International Journal of Smart Home
Vol. 9, No. 3 (2015), pp. 195-204
http://dx.doi.org/10.14257/ijsh.2015.9.3.18

Remotely Controlled Management on a Small Firewall Server Using a Virtual Server

NamHo Kim

Dept. of Internet Contents, Honam University, Korea
nhkim@honam.ac.kr

Abstract

This study suggests a firewall management method using a virtual server in order to allow a manager equipped with a smart phone not only to detect and prevent security threats but also to control firewalls anytime, anywhere.

Recently, hackers' threatening over security is constantly increasing, but companies or institutions operating a small PC server are exposed to a serious threat on security as they cannot afford to maintain manpower that can control it for 24 hours. As a solution for it, this study suggests a way to provide stable services and also save time and money by detecting an illegal access or intrusion at an early stage and reporting it to the server manager in a remote place via a smart phone so as to cope with it properly. For the solution proposed here, this researcher has designed and realized a system which conducts a pattern matching inspection on the packet using the virtual server and Aho-Corasick algorithm to monitor and detect an intrusion and can realize prompt safety management in a remote place with the system control that is realized by an android app.

Keywords: *Firewall, PC Server, Android, Security, Remote Control*

1. Introduction

The server host connected by the internet is suffering from hackers' attack and damage resulted from it more and more. As the ways of attack are getting more diversified, it is hard to block the hackers' attack only with the server itself, so we are coping with it with either the intrusion detection system or firewall installed on the PC, [1, 2] But in this situation not to know when such kind of attack will take place, it is, in fact, very difficult to monitor it for 24 hours continuously and detect it without a mistake. As a solution for it, we can detect an illegal access or intrusion at an early stage and report it to the server manager so as to cope with it properly, and in this way, we will be able to realize the improvement of services targeting customers by providing stable services and also saving time and money.

To realize this, it is needed to use the virtual server to be connected to the real server and the client, monitor the condition of the network, and deliver it to the PC application. The PC application should be designed to deliver all sorts of information so that the user can control the volume of communication or all kinds of policies through communication with the smart phone that has created the PC application. If there is any access or attack to the user's computer with malicious intention, it should be informed to the manager and blocked through the application. An android application should be designed to be constantly connected to detect and inform any intrusion immediately and also perform firewall control that can be done at the PC application from a remote place, too.

ISSN: 1975-4094 IJSH

In this study, the researcher is going to suggest a way to develop a security control solution to cope with a security threat by detecting it at an early stage and notify it to the manager by a smart phone app and also the PC screen simultaneously so that he can find it out immediately.

2. Related Work

2.1. Windows Basic Firewalls

Windows' firewalls are the program basically provided by Windows OS. It is the firewall function provided internally by the OS itself for users from the Windows SP2 version. The picture below shows the access from Windows' control panel to its firewall. The user can easily turn on or off the firewall, and when the user does not use the firewall, it alerts him with a warning window.

Figure 1. Windows's Firewall Initial Screen

If the user wants to manage the computer by setting up more detailed security policy, it is possible to filter all the inbound and outbound packets with the rules of each process, port, or IP as below. And the user can change the policy to the one that has been stored or such by sending out or bringing the policy.

2.2. Packet Filtering

The packet filtering-based firewall uses layers higher than layer 4 in OSI 7 Layer, so it is relatively faster and simpler. And with a policy setting, it can be controlled easily. Once the packet is sent, the part where the packet is connected gets inspected. It examines whether it does not apply the generally used connections like GET, POST, or HEADER [3, 4]. After then, each of the headers is tested in order. After the test on the packet is finished, if the packet is found to be good, it is transmitted, and then, the state of transmission is displayed on the screen.

If it is found to be some other file resource from the server, not a legitimate URL, or a packet dubious for another attack, it is abandoned and then reported to the user. The program notifies it has been blocked, and at the same time, the smart phone sends out a message to notify the blocking

2.3. Pattern Matching

The firewall inspects the packets that are not desirable. Normally, they include DDos, buffer overflow, malignant codes, or SQL injection. To inspect those dubious packets, pattern matching is conducted. There are several ways of pattern matching, but because it is needed to compare several patterns at the same time through favorable communication between the virtual server, actual server, and the client, it is hard to get good performances only with the algorithm often used in simple pattern matching [5].

