http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (7): 1049-1053, 2009
ISSN 1812-5638

The Design of Firewall in Mobile Phone Based on Cross-Layer Collaboration

Hao Yu, Ming-Xiang He and Hai-Chun Sun
College of Information Science and Engineering, Shandong University of Science and Technology,
Qingdao 266510, China

Abstract: Being different from the traditional packet filter firewall, this study gives a design model of mobile phone firewall which is based on the cross-layer collaboration. Firstly, author designed the functional model and the overall framework. Secondly, author devised the key process and algorithm. At last, the author validated the advantage of model through simulation experiments. Through, the simulation experiments, the model is proved to be effective to reduce the firewall's consumption of resources and improve the efficiency and quality of firewall in mobile phone.

Key words: Cross-layer collaboration, firewall, mobile phone security

INTRODUCTION

With the development of wireless communications, computer and 3G technology, the sorts of mobile phone services are becoming more and more. Phones have become a man-machine interface that is as important as PC. But the businesses of plentiful mobile phone are easily imposed by virus. Cell phone is becoming a new target which is under the threat of virus and hackers. What's worse, people's safety awareness about mobile phones is still quite weak. They ignore these harms such as personal privacy posed by disclosure, important information stolen and top secret information used, which are caused by the hackers and virus invasion. Users suffer a serious loss (Zhuang, 2007).

At present, the secure researches of mobile phones are focused on the firewall, such as SMS firewall, Call filter firewall. Their main functions are used to put an end to harassment of illicit calls and messages. The virus firewall research of mobile phone has gradually become a hot issue. Instead of the simple function of filter calls and messages, it intercepts illegal data from lower layer of the phone. However, the virus firewall consumes the limited resources of mobile phones too much. It has become one of the most important issues about security of mobile phone that how to protect data to be confident, integrity, available of applications and prevent their illegal use, tampering and copy on mobile terminals and decrease the consumption of limited resources of mobile phone.

THE DEFINITION AND PRINCIPLE OF PACKET FILTER FIREWALL

First-generation firewall checks each packet in the network. Whether packages are allowed to pass or not depends on the set of rules established. This is known as packet filter firewall. Packet filter firewall generally works in routers to filter the content which user wants to filtrate such as the IP address. Because packet filter firewall works in the network layer, it has good transmission performance, scalability and strong. However packet filtering firewall has some defects. Because packets are not checked in the application layer, the packet filter firewall does not understand the contents of communications and may be easily broken by hackers (Wang, 2009).

A list of rules that decide to accept or prohibit packet is the core of Packet filter firewall. The rules are clearly defined what kind of package will be allowed or prohibit through the interface of network. Those data which are transmitted between trusted network and not trusted networks are controlled by packet filter firewall. The firewall independently filters packets which pass the interface, but it can be completely different rules between packets of input and output. The list of filter rules can be called a rule chain. Each packet is matched with the rules one by one until a rule is matched or all rules have been exhausted by Wang (2003, 2009).

Packet filter firewall works in the IP network layer. Because it only checks source address, destination address and corresponding port of the IP packets, it is efficient and able to handle more concurrent connections, but shortcoming is that application-layer is easily attacked. In order to make full use of the advantages of packet filter firewall and overcome the shortcomings, the author designs the firewall of mobile phone based on collaboration in cross-layer (the design of firewall in mobile phone based on cross-layer collaboration referred to FMCC).

Corresponding Author: Hao Yu, College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao 266510, China

THE DESIGN OF THE FIREWALL OF MOBILE PHONE BASED ON COLLABORATION IN CROSS-LAYER

The analysis of collaboration in cross-layer: Traditional packet filter firewall works in the network layer. Because resources of mobile phones are very limited such as CPU and memory, mobile phone will consume a large amount of resources if the traditional packet filter firewall is migrated to mobile phones. Thus, it will seriously debase the efficiency of mobile phones and bring us a lot of inconvenience. Through simulation experiments, we know that the firewall consumes much less resources while it is working in the lower layer of mobile phone. If the packet filter firewall is installed in the lowest level of work, the phone will be easily attacked in the application layer. In order to solve this problem, FMCC is designed into four parts: the physical layer firewall, IP level firewalls, application layer gateways and suspicious data in decision-making module.

The data packages are matched with the rules of filter firewall in the IP layer and physical layer. The XML Gateway of Application Layer dynamically detects data packet. If data packet is detected to be illegal, it will modify the rule sets of packet filter firewall of IP layer or physical layer, so that the firewall will intercept the illegal data flow in time from the bottom of the mobile phone.

This can not only reduce consumption of mobile phone resources mostly, but also can effectively enhance the comprehensive security of mobile phone.

General design (General description): While, designing the firewall of mobile phones, we fully take the combination of practicability, validity and security into account. We try our best to enhance its security on the premise of normal work of mobile phone. We will dentally introduce the architectural design of FMCC.

The FMCC mainly includes two functional modules: management module and monitoring module. System management module includes: log management, temporary tables, system configuration and part of the contents of the four rule sets. Real-time monitoring of modules include: log management, data analysis reports, rules updates, illegal data to confirm the contents of four parts (Jiang, 2007). The function of specific design as shown in Fig. 1.

