Design and Implementation of Mobile Phone Information Security System based on Android Platform

Jiajin Hong, Shujian Huang, Anqi Gao, Yuhuang Lin

Fuzhou University of International Studies and Trade, China

Abstract: With the rapid development of the information age, People's Daily life has been inseparable from mobile apps. However, the excessive collection of personal information by some mobile apps directly or indirectly leads to the disclosure of user information, resulting in the endless problems of user property losses. At present, there is a lack of effective means to deal with this phenomenon in the market, and it is urgent to strengthen the protection of personal information and privacy when users use mobile apps. The research purpose of this project is to summarize the global mainstream anti-phishing mechanism and related technologies, and to design a lightweight mobile platform phishing identification and detection application based on C/S architecture, so as to reduce the risk of users being threatened by phishing attacks and protect personal sensitive information and property security.

Keywords: App; Android; mobile phone information security guards

1. Introduction

With the development of mobile communication technology, it brings convenience to people's life, but also has multiple security risks. For example, the open source nature of Android system brings security problems [1]. Therefore, domestic and foreign scholars mobile manufacturers continue to innovate mobile security technology.360 launched a mobile phone security product in 2012 that mainly features anti-harassment features; Tencent launched its mobile butler in 2014, which added the ability to deep clean phones in addition to anti-harassment. Baidu launched Safeguard in 2015, mainly adding virus-killing capabilities. Jiao Dan-Dan, a foreign expert, designed an information security guard for Android system based on SQLite environment, aiming to eliminate the hidden danger of information security in the mobile phone system [2]. In this paper, based on the comprehensive security products on the market, the communication guard and process, software management functions are developed, aimed at strengthening the user's security at the same time, improve the convenience of the product.

2. Related Technologies

2.1. The Android Technology

In our system, we use Android as our Development platform and Android Development Tools as our Development environment. The Android operating system first supports Java language written application system, so the Android project development environment and Java project development environment can use the Eclipse platform [3].

2.2. Java Technology

In our system, we use Java as our development language.JAVA is a kind of object-oriented programming language launched by Sun Company, and it is cross-platform. The cross-platform nature of Java makes it very suitable in enterprise and Internet environments [4].

2.3. SQLite Database

SQLite is a very popular embedded small memory database, run often reside in memory, the memory in the operation of the memory of the proportion is very small, about the size of the runtime only need 100 k of memory, and can be combined with many languages are used together, is a relational database management system, by performing ACID four elements transaction execution, can quickly access the database [5].

3. Design of Mobile Phone Information Security Guard System

3.1. Total System Functions

Mobile information security guard is a security protection system developed based on Android system. The overall module of APP system design of mobile information security guard is shown in the following figure. Each system module function is realized through the main interface loading. As shown in Figure 1.

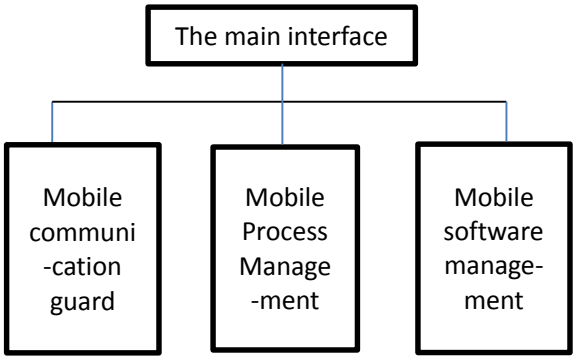

Figure 1. System general function diagram

3.2. Data table Structure Design

According to the analysis of the business process of mobile phone information security guard management system, the user login table, blacklist table, software management table, ownership surface, mobile phone version management table and interception mode table are defined. The table structure design is shown below:

(1) The user login table is mainly used to store user number, user name, user password, and whether login is allowed, etc. As shown in Table 1.

Table 1. User login table

Field names	Data type	Length	Whether is empty	Describe	Note
YId	varchar	25	NULL	user id	PK
Yname	varchar	50	NULL	user name	
Password	varchar	50	NULL	user password	
Login	bit	1	NULL	Whether login is allowed	

(2) The blacklist table is mainly used to store information such as blacklist number, mobile phone number, intercept number, intercept start time and intercept cutoff time, etc. As shown in Table 2.

Table 2 Black list table

Field names	Data type	Length	Whether is empty	Describe	Note
HId	varchar	25	NULL	Blacklist number	PK
HPhone	varchar	50	NULL	Mobile phone number	
LId	varchar	50	NULL	Intercept number	
StartTime	bit	8	NULL	Intercept start time	
OverTime	bit	8	NULL	Interception cut-off time	

(3) The attribution surface is mainly used to store the number, name and remarks of the mobile phone's attribution site.

