Development of Mobile Security Guard Based on Android System

Li Fuling Li Yong

North China Technical College, Beijing 101601, China

huner2011@foxmail.com

Keywords: Mobile security guard, Android, Prevention of burglary, Anti virus

Abstract. Mobile security guard has the functions of prevention of burglary, software management, process management, cache cleanup, mobile anti virus and intercepting the call and message of blacklisted numbers. The program uses Eclipse + ADT plug-in for development. And implementing the functions of inquiring number attribution and commonly used numbers, and mobile anti virus uses SQL technique to inquire the database. For mobile prevention of burglary, broadcast technology is used to monitor and intercept the message to ensure that common messages and command messages are achieved separately. For intercepting the call and message of blacklisted numbers, reflex mechanism of Java, AIDL, content observer and content provider of Android is used to implement.

Introduction

With the development of information-based society, Android intelligent products have become the mobile terminal products for more and more people. In China, Android mobile users increase rapidly. According to the statistic data of Information Ministry, there are nearly 740 millions of mobile users in China. With the increasing expansion of mobile group and with the progress and development of IT industry, various mobile application layers emerge, which makes some potential safety hazard. And it may have the problems that personal information leaks, bank account loses and cellphones are stolen, which not only brings inconvenience for users, but also even leads to disputes. In order to meet the security requirement of mobile users, it is very important to develop a mobile security software meeting the user requirement.

There are many software about mobile security, but there are many problems such as ugly interface, implantation of advertisements and irregular notification push, which brings bad experience for users. So developing a healthy mobile security software not only can make the users have satisfying application experience, but also is easy for users to manage mobile phones.

Requirement Analysis

The system has the following functions. Mobile prevention of burglary function. It needs to set the password when the function of mobile prevention of burglary starts.

Communication guard function. Communication guard is used to intercept crank calls and messages. It adds the intercepted telephone numbers to the blacklist.

Software management function. The software of cellphones includes the software which is installed by the users and the software of the system. The software which is installed by the users can be unloaded, started and shared. And the software of the system needs root authority when it is unloaded.

Process management function. According to user requirements, some unnecessary software can be ended selectively. For example, after the users installing the rogue software, the software can steal flow at the backstage, which makes great puzzle for the users.

Traffic statistics function. Traffic statistics means to compute online traffic of users, and prompts the users that how many traffic is taken by the applications of mobile phones, and prompts the surplus flow for the users, which makes unnecessary loss for the users.

Mobile anti virus function. The function protects the user information to prevent from the leakage of user information.

Cache cleanup function. After operating for some time, the software of mobile phones can generate many useless files such as browser. It can cache some useless files to SD Card of the mobile phones of users or internal storage of mobile phones. Long-time browse can accumulate many useless files, and the function implements the cleanup of useless files.

Advanced tool function. Advanced tools should have the inquiry of telephone number attribution and commonly used numbers, message backup and application lock.

Setting center function. The configured content includes the setting of automatic update, display of telephone number attribution, attribution prompt box style, attribution prompt box display place, blacklist interception and application lock.

System Design

Mobile prevention of burglary function. It needs to set the password when the function of mobile prevention of burglary starts, the reason for which is that there are some commands in the cellphone. If the cellphone is lost or is stolen, the thief can know the commands. And it has no significance for mobile security software. So the objective of setting password is to make the cellphone have the ability of counter-reconnaissance. When we normally enter mobile prevention of burglary interface, it prompts to set mobile prevention of burglary function. And the content includes SIM card modification alert, GPS trace, teledata destroy, long-distance lock screen and binding SIM card. The command of GPS trace is #*location*#. The command of playing alert music is #*alarm*#. The command of deleting data remotely is #*wipedata*#. And the command of locking screen remotely is #*lockscreen*#.

Communication guard function. Communication guard is used to intercept crank calls and messages. It adds the intercepted telephone numbers to the blacklist, which plays the role of intercepting calls and messages.

Software management function. The software of cellphones includes the software which is installed by the users and the software of the system. The software which is installed by the users can be unloaded, started and shared. And the software of the system needs root authority when it is unloaded. It can share, manage and protect software and programs of mobile phones. Sharing software is implemented by using messages to send the loading address of the software to mobile phones of friends.

