Analysis of Effectiveness of Slow Read DoS attack and Influence of Communication Environment

Shunsuke Tayama
National Defense Academy
Kanagawa, Japan
em55035@nda.ac.jp

Hidema Tanaka
National Defense Academy
Kanagawa, Japan
hidema@nda.ac.jp

***Abstract*—Slow Read DoS attack is a technique of exhausting connection resources by delaying communication after three-way handshake. In this paper, we analyze the effectiveness of Slow Read DoS attack by experiments in virtual network simulating real communication environment. We also propose a Synchronous Slow Read DoS attack method. From the analysis, we found that the communication speed and the Timeout of server affect the effectiveness of attack and we derive the optimal settings for proposed attack method. As the result, we confirmed that our method is more advantageous than previous schemes under the condition of the same total number of attack connections.**

***Index Terms*—Slow Read DoS attack, communication speed, timeout**

I. Introduction

In recent years, cyber-attack technique is sophisticated and the scale is increased [1], [2]. In this paper, we focus on DoS attack which is one of cyber-attacks having the purpose of stopping or obstructing services possessed by target Web server. DoS attack is an attack technique such as overflowing bandwidth and exploiting the vulnerability of the system. In particular, there is technique called Slow HTTP DoS attack which exploits TCP-based protocol vulnerability. This attack scheme makes the communication slow down and exhausts the resources of the target after establishing valid connection with the target server. As a result, legitimate clients will no longer be able to use resources and will not be provided services. Since this attack is against the application layer, it is difficult to detect in advance, and the main countermeasure is reducing the effectiveness of attack after detecting [3], [4]. In this paper, we pay attention to Slow Read DoS attack among Slow HTTP DoS attacks. This attack is developed by Sergey Shekyan in 2012 [5], [6], and several defense methods also have been proposed [7]–[11]. However, there is no effective method that can surely prevent. Paper [12] focuses on secure setting of the server but they do not consider the successful condition for the attacker.

In such previous works, an ideal environment for an attacker is assumed. It is appropriate to give favorable conditions to attackers in considering countermeasures. As the result, in the previous works, they assume that the communication environment is lossless. However, the actual communication environment is complicated due to various factors, which greatly affect not only the server but also the attacker. There are no previous works that assumed attacks in real communication environment and examined under what conditions efficient attack could be made.

In addition, attack by a single attacker is easily protected by security system like IP filtering. Paper [14] also shows the effectiveness of Slow Read DoS attack by multiple attackers. In that work, it is found that attacking by multiple people is effective for a Web server to which a security countermeasure are applied. However, it can be said that it is not realistic for the reason described above. In this paper, we conduct an attack experiment on a virtual network simulating actual communication environment, propose a more realistic attack method, Synchronous Slow Read DoS attack, and analyze its effectiveness.

II. Slow Read DoS attack and previous analysis

A. Mechanism of Slow Read DoS attack

Slow Read DoS attack is one of Slow HTTP DoS attacks that exhausts the connection resources of target server. This attack has following three steps.

1) The attacker establishes the connection to the target server using valid three-way handshake.
2) The attacker sends data request packet with the window size extremely small to the target server, and almost stops the communication. As the result, the target server is in the state of occupying the connection resource.
3) By repeating above procedure and occupying connection resources, the target server becomes impossible to provide any service.

This attack is difficult to detect because all packet is valid and there are no invalid protocols. Therefore, the target server cannot detect until they notice exhaustive consumption of connection resources. In order to release resources once occupied, the target server has to disconnect these attack connections or wait for forced disconnection by Timeout. On the other hand, WAF and ModSecurity [13] are common countermeasures against general DoS attacks. They mainly identify the attack by the speed of communication and the number of connections per IP address. However, the introduction of WAF is costly and ModSecurity has been reported to be vulnerable against “ Slow Read Distributed DoS attack [14] ” .