That is why the pattern matching algorithm is applied to compare various patterns so as to detect different attacking patterns. In other words, multiple pattern matching is applied, and the pattern matching using this algorithm is Aho-Corasick pattern matching [6].

This is an algorithm based on the tire, and it has an advantage that it can extract results only with a single scan on several patterns to prevent different kinds of malicious deeds.

3. System Design

The solution (Smart Guard) suggested is a system which conducts a pattern matching inspection on the packet using the virtual server and Aho-Corasick algorithm to monitor and detect an intrusion and can realize prompt safety management in a remote place with the system control that is realized by an android app.

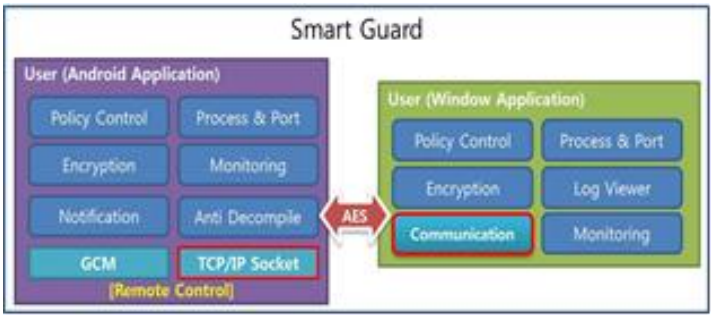


Figure 2. System Architecture

The information of connection is entered by the virtual server, and after being processed by the Windows application, it is transmitted to the real server. If it is a right connection, the response gotten from the server is delivered as it is, and the information of connection coming from the server does not go through the processing separately. When any situation occurs, the message is delivered to the smart phone, and it gets blocked.

3.1. Analysis of Requirements

The developmental plan to draw requirements for the system of the server has been established as below:

- The Platform: It is made to operate preferentially in the Windows environment which a personal server manager normally uses. The Linux server is also often adopted lately, but it is hard to be operated in a small system, so Windows is preferred here.
- The Virtual Server: The virtual server connects the real server and the client and monitors and delivers the condition of the network to the PC application.

- Connection with the Smart Phone: For easier connection, the authentication code is provided now, but later, many other methods can be employed, too, for connection from a remote place such as email authentication.
- Connection Filtering: If there is any connection detected as malicious purpose, it is blocked, and then, it is informed to the smart phone if there is any that has been approved previously.
- The Linking Algorithm: Connection between the smart phone and the server should be encoded so that any third person cannot know about it when it is leaked.

3.2. Virtual Server

The virtual server connects the actual server and the client and also monitors the network status and delivers the information to the PC application.

The virtual server has its purposes as below:

- It is safer to operate it in another program that is a bit distant from it than to control it directly in the server.
- It is because it is such a hard task to do to inform any particular situation to the smart phone. It is almost equivalent to restructuring the server.
- It is also because it is possible to control the server simply by turning off the virtual server instead of restarting it when it is overloaded.

3.3. PC Application

The PC application is designed so that the user can manipulate the traffic and all kinds of policies. It is an application that can transmit all kinds of information through communication with the android, and when any attack or access to the user's computer is made with malicious intention, it reports it to the manager via an application and blocks it.

The PC application should be designed to allow the user to check and manage his computer easily. The PC application is supposed to display the condition of the firewall, policy setting, connection to the android, or the list of the blocked.

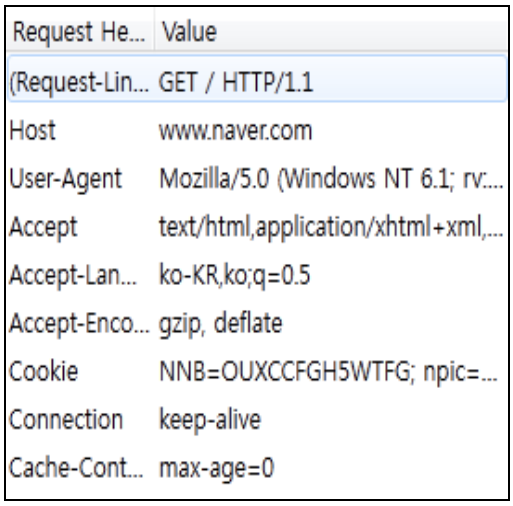
- The PC application allows the virtual server to be connected to the real server. The PC application is always present in the process and receives connections for the real server.
- The operation of the firewall is based on packet filtering. Because the firewall employing packet filtering uses the seventh OSI stratum or the one higher than the fourth only, it is relatively faster and simpler. It can be easily controlled by policy setting.
- How packet filtering is done is described below:

● If the header has not received any request for testing or there is any header that is not the one normally used such as GET, POST, and HEAD, it is blocked.

