Research on security detection and risk rating of Android applications

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

Abstract: With the development of mobile Internet, mobile devices have gradually become the largest traffic inlet of the Internet, and Android devices with a large user base are the main force. With the continuous growth of the number and volume of Android applications, security problems are also emerging. On the one hand, due to the open source characteristics of the Android system, the decompilation difficulty of Android applications is relatively low, and many manufacturers have adopted reinforcement technology to protect the core code of applications, so the reinforcement is also constantly developing, and the form is implemented through dynamic bytecode loading, bytecode non-landing memory loading, class instruction extraction and other reinforcement technologies. Among them, the hybrid reinforcement technology combining the latter two is more common. On the other hand, security threats in Android applications seriously affect people's information security. In view of the above problems, this paper proposes an application security detection device, including: run module, used to run at least one target application; The malicious behavior detection module is used to detect whether there is malicious behavior in the target application program. If the malicious behavior occurs when the target application program is running, the target application program is added to the first detection 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

Entering a new era, the world has ushered in a new round of information technology revolution, with the Internet as the core of information and communication technologies and their applications and services undergoing qualitative changes. The informationization and networking of human society have reached an unprecedented level, and the information network has become the "central nerve" of the whole country and society. However, the trend of networking has brought two contradictions: first, the attack technology is always ahead of the defense technology; Second, the more complex and comprehensive the functions of information technologies and applications, the greater their vulnerabilities, vulnerabilities and security risks. Judging from the trend of technological development, these two contradictions will become more and more prominent, and the situation of network and information security is not optimistic. A very important measure to ensure network information security is to eliminate the known security risks in the information system.

Aiming at the above problems, this paper puts forward an application program security detection device, including: run module, used to run at least one target application program; Malicious behavior detection module is used to detect whether there is malicious behavior occurring in the target application program. If the malicious behavior occurs when the target application program is running, the target application program is added to the first detection list; Permission information detection module is used to 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. The device solves the technical problem that the security detection of the application program is not comprehensive.

1. Literature review

1.1 Research background and significance

Mobile operating systems active in today's smart market include Android, Apple and blackberry. As an open source operating system, Android is favored by major Oems. For example, Xiaomi, Meizu, HTC, Huawei and other major mobile phone manufacturers have deeply customized Android system, and launched many excellent operating systems such as Xiaomi's MIUI, Huawei's Emotion UI, Meizu's Flyme, etc., which are favored by many mobile phone users. In 2010, Android system successfully defeated Symbian system and became the largest smartphone operating system in the world, and millions of new devices equipped with Android system are activated every day. One of the main reasons for the popularity of Android phones is the ability to download a wide variety of applications in the app market, and the operating system is highly customizable. For example, users can change their wallpapers and themes, and they can also tap into their favorite third-party systems. According to data shared by NetMarketShare from April to June 2017, Android is the undisputed leading platform for mobile operating systems, with Android's market share increasing from 65.43% in April to 69.76% in June. While iOS lagged far behind, dropping sharply from 31.65% in April to 27.94% in June.

Since Google released Android version 1.0 in 2008, the Android operating system has been continuously introduced with new versions, both in terms of features and complexity. Android system has a very complete ecosystem, application developers, end users and manufacturers promote each other, common development continues to add new vitality to the Android ecosystem, and promote the Android system to continue to progress and development. Mobile smartphones generally store sensitive user information, but also can access the user's email, text messages, and public and specialized network services. As with all software, the growth in functionality and complexity comes with increased security risks.

1.2 Research status at home and abroad

Android system ranks first in mobile intelligent devices. With its rapid development, its security has attracted the attention of people from all walks of life. The first direction of its security research is the security of the Android system itself. There are many security protection mechanisms in the Linux kernel of the Android system. The second direction is the security of Android applications. The main research directions of application security are divided into two parts: static analysis and dynamic analysis. As a method in software security detection, static analysis mainly refers to the code detection of software without running the program, so as to find the possible or existing problems in the code. The dynamic analysis method is mainly to run the application program in a specific system environment, by obtaining the behavior and function call information of the application program in operation, and analyze the information to judge the security of the application program.