2379-1896/17 $31.00 © 2017 IEEE
DOI 10.1109/CANDAR.2017.21

B. Previous analysis

Park et al. measured the effectiveness of Slow Read Distributed DoS attacks focusing on server settings [14], especially Timeout and maximum number of simultaneous connections (MC). As a result, they derived theoretically infinite attack method by the next attacker starting to generate the connection at the time before the previous attacker's connection is forcibly disconnected. However, this has some problems that they do not consider the influence of the communication environment. In fact, there are various restrictions such as Round-Trip Time (RTT) and communication speed. In addition, Park et al. allow attackers to generate unlimited number of connections, but the number of connections for each client tends to be restricted by IP filtering. In this paper, we analyze the effectiveness of our proposal in a more realistic environment by considering RTT and communication speed.

III. Experiment environment and analysis of RTT

The value of RTT indicates the delay of communication and it is one of the factors which has great influence of the throughput. This value means the time it takes for a response to be returned after sending data to a receiver. Since RTT depends on the physical distance to the receiver, the number of devices to relay or transfer on the route, and the processing time thereof, fundamental improvement is difficult. If RTT is large, the actual throughput greatly slows down even though broad bandwidth and high speed communication.

We measured influence of RTT against effectiveness of Slow Read DoS attack. As an experiment environment, we constructed a virtual environment using VMware [15]. We use slowhttptest [16] as an attack tool and Apache HTTP server [17], [18] for the target Web server (TABLE. I).

TABLE I
Experiment environment

Parameter	Version or Value
Host OS	Windows 10 Home
Software for virtual environment	VMware Workstation 12.1.0 [15]
Guest OS	CentOS6.7
Memory capacity of guest	1GB
Attack tool	slowhttptest-1.6 [16]
Web server	Apache (httpd-2.2.15) [17]
Web page size	100KB

TABLE. II shows the parameters of the target Web server and attacker. In particular, as parameters related to experiments, Timeout is the time until the connection is forcibly disconnected, and MaxClients (MC) indicates the maximum number of simultaneous connections to the server. Also, number of attack connecntion is the total number of connections sent by the attacker to the server in one attack, connection rate is the number of connections sent per second in the number of attack connection, and window size is the data size that the attacker requests for the server.

Note that, since the simulator is executed on virtual environment, we cannot evaluate the influence of RTT exactly. We simulated RTT using virtual switch delay-option. From the above condition, the attack finishes in 10[sec]. When Slow Read DoS Attack is delivered, service unavailable state of Web server is detected when the number of attack connections is reached MC = 300. Figure 1 shows the result, and we can find that the all attack setting succeed from 15[sec] to 71[sec], and RTT does not affect the effectiveness of attack. These results are obviously from the mechanism of Slow Read DoS attack, however, difference in time until the target server is down from the starting of attack is caused by this fact. In some attack scenarios, the difference will cause attack fail. In this paper, we do not consider the exact time schedule of attack, we can conclude that RTT is negligible in the followings.

TABLE II
Parameter of experiment

	Parameter	Value
server	Timeout	60 sec
	MaxClients	300
attacker	Number of attack connection	500
	Connection rate	50 [/sec]
	Window size	0 Byte
	Communication speed	1Mbps
	RTT	10ms (domestic)
		100ms(domestic-EU)
		200ms(domestic-US)