Process management function. According to user requirements, some unnecessary software can be ended selectively. For example, after the users installing the rogue software, the software can steal flow at the backstage, which makes great puzzle for the users. And unnecessary software can be ended selectively to make the mobile phone operated under safe environment. In order to make users have better experience, widget plug-in is used by the users to clean up the useless progress at the backstage, which protects the safe state of mobile phones.

Traffic statistics function. Traffic statistics means to compute online traffic of users, and prompts the users that how many traffic is taken by the applications of mobile phones, and prompts the surplus flow for the users, which makes unnecessary loss for the users.

Mobile anti virus function. It means to scan all software of mobile phones of the users to get some marking information. If the marking information matches with the information in virus base, the application is judged to be a virus. And the users are prompted to unload the software. It is superior to directly unload software with marking information of virus from the mobile phones of users, which not only protects user information, but also prevents from the leakage of user information.

Cache cleanup function. After operating for some time, the software of mobile phones can generate many useless files such as browser. It can cache some useless files to SDCard of the mobile phones of users or internal storage of mobile phones. Long-time browse can accumulate many useless files, which makes the mobile phones of users slow. And it is unfriendly for experience of users.

Advanced tool function. Advanced tools should have the inquiry of telephone number attribution and commonly used numbers, message backup and application lock. The inquiry of telephone

number attribution has the effect of vibration, which provides better user experience. The inquiry of commonly used numbers are very important. When the mobile phones are in the environment without network, and some commonly used numbers need to be inquired, the function provides convenience for users. Message backup means to back up some important messages to the local, which avoids the situation that the original important messages can't be found out after deleting messages. Program lock is to protect applications of users.

Setting center function. The configured content includes the setting of automatic update, display of telephone number attribution, attribution prompt box style, attribution prompt box display place, blacklist interception and application lock.

Implementation of Mobile Communication Guard

Blacklist management. (1) Creating blacklist database and data list blacknumber(_id：key, number: blacklist number, mode: interception mode (telephone interception, message interception, and whole interception). (2) Creating classification BlackNumberDao, in which the addition, deletion, modification and inquiry of blacklist database is implemented.

Intercepting message. (1) In order to support manually starting and closing message interception, the broadcast receiver（InnerSmsReceiver）is created in service（CallSmsSafeService）and is registered in function list file. (2) The function of starting and closing message interception service is added to setting

Intercepting calls.

Principle of intercepting call. When there are calls, the call ends immediately and the calling record is cleaned. If the performance of mobile phones is good, there is no method to see the process, which achieves the effect of interception.

(2) Monitoring the present calling state.

Monitoring the codes of incoming call,

tm = (Telephony Manager) get System Service(TELEPHONY_SERVICE).

tm. listen(listener, Phone State Listener. LISTEN_CALL_STATE).

Using API hidden in reflex call system to end call

The early version end Call() of APT to end call can't be used now. But the function of ending call exists.

Reading get System Service() source node. We can find that the service of get System Service() hides the relating API, and only provides the common methods. And Java reflex mechanism needs to be used to get the original Telephony Manager.

Conclusions

Under the condition that the safety of mobile phones attracts more and more attention, the system designs and implements a mobile security guard software. Compared with the similar software, the software has the function of mobile positioning, locking mobile phone, automatic prevention of burglary and friendly interface. The implementation of the system provides reference for applying and developing mobile based on Android.

References

[1] Lin Cheng, Android 2.3 application and development practice, Machinery Press, 2011:17-321.

[2] Han Chao, Android classical applications development, Human Resource Press, 2011:5-18.

[3] Liu Weiguo, Chao Yuyu, Research and implementation of timely communication between Android and J2ME platform, Information Science and Engineering College, 2008 (12), 118-120.

[4] Liu Ping, Data exchange of Android mobile phone accessing to server, Xi'an Fiance College, Network and Modern Education Technology Center, 2010-09:96-102.

[5] Zhao Liang, Zhang Wei, Interface design and research based on Android technique, Xuzhou: Xuzhou Architectural Vocational College, 2001.

[6] Chen Jing, Chen Pinghua, Li Wenliang, Analysis of Android kernel, Guangdong Industry University, Computer College, Practice and Experience, 2009:112-115.