Research of Cloud Security Communication Firewall Based on Android Platform

Miao Cai, Qinsheng Hou, Fangfang Jing, Qiao Ding
School of Computer Science and Technology
China University of Mining and Technology
Xuzhou China
miaocai@cumt.edu.cn

***Abstract*—To solve communications security problems of smartphones, this paper analyzes today's firewall models' lopsided and mechanized characteristic and points out their defects and limitations. Then this paper proposes a new communications firewall model based on the Android platform innovatively with combination of today's hot cloud technology. By using a C/S architecture, black-grey list mechanism and cloud push and collecting system, this firewall can filter harassing phone calls and spam messages effectively and rapidly, as well as collect, process, share information dynamically. This system fully relieves the workload of the client and embodies the future firewall's development trend.**

Keywords- Android; Cloud technology; Firewall

I. INTRODUCTION

Android mobile phone operating system was developed by Google on November 2007, which is based on Linux operating system. In recent years, Android-based smart phones have developed so quickly that they have occupied a major share of the market. However, there are more and more phone calls and messages with the nature of the fraud and harassment appearing at the same time, which are used for some improper economic benefits.

This paper mainly analyzes the smartphone's communication security status and measures at present, and points out the defects of the firewall model, so it's very helpful to improve. At last, we use some advanced technologies, such as the smartphone, cloud technology and 3G WLAN, to build a new-style cloud security communication firewall based on Android platform.

II. THE BACKGROUND OF RESEARCH

A. The smartphone's communication security status at present

Mobile communication has been developing very quickly in recent years. The Ministry of Information and Industry's data shows that the quantity of mobile phone users was more than 805 million in China, and 150 million among them were smartphone user in 2010. The time of mobile call was more than 3177 billion minutes from January to November in 2010. In the first quarter of 2012, a firewall product belongs to 360 company had intercepted almost 4 billion spam messages for 100 million users [1]. The research by Chinese Academy of Science in 2010 named "Smartphone Users' Perception and Coping Behavior of Mobile Security Threat" shows that 68.6% mobile phone users were faced with mobile security threat. Those harassing phone calls and spam SMS not only cause serious waste of communication resources, but also violate the interests of users and disturb the normal social order. So the communication security problem for smartphone must be solved as quickly as possible.

B. The research of firewall model at present

Existing communication firewall system models can be divided into two types depending on their location. One is the firewall models in the user terminal, the other one is the monitoring equipment and the dedicated website controlled by operators [2].

The former one is mainly aiming at single-user's defense on telephone and SMS. In one sense, some pieces of software like these are one-sidedness. These pieces of software put most attention on single-user's security and ignore the link between the users, they are independent of each other, a user means a small database, so they can't share the interception information, which increase the successful possibility of harassment and deception in connection with multi-user.

The later one can handle a certain number of harassing phone calls and spam messages. But it has a higher missing rate due to its mechanized operations and ignores some users' personalized filtration requirements. What's more, it doesn't exert users' potential effect on filtering the harassing phone calls and spam messages. Although the online website platform curb the proliferation of harassing phone calls and spam messages on some extent, but it's too late for users to inquire information after great loss.

In a word, both these two types of firewall separate the relationship between them. Therefore, a communication firewall that has functions of shared and inception of both harassing phone calls and spam messages has become the focus of people's attention.

III. THE DESIGN OUTLINE OF THE FIREWALL SOFTWARE SYSTEM

Cloud security is an important branch of cloud computing, which has been widely used in the field of anti-virus. It achieves the abnormality detection of the network software behavior through the reticular large client, then gets the latest information for Trojans and malicious programs in the Internet and pushes the information to the server to analyze and handle automatically, finally server

Published by Atlantis Press, Paris, France.

distributes the solution of viruses and Trojans to each client. In brief, these clients and servers have built a large "cloud" together [3].

Fig.1 shows the system framework of cloud security communication firewall based on Android platform. In essence, the system regards spam messages and harassing calls as Trojan and computer virus and uses the Client/Server structure, which can make full use of the advantages of the hardware environment and assign tasks to Client and Server reasonable. The server side collects, processes and shares the information while client sides receive, update information and intercept locally. In this way, we can allocate the heavy task of process and analysis to the server side which has a strong processing ability while the client sides only need to receive and update information, do interception and filtration work based on the updating data. So, we can build an efficient and reliable sharing intercepting firewall, which has a less spending of work.