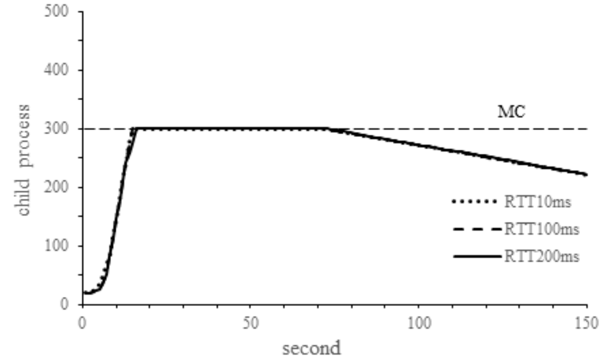


Fig. 1. Effectiveness of Slow Read DoS attack and RTT

IV. Synchronous Slow Read DoS attack

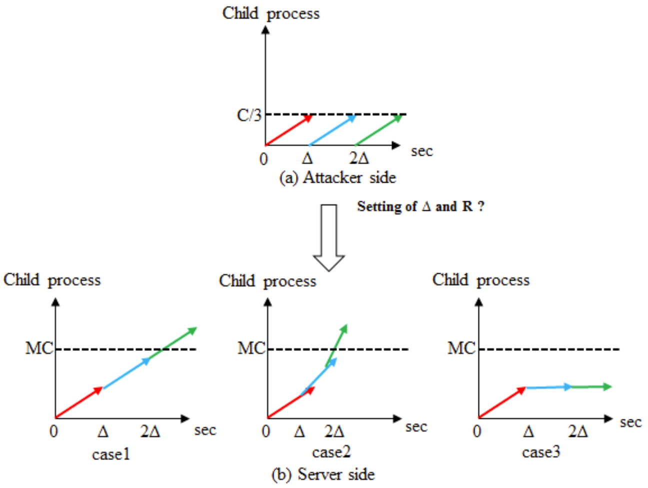
We propose a new method, “ Synchronous Slow Read DoS attack ” . The basic strategy is same as Slow Read Distributed DoS attack, but while Park treats attacker based on unit, our proposal method is based on individual. Therefore, there is big difference in attack scenario, but to pay attention to influence of communication environment. However, comparing with Park's Slow Read Distributed DoS attack [14], it has following important different conditions.

Total number of attack connection is restricted. In paper [14], they increased the number of each attacker's connection until successful attack, however, it will be easy to detect by the target server. On the other hand, we set enough total number of attack connections beforehand, and distribute to each attacker equally.

Timeout is set as default value. In paper [14], they set Timeout as attacker profitably. We set it reasonable value, focusing on 60 [sec] which is the default value of Apache.

Connection speed is considered. In paper [14], they did not consider the delay caused by RTT and communication speed. As already shown in section 3, RTT does not have significant influence to Slow Read DoS attack in the original attack scenario. Therefore, we should consider the influence of communication speed.

Figure 2 shows the outline of proposed attack with three attackers. Figure 2(a) shows the attacker side strategy. Let Δ be an interval time between previous attacker and next attacker. Figure 2(b) shows different patterns of the increment of connection in the target server.



(a) Attacker side

(b) Server side

Fig. 2. Outline of proposal with three attackers

- case1: This is the optimal case. Repeating the attack with time-interval of 3Δ, the target server is in infinite denial-of-service state following Park's strategy [14]. And the risk of attack detection can be minimized. However, this situation can only be achieved in loss-less communication environment.
- case2: This case will be caused when time interval is set faster comparing with communication speed. Although this case success the attack, the attack will be easy to detect because of abnormal increment of connection packets.
- case3: This case will be caused when time interval Δ is set slower comparing with communication speed. This case never success the attack.

In addition, connection rate R of attacker and Timeout T of the target server are significant factors for effectiveness of attack. Our proposal attack method, is parameterized using number of attacker, total number of attack connection C, time interval Δ, connection rate R, communication speed X, Timeout T, and MC of the target Web server.

V. Experiment

A. Purpose of experiment

As shown in section 3 and 4, communication environment affects the effectiveness of attack. Since these conditions are given, there is no chance for the attacker to improve them for successful attack. Therefore, the attacker has to adjust the value of Δ and R (see Figure 2(b)). On the other hand, the target server is also affected of X, but they can oppose on attack by MC, T and processing power (generating child processes for connection per second). The value of MC can be set intentionally, but processing power depends on the specification of server. Since the value of MC has influence to QoS, it is set as relatively large. In our experiments, we set them as TABLE. III.

TABLE III
Parameter of experiment environment

Parameter	Value
Number of attackers	3
Total number of attack connection C	1,500
Time interval $\Delta[sec]$	10, 20, 40
Connection rate $R[/sec]$	20, 40, 60, 80
Communication speed $X[bps]$	100K, 500K, 1M
Timeout $T[sec]$	30, 60(default), 90
MC of server	1,200

For the value of T, the default setting of Apache is 60. In addition, we set 30 and 90 for comparison. For the value of X, we set 100K, 500K and 1M. Because of the limit of performance of VMware, we set connection rate $R = 20, 40, 60, 80$. In addition, we set three attackers with $\Delta = 10, 20, 40$.

Under the above conditions, we observe the maximum number of connections using C. As already shown in Figure 2(b), if the maximum number of connections cannot achieve MC, the attack clearly fails. On the other hand, if the attacker success to reach MC once, they will be able to apply Park's strategy [14] and make their attack succeed infinitely. Therefore, in the followings, our purpose of experiment is to observe the maximum connection number of attacker under those conditions.

