International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.57-66
http://dx.doi.org/10.14257/ijsia.2015.9.12.07

A Study on the Dos Prevention System for SPT-based Sync Flooding Protection

Keun-Heui Kim[1], Young-Mo Kang[2], Mi-Ran Han[3], and Jong-Bae Kim[4*]

[1, 2]*Department of IT Policy and Management, Soongsil University, Seoul 156-743, Korea*
[3, 4*]*Graduate School of Software, Soongsil University, Seoul 156-743, Korea*
[1]*interbp@hanmail.net,* [2]*cnn5001kr@naver.com,*
[3]*agua1978@naver.com,* [4*]*kjb123@ssu.ac.kr*

Abstract

Sendmail, an open-source-based software, is the most typical mail system that uses SMTP (Simple Mail Transfer Protocol). SMTP (Simple Mail Transfer Protocol), a protocol to deliver various types of files and messages, is being utilized not only in E-MAIL, but also in MMS (Multimedia Message Service) data transfer in mobile environment. Sendmail, an open source based software, is the most typical in mail systems using SMTP. It is exposed to service denial attacks such as mass spam mail because of its process structure that is vulnerable to external service attacks. In this paper, we discuss our design of a security architecture that can respond efficiently to mass mail and Sync Flooding attacks from the internet. Also, to apply our proposed service denial attack security architecture, we used SPT (Safe Proper Time) technology, which ensures the reliability of TCP/IP communication. By analyzing the pros and cons of the security architecture in accordance with each phase of the network, we propose a network architecture that can most efficiently fight external malicious attacks.

Keywords: *IPS, IDS, SPAM, DOS Attack, SMTP, SPT, MQSPT*

1. Introduction

A mail system is divided into four stages: the Mail Send Client, the Mail Transfer Agent, the Mail Delivery Agent, and the Mail Receive Agent. The problem with the existing mail system is its vulnerability to service denial (DOS) [5] attacks through its mass-mailing. The mail system can disable mail transmission and receipt due to service denial attacks. Due to this, when the same system provides services such as web services other than a mail system, it becomes a threat to service availability, even to that of this web service. Availability threats would damage other system networks due to the network bandwidth consumption in the same section of the information system. To prevent service denial attacks, the proposed DPS (Dos Prevention System) system was applied in the optimal network stage by analyzing the pros and cons of the network stages.

The composition of this paper is as follows. In Chapter 2, by deriving the mail system architecture process view, it analyzes the design vulnerability for denial service attacks in the structural aspects. In Chapter 3, by analyzing the pros and cons of each band of network, it provides optimal application position of DPS (Deny of Service Prevention

Jong-Bae Kim is the Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 1738-9976 IJSIA

System) to be proposed in this paper. Finally, it describes the conclusions and future studies in Chapter 4.

2. Mail System Architecture Study

The mail transfer procedure will be processed in four stages. Beginning with the Mail User Agent (MUA), the Message Transfer Agent, SMTP (Simple Mail Transfer Protocol), and the Message Delivery Agent are delivered in that order to the POP3/IMAP protocol. They consist of the MUA, which receives the mail via POP/IMAP in the end. The diagram in Figure 1 shows the mail delivery process.