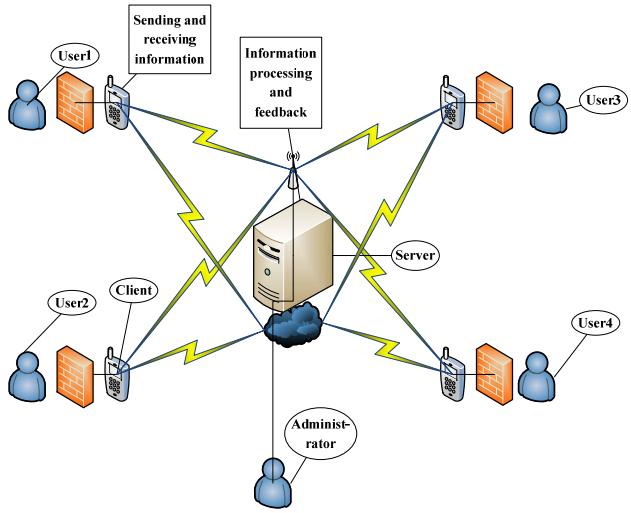

Figure 1. Firewall System Framework

The server of Server layer does the dynamic monitoring for the whole firewall system in the clouds. It contains information sending and receiving functions, and data storage, processing functions. It also should be controlled by the administrator. Here is the server's specific workflow, when some client sides send their newly acquired information, the server will sample and collect all information. After collecting, the server filters the information judging by algorithms and the remaining information will be stored in the server database. Then, after a certain time interval, the server will notify the clients update their information, the clients take the initiative and connect to the server and update their information.

The client layer is the software installed on the users' smartphones, with functions of sending and receiving information, data storage, intercepting calls and SMS. Here is the client's specific workflow. Clients will send the information stored locally to the server. When the server shares the information of database to every client after a certain time interval, the clients will receive the information. After receiving, clients will update their own database according to the recently sharing information. The intercepting module of client sides will do the calls and SMS interception work based on the database after updating. In this way, we can realize that share information among users in the whole firewall system.

In summary, here are the advantages of the cloud security communication firewall based on Android platform.

- It's based on Android platform. The system can run on a variety of Android devices, has lower system operating costs and can popularize.
- This firewall system software uses a modular design concept, the system has better logic, taking fully account of transplantation, maintenance and expansion later.
- The system uses Client/Server structure and reduces the pressure of the client fully, reflecting the development trend of the future firewall.

The system combines with cloud technology, abandon the passive defense of the traditional firewall and achieve the dynamic, collaborative, proactive defense.

IV. MODULE DESIGN OF FIREWALL SOFTWARE SYSTEM

A. Design of client module

1) User interface system

The user interface provide the platform of human-computer interaction, mainly are database operation interface and prompt interface, including database CRUD, query operations, as well as prompt information of supplementary blacklist data sent by the server system. We can access database information easily and timely through the user interface. All data are stored in a local SQLite database of Android system.

2) Call filtration system

The call filtration system in clients is mainly responsible for the interception of offensive or harassing calls and uploading information regularly which stored in local blacklist database of the clients, these data are provided for processing and analysis by the cloud server. Fig.2 shows the process of call filtration system. The blacklist information in clients can be stored in the Android SQLite database. When a new call comes, first, this number will be identified by the software based on the information in the blacklist database. If the phone number does not belong to the numbers in the blacklist, the normal answer, or interception of call. When server's database updates, it will inform the client base and they will take the initiative and connect to the server to receive new data, while storage of records in client sides sending to the cloud server, the server collects and updates its database dynamically, and complete a process of cloud data push and collect.

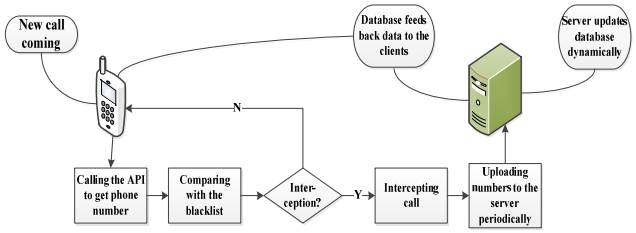

Figure 2. Process of Call Filtration

The telephone services are provided by the Phone module in Android system, the operation mechanism of the entire Phone module is realized through the registration and notification of messages, shown in Fig.3. When a call is coming, it will enter an Activity managed by the class IncallScreen.java. The upper class use Handler and Message mechanism to monitor the underlying message. Class IncallScreen will register a handler object with CallManager to manage. CallManager is a intermediary of entire message link, so CallManager will register both content at the same time, one is the Handler and Message owned by IncallScreen mentioned previous, another is the Handler and Message registered with the PhoneBase under CallManage. Finally PhoneBase receives the message sent by the underlying RIL according to the mode of phone network(GSMPhone or CDMAPhone), RIL inform the PhoneBase [4] of transformational modem message.