B. Experiment results

Timeout 60 (default setting of Apache). From the result shown in Figure 3, we can find easily that any attack under the condition in $X = 100K[bps]$ always fail. And the attack with $\Delta = 40$ always fails attack, because of too late connection feedings. In the case of $X = 500K[bps]$, too high connection rate will defeat its own purpose. From these results, we can conclude as follows.

Property-1: $X = 100K[bps]$ is secure against Slow Read DoS attack and any settings of Synchronous Slow Read DoS attack.

Property-2: $\Delta = 40$ is too late for any communication speed.

Property-3: R between 20 and 40 with $\Delta = 10, 20$ will be appropriate.

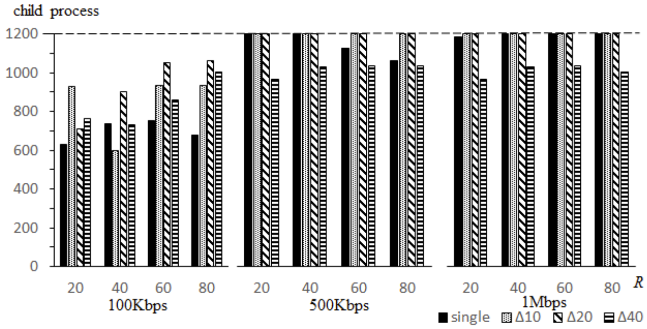


Fig. 3. Experiment result of Timeout 60

Timeout 30. We expected that setting of short T will make sever secure against Slow Read DoS attack, and we can also confirm that. From the results shown in Figure 4, all settings fail attacks. The setting of $\Delta \geq 20$ is too late for connection feeding and $X = 100K[bps]$ to secure against any settings in the same case of $T = 60$ (Property-1). However, as already mentioned above, short T settings are quite wrong QoS, such situation is not realistic also for attacker.

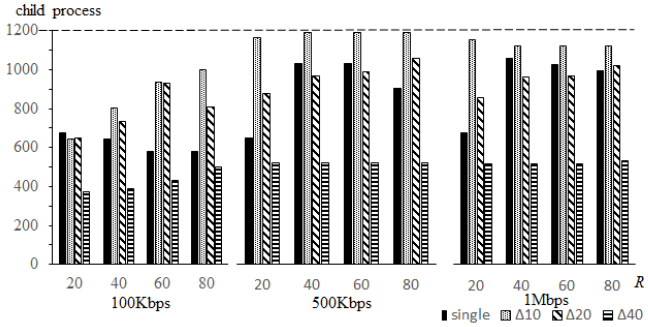


Fig. 4. Experiment result of Timeout 30

Timeout 90. Figure 5 shows the experimental result with $T = 90$. This setting is user-friendly and it will be easy to attack. Therefore, even if $X = 100K[bps]$ (Property-1), appropriate choice of combination of R and Δ, the attack will succeed. In this experiment, it succeeds when $(R, \Delta) = (60, 40), (80, 20), (80, 40)$. And when X is higher than $100K[bps]$, all settings of R and Δ success the attack. On the other hand, there are some failure cases for single attacker with high connection rate (e.g. $R = 60, 80$). From the results, too high R will defeat the effectiveness. Through the case of experiment, we can find that Property-1, Property-2 and Property-3 hold. In particular, Property-1 holds in almost cases. Therefore, $X > 500K[bps]$ is necessary condition for Synchronous Slow Read DoS attack. The setting of Δ (Property-2) depends on X, however, we concluded $\Delta \geq 30$ in almost useless for any communication environment and server settings. Therefore, we conclude that Property-3 shows the most appropriate setting range ($20 \leq R \leq 40, 10 \leq \Delta \leq 20$) for Synchronous Slow Read DoS attack. Detailed analysis is shown in next section.