Dong Guowei and Wang Meilin et al. proposed an Android application vulnerability analysis framework based on feature matching, which can summarize Android applications from three different levels, and combine static analysis technology to conduct pattern analysis of applications, so as to dig out security risks in Android applications. Chen Lu and Ma Yuanyuan et al. divided Android application security problems into three types: vulnerability defects, component defects and configuration defects, and carried out static analysis of Dalvik bytecode files based on the above three types of problems. The visitor mode was used to detect the bytecode, and vulnerability detectors were made for the three security defects respectively.

Le Hongzhou and Zhang Yuqing et al studied the problem that current static blemish analysis tools can not perform effective blemish analysis on the dynamic loading and reflection mechanism of Android, and proposed a strategy of replacing reflected call statements with non-reflected call statements. And developed a tool --DyLoadDroid, which can perform priority blemish analysis on Android dynamic loading and reflection mechanism.

At the 2015 Black Hat Technology conference, Yucheng Lin of MediaTek Inc in Taiwan introduced a tool for detecting security vulnerabilities in Android applications, which is based on the AndroGuard open source project as a basic framework, and adds a vulnerability detection system on top of it. And adds static DVM, an efficient string search engine and filtering engine, and support for custom attack vectors. The framework is capable of scanning known code vulnerabilities and supports custom extensions. Belarc Security Advisor, as an Android vulnerability scanning tool, can quickly return scan results by scanning applications in the Android system. However, the main problem of this application is that the detection results for different Android versions of the system will be very different.

Shekhar et al. analyzed third-party ads in current applications and found that most AD SDKS request additional sensitive permissions to the Android system, which are highly likely to be used by attackers and cause damage to the user's property. In this paper, the AdSplit tool is developed to separate the Android application process from the advertising application process, so that they can use their own permissions separately. Batyuk and Schmidt et al. proposed an application sandbox for static analysis and dynamic analysis. The sandbox can record the information of the application's interaction with the system at a lower level for further analysis. AASandbox could be deployed in the cloud and used in Google's Android Market mobile app store to quickly spot suspicious software.

Takemori and Kubota et al. proposed an application behavior detection system based on the Android system kernel. By running an application in a sandbox environment, the behavior and function calls of the application during running are obtained, and then the system function call rule base is matched. It is used to detect whether there are security vulnerabilities or malicious behaviors in the application.

At the same time, the frequent security problems of mobile terminals have attracted the attention of major mobile device manufacturers, which have pre-installed security software on mobile phones and set up security departments to conduct security detection on Android system. To sum up, the following problems still exist in the field of application security analysis: how to efficiently discover security problems in complex protocols and design detection devices in the field of application vulnerabilities and security problems research. In this paper, the corresponding detection device is proposed for these problems. The main work of this paper is to introduce a kind of application program security detection device in view of the following problems still exist in the field of application program security analysis.

2. Application program security detection method

2.1 Overview

A security detection device for an application is characterized in that it includes: a running module for running at least one target application; The malicious behavior detection module is used to detect whether there is malicious behavior occurring in the target application program. If malicious behavior occurs when the target application program is running, the target application program is added to the first detection list; Permission information detection module is used to 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; SDK detection module, used to detect all third-party SDK of the target application whether there is a third-party advertising SDK, if there is, the target application is added to the third detection list; The risk level determination module is used to 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.

In some embodiments, the security detection device of the application also includes: acquisition module, which is used to obtain the installation package of at least one application under test; An installation module for installing the installation package to obtain the corresponding target application.

Summary

This article focuses on the application's security detection device. Specific research contribution: The application security detection device is proposed. The device 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, it can detect the security of application programs more comprehensively, and solve the problem that the existing detection methods can not detect the security of application programs comprehensively.

References:

[1] Lina Gu. Research on Power safety Guidance operating system based on Android [D]. Southeast University,2016.

[2] Yinan Yao,Shijun Zhai. Research on Vulnerability and Security Threat of Android Platform [J]. Mobile Communications,2015,39(11):34-38.

[3] Liping Ding. Security Analysis of Android Operating System [J]. Information Network Security,2012(3):28-31.

[4] Guowei Dong,Meilin Wang,Shuai Shao, et al. Feature matching based Android application vulnerability analysis framework [J] Journal of Tsinghua University (Natural Science Edition),2016(5):461-467.

[5] Lu Chen,Yuanyuan Ma,Congcong Shi, et al. Research on static Analysis of Android Application Security Defects [J]. Computer Engineering and Applications, 2018(4):117-121.

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