Development of protection mechanisms against DRDoS-attacks and combined DRDoS-attacks

Yana Bekeneva[1], Andrey Shorov[2]
Saint Petersburg Electrotechnical University "LETI", St-Petersburg, Russia
[1]Corresponding author
E-mail: [1]*yana.barc@mail.ru*, [2]*ashxz@mail.ru*

Received 25 April 2017; accepted 26 April 2017
DOI https://doi.org/10.21595/vp.2017.18546

Abstract. Distributed "denial of service" attacks based on the traffic reflection and amplification (DRDoS attacks) still are a powerful threat for computer networks. More than half of all attacks were executed by using multiple types of attacks. Development of new protection mechanisms against such attacks is one of the most important tasks in the field of computer security. In this paper, we present experiments on DNS attack, NTP attacks and combined DRDoS-attack simulation. We simulated several protection mechanisms as well as a mechanism developed by us. We compared these protection mechanisms for different kinds of attacks.

Keywords: DRDos-attacks, combined attacks, simulation, reflection attacks, amplification attacks, DNS attack, NTP attack.

1. Introduction

Distributed "denial of service" attacks based on the traffic reflection and amplification (DRDoS-attacks) still are a powerful threat for computer networks. Those kinds of attacks are executed as follows. The attacking nodes generate some requests where the source IP address is replaced by the IP address of the attacked host. These requests are sent to servers or other devices that may be used to reflect network traffic. The replies to these requests are sent to the target node. The mechanism of traffic reflection increases the complexity to identify the real source of the attack.

According to reports [1], in 2016 the total number of DDoS-attacks increased significantly, those attacks became more powerful than before. More than half of all attacks were based on UDP protocol. The most common attacks were based on traffic amplification, such DNS, NTP, SSDP and Chargen attacks. It is also noted that more than 60 % of all attacks were executed by using multiple types of attacks. As the most frequently attacked services cloud environments, web-financial corporations, political organizations, online commerce, media and entertainment companies, as well as telecommunications are mentioned. Not only the important user's documents stored in the cloud are in danger, but the financial health of users of online banks and online stores is in danger as well. According to analysts, in 2017 it is expected that DDoS-attacks will become more and more powerful and complicated, their total number is supposed to increase [2].

Development of new protection mechanisms against such attacks is one of the most important tasks in the field of computer security. The tendency to execute various types of attacks in a single attack increases the requirements on the mechanisms of abnormal traffic detection. The mechanism of traffic reflection makes the identification of the real source of the attack more complicated, as for victims of computer attacks source is used to reflect the server, which a priori is a legitimate site. Therefore, protection methods for traditional DDoS-attacks are unable to adequately detect DRDoS-attacks and to identify the sources of these attacks. When using only traffic reflection, it is impossible to achieve the high power, but some vulnerabilities of specific protocols allow to amplify reflected traffic, thereby significantly increasing the attack power. There are some requests causing responses which are several times larger than requests. Thus, attackers do not need to send a large amount of traffic for the successful implementation of the attack, but to send the requests of small size, while having the desired effect. Record values of attack power were achieved by the attacks based on the traffic reflection and amplification [2].

In [3] 14 popular protocols that can be used to implement traffic attacks with amplification were described. These protocols are based on UDP. Existing protection mechanisms against DRDoS-attacks are mainly been developed for the DNS-attack. They can be used for other types of DRDoS-attack with appropriate modifications. Furthermore, the use of certain methods for protection against multiple types of attacks may require large volume of memory. It is therefore necessary to develop protection methods against any DRDoS-attacks without requiring a large amount of resources taking into account not only the reflection realization in general, but also the characteristics of each type of attack.

In this paper, we propose a new method of protection against DRDoS-attacks, carried out experiments to test its effectiveness in comparison with existing methods.

2. Related works

Nowadays, many groups are doing research related to the investigation of DRDoS attacks and protection mechanisms against them.

In [4] the authors propose a protection method, that is based on the fact that the victim receives more replies than requests were sent. Their protection mechanism is called DNS Amplification Attacks Detector (DAAD). The authors propose to monitor to which DNS servers the requests were sent from each node and store the information in a database. All replies from a DNS server are checked and if the incoming packet is really a reply to the request it will be accepted. If the node did not send the DNS request, the response is rejected.

The authors of [5] propose to install a preliminary DNS resolver and create a tunnel using IPSec or the SSL protocol between the preliminary resolver and the DNS resolver on the client side. All external DNS requests arrive at the preliminary DNS resolver and cannot directly enter the client’s DNS server from external sources.