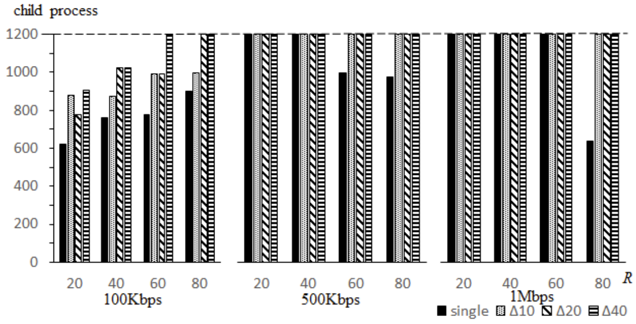


Fig. 5. Experiment result of Timeout 90

VI. Discussions

A. *Influence of communication speed*

Slow Read DoS attack is to make window size intentionally small, and communication is stopped, so the influence by which communication speed gives it to the effectiveness of attack seems small. However, we can easy to see the influence from the experiment results shown in section 5. It is three-way handshake that communication speed is related directly in the procedure of Slow Read DoS attack. Communication line is established between attacker and the target server by a valid protocol certainly here. Therefore, bandwidth is occupied, so it has influence on timing in delay of other communication requests from attacker. Obvious influence could not be found from our experiment results, however, it is clear to have influence on the effectiveness of attack by a relation between the specification of target server and communication environment. The detailed analysis is our future work. We consider communication speed also has an influence on choice of effective connection rate. We discuss this problem in later section.

B. *Advantage of multiple attackers*

Almost of all attack results show that the effectiveness of attack by multiple attackers are obviously greater than one by single attacker. There are many cases which are impossible to attack by single but are feasible by multiple attackers. Therefore, we can conclude that our Synchronous Slow Read DoS attack is more effective than general Slow Read DoS attack. However, we need to adjust the interval time Δ for the effectiveness.

For example, $\Delta = 40$ for $T = 30$ condition is always lower effective than single attack. In the case of single attack, the resource of target server is occupied continuously. On the other hand, in the case of $\Delta = 40$, because it is slower than T, the resources occupied by the first attacker are forcibly disconnected before start of third attacker. For example, in the case of $R = 40$, and $T = 60$, single attacker can generate 1500 connections after 37.5 [sec] in theoretically. Since disconnection rate by server after T equals to $R = 40$, the number of occupied resources decrease 40 connections per seconds. Thus, after 80 [sec] from attack start, 700 of connections for attack remain on the target server. On the other hand, for our Synchronous Slow Read DoS attack, since each attacker has 500 of connection per attack, each attacker ends attack after 12.5 [sec]. Then, 2nd attacker starts after 40 [sec], and ends after 52.5 [sec]. At this time, the target server is occupied until 1,000 of attack connections. But, before 3rd attacker starts after 80 seconds, the disconnection by Timeout starts. Therefore, at 80 [sec], the number of attack connection decrease 300 connections, and continuous decreasing.

As the result, the attack under the condition of $\Delta = 40$, the number of connection in the target server does not increase effectively. As the result, the attack under $\Delta = 40$ will be almost useless against target server.

C. Effectiveness of short Timeout

From the results shown in Figure 4, we can conclude that short T setting makes the server secure against Slow Read DoS attack. It is effective irrespective of X and R of attacker. However, such counter measure also decreases QoS. Therefore, we can conclude that it is not a fundamental countermeasure.

D. Effectiveness of connection rate

It is obvious that low connection rate has no effect on attack (see Figure 2, case 3). On the other hand, high connection rate also has little effectiveness (see Figure 3 and Figure 4). The following two factors are considered as the reasons.

- Generation rate of child process for connection in the target server (processing power of server)
- Communication speed

Since the processing power of server depends on the specification of HW of server, there are some limitation in it. We can expect that the optimal attack is executed when R of attack and processing power of server are almost equal. On the other hand, when R is larger than processing power, exceeded connection requests from attacker which cannot be processed by server are held in request queue and they are not processed immediately. When request queue become large, they will be disconnected by T before connection to server, then such connections become wasteful. As the result, high R will be useless for the attack.

It is obvious that X has an influence on the effectiveness of attack from the results shown in section 5. Since the C from attacker in decided by the X, we expect that connection request beyond it fail in process by server and are lost. Our additional experiments show that $20 \leq R \leq 40$ is optimal range for almost case of X.

E. Improvement

In our attack experiments, we set the condition of three attackers and $C = 1,500$ to simply the observation. From the conclusion in [14], it is obvious that condition of more number of attackers and more C is more favorable to attack. From that point of view, since our experiments are small scale, we only point out the possibility of threat scenario. The analysis of realistic threat by large scale attack is our future work.