(4) The mobile version management table is mainly used to store the information of mobile version number, version type, version characteristic code and version release time.

(5) The interception mode table is used to store information such as the interception number and the name of the interception.

3.3. The System is Designed by Functional Modules

3.3.1. Communication guard function module design

The communication guard function is mainly divided into two modules, one is the blacklist module, the other is the intercept module. Blacklist of modules need to store a blacklist, blacklist, the establishment of the need to use database to realize the corresponding mobile number is added in the database, and you need to set up a monitoring function, when receive calls or text messages, monitor function open, to identify whether the number exists in the database in the blacklist, if present, is to intercept the calls or text messages, if not, shows the call or SMS [6]. In addition, users can choose the blocking mode for each mobile phone number in the blacklist. The blocking mode can be divided into three kinds. The second is to block only text messages. Third, intercept both incoming calls and text messages. Finally, if the user does not want to store the mobile phone number in the blacklist, he can click the "Move Out" button behind the mobile phone number, and the mobile phone number will be removed from the blacklist. As shown in Figure 2.

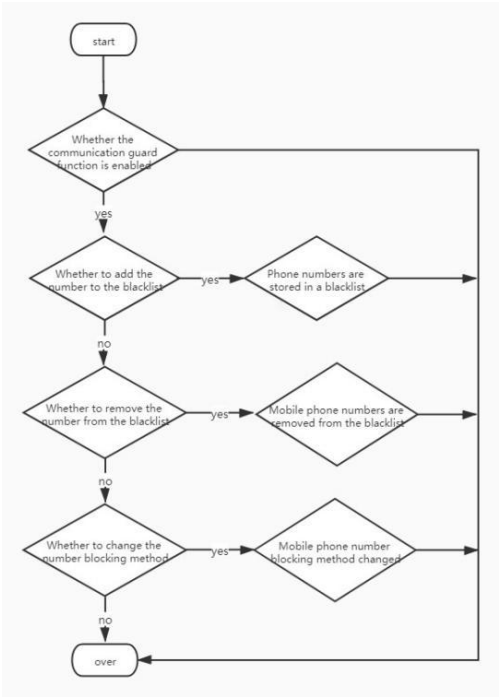

Figure 2. Communication guard module design flow chart

3.3.2. Process management function module design

The process management function is mainly used to clean up the resource space occupation after the software application. When the user closes the software, the background does not completely clear the memory occupation brought by the software, because the operation of a software often involves the assistance of other child processes [7]. Process through the management functions, the user interface in process

management function, the user can see whether the software has the rest of the child process, if there is the child, you can choose whether to clean up the child, choose to clean up after the child process to delete pair will process to the release of the software is currently held by resource space, save mobile phone memory space, to avoid resource waste of space. As shown in Figure 3.

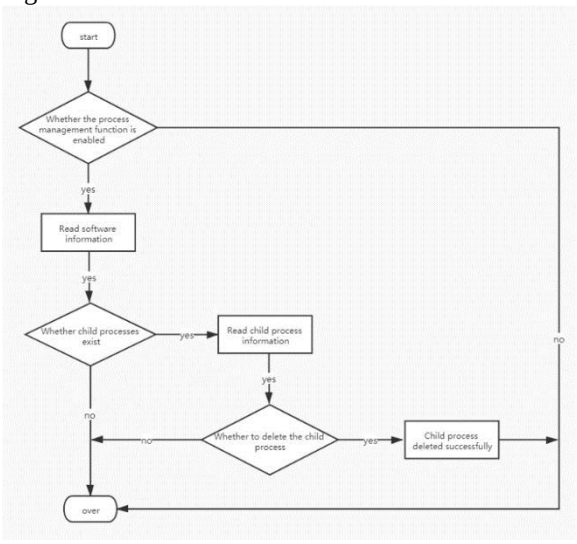

Figure 3. Process management module design flow chart

3.3.3. Software management function module design

The software management function is mainly used to manage the application on the phone, mainly used to uninstall the application on the phone. In the feature, users will be mobile phones are downloadable application listed in the page, and set a behind the uninstall button in each application, when users don't want to use the software, want to uninstall the software, can enter the software management function interface uninstall button, click on the corresponding software to complete the software uninstall. As shown in Figure 4.

