Analysis of Slow Read DoS attack

Junhan Park*, Keisuke Iwai*, Hidema Tanaka* and Takakazu Kurokawa*
*Department of Computer Science,
National Defense Academy, Yokosuka, Japan
Email: junhanp78@gmail.com, {iwai, hidema, kuro}@nda.ac.jp

***Abstract*—The idea and techniques of DoS(Denial of Service) / DDoS(Distributed DoS) attack strategy become more effective and more complex. In our research, we focus on a Slow Read DoS attack which is one of sophisticated DoS techniques. This technique prolongs time to read the response from the Web server, although an attacker sends a legitimate HTTP request. When an attacker sends many legitimate requests, he can keep many open connections to Web server and eventually cause DoS situation. In this paper, we analyze the effectiveness of Slow Read DoS attack using the virtual environment. Furthermore, we propose the Slow Read DDoS attack based on collusion technique and discuss the countermeasure scheme.**

I. Introduction

DoS attacks are evolved and consolidated as severe security threats to network service, not only for providers but also for governments. Earlier DoS attacks use flood-based high-bandwidth approach and exploit the resource of network and transport protocol layers. Since DoS attacks are simple, they can be prevented by filtering the source IP address. In order to break through this countermeasure, DDoS attacks deliver a DoS attack by many attackers. However, there is a problem using high-band width in DoS/DDoS attacks, and many solutions are proposed. One of such solution is low-band width approach. The latest attack method using such approach is low-bit rate type which exploit vulnerabilities of application layer protocols to accomplish DoS attacks[1]. In this paper, we focus on the technique called the Slow Read DoS attack that has been designed by Sergey Shekyan[2]. This attack is that an attacker basically sends a legitimate HTTP request to the Web server and then very slowly reads the response. If an attacker sends many legitimate requests, the Web server quickly reaches its maximum capacity and becomes unavailable for new connections by legitimate clients. Moreover, it is very hard to detect these attacks if we do not monitor the network layer, because those requests are indistinguishable from other legitimate clients[3].

In this paper, we analyze the effectiveness of Slow Read DoS attack using the virtual network environment. We adopt *slowhttptest* as a general Slow Read DoS attack scenario. It is freeware and available at [4]. We set the target Web server using *Apache* which is most popular one[5]. From our analysis, we found the limitation of effectiveness of attack and improvement technique using collusion attack scenario. As a result, we propose a new attack method "Slow Read DDoS attack" and discuss the countermeasure against it. We found that the effectiveness of Slow Read DoS is determined by the setup of Timeout parameter of Web server. However, when we use our new attack method, we can ignore the restriction of Timeout parameter and keep on attacking. From our analysis, we found that the countermeasure for our new attack has trade-off relationship with QoS of Web server.

II. Slow Read DoS attack

A. Outline of Slow Read DoS attack

Slow Read DoS attack is one of Slow HTTP attack. Slow HTTP attack does not aim at the network layer like DoS/DDoS attacks, but exploits the application layer. If an HTTP request is not complete, or if the transfer rate is very low, the Web server keeps its resources busy waiting for the rest of the data. Slow HTTP attack is based on this fact. Thus when the Web server keeps too many resources busy, this situation becomes like DoS attack. To realize this malicious condition, the attacker can take following two types of techniques[6].

1. The technique of sending request slowly
2. The technique of reading response slowly

Type 1 is well-known technique and Slowloris† or Slow HTTP POST attacks are famous. Slow Read DoS attack is categorized into type 2 and this is the latest technique.

B. Attack strategy

Slow Read DoS attack is delivered by exploiting the flow control of TCP. First, the attacker sends a legitimate request after 3-way-handshake. After that, the attacker advertises window size smaller than usually, and makes slow down the HTTP response operation. When the attacker advertises window size equals to 0, the Web server will stop sending data although hold the connection. As a result, the attacker succeeds in Web server making resource waste.

III. Analysis of Slow Read DoS attack effect

A. Experiment preliminary

Fig. 1 shows experiment environment. We set the Web page size 100KB and use *Wireshark* in order to observe packet between attacker and Web server. TABLE I shows the default directives of httpd.conf which controls a connection with a client in the configuration of the Web server which is the attack target. TABLE II shows the default configuration of prefork MPM(Multi Processing Module) which controls the start of process when a connection is established. TABLE III shows setting of Slow Read DoS attack.