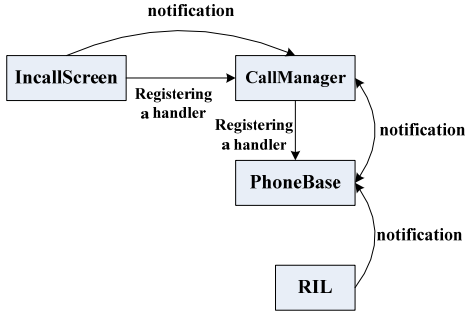

Figure 3. Process of a New-coming-call System Message Transmission

Android system has a call management API: TelephonyManager, this API can monitor call states. In the ringing stage TelephonyManager can get phone numbers. If the caller's number is in the blacklist, you can use call the system call manager to hang up automatically. Android system provided this API in earlier version. Google has hidden the API after Android 1.1, and so only can find this class by the Java reflection mechanism.

3) SMS filtration system

Fig.4 shows a process of SMS filtration system. SMS filtration system requires to provide two types of functions. First, intercepting messages based on the local SMS blacklist records and exchanging and updating data with the cloud server regularly, similar to call filtration system, second, analyzing and processing the SMS timely and dynamically according to the SMS text content. It means that clients upload encrypted SMS text to the server by mobile Internet for processing by the server. There is a SMS text log database in server SMS filtration system in cloud and its role is as a buffer prevented from network congestion or deadlock of SMS filtration system, in case clients fail to receive information result timely from the server. The buffer will return the SMS to the clients.

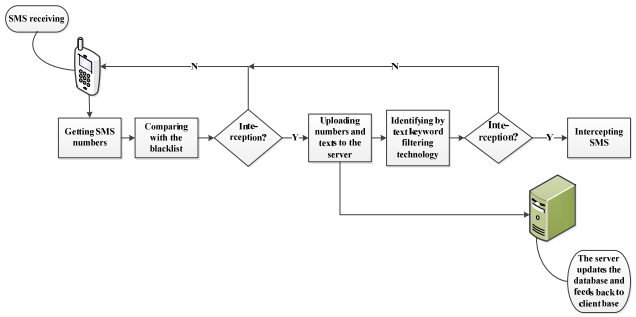

Figure 4. Process of SMS Filtering

SMS broadcast transmits orderly in the Android system, the framework layer will send the broadcast "android.provider.Telephony.SMS_RECEIVED". When a message comes, PrivilegedSmsReceiver will receive the broadcast, call onReceiveWithPrivilege() method of the parent class SmsReceiver, this method start SmsReceiverService services. If you do not intercept, SmsReceiverService will insert this message into the database in the form of ContentValues. Based on this principle, we can create a broadcast receiver (BroadcasterReceiver) to subscribe to the SMS broadcast sent by system and adjust the priority of yours higher than the system's broadcast receiver. So this can get SMS information before the system and interrupt the transmission of the broadcast. SMS information contains the number of the SMS sender.

4) Data storage and transmission system

Data storage system is designed for storing local blacklist database, can be divided into the local phone number blacklist and local SMS number blacklist database, these data are stored in a SQLite database of Android, managed by class SQLiteDataBase [5].

Data transmission system is designed for communication transmission between client base and the server, mainly supporting for push and collect service of cloud server [6]. Users can receive updated information by using their own smartphone as a terminal. Data transmission module in the client needs to start a thread to receive remote data.

B. Design of Server Module

The server is consist of the cloud information push and collecting system, the number analysis system, the SMS text analysis and filtration systems, the database systems, the self-learning modules and other information database. Server make full use of the "cloud security", set up a dynamic database for groups of users and use algorithms

along with user's feedback data to update content of the database regularly. The most essential characteristic of cloud security communication firewall based on the Android platform is its dynamic and intelligence, depends concentrated collecting and sharing by taking full advantage of cloud, thereby realizing active security services.