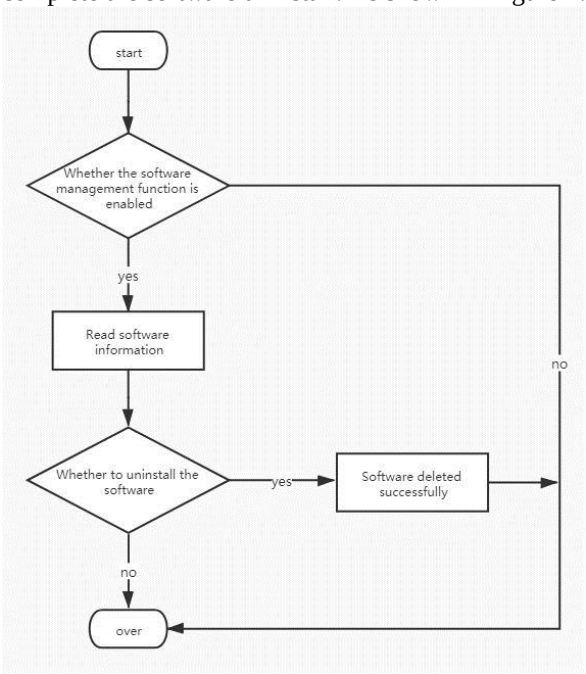

Figure 4. Software management module design flow chart

4. Function Realization and Test of Mobile Phone Information Security Guard System

4.1. System Environment Development and Construction

For the above functional modules, our system environment is developed and built as follows:

Developed operating system: Microsoft Windows 7 Ultimate

Development platform: Android

Development environment: Android Development Tools

Development language: Java

Database: SQLite

4.2. System Function Module Realization

4.2.1. Main interface function module realization

Our mobile phone information security guard system page is divided into the upper and lower parts. The upper part is a mobile phone security performance scan. After the user clicks the scan now, the system will display the current mobile phone security performance score according to the current mobile phone security situation and memory occupation situation [8]; the lower part is the four functions of our system, among which the three core functions are communication guard function, process management function and software management function respectively, and the last one is more function, in which users can give us some feedback and valuable suggestions. As shown in Figure 5.

Figure 5. Main interface function interface effect

4.2.2. Communication guard function module realization

When into our guard function of communication interface, the user will see a add button, top right is when users click the add button, a dialog will appear, can input you want to add to the list of mobile phone number, and can put the don't want to stay in the blacklist moves from cell phone number, or changes to the mobile phone number intercept method.

5. Conclusion

The security of Android system is not only an important topic for scholars, but also a hot issue for common people. The mobile phone security guard developed based on Android system in this paper adopts the embedded database SQLite, takes Java as the Development language, and Android Development Tools as the Development and construction environment. Its system functions have been repeatedly debugger and tested to ensure that it can meet the system needs of Android users. However, the system development and design still have shortcomings, such as not yet to achieve the packet intercept, automatic system fault repair and other functions. In the future, the author will continue to improve the functions of the mobile phone information security guard, and strive to provide a more practical and sound Android protection system for the Android market.

Acknowledgment

This work was supported by the [2019 National Undergraduate Innovation and Entrepreneurship Training Program] under Grant [number 201913762010].

Reference

[1] Kuang, F.F. Research and Design of Mobile Phone Security Guard Based on Android Platform. *Computer Knowledge and Technology: Academic Exchange*, **2015**.

[2] Jiao, D.D. The mobile security guards based on Android. *heilongjiang science*, **2016**.

[3] Yan, R.F. Design and Implementation of Mobile Phone Security Guard System Based on Android Platform. *Jiangxi University of Finance and Economics*, **2016**: 10-11.

[4] Wang, F.F. Research on Detection and Protection Technology of Mobile Malicious Code Based on Android Platform. *Beijing Jiaotong University*, **2012**.

[5] Wang, M. Research and Application of Software Development Method Based on Android Platform. *China New Communications*, **2015**, 18.

[6] Tao, M.L. Research on Causes and Protective Countermeasures of Personal Information Leakage of Mobile Intelligent Terminal Users. *Anhui University of Finance and Economics*, **2017**.

[7] Li, T.; Qin, H.C. Research on Mobile Phone Security Protection System Based on Android. *Modern Computer*, **2011**.

[8] Alabi, A.A.; Ogundoyin, I.K. A Simple Face-based Mobile Security System Design for Android Phone Protection. *International Journal of Computer Applications*, **2017**, 161(11): 17-23.