VII. Conclusion

In this paper, we analyzed influence of communication environment to effectiveness of attack by experiments using virtual network. We focus on RTT and communication speed, we concluded that RTT has little influence and communication speed is a significant factor. From the experiment results, we concluded $20 \leq R \leq 40$ of attacker is optimal for almost communication environment. Therefore, we derived the realistic successful attack condition comparing Park's policy [14] which can make R larger and larger. And we confirmed that, in almost cases, Synchronous Slow Read DoS attack has more effective the single attacker, under the condition of same number of total attack connection.

In theoretically, our proposal attack method can make the target server in infinite-service unavailable state. Under the real network, the simulation and analysis of attack against real server are our future work. In real threat scenario, Slow Read DoS attack is effective for opportunity loss such as online trade. In such cases, we need correct time to starting effectiveness of attack, it is necessary to analysis of delay factor which is caused by RTT and three-way handshake. This analysis is also our future works.

References

[1] D. Antsee, P. Bowen, C.F. Chui, G. Sockrider, "Worldwide Infrastructure Security Report Volume 11" Arbor Networks, Burlington, 2016.

[2] Survey on countermeasures against denial of service attacks. IPA, Japan, 2010.

[3] Researcher devises hard-to-detect DoS attack against HTTP servers, http://www.infoworld.com/article/2618359/security-management/researcher-devises-hard-to-detect-dos-attack-against-http-servers.html, last accessed 2017/5/14.

[4] T. Hirakawa, K. Ogura, B.B. Bista, T. Takata, "A Defense Method against Distributed Slow HTTP DoS Attack" 19th International Conference on Network-Based Information Systems, pp. 152-158. IEEE, Ostrava, 2016.

[5] Qualys Blog, https://blog.qualys.com/securitylabs/2012/01/05/slow-read, last accessed 2017/5/14.

[6] New Denial-Of-Service Attack Cripples Web Servers By Reading Slowly, http://www.darkreading.com/attacks-breaches/new-denial-of-service-attack-cripples-web-servers-by-reading-slowly/d/d-id/1136886?, last accessed 2017/5/14.

[7] N. Tripathi, N. Hubballi, Y. Singh, "How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection" 11th International Conference on Availability, Reliability and Security, pp. 454-463. IEEE, Salzburg, 2016.

[8] J.J. Li, T. Savor, "Detecting DoS Attacks on Notification Services" IEEE Eighth International Conference on Software Security and Reliability-Companion, pp. 192-198. IEEE, San Francisco, 2014.

[9] How To Mitigate Slow HTTP DoS Attacks in Apache HTTP Server, https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/, last accessed 2017/5/14.

[10] Slow DoS attacks: definition and categorization, http://www.inderscienceonline.com/doi/ref/10.1504/IJTMCC.2013.056440, last accessed 2017/5/14.

[11] E. Cambiaso, G. Papaleo, M. Aiello, "Taxonomy of Slow DoS Attacks to Web Applications" International Conference on Security in Computer Networks and Distributed Systems, pp. 195-204. Springer, Thiruvananthapuram, 2012.

[12] J. Park, K. Iwai, H. Tanaka, T. Kurokawa, "Analysis of Slow Read DoS attack" 2014 International Symposium on Information Theory and its Applications, pp. 60-64. IEEE, Melbourne, 2014.

[13] ModSecurity, http://www.modsecurity.org/, last accessed 2017/5/15.

[14] J. Park, K. Iwai, H. Tanaka, T. Kurokawa, "Analysis of Slow Read DoS Attack and Countermeasures on Web servers" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(2), 339-353, 2015.

[15] VMWare, https://my.vmware.com/jp/web/vmware/details?productId=524 &downloadGroup=WKST-1210-WIN, last accessed 2017/5/15.

[16] Slowhttptest, https://github.com/shekyan/slowhttptest, last accessed 2017/5/15.

[17] Apache HTTP server project, http://httpd.apache.org/, last accessed 2017/5/15.

[18] W3Techs - World Wide Web Technology Surveys, https://w3techs.com/, last accessed 2017/5/15.