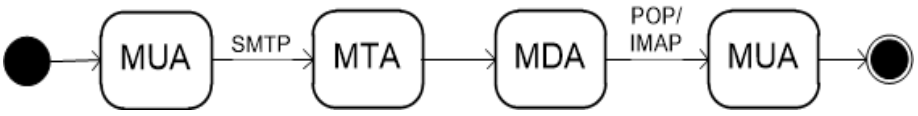

Figure 1. E-mail Delivery Process

The subject of this study is the MTA (Message Transfer Agent). The receipt of mass messages from the MUA is due to the depletion of the available resources of the service, which results in a delay or failure in the internal mail system. To process mail for which a request for transfer is received from the outside using SMTP, a receiving process is needed. For such receiving process, TCPSERVER is used. A mail system is vulnerable because the process starts in accordance with the number of mails received from the TCPSERVER. Such a method is called the multiprocessing method. In the communication structure of the multiprocessing method, as many internal handling processes as accesses are activated, which depletes the system resources (the CPU, memory, File Descriptor, *etc*.). In order to prevent system's service denial attacks via remote network attacks, it must accurately detect the attack session status. In this study, applies SPT (Safe Proper Time [1]) module to TCPSERVER for detecting the session status, and designs DPS (Deny of Service Prevention System) system architecture by utilizing this. For the mail system of study subject, if analyzing 4-stage architecture of the logical modeling, it is possible to grasp the vulnerabilities of external service denial attacks due to structural problems. In this study, we develop a security policy necessary for preventing the visualized vulnerabilities in the logical model. Also, we design DPS (Dos Prevention System) in order to prevent service denial attacks. Then, study the phased network application measure to find the optimal position on the network for applying the designed system.

Mail system architecture is configured in a transmission-possible communication protocol being attached different types of data. Also, depending on the increase of the external connection sessions, it is designed in a multi-processing structure that internal processes are increased. In such a structure, the service becomes not available if the internal processes come to an increase. Such principle is called a service denial attack. Also, the phenomenon that the connection is no longer impossible by depleting the Back Log Queue memory which is called Sync Flooding occurs. E-MAIL system architecture, being caused by handling mail transmission process depending on mail transfer requests, becomes a target of service denial attacks. If it is exposed by service denial attacks, the range of damage is different depending on the process design within the system. The Figure 2 is a blueprint that analyzed E-Mail system via Reverse Engineering.

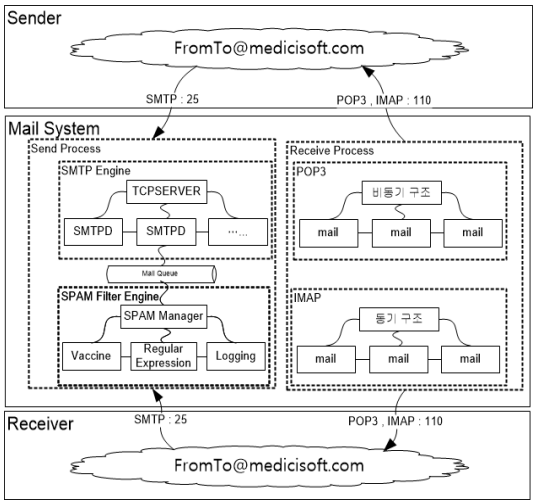

Figure 2. E-MAIL System Process View

Analyzed E-MAIL System Process View, not only Sync Flooding vulnerability from external malicious attacks, can have mail service delay even when processing normal mass mail receiving such as News Letter. The cause is because the process is started in response to the number of receiving mails. In order to improve such vulnerability, to control the session for the external connection requests is sufficient. If introducing a security policy to DPS (Dos Prevention System) which is designed in this paper, it is possible to prevent Service Denial Attack because it is able to effectively control the external connection requests.

The spam mail transmission technique, a kind of Service Denial Attack, is divided into four Techniques as shown in Table 1[1]. First, in the open relay transmission technique, the MTA designed in the SMTP, which is set as the Relay Forward, sends mass mails in the middle, and transmits them by modulating the senders' shipping information (IP). Second, the open proxy technique makes tracking impossible because the unauthorized mail sending address is recorded in a proxy server. Third, the malicious code technique transmits the malicious code by using a mail transfer agent illegally installed in the user's PC. Fourth, the technique transmits spam mails by modulating the MTA maliciously. Corresponding methods for spam mails are effective if they block all unauthorized senders by identifying network sending places based on Traffic Management, and configuring the Bastion Host. The packet sent by disguising the normal sender can be effectively controlled using the DPS security policy.

Table 1. Spam Mail Transmission Techniques

Technique	Description
Open Relay	Transmits mails with SMTP Relay Forward in the middle
Open Proxy	Tracking is not possible because the mail is recorded in a proxy server
Malicious Code	Transmits mails using an illegally installed mail transfer agent
SMTP Server	Transmits mass spam mails by configuring the SMTP Server

3. Computing Protection Policy and Mechanism Against Sync Flooding

3.1. Network Analysis for Sync Flooding Block

Among the different types of Service Denial Attacks (Dos), the biggest threats are the depletion of system resources and Sync Flooding Attacks. Vulnerability to system resource depletion attacks is due to the limitation of available resources provided by the system, when more sessions are requested than the File Descriptor limit value, thereby exceeding the system's threshold due to code vulnerabilities, *etc*. This is because it becomes greater than the maximum file descriptor of the standard 1,024 sessions assigned to each process, so the process would be abnormally terminated. To effectively prevent external attacks, the protection policy is important, but the defense point selection to minimize the damage is also important. Therefore, in this study, a method of selecting the optimal network position was found by analyzing the pros and cons of each section of the network. Table 2 presents the physical view by analyzing the network model most used to derive phased network improvements, and presents the pros and cons per section by classifying the firewall equipment into five steps [11].