● If the packet has not been tested properly in the order of the headers or is suspected to be attacked, it is discarded and then informed to the user. And if it is connected to the android app, it is informed to the smart phone, too.

● If it is a right packet, it is delivered to the real server, and after getting a response, it is transmitted to the client just as it is.

- Since GCM supports unidirectional connection only, HTTP connection with high security is to be done for the sake of bidirectional connection.



Request He...	Value
(Request-Lin...	GET / HTTP/1.1
Host	www.naver.com
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:...
Accept	text/html,application/xhtml+xml,...
Accept-Lan...	ko-KR,ko;q=0.5
Accept-Enco...	gzip, deflate
Cookie	NNB=OUXCCFGH5WTFG; npic=...
Connection	keep-alive
Cache-Cont...	max-age=0

Figure 3. Normally connected HTTP packet

3.4. Android Application

An android application is designed so that manipulation on the firewall that can be performed in a PC application can also be done in a remote place

To draw requirements for developing the smart phone app, a developmental plan has been made as below:

- The Platform: It is made to operate in the android environment preferentially as it is the most frequently used by those using a smart phone.
- Functions: Some of the functions operated in the PC application are realized here.
- Monitoring: The smart phone can monitor the situation of the server and also can do the simple setting.

3.5. Between PC and Android Phone Communication Protocol Design

Because a smart phone can receive information about the firewall and manipulate it, malicious deeds can be done through packet sniffing. This is why it is needed to encode the packet [7]. Since GCM does not secure message transmission or transmission order, a protocol is designed to complement it.

Encoded communication standards were investigated for communication between the PC application and the smart phone.

- The server can inform the android based on GCM, but only unidirectional communication can be done. Every time that the PC application distributes it, an additional Google API Key is needed.
- Since GCM also provides unidirectional transmissions only, encoded HTTP connection is adopted.

3.6. Application of the Method to Protect the App

Anti-decompile technique is applied to prevent malicious use or transformation of android applications through decompiling [8].

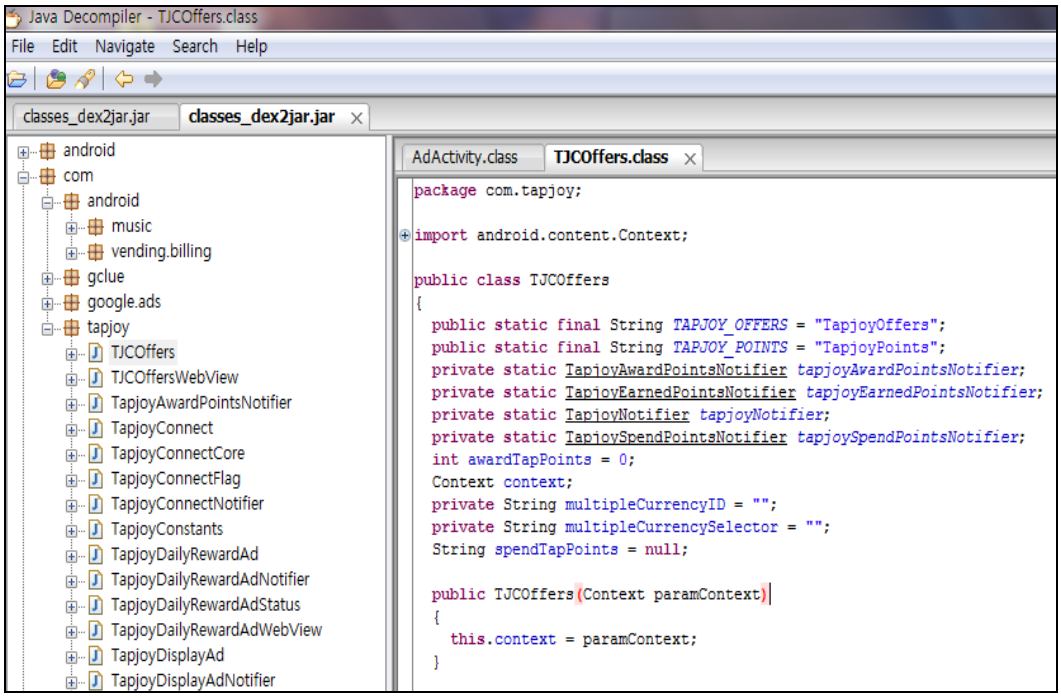


Figure 4. Decompiled Android Application

The android basically applies JAVA, so it is usually poor at security.