†also known as Slow headers or Slow HTTP GET

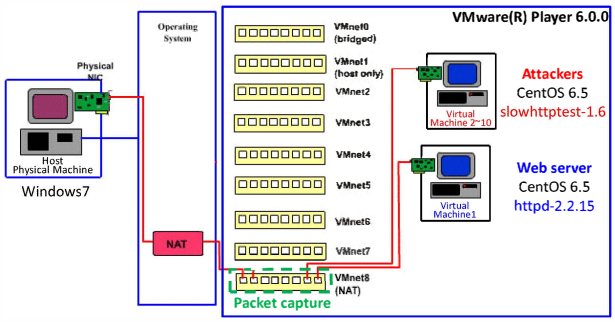

Fig. 1: Experiment environment(source : [7])

TABLE I: Directive

Directive	Value
Timeout	60
KeepAlive	Off

TABLE II: Prefork MPM

Directive	Value
StartSevers	8
MinSpareServers	5
MaxSpareServers	20
ServerLimit	256
MaxClients	256
MaxRequestChild	4000

B. Function of parameter

When a Slow Read DoS attack is implemented, a service unavailable state of Web server is detected when the attack connection is reached the limit of a Max Clients(MC in the following) in TABLE II. When the number of attack connections are larger than MC, there are no child process to use. As a result, the Web server becomes service unavailable state. However, if the time setup of Timeout(TABLE III) passes, the attack connection is disconnected compulsorily, and will return to service available state. Thus, Timeout parameter has a function which controls connection between them. And the value of MC controls the number of connections between clients and a Web server.

C. Experiment

From the facts shown in Section III.B, we fix the parameter of attacker as shown in TABLE III, and set up five types of target Web server as shown in TABLE IV. Note that parameter MC/SL means that the value of MC and SL(Server Limit) are the same because effective value of SL is not larger than MC.

When implementing a Slow Read DoS attack experiment, we define the status of attack as follows.

- Attack success : unacceptable new legitimate connections.
- Attack failure : acceptable new legitimate connections.

"Attack success" means that the number of connected attack connections is larger than or equal to the value of MC/SL. On the other hand, "Attack failure" means that the number of connected attack connections is less than the value of MC/SL. The effectiveness of successful attack is estimated by time length(second) of maintaining service unavailable state.

TABLE III: Setting of Slow Read DoS attack

Option	Value
Number of Attack connections	500
Receive window ranges	8-16byte
Pipeline factor	1
Read rate from receive buffer	5byte/sec
Connections Rate	50
Timeout for probe connection	10
Using proxy	no proxy

TABLE IV: Target Web server of experiment

Experiment number	Timeout	MC/SL
1	100	300
2	200	300
3	100	600
4	200	600
5	10	300

D. Result of experiments

1) Experiment1, Experiment2: The graph of an experimental result shows time transaction of the number of child process of Web server(blue line), and the number of established connections of TCP to the port #80(red line) after starting an attack at time 0 second. Fig. 2 shows the result of the experiment 1. The number of child process reaches 300 which is the value of MC/SL after 14 seconds. As a result, we can succeed in attack. However, by setup of Timeout, attack connections begin to be disconnected after 107 seconds, and it returned to the service available state. Therefore, the attacker is able to maintain attack success status for 93 seconds.

Though MC/SL is set to 300, the number of established connections of TCP becomes 428. The reason for this situation is these 128(=428-300) attack connections which is contained by 3-way-handshake of TCP and treated as pending connections. By setup of Timeout, the number of TCP established connections also decreases after 93 seconds. On the same time, pending connections are processed, but also disconnected after 187 seconds. Although the attack itself is ended after 10(=500/50) seconds, the attack connections are effective until 194 seconds. As a result of experiment 1, we can conclude that the attack succeed between 14 and 107 seconds.

