if so, add the target application to the third detection list;

Determine the risk level of the target application according to the first test list, the second test list and the third test list.

2.2 Method Architecture

This method makes the application more secure by detecting malicious behavior, permission information, and all third-party SDKS accordingly. Compared with the existing technology that only detects suspected fraud and malicious programs, the security of the application can be detected more comprehensively, and the problem that the existing detection method can not detect the security of the application is not comprehensive. As shown in Figure 1, the architecture of the security detection method for the application program.

Start to run at least one target application. The home page first detects whether malicious behavior occurs in the target application. If malicious behavior occurs during the running of the target application, the target application is added to the first detection list. The behavior here refers to a combination of a series of events (events, referring to the application to execute commands such as sending text messages, making phone calls, etc.), that is, the behavior can be a series of continuous events composed of the start event and the end event. For example, the user edits and sends a short message under the operation interface of the application, and this behavior of sending a short message is a normal behavior; While the application sends short messages under the lock screen state is abnormal and belongs to malicious behavior. Among them, the malicious behavior includes secretly executing the order business or paying fees, deceiving click on the order business or paying fees, and obtaining and storing user information without authorization. The user information includes personal information (i.e., user name, user password, etc.), bank account information, payment password information or other non-public information.

When the target application is running, if the above violations occur, the target application will be added to the second detection list after the steps of adding the target application to the second detection list, if the application has the following conditions, the target application will be added to the second detection list: Detect the password strength and password retrieval verification mechanism of the target application program, if the password strength does not reach the predetermined setting or the password retrieval verification mechanism is incorrect; Detect the first user data information of the target application program is executed without the user's permission to delete or modify the instruction; The second user data information stored in plain text in the communication packet is detected, and the second user data information includes account information, password information, mobile phone number information and URL information. It is shown in Figure 3. The security of the application is further improved by the supplementary method, which detects the security of the application more comprehensively.

Next, all third party SDKS of the target application are detected for the presence of third party advertising SDKS, and if so, the target application is added to the third detection list. The specific steps of detection are as follows: obtain all third-party SDKS of the target application, decompile each third-party SDK, obtain the corresponding target apk file, determine whether the target apk file contains the malicious advertising platform code, if it does, determine the corresponding SDK for the third party advertising SDK.

Finally, according to the first detection list, the second detection list and the third detection list to determine the risk level of the target application: calculate the number of the target application in the first detection list, generate the first risk value; Calculate the number of the target applications in the second test list to generate the second risk value; Calculate the number of target applications in the third test list to generate the third risk value; Determine the risk grade according to the first risk value, the second risk value and the third risk value; If the first risk value is not zero, the target application is determined to be a high-risk application; If the first risk value is zero and the second risk value is not zero, the target application is determined to be a medium-risk application; If the first risk value and the second risk value are zero, and the third risk value is not zero, then the target application is determined to be a low-risk application; If the first risk value, the second risk value and the third risk value are all zero, then the target application is determined to be a safe application.

Summary

This article focuses on the application's security detection methods. Specific research contributions: A security detection method for applications is proposed. This method makes applications more secure by detecting malicious behavior, permission information and all third-party SDKS accordingly. Compared with the existing technology that only detects suspected fraud and malicious programs, it can detect the security of applications more comprehensively, and solve the problem that the existing detection methods can not detect the security of applications comprehensively.

References:

[1] Luying Han. Technical analysis of Java Web Application Security [J]. Information recording materials, 2021, 22 (8) : 115-116. The DOI: 10.16009 / j.carol carroll nki cn13-1295 / tq. 2021.08.052.

[2] Yang Wenbo. Several safety analysis of mobile application technology research [D]. Shanghai jiaotong university, 2020. The DOI: 10.27307 /, dc nki. Gsjtu. 2020.000266.

[3] Heng Zhao.Java Web Application Security Technology [J]. Electronic Technology and Software Engineering,2019(04):194.

[4] Wenzhu Li,Changlin Zhao. Effective application security testing [J]. Network Security and Informatization,2018(07):110-111.

[5] Chengcai Zhang. Research and application of safety risk hierarchical management and control Method in coal mine [J]. China Science and Technology Journal Database Industry A, 2023(2):4.

This paper was supported by the General Project of the Ministry of Education (22YJC630167) and the 2023 project of the Sichuan Key Laboratory of Intelligent Police (ZNJW2023KFQN006).