- The DEX file that comes out when the APK file is decompressed is a tool that can be easily found on the internet. Because it can be converted to a source file, it is needed to build measures for security.

- About the part made in JAVA, either changes the class name or variable name or generate or arrange meaningless fields, and then, use the method of using odd numbers only and conduct obfuscation using tools like Proguard.

- When making an android application, you can produce ordinary parts with JAVA but the parts that are nuclear or should be confidential with C/C++ by using JNI.

4. Implementation

4.1. PC Applications

PC applications show the status of the firewall, policy setting, android connection, and the list of blocking, *etc.*

PC applications make the virtual server and connect it to the actual server. PC applications are always present in the process and become connected instead of the actual server. The firewall system can also block the IPs or URLs that the user does not want through IP inspection or URI policy setting. If the packet contains the IP addresses or URIs that have been entered, it is blocked.

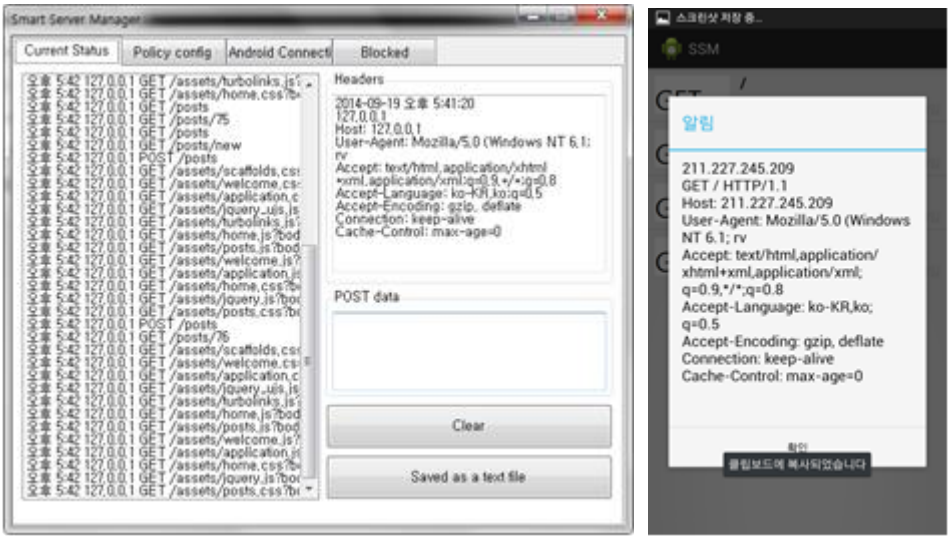


Figure 5. PC & Android Applications

- It shows the condition to be connected to the server.
- The time, IP, and connection type are outputted.
- By selecting the menu, you can see the header of the connection.
- All the list can be stored as a text file.

4.2. Android Applications

PC applications and android applications require communication to receive data about the danger detected and manipulate the firewall policy. Also, they provide push services for the user to inform him of the danger.

For practical communication, it is supposed to take the direct connection to the server by using standard HTTP connection. The function of android applications realizes a part of the function that PC applications have. As the most important function, they give a warning of a dangerous deed by showing the packet corresponding to it, and they also realize such functions as the user's policy setting and firewall start/stop. Yet, as the log function requires too much traffic, it is not updated automatically but upon the user's request.

5. Testing and Evaluation

5.1. The Rate of Pattern Matching

For measurement, a code to measure time is inserted to the projector. At the pattern matching, whenever it is accessed to the code compared, the time is recorded automatically in the log form. To verify this item, the actual server environment is supposed, and the server is made and measured with the engine actually being operated.