In [6] a mechanism called Response Rate Limiting (RRL) is outlined. It is designed to limit the number of unique responses from the DNS server. This protection mechanism is used on the DNS server side and analyzes outgoing traffic only. It completely ignores the incoming traffic. The method bases on the fact that the addresses to which the replies were sent are recorded. The number of replies from the server to each address is limited. If this limit is exceeded, no answers will be sent.

In [7] a method based on the detection of traffic deviation with respect to a template is proposed. The authors analyzed the number of incoming packets of the DNS protocol as well as their size. If the number and size of the packets exceed a predetermined value, the situation is recognized as an attack.

In this paper, we compare the performance of some of the protection mechanisms against DRDoS attacks using the developed simulation library. We also offer a protection mechanism against DRDoS attacks which has been designed using our simulation library [8]. Experiments have shown that the developed protection mechanism is quite versatile and an effective method to protect against DRDoS like attacks.

3. Experiments

In this section, we discuss experiments on reflection attacks and protection mechanisms against them.

To perform the experiments, a simulation environment described in [8] was used. This system is based on discrete event simulation system OMNeT ++, as well as libraries INET and ReaSE. The system allows to create scripts of user’s behavior as legitimate and malicious traffic, and also to create models of different servers and implement the mechanism of traffic reflection and amplification. The authors have created models of various types of servers used to reflect traffic. For any protocol, we have developed the models of legitimate traffic and attack traffic, taking into account differences in the packet header and a data field. Depending on the request content different responses are generated, including in some cases traffic amplification is realized.

For our experiments, we have chosen the DAAD and the RRL methods since they have different location and they are based on different rules.

In the simulation, the DAAD method has a database, which stores the destination address of the DNS-requests are sent from the local network. After receiving a DNS-packet, the source address is checked against the record in the database. If there is such address in the database, the packet is passed, and the entry is deleted from the database. Adding a new record to the database takes into account only the fact of sending a request from a particular source address to the particular destination address using a particular port.

The RRL protection mechanism is used on the server side that is used for reflection and analyze outbound traffic only. The destination addresses are recorded. The number of responses for each address are limited. If the threshold is exceeded, the answers to this address are no longer available. In this experiment threshold was 1000 packets, locking time of 5 seconds.

3.1. Experiments on DNS-attack simulation

At first, we describe a reflection attack with small amplification. The protection mechanisms against such attacks, namely DAAD and RRL, as well as our protection mechanism were run.

The attack power was 6.7 Mbit/s. Legitimate and attacking nodes were located in several local networks, traffic reflection was performed by 3 DNS servers. The amplification factor was 3.5. Throughout the experiment the attacked nodes generated legitimate DNS-requests to different DNS servers. The figures show the false positive errors (FP) Fig. 1 and false negative errors (FN) Fig. 2.

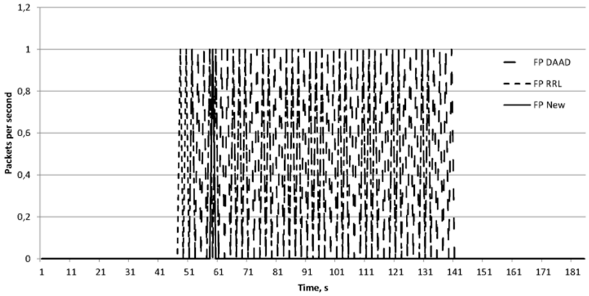

Fig. 1. False positive for DAAD, RRL and proposed approach against DNS reflected attack

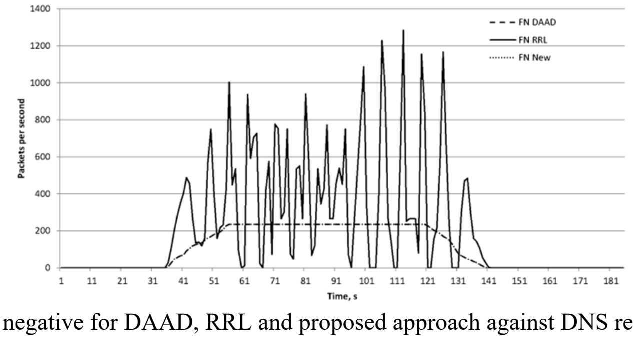

Fig. 2. False negative for DAAD, RRL and proposed approach against DNS reflected attack

The DAAD method does not analyze the request type and its content. Similarly, after receiving the responses they are not analyzed by the type and their contents. The main factor is the number of requests sent from a particular node. The reason of the errors is follow. If the victim server sends a legitimate request to a DNS-server its address is stored to the database. If the same

DNS-server is used for traffic reflection, the malicious packet can be passed since it has the source address stored in the database. If the legitimate response comes after passing the malicious packet there is no more entry with such source address and this legitimate packet is blocked.