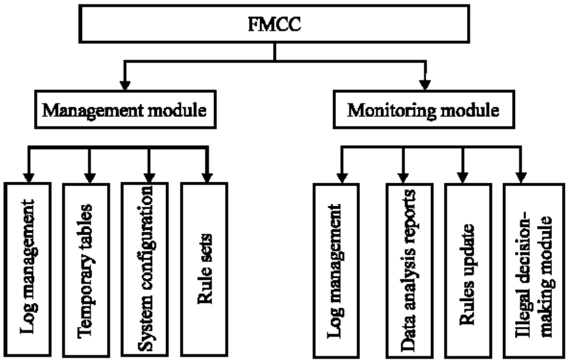

Fig. 1: The composition modules of FMCC

The firewall of mobile phone contains four parts: physical layer packet filter firewall, IP layer packet filter firewall, XML gateway and suspicious data decision-making module. The physical layer packers filtrating firewall hold up illegal data packets which can be detected in physical layer. By holding up some illegal data in physical layer, the efficiency of firewall is largely improved. At the same time, the source of mobile phone is saved. The IP layer packet filter firewall analyzes data packets which have been detected by physical layer packet filter firewall. The function of this firewall is improving the safety of mobile phone. XML analyze data packets belong to application layer. When some suspicious packets are detected, it sends message to suspicious data decision-making module and the suspicious data decision-making module record this suspicious packet. If amount of suspicious data reach the threshold, in order to hold up illegal data effetely, the rules of physical layer packet filter firewall and IP layer packet filter firewall will be updated (Chen, 2009; Langendoerfer *et al*., 2007). The design framework of FMCC in mobile phone is shown in Fig. 2.

The key process: Considering the relatively scarce of resources and the need of the safety in mobile phones, when a mobile phone firewall is designed, the suspicious packet should be detected as early as possible in bottom layer. Thus, it can save the limited resources of mobile phones effectively. For the suspicious packet that be detected in high layer, in order to detect these packets in bottom layer next time, the firewall rules of the bottom layer should be updated. The detect process is show as Fig. 3.

The algorithm:

```
While (get a data packet) {
    If (Packet doesn't belong to packets after connection
      is established)
      Transmission Packet to the physical layer packets
      filtrating firewall
      If (packet is illegal)
        Forsake;
```