Table 2. Network Physical View: Five Steps

Section	Network physical view: five steps
Front of the router	Pro: Can detect all attacks before entering the network Con: Distinction of the invading information from the normal information is difficult.
Back of the router	Pro: Can detect actual attacking persons [7] Con: Depletes the router's resources through the router's packet filtering function
Back of the first firewall	Pro: Can detect even attacks flowing outside from the inside [8] Con: Network linkage with the firewall policy is difficult
Internal Network Zone	Pro: Can monitor internal network hacking Con: Has a limit in detecting an external network
DMZ Zone	Pro: Can be used to detect internal/external attacks on the DMZ Con: Requires a separate system for trespassing detection

3.2. DPS Proposal

For the accurate functioning of the security policy for preventing malicious attacks, the reliability of the TCPSERVER connection session status (connected, disconnected, or delayed) must be ensured. A Sync Flooding Attack, if it repeats the forced termination after creating connection sessions of more than 1,000 cases per second due to the non-regular TCP State (FIN_WAIT1~1, CLOSE_WAIT, LAST_ACK, or TIME_WAIT), the connection becomes impossible while it exceeds the Backlog Queue memory. To prevent this, a malicious system must be impossible to re-connect to the hacker through Black List processing after immediate blocking of the hacker, by accurately identifying the transmission information. To apply such a security policy, accurate determination of the network session state must be allowed. In this study, the SPT (Safe Proper Time) [1] technique is presented as a method of increasing the accuracy of the session processing. This technique makes it possible to finely apply the security policy because it can grasp the correct session state. The following figure is a mail system architecture to which the SPT module was applied.

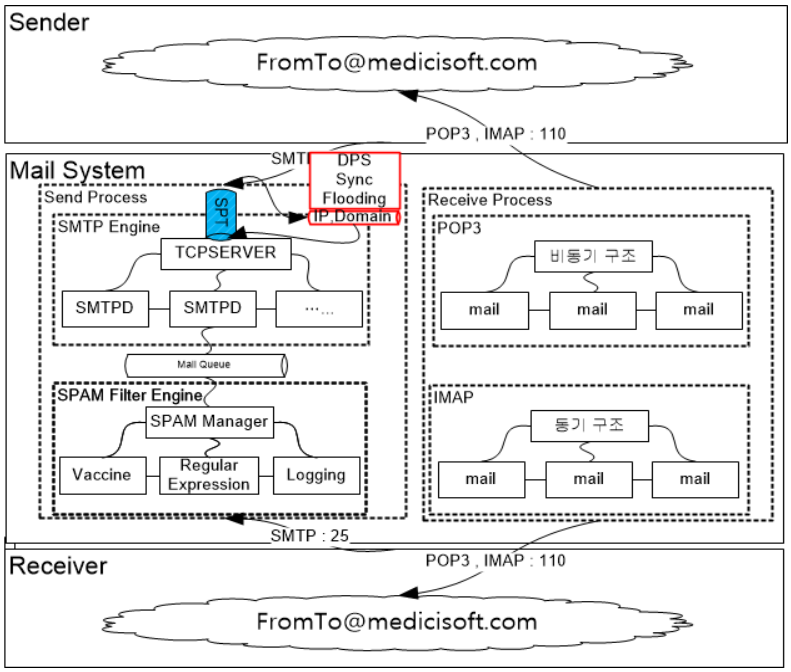

Figure 3. DOS Prevention System Proposal Process View

Figure 4 shows the transaction sequence diagram of the MUA, from its sending/receiving of mail with the TCPSERVER. If the MUA first sends a "Hello" message, the TCPSERVER responds with "250 Pleased to meet you." In this case, a File Descriptor is assigned to the Socket of the TCPSERVER. Since the maximum allocated File Descriptor is 1,024, if more than 1,024 accesses are repeated by disguising the MUA, it will consume all the Backlog Queues in the server side, due to which connection of the Start of backlog queue to the end of buffer will no longer be possible