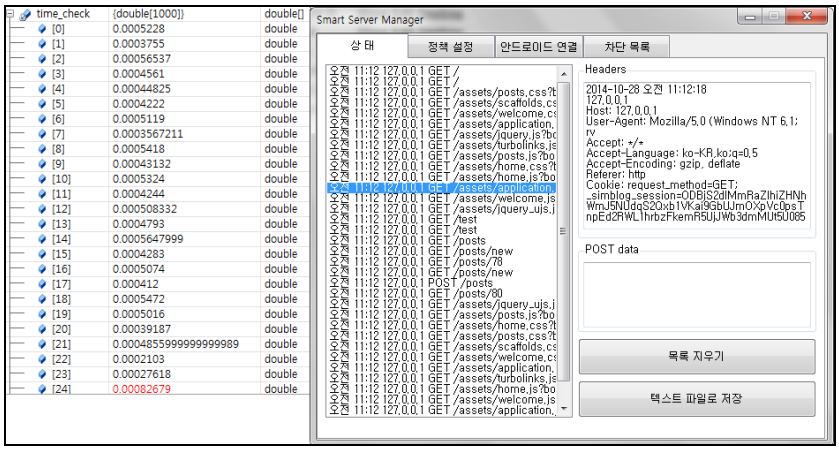


Figure 6. Testing of Pattern Matching Rate

5.2. Notification of the Smart Phone in Danger

After operating the server and the firewall program, the smart phone is connected to the firewall program. After that, it is measured whether the smart phone can receive notices in different situations. Yet, due to the characteristics of the measurement, it cannot be measured accurately on the code, so an analogue method is adopted.

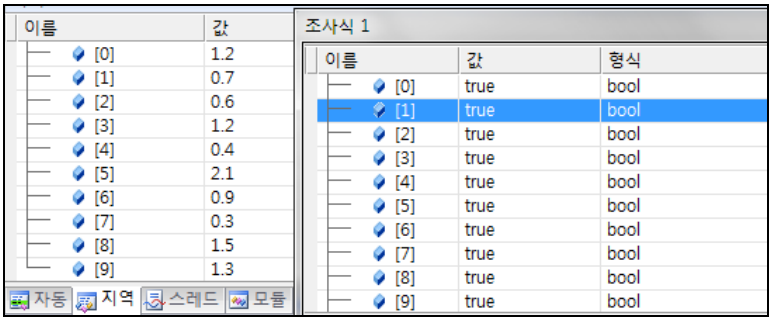


Figure 7. Testing of Notification for Smart Phone

6. Conclusion

The system suggested here conducts its functions of blocking the access of the IP/Port not permitted, setting up the Snort Policy and arbitrarily added policies, and also receives and detects the packet corresponding to it. The result shows that it can block most of the security treats taking place in a small server effectively with the firewall and the intrusion detection system, and it can also block the security threats that might occur in communication between Android/PC Applications without much difficulty.

This study has designed and implemented the firewall and intrusion detection system for small Windows servers and the android application that can be controlled from a remote place to build an efficient as well as reasonable small server management system model. Because it can easily prevent, detect, and control security threats taking place in the operation of small servers, it is expected to enhance security of a small server.

References

[1] D. B. Chapman and E. D. Zwicky, "Building Internet Firewalls", O'Reilly & Associates, Sebastopol, **(1995)**.
[2] D. Y. Lee, "A Development of Web-based Integrated Security Management System for Firewalls", The transactions of the Korea Information Processing Society, vol. 7 no. 10, **(2000),** pp. 3171-3181.
[3] S. H. Lee, "The model design of packet filtering for Firewall systems with protecting Malicious Usages", Proceedings of the Korea Information Science Society, vol. 29, no. 2, **(2002).**
[4] W. R. Stevens, "TCP/IP Illustrated", The Protocols, Addison-Wesley, vol. 1 **(1994).**
[5] A. Aho and M. Corasick, "Efficient string matching an aid to bibliographic search", Co-mm. ACM, vol. 18, **(1975),** pp. 333-340.
[6] S. Kumar and E. H. Spafford, "An Application of Pattern Matching in Intrusion Detection", Technical Report 94-013, Purdue University, **(1994)**.
[7] C. Kaufman, R. Perlman and M. Speciner, "Network security: private communication in a public world", Prentice Hall, **(2002).**
[8] G. Nolan, "Decompiling Android", Apress, **(2012).**

Author

NamHo Kim, He has been a professor in the Department of Internet Contents, Honam University, Korea, since 1998. He received the MS degree in Dept. of Information & Communication from POSTECH, Korea and received Ph.D. degrees in Dept. of Computer Science & Statistics from Graduate School Chonnam National University, Gwang-ju, Korea, in 2013. His research interests include future internet, internet security, ubiquitous computing, big data processing, cloud computing, and biometrics information security.