The experiment showed that the proposed algorithm using all legitimate answers to requests reached the goal, in case of incorrect locking package occurred only once, and the error of the first kind is practically absent. The presence of a certain number of packets received incorrectly due to the fact that present components, generating requests attacking the attacked network server. Since the source address was changed to the address of the victim, then these requests, leaving local network have been fixed, and the answers to them are regarded as legitimate.

The RRL method also analyze the content of outgoing packets and the restriction is only the number sent to the same address of the packet. Thus, all malicious packets are passed until a threshold value is reached. Moreover, if during the lockout the responses to legitimate requests are sent, the answers to them are blocked. The response period and the threshold may vary, however, increasing the threshold will increase number of passed malicious packets. In contrast, decreasing the threshold may increase the number of blocked legitimate packets. Increasing the blocking time will also lead to the false positive error. Reducing this period will allow a greater number of malicious packets reach the goal.

Therefore, almost all legitimate packets reached their destination node because the proposed mechanism analyses not only the event of sending packets by vulnerable protocol but the type of request. It helps to differ packets by the type and no to allow amplified responses to pass instead of responses to standard requests. We put some attacking nodes in the same network as the victim server, the spoofed requests of such nodes were rated as legitimate and the responses to them were rated legitimate as well. Therefore, it caused the false negative error.

3.2. Experiments on NTP attack simulation

Further experiments of the attacks simulation implementing traffic reflection with amplification were performed. As an example of such an attack NTP type of attack it has been performed. The simulated attack power was 127 Mbit/s. Legitimate and attacking nodes were located in several local networks, traffic reflection carried out with the help of three NTP servers. The amplification factor was 37. During the entire time of the experiment the attacked node generate NTP-legitimate requests to one NTP server. Since NTP legitimate traffic is usually small, the number of missed incoming packet does not exceed the number of outbound and was accordingly low. However, there are some false positive and false negative errors.

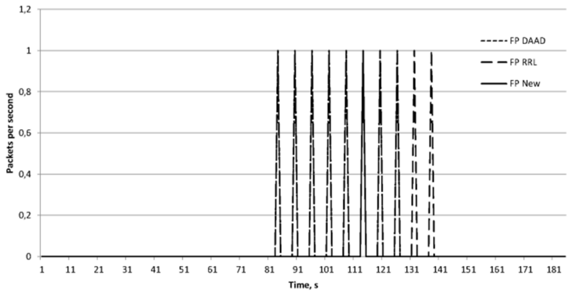

Fig. 3. False positive for DAAD, RRL and proposed approach against NTP reflected attack

The figures show the false positive errors (FP) Fig. 3 and false negative errors (FN) Fig. 4.

The reason of the errors is the same as discussed in the section dedicated to the modeling of the DNS protocol attacks. Obviously, the attack based on the reflection, represent a serious threat to the computer networks. It is therefore necessary to develop methods for their detection and improve their accuracy. As can be seen from Table 1, the proposed method in the experiments showed the same kind of error 2, compared with the method of the DAAD. However, for the attack scenarios, the proposed method showed the best result by mistake one kind.

For the attacks based on NTP protocol, similar results were obtained. We compare the results. As can be seen from Table 2, the proposed method showed again the same result for false negative error as DAAD but showed the best result for false positive. It means that during the attack there were almost no blocked legitimate packets.

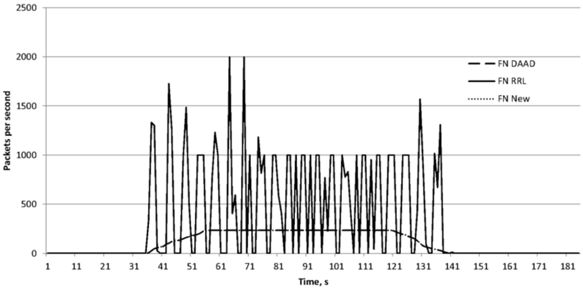

Fig. 4. False negative for DAAD, RRL and proposed approach against NTP reflected attack

Table 1. Comparison of FPR and FNR for protection mechanisms against DNS attack

	FPR	FNR
DAAD	0.54	0.15
RRL	0.31	0.29
New	0.01	0.15

Table 2. Comparison of FPR and FNR for protection mechanisms against NTP attack

	FPR	FNR
DAAD	0.4	0.012
RRL	0.5	0.03
New	0.05	0.012

3.3. Experiments on combined attack simulation

As an example of a combined attack we executed an attack consisting of two types of DRDoS-attacks: DNS and SSDP. To reflect traffic 3 DNS-servers and 4 SSDP devices were used. Their models have been developed and implemented by the authors. The attack power was 8 Mbit/s. The attacked server generates legitimate traffic by both used protocols. We tested the effectiveness of proposed protection mechanism and compared it only with the DAAD method.