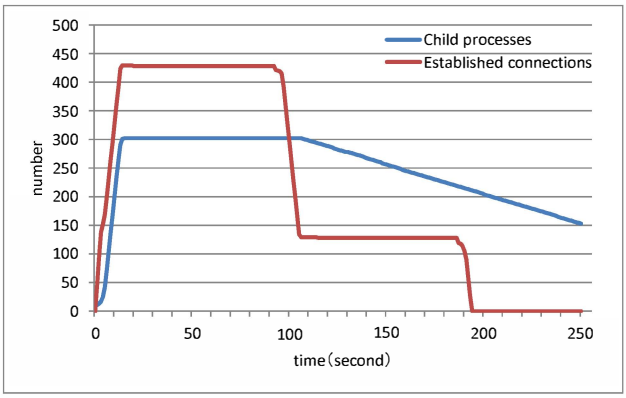

Fig. 2: Experiment 1(Timeout 100, MC/SL 300)

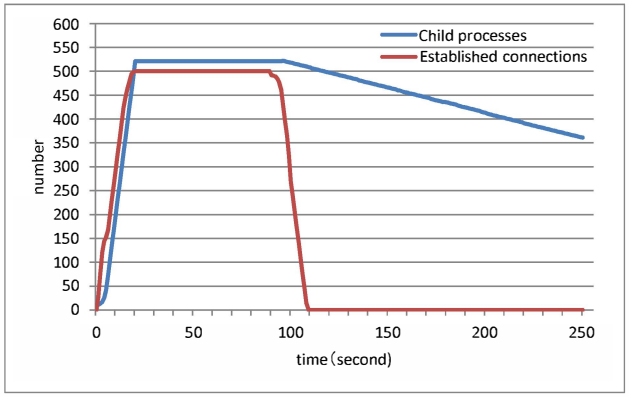

Fig. 3: Experiment 3(Timeout 100, MC/SL 600)

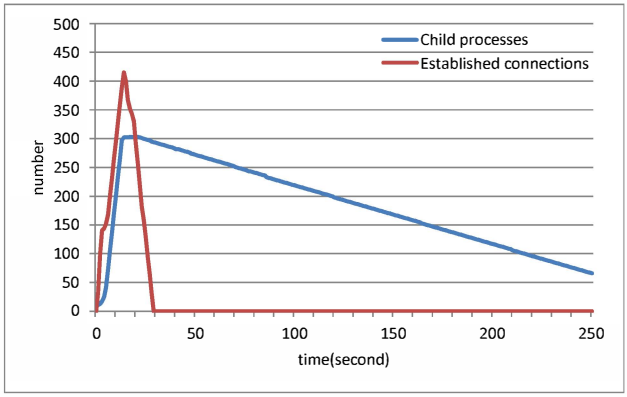

Fig. 4: Experiment 5(Timeout 10, MC/SL 300)

In the experiment 2, we set the value of Timeout to double(200seconds) compared with the experiment 1. We can find that the attack success status is between 14 and 201 seconds, and the length is almost double of experiment 1.

2) Experiment3, Experiment4: Fig. 3 shows the result of experiment 3. Naturally, we cannot succeed in attack, because the Web server has an enough resource against the number of attack connections. We can find two characteristics from the result. One is that the setup of Timeout also works after 98 seconds. Another is that we can find 520 of child processes, though the total number of attack connections is 500. This is because the setup of MaxSpareServer is added as shown in TABLE II.

3) Experiment5: Fig. 4 shows the result of experiment 5. We can also succeed in attack. However, the attacker is able to maintain the attack success status for just 8 seconds, since the value of Timeout is extremely short. We can find that the value of Timeout is a main factor which determines length of attack success status.

E. Consideration

To analyze the relationship between attack success status and the Web server parameters; Timeout and MC/SL, we did the attack simulations under the condition shown in TABLE III. As a result, we can find following three elements that have determined attack success status.

1. The value of Timeout of Web server.
2. The value of MC/SL of Web server.
3. Total number of attack connections of Attacker.

In general, the setup of Timeout is recommended for 10 seconds or more. If Timeout is set up short, Slow Read DoS attack can be prevented, but QoS is also reduced remarkably. If MC/SL is set up large, Slow Read DoS attack can be prevented, but there is restriction of resource of Web server. The number of attack connections is more effective if it sets up large from the relationship between Timeout and MC/SL. However, it depends on an attacker's cost. In addition, the attack connections from the same IP address is easy to be detected. From these three results, wet can conclude that the effectiveness of only one attacker's Slow Read DoS attack is restrictive.