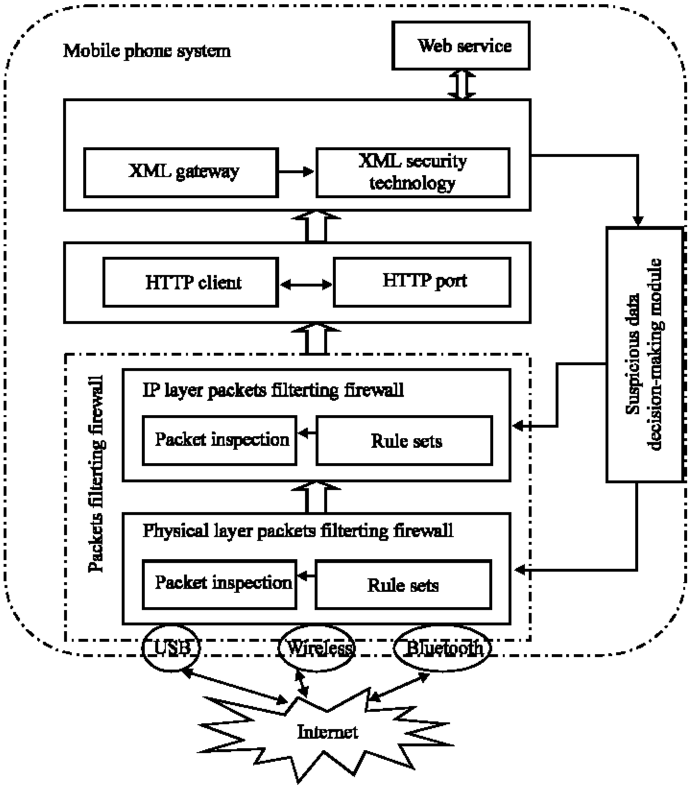

Fig. 2: The design of FMCC

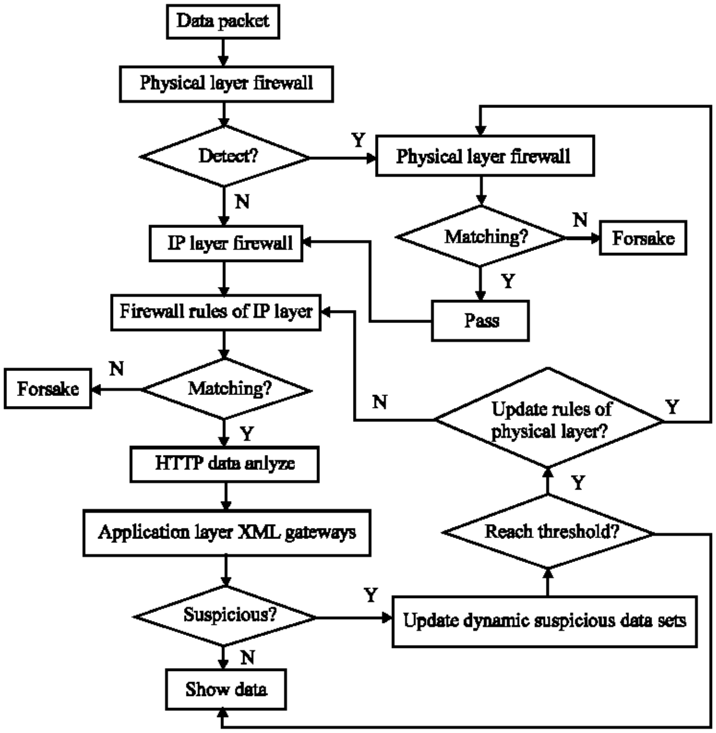

Fig. 3: FMCC packet inspection flowcharts

```
Else
Transmission Packet to the IP layer packets
filtrating firewall
 If (packet is illegal)
 Forsake;
 Else
    Transmission Packet to the application layer
    XML gateways;
       If (XML gateways find suspicious data)
            Update dynamic suspicious data sets;
            If (Suspicious data reach threshold)
             Forsake packet; Update firewall rules of
             IP layer and physical layer
             Else
             Show date;
                           }
```

Performance analysis: In order to test the working efficiency of FMCC, this study gives five simulation experiments. In these simulation experiments, the data packets contains: illegal date packets, normal data packets, suspicious data packets and the mixed packets of the three packets. The specific of these experiments are listed as follows:

- The first experiment using the traditional mobile phone firewall when there is no illegal date in date packets
- The second experiment using the traditional mobile phone firewall when all of date in date packets is illegal
- The third experiment using the traditional mobile phone firewall when there is a mixed packet which contains illegal date, normal data and suspicious data
- The fourth experiment using the mobile phone firewall in this study when there is a mixed packet which contains illegal date, normal data and suspicious data
- The fifth experiment using the mobile phone firewall in this study when all of date in date packets is illegal

The results of these simulation experiments are showed as Fig. 4.

In Fig. 4, the advantages of packet filter firewall based on Cross layer design is obvious. Using the traditional mobile phone firewall, the consumption of CPU is about 40% in the first three experiments. Compared with that, using the firewall in this study, the consumption of CPU is 27.34% in the fourth experiment. Even, the consumption of CPU is 6.43% in the fifth experiment. It shows that the advantages of FMCC will be more apparent when the data packets are larger or the proportion of illegal date is bigger. Thus, we verified practicality and safety of the packet filter firewall based on cross layer design.

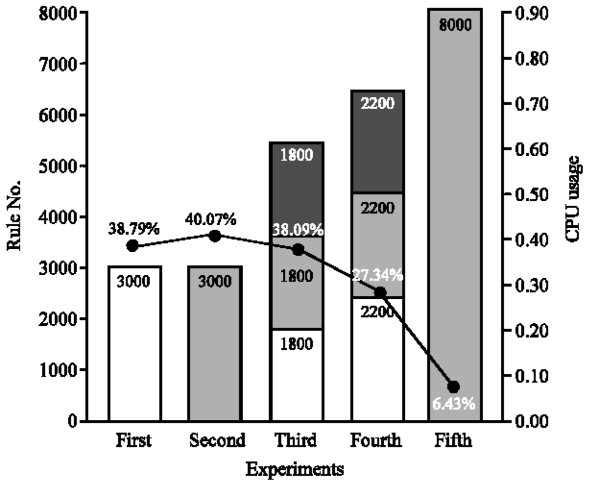

Fig. 4: The results of simulation experiments

CONCLUSION AND FURTHER WORK

In order to solve the problems existing in mobile security, this study designs a mobile phone firewall based on span of cooperation. This study designs the main functional modules contains in the mobile phone firewall. Then, this study offers the design plan of the mobile phone and its packet inspection process. Furthermore, the advantages of the mobile firewall have been proved by several simulation experiments. The two most prominent feature of the mobile phone firewall are practicality and safety. There are still some deficiencies in present study and the optimization and the credibility of Packet filtering rules will be our problems to be solved in the future.

REFERENCES

Chen, V.J., 2009. The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics. J. Inform. Manage., 46: 241-248.

Jiang, G.S., 2007. Design and Implementation of Firewall of Smart Phones Based on Symbian OS. University of Electronic Science, Cheng Du, pp: 22-28.

Langendoerfer, P., P. Krzysztof, P. Steffen and L. Martin, 2007. Crosslayer firewall interaction as a means to provide effective and efficient protection at mobile devices. Wired/Wireless Internet Commun., 30: 1487-1497.

Wang, X.F., 2003. The Study of Distributed Firewalls Based on the Technology of Packet Filtering. Nanjing Institute of Meteorology, Nanjing, pp: 4-40.

Wang, X.Y., 2009. Research on cellphone security system based on IPSec VPN. J. Comput. Security, 1: 1-3.

Zhuang, Y.P., 2007. Control strategy of software performance base on trusted computing on mobile devices. J. Comput. Appl., 12: 113-115.