1) cloud information push and collecting system

The cloud information pushing and collecting system [7] [8] realizes the function of data between client and serve. Comparing to traditional pulling with the problem of a large amount of consumption of power and flux in Android terminal, the cloud security communication firewall based on the Android platform uses pushing to replace it. When server in the cloud exists update, then sends a notification message to client port, the client will connect to the server initiatively to synchronize the latest data in the cloud. The contents of the information pushed is sharing data on server, reflecting the sharing characteristics of the Android cloud security communications firewall. Fig.5 shows the process of pushing system, specific implementation steps are as follows:

a) The server port sends message to each client after a period of time with existence of update. The server port will wake up the threads from the thread pool to push this notification to each individual client.

b) Those clients which have received response messages start a thread initiatively to connect to the server, and establish a simplex push channel.

c) Connection is established and clients synchronize the latest shared data information in the server.

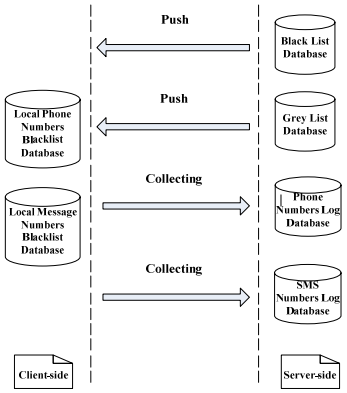

Figure 5. Cloud Information Push and Collecting System

The cloud information collecting is aiming at blacklist database stored in the client base, including local phone number blacklist and local SMS number blacklist database. Information collected is stored in the server-side's phone number log database and SMS number log database, number analysis system analyzes, identifies and digs these records, providing a reliable data basis for black-grey mechanism.

2) Database System

Fig.6 shows the database system. It includes black-grey list database, SMS text filtration system database, the number log database and SMS text log database. Black-gray list database stores number records which have been confirmed with aggressive or suspected aggressive, while server in the cloud will collect blacklist records stored in the client base, number records updates according to certain mechanisms and black-grey lists records exchange mutually. SMS text filtration system database includes the sub-word lexicon, disable thesaurus, thesaurus, and serviced for SMS filtration algorithm [9]. The number log database stores number records to be analyzed, including phone numbers and SMS numbers. SMS text database stores uploaded encrypted SMS text, it is also used as a buffer at the same time due to the case of time difference between SMS text filtration system processing and SMS receiving, the real-time SMS text filtration system generating congestion or dead lock during the operation, faulty transmission and data loss occur in the transmission process of mobile communication network. The buffer guarantees the timely receipt of the SMS and avoiding information loss phenomenon.

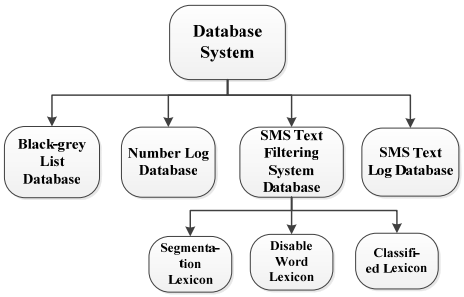

Figure 6. Database System

3) Self-learning modules

Self-learning module is a manifestation of the intelligent server system which can be divided into black-gray list mechanism and SMS text filtration system.

Black-gray list mechanism are supported by black and gray list database and number analysis system, which embody the intelligence of cloud security communication firewall based on the Android platform. Blacklist stores calls and SMS numbers records with the nature of the fraud, harassment which are determined, while the gray list stores the harassing calls and SMS numbers records which are suspected fraudulent. These records, in accordance with a scoring system set by the system, stored in black list and gray list can transform into each other. The data in black and gray list flow dynamically back and forth. In general, there are two key factors that affect the definition of harassment Number record. One is the time interval and another is probability of this number in the acquisition records. Assume that the server collects client data periodically in the time interval of Δt, which is changeable. Set the number i record C_i 's probability as a variable

$P(C_i)$. Set the number i record's liveness in the time interval Δt as a variable A_i. A_i is formulated as follows:

$$A_i = \frac{P(C_i)}{\Delta t} \qquad (1)$$

At the same time liveness also identifies the number suspicious degree, which is the eigenvalue of the number in this period of time. Liveness A_i of the data is stored in the black-list database achieves the conversion automatically based on the threshold χ and update. Specifically, black list and grey list both has a threshold χ as a standard, when the liveness above or below the threshold, they transform in the direction of being screened, grey list, black list, or the opposite direction, thereby completing an automated intelligent screening process.