IV. Proposal of Slow Read DDoS attack

A. Outline of proposal technique

Since the attack connection is compulsorily disconnected by passing the Timeout, the service unavailable state of Web server return to available. From experiment 5, we found that the countermeasure with 10 seconds of Timeout is effective against Slow Read DoS attack which is parameterized as TABLE III. Moreover, if the number of attack connections is less than MC/SL, the attack cannot success. So the effectiveness of attack by only one attacker is small as described in Section III.E. However, if another attacker sends new attack connections before attack connections are disconnected, it will be expected that the length of attack success status can be maintained efficiently longer. Thus, we consider the scenario with which two or more attackers collude. In this paper, we call this attack technique is "Slow Read DDoS attack".

B. Conditions for attack success status

From the result of experiments shown in Section III, we can deduce the conditions of successful attack. TABLE V shows the variables. Let A be the total number of attack connections. Then the condition of $M \leq A$ is necessary for successful attack. There are two cases of calculations for A under the conditions of t_0 and t_z. In the case of $t_0 \geq t_z$,

$$A_{(t)} = C \times t. \tag{1}$$

In the case of $t_0 < t_z$,

$$A_{(t)} = \begin{cases} C \times t & (t < t_0) \\ C \times t - K \times (t - t_0) & (t \geq t_0), \end{cases} \tag{2}$$

where $t \geq 0$ denotes time progress after attack starts($t = 0$).

C. Proposal technique

Eq. (1) is in the case that Timeout t_0 is enough large. Therefore, even if the attack finished at t_z by only one attacker, it will be maintain the attack success status until t_0. However, since Timeout t_0 is shorter than t_z, in the case of Eq. (2), it is difficult to maintain the attack success status by only one attacker(see experimet 5). Former attack connections will be disconnected after Timeout t_0. This situation causes the restriction of effectiveness of attack. In order to solve this

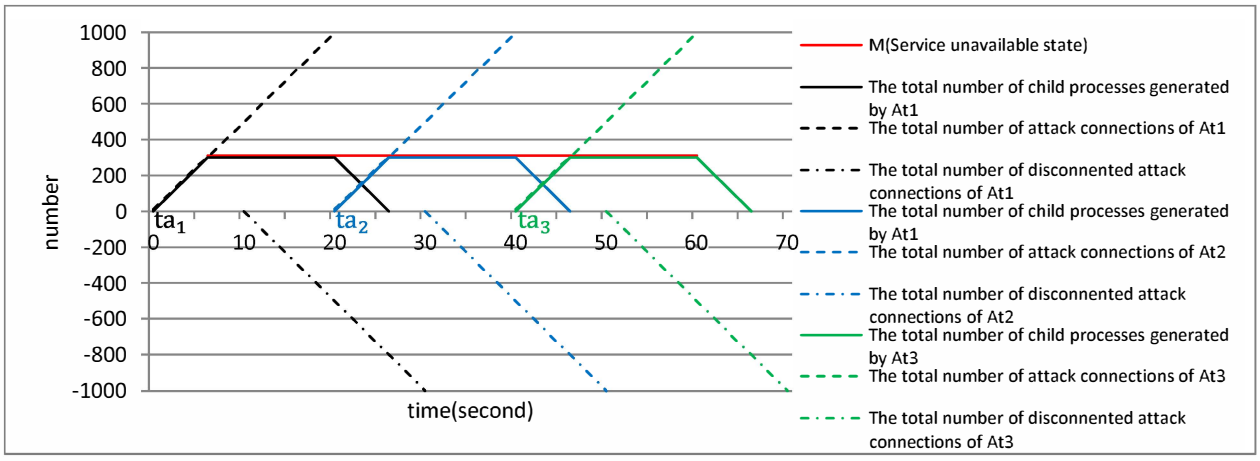

Fig. 5: Diagram of attack

TABLE V: Variables of calculation

Parameter	Explanation
t_o	The value of Timeout
t_z	Finish time of sending attack connections ($t_z = N/C$)
N	The total number of attack connections
C	The number of attack connections which send per second
K	The number of disconnected connections per second after t_o
M	The total number of connections that Web server can process (MC/SL)
$A_{(t)}$	The total number of attack connections which the attacker sent at time t

problem, we consider colluded attack scenario with some attackers.