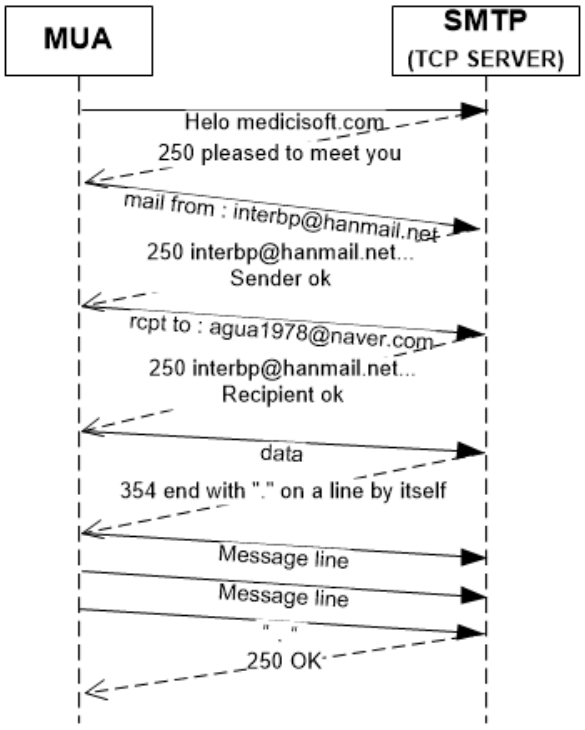

Figure 4. E-mail Transaction Process Sequence Diagram

3.3. Experiment Design

An attack mechanism for the experiment of this study, utilizing a multi-thread method [10] based on network connections, was made to give the effect of maximum attack with minimum resources. Implementation mechanism of the Attack Agent for test is as follows.

```
Algorithm : MailUserAgentDosAttack
Begin :
Send_start {
        var szDataTrans; // Data Processing Variable
        var resFd; // socket descriptor
   ...
   While(True) {
     pthread_create(); // Parallel Connect
      connect_smtp() { // connect
                  resRtn =connect(resFd);
               }
              IF runtime(sendSPT("Helo", resFd) is true THEN
                 ReceiveSPT(szDataTrans, resFd); // send
              End
     ...
       }
End
```

Figure 5. Mail User Agent Attack Mechanism

To effectively defense attacking Agent, it should apply by replacing TCPSERVER sending/receiving module with SPT (Safe Proper Time) module, and through this, it is possible to determine the exact state of non-regular sessions.

Following Figure 6, is a state diagram of E-Mail system. The following system is composed of the MUA (Mail User Agent) to transfer mails, and TCP SERVER to process receiving mails. The application section of Safe Proper Time module is a TCPSERVER area, which would transmit the information to DPS (Dos Prevention System) by extracting correct information about connection sessions, then would be able to do classification processing for messages based on protection policy.

Figure 6. Mail User Agent Attack Mechanism

It implemented the mechanism described in the previous Figure 6 with DPS (Dos Prevention System) algorithm of Figure 7. If it notifies to the security policy algorithm after accurately identifying the sending information, by using SPT(Safe Proper Time) mechanism for detecting the session status of the sender location, protection will be possible as classifying into pass, temporary block, and permanent block based on the policies.

```
Algorithm : DosPreventionSystemSafeProperTim
Begin :
Send_start {
        var szDataTrans; // Data Processing Variable
        var resFd; // socket descriptor
   ...
   While(True) {
      nFd=Accept(fd,&sockaddr,nLen)
       IF runtime(nFd) is true THEN
         IF WhiteList(nFd) is true THEN // Attack detection
              Call smtp (); // by Pass
         IF BlackList(nFd) is true THEN
              Close(nFd); //  Rejct
         IF BlockList(nFd) is true THEN
             Call CheckBlockTime(nFd); // Check Block Time
         Else
              Call DeleteBlockList(nFd); // Expire Time ,By Pass
         End
       End
     ...
        }
End
```