The figures show the false positive errors (FP) Fig. 5 and false negative errors (FN) Fig. 6.

Table 3. Comparison of FPR and FNR for protection mechanisms against combined attack

	FPR	FNR
DAAD	0.03	0.25
New	0.006	0.2

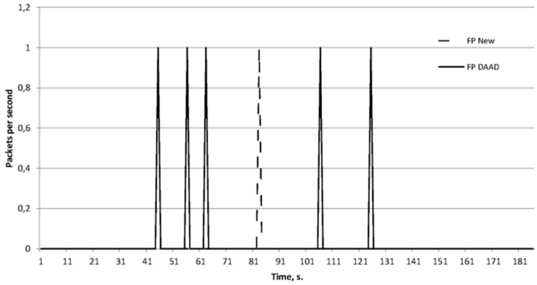

Fig. 5. False positive for DAAD and proposed approach against combined reflected attack

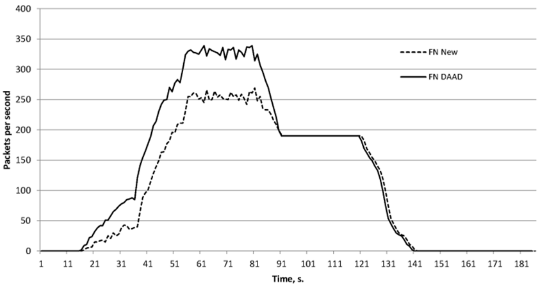

Fig. 6. False negative for DAAD and proposed approach against combined reflected attack

4. Conclusions

The obtained results show that due to more accurate analysis of packet parameters the method proposed by the authors has the best result for the combined attacks. The proposed method has been developed to protect the networks against the maximum possible types of DRDoS-attacks and contains the parameters of the legitimate and non-standard traffic for each of the specified protocol. The DAAD is based on traffic symmetry and filters packets based only on parameters such as addresses and source and destination ports. However, both methods show a quite high false negative error because some of malicious nodes are located on the same local network as the victim server. Outgoing malicious requests with spoofed source address are marked as legitimate, so the responses to them are allowed. Thus, the mechanism of outgoing traffic filtering is necessary to substantially modify in order to reduce the errors and make the computer networks more protected from malicious actions. It can be concluded that the proposed method by the authors is quite effective to protect computer networks against DRDoS-attacks, but is intended to identify only attacks based on the reflection. In cases when the combined attack includes other types of attacks, including direct DDoS-attacks, it is necessary to use additional methods of traffic analysis.

Acknowledgements

This work was supported by the Ministry of Education and Science of the Russian Federation in the framework of the state order “Organization of Scientific Research”, Task #2.6113.2017/6.7.

References

[1] Verisign Distributed Denial of Service Trends Report. https://www.verisign.com/assets/report-ddos-trends-Q42016.pdf.

[2] **Hickey A.** Report: 1 Tbps DDoS Attacks to Increase 500 Percent in 2017. URL: https://www.a10networks.com/blog/tbps-ddos-attacks

[3] **Rossow C.** Amplification hell: revisiting network protocols for DDoS abuse. Symposium on Network and Distributed System Security (NDSS), 2014, http://www.internetsociety.org/sites/default/files/01_5.pdf.

[4] **Kambourakis G., et al.** Detecting DNS amplification attacks. Critical Information Infrastructures Security, 2008, p. 185-196.

[5] **MacFarland D. C., Shue C. A., Kalafut A. J.** Characterizing optimal DNS amplification attacks and effective mitigation. Passive and Active Measurement Conference, New York, 2015, p. 15-27.

[6] **Rozekrans T., Mekking M., de Koning J.** Defending against DNS reflection amplification attacks. University of Amsterdam, Technical Report, 2013, https://nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf.

[7] **Huistra D.** Detecting reflection attacks in DNS flows. 19th Twente Student Conference on IT, 2013, http://referaat.cs.utwente.nl/conference/19/paper/7409/detecting-reflection-attacks-in-dns-flows.pdf.

[8] **Bekeneva Y., Shipilov N., Shorov A.** Investigation of protection mechanisms against DRDoS attacks using a simulation approach. 16th International Conference on Next Generation Wired/Wireless Advanced Networks and Systems New2AN, St-Petersburg, 2016, p. 316-325.