The basic idea for maintain the attack success status is that following attacker begins to send new attack connections before former attacker's t_z. Therefore the collusion attackers can maintain the attack success status of Web server by repeating it.

Let us consider N attackers At_1, At_2, ..., At_N. Attacker $At_n (2 \leq n \leq N)$ begins the attack at ta_n, which calculated as follow.

$$ta_n = \sum_{i=1}^{N} \frac{N_i}{C_i} \qquad (n \geq 2), \tag{3}$$

where C_i and N_i are the values of C and N which attacker At_i set up, respectively. Note that $ta_1 = 0$. For example, Fig. 5 shows the theoretical attack diagram of a Slow Read DDoS attack by three attackers. We assumed that target Web server is the same as experiment 5. Because, it is the most resistant against Slow Read DoS attack. The almost setting of attacker is the same as Section III. However we set to $N = 1000$, in order to hold the condition $t_0 < t_z$. As the results, we set the values of parameters to $C_1 = C_2 = C_3 = 50$, $N_1 = N_2 = N_3 = 1000$, $t_0 = 10$, $t_z = 20$ and $M = 300$. Thus, we can deduce the attack diagram(Fig. 5) of a Slow Read DDoS attack using these parameters. And from these settings, we can expect that the attack success status can be maintained from 6 to 60 seconds.

V. Attack Simulation by the Proposal Technique

A. Outline and result of simulations

We set the parameter of attackers and Web server like Section IV.C in an attack simultion, and they are summarized in TABLE VI. Before Slow Read DDoS attack simulation, in order to analyze the effectiveness using huge number of attack connections, we did attack simulation by only one attacker with $N = 1000$(Simulation 1). Next, we simulated Slow Read DDoS attack by three attackers($At_1 \sim At_3$)(Simulation 2) following the attack diagram shown in Fig. 5.

TABLE VI: Parameter of attack simulation

Parameter		Value
Apache Web server	Timeout	10
	ServerLimit	300
	MaxClients	300
Attackers	Connections Rate	50
	Number of attack connections	1000

From the result of simulation 1, we can find longer attack success status(20 seconds) than the result of experiment 5(8 seconds). We confirmed that the increasing N is adequate for improving attack result.

Fig. 6 shows the result of simulation 2. We can find that the attack success status was maintained for 68 seconds(14∼82seconds). It is longer than the theoretical attack diagram shown in Fig. 5(54 seconds).

B. Consideration

From the simulation 1, we can consider that pending connections was also increased and newly processed even if Timeout passes. Because the total number of attack connections(N) was increased to 1000 from 500, attack success status was maintained more longer than experiment 5.

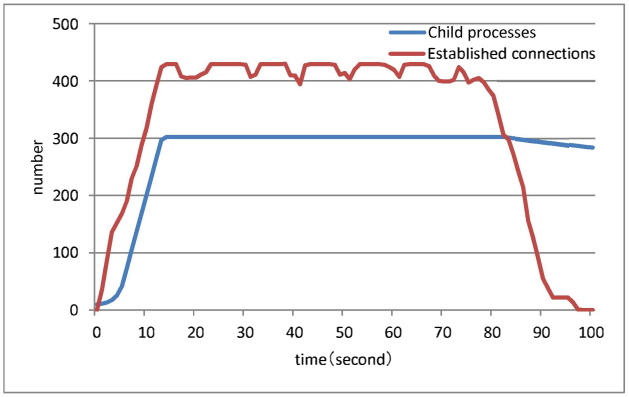

Fig. 6: Attack result of attackers of At1∼At3(Simulation 2)

In experiment 5, attack rate[second/one-attacker] is 20.0. On the other hand, attack rate of simulation2 is 22.7. As a result, we can find Slow Read DDoS is more efficient and lower-cost attack than simulation 1.

We can find two facts between the attack diagram(Fig. 5) and the result of simulations(Fig. 6).

1. Time lag of child process creating.
From the result of attack shown in Fig. 6, we can find that the attack starts to success after 14 seconds. On the other hand, from Fig. 5, we expected after 6 seconds. Therefore there is 8 seconds of time lag. The reason is that we did not consider the delay time which computer creates the child process. By predicting this time lag in advance, we will be able to set the attack start time to success exactly.