Intelligentization of SMS text filtration system is mainly reflected at the self-learning and self-renewal characteristics of Bayesian algorithm itself [10], shown in Fig.7. When a large number of new SMS arrives, we use Bayesian filters analysis eigenvalue constantly appearing in the SMS to calculate the probability of spam messages. Meanwhile, the probabilities of the eigenvalues in SMS Bayesian filter will be updated too, which makes Bayesian algorithm system more accurate. We repeat the above operation thereafter whenever new messages are received, with the increase of processing among numbers of SMS, we can update the eigenvalue probability in order to achieve the goal of intelligentization. In addition, the algorithm is based on probability and statistics, while the premise is depending on the independent of each individual eigenvalues. When the training data meet this assumption of independence that classification would be more accurate, otherwise, would be less. Therefore only reduce the dependent of attribute independence in order to improve the accuracy of the Bayesian filter.

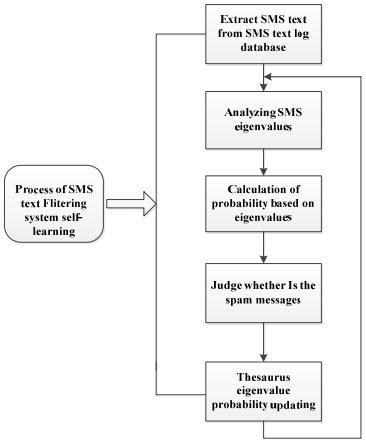

Figure 7. Process of SMS Text System Self-learning

V. CONCLUSION

Communications firewall system based on the Android platform is in the framework of cloud security technology, uses technology such as cloud security, black-gray list, data storage and processing and text filtration algorithm to integrate a large number smartphones terminal equipped with cloud security client software into the smart server and to share information and collaborate with each other, realizes the goal that filtering harassing phone calls and spam messages fast, effectively and safely. At the same time, system exists problems like numbers and SMS text leak in the wireless transmission process, technology about storage security of large amount of data and server concurrent processing need to improve and solve in the future work.

ACKNOWLEDGMENT

The authors are grateful to the support of the Students' Practice and Innovation Program Project of China University of Mining and Technology (No. 201210290073). Furthermore, the anonymous referees are much appreciated for their helpful comments and suggestions.

REFERENCES

[1] Zhou Zong-jun, Su Hong-qi, "Designer of Android Smartphone Intrusion Detection System," Science & Technology Information, no.18, Aug. 2012, pp. 30-32.

[2] Li Zhe-fu, "Research of Spam Call System Based on Cloud Security," Microcomputer Information, vol.27, May. 2011, pp.617-169.

[3] Xu Hai-lang, Yuan Jia-bin, "Research on Cloud Monitoring Oriented to Mobile Terminal," Computer Science, vol.39, Aug. 2012, pp.55-58.

[4] Peng Hai-wen, "Applied Research on Android of Call Block and Call Insert," Computer Knowledge and Technology, vol.7, Mar. 2011, pp.1589-1590.

[5] Lin Cheng, Android 2.X Development and Application, Tsinghua University Press, Beijng, 2011.

[6] Jarle Hansen, Tor-Morten Gronli, Gheorghita Ghinea, "Cloud to Device Push Messaging on Android: a Case Study," Proc. IEEE Symp. Advanced Information Networking and Applications in Scheduling, IEEE Press, May. 2012, pp. 1298-1303, doi: 10.1109/WAINA.2012.96.

[7] Zhou Hai, Li Qiang, Que Hui-li, Research and Implementation of Cloud Pushing Based on Android C2DM Service, Computer Technology and Development, vol.22, Jul. 2012, pp.29-32.

[8] Caner Kilinc, Todd Booth, Karl Andersson, "WallDroid: Cloud Assisted Virtualized Application Specific Firewalls for the Android OS," Proc. IEEE Symp. Trust, Security and Privacy in Computing and Communications, in Scheduling, IEEE Press, Feb. 2012, pp.887-883, doi:10.1109/TrustCom.2012.298.

[9] Zhen Hua-jun, "Analysis and Research of Filtering Method for Spam Short Message," Computer Era, vol.5, May. 2010, pp.15-16.

[10] Ding Yue-wei, Pan Shou, Using Bayesian method to filter garbage message form package message contents in an analyzing system, University of Shanghai for Science and Technology, vol.30, Jan. 2008, pp.75-78.