Figure 7. Dos Prevention System Mechanism

4. Conclusion

The major architectures of the open-source-based Sendmail system were analyzed to understand the mail system structure through reverse engineering. Based on this analysis, the network policy for protection was derived considering the characteristics of the mail system. For us to be able to correspond with an external Sync Flooding Attack, the correct session status must be derived. In this study, by reflecting the status information on the security policy through exact derivation of the session status, the defense policy was effectively protected from attacks. It is thus concluded that it is most important to accurately determine the session status that connects to the TCPSERVER. In this study, the SPT [1] sending/receiving module was used to accurately determine the communication status. The most important point of the DPS proposed in this paper is the protection policy, the protection rate of which can be made to suit the situation by flexibly specifying the protection policy depending on the type of external attack. As shown in the test results, before the application of DPS, the non-regular TCP State increased continuously then fell into the state in which services were no longer available. After the DPS application, the non-regular TCP State increased gradually then was managed in the Block List based on the criteria for the defined security policy. Afterwards, even when the attack continuously occurred, if it was added to the Black List, it was able to basically protect the system by rejecting the request for additional connections. A further study may be conducted on how effectively the additional attacks corresponds to the attacks that violate the DPS policy by forging the address information of the mail send system at a remote location.

References

[1] K-H Kim "Data Transmission Method and Stock Trading System Reflecting the Method ", Korea, Registration No. 10-1458436 ,2014.
[2] Study on Low-Latency overcome of XMDR-DAI based Stock Trading system in Cloud_Journal of the Korea Institute of Information and Communication Engineering (2014) V.2.
[3] K-H Kim, M-r Han and J-B Kim "Design and Implementation of MQSPT Protocol for Establishing Financial Next-Generation Project PUSH Architecture" , ASTL Vol. 86, No. 22, (2015).
[4] B-S Kim "ADDoS Protections for SMTP Servers: Soongsil University, IEEE, (1976).
[5] M. Still & E. C. McCreath "An In-Line System Network Composition Model Expansion to Secure Service Availability from DDoS Attack", International Journal of Computer Science and Security, (2011), Volume 4, Issue 6.
[6] Roesch et al" Snort: Lightweight intrusion detection for networks. in LISA", vol. 99, 1999, pp. 229–238.
[7] Jain and A. K. Singh "Distributed denial of service (ddos) attacks-classification and implications", Journal of Information and Operations Management , pp. 0976–7754, (2012).
[8] F Jalili, M. Imani-Mehr,. Amini, and H. R. Shahriari "Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks", in Information Security Practice and Experience. Springer, (2005), pp. 192–203.
[9] M. Walfish, H. Vutukuru, D. Balakrishnan, Karger, and S. Shenker " Ddos defense by offense, ACM Transactions on Computer Systems (TOCS)", vol. 28, no. 1, p. 3, (2010).
[10] S, B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A recent survey on ddos attacks and defense mechanisms", in Advances in Parallel Distributed Computing. Springer, (2011), pp. 570–580.
[11] S. Youn, H-c Cho, "Improved Spam Filter via Handling of Text Embedded Image E-mail", Journal of Electrical Engineering and Technology, vol. 10, iss. 1, 2015, pp. 401-407
[12] Ji-Yeu Park, Rosslin John Robles, Chang-Hwa Hong, Sang-Soo Yeo, Tai-hoon," IT Security Strategies for SME's", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, 2008

Authors

Keun-Heui Kim received his Master degree in Software Engineering from Sogang University in Korea, (2013). He worked in the IT field as a System Engineer over 16 years. His research interests are in areas of Software Engineering, Open Source Software, Security and Low latency Network.

Young-Mo Kang was a CEO at A/GE. He is studying his doctor's degree in Software Engineering in Graduate School at Soongsil University, Seoul. His research interests are in areas of Policy of Information Technology, IT Convergence and AI.

Mi-Ran Han received her bachelor's degree of Statistics in Dongguk University, Seoul (2002). She is currently taking her master's degree in Software Engineering at Graduate Schoool of Soongsil University, Seoul. Her current research interests include Open Source Development and Security

Jong-Bae Kim received his bachelor's degree in Business Administration at University of Seoul, Seoul (1995) and master's degree (2002), doctor's degree in Computer Science at Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software at Soongsil University in Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.