2. Influence of the pending connections for establishment.
Pending connections will be made, when the total number of attack connections(N) are set more than MC/SL. And they will be newly processed to establishment, when Timeout passes. For this reason, we can consider that the pending connections make extension of the length of attack success status. Thus, It was extended longer than the theoretical(Fig. 5).

Therefore, there are two new problems for the future works.

1. Analysis of child process creating.

2. Analysis of processing pending connections.

If we can solve above problems, we can realize more precise and lower-cost attack.

From the simulation 2, we can conclude that the countermeasure with short Timeout does not work against our new attack. In order to prevent Slow Read DDoS attack, we should consider to control TCP window size which is advertised by clients. When the size is set tiny, we can detect it as Slow Read DoS/DDoS attack and disconnect to prevent the attack. However, this countermeasure will reduce communication efficiency such as wireless LAN and mobile phone. Therefore we concluded that, this countermeasure against Slow Read DDoS attack also has a trade-off relationship with QoS.

VI. Conclusion

In this paper, we analyzed the relationship between Slow Read DoS attack and Timeout, MC/SL of the Web server. Moreover, we found that effectiveness of the Slow Read DoS attack by only one attacker is restrictive, and its damage is not actually so large. We also proposed the Slow Read DDoS attack. As a result, we clarified the limitations of Slow Read DoS attack and the superiority of a Slow Read DDoS attack by computer simulations.

Since we did simulation in only one-hop virtual environment, we have to postulate following situations in the actual attacks.

- Existence of intermediate servers and routers.
- Existence of legitimate users who has connected.
- Countermeasures which restrict a lot of request from the same source IP address.

The attack simulations above situations are our future works.

References

[1] Cambiaso, E., Papaleo, G., Chiola, G. and Aiello, M., "Slow DoS attacks: definition and categorisation," Int. J. Trust Management in Computing and Communications, Vol. 1, Nos. 3/4, pp.300-319, 2013.

[2] Sergey Shekyan, "Are you ready for slow reading?," https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read, January 5, 2012.

[3] Kelly, J. H., "New Denial-Of-Service Attack Cripples Web Server By Reading Slowly," http://www.darkreading.com/attacks-breaches/new-denial-of-service-attack-cripples-we/232301367, January 5, 2012.

[4] Sergey Shekyan, "slowhttptest," https://code.google.com/p/slowhttptest/, December 28, 2011.

[5] Netcraft, "October 2013 Web Server Survey," http://news.netcraft.com/archives/2013/10/02/october-2013-web-server-survey.html

[6] Cambiaso, E., Papaleo, G., Chiola, G. and Aiello, M, "Taxonomy of Slow DoS Attacks to Web Applications," SNDS, 2012.

[7] ExtremeTech, "Virtual Machines & VMware Part II," http://www.extremetech.com/computing/72268-virtual-machines-vmware-part-ii, December 28, 2001.

[8] KISA, "The response guide against DDoS attack," https://www.boho.or.kr/kor/data/technicalList.jsp, October 8, 2012(in korean).

[9] ha.ckers, "Slowloris HTTP DoS," http://ha.ckers.org/slowloris/

[10] Kelly, J. H., "Researchers To Demonstrate New Attack That Exploits HTTP," http://www.darkreading.com/attacks-breaches/researchers-to-demonstrate-new-attack-th/228000532, November 1, 2010.

[11] H., Kurakami, "The advanced DDoS attack and countermeasure," Information Processing, Vol.54 , No.5, pp.475-480, May, 2013(in japanese).

[12] Ronen, K., "Why Low & Slow DDoS Application Attacks are Difficult to Mitigate," http://blog.radware.com/security/2013/06/, June 10, 2013.

[13] J., Park, K., Iwai, H., Tanaka and T., Kurokawa, "The Reaserch of Slow Read DoS attack to Web server," SCIS2014, January 21-24, 2014(in japanese).

[14] VMware Player, http://www.vmware.com/jp/products/player

[15] Apache, http://httpd.apache.org/

[16] Wireshark, http://www.wireshark.org/