Journal of Engineering and Applied Sciences 12 (3): 475-480, 2017
ISSN: 1816-949X


# Effective Amplification Mitigation and Spoofing Detection During DNS Flooding Attacks on Internet

Dana Hasan, Masnida Hussin and Azizol Abdullah
Faculty of Computer Science and Information Technology,
University Putra Malaysia (UPM), Selangor, Malaysia

**Abstract:** Recent flooding attacks using Domain Name System (DNS) is used by cybercriminals to launch hundreds of gigabytes of attack traffic to paralyze their victims. The lack of security features in DNS protocol and adding security layers to this protocol is subject of further studying. In this reserach, we proposed a distributed mechanism to counter DNS reflection based attacks with high detection accuracy and little overhead on network channels. We suggested Distributed Defense Scheme (DDS) to provide authenticity to DNS transactions (i.e. request and response) through authentication message exchange. Then our classification filtering plays an important role in distinguishing between real bogus DNS requests and discarding the fake requests. Our analysis shows how DDS can remarkably reduce amplification factor for attack traffic without affecting normal traffic flow.

**Key words:** DNS security, DNS reflection/amplification attacks, DNS authentication, authentication message, classification filtering

## INTRODUCTION

Domain Name Service (DNS) is an important part of internet infrastructure that translates domain names into IP addresses and vice-versa. It is a distributed, hierarchical system for naming computers, resources or services linked to a local network or the Internet (Anagnostopoulos *et al*., 2013; Bilge *et al*., 2011). Any unavailability of such service causes big impairment on the internet which leads to catastrophic results. DNS queries mostly rely on User Datagram Protocol (UDP) packets which is connectionless protocol. It requests with one packet and in most of the times responds with one packet (Anagnostopoulos *et al*., 2013; Ye and Ye, 2013) which leads to source authentication issue. Furthermore, filtering mechanisms do not provide complete separation and identification of legitimate UDP packets and the fraud packets. Which results network communication path from upstream networks to user/victim is flooded with bogus traffic because of the DNS amplifies responses (MacFarland *et al*., 2015).

In this research, we propose classification-based filtering to identify and detect DNS reflection/ amplification attack. Our defense mechanism is supported by DNS authentication message exchange process where each DNS request query is examined before providing any response. Our classification-based defense mechanism able to distinguish between legitimate and fraud packets with better detection accuracy and reduces processing overhead.

DNS reflection/amplification is a method used to perform Distributed Denial of Service (DDoS) attacks. By using DNS server as a resource, DDoS had been used by attackers to take down the network infrastructure and resources. It occurs when an attacker sends DNS name resolution requests to DNS servers with spoofed source address that impersonate as the target's IP address. When DNS server sends back the response, it forwards it to the target instead. Typically, attackers will submit a request for as many zones information as possible to maximize the amplification effect. Due to the size of the response which is significantly larger than the request, the attacker can raise the amount of traffic directed to the victim. The attacker uses a Botnet to produce a large number of spoofed DNS requests (Marrison, 2014; Zargar *et al*., 2013).

Hence, the network traffic becomes congested and busy. Typically, attackers submitted the request to many domains as possible for enlarging amplification effect. Therefore, many researchers, such as (Liu *et al*., 20 15; Kambourakis *et al*., 2007; Zargar *et al*., 2013) used amplification factor for calculating the attack strength. It is the ratio between the traffic volume of response packets and request packets. Higher the amplification factor results in further bottleneck and delay in a communication network.

**Corresponding Author:** Dana Hasan, Faculty of Computer Science and Information Technology,
University Putra Malaysia (UPM), Selangor, Malaysia

To launch DNS reflection/amplification attack, two tasks executed by the attacker. First, the attacker needs to spoof the victim's IP address to make the traffic heavy loaded. By spreading the task, the attacker achieved reflection and causes all the replies from the DNS server to be directed to the victim's server. The second task is that the attacker seeks for the responses that are several times larger than the request. Hence, the higher amplification factor is achieved. More significant amplification also can be accomplished when DNSSEC signatures are used where it leads to increase the size of the response (Rozekrans *et al*., 2013).

**Literature review:** The researchers in Rossow (2014) proposed the mechanism to reduce the amplification factor by increasing the request query size and disabling responses to some Resource Records (RR) (i.e., "ANY"). The advantage of the mechanism is it reduces the amplification factor to a certain level. However, the increase in traffic across the Internet would not be desirable. Also disabling (RR) cause services which depend on the disabled records stop working. In addition to lowering amplification factor, the amplifiers might need to be configured in order to respond to a limited number of requests from each IP or network address within a given time frame. Response Rate Limiting (RRL) is a technique protects against using authoritative name servers to be used as amplifiers. However, when the attack traffic gets sophisticated (for example by sending the attack traffic from a botnet with low request rate), it does not take much effort to find a sufficient number of different amplifiers to perform a reflective DDoS attack. Also, this mechanism can only be applied to authoritative name servers, and it is not applicable for recursive servers (Rossow, 2014).

Koc *et al.* (2012), they suggested new and alternative Internet architecture for preventing illegal access to the network communication; called Content-Centric Networking (CCN). It removes any existing of DNS reflection/amplification attacks, results that DNS is not required in this architecture. While deploying CCN, ISPs can launch content routers to cache data that requested by many users. However, CCN utilizes the request/response model in the form of "Interest" and "Data" packets. It is currently hard to know how flexible the network architecture to amplify the future attacks or other forms of DDoS attacks.

Usually, by the time flooding attack is detected, there is nothing that can be done except to disconnect the victim from the network and manually fix the problem. All of the flooding attacks waste a lot of resources (e.g., processing time, space and other resources) on the communication paths. Hence, the ultimate goal of any defense mechanism is to detect them as soon as possible and stop them as near as possible to their sources (Zargar *et al*., 2013). There are two main types of defense mechanisms are centralized and distributed.

Centralized defense mechanism depends on single-node deployment either it is source-based, destination-based or intermediate_network-based deployment. Basically, the source-based deployment is organized near to the source of the attack and prevent network users from suffering flooding attacks. The benifit of the method is that it can filter and respond (i.e., monitor) the communication traffic at the source, hence prevent any network attacks come into the resources. However, the sources are distributed among different domain. Therefore, it is difficult for each of the sources to detect and filter attack flows accurately. Also, it is hard to differentiate legitimate and DDoS attack traffic at the sources, since the volume of the traffic is limited. In the destination-based deployment, the detection and response procedures are mostly prepared at the attack destination. It is easier and cheaper than other deployment methods in DNS transaction with most accurate capabilities. The drawback is that when the attack is detected, upstream networks and resources are suffering starvation because of the attack traffic (Zargar *et al*., 2013). The intermediate-network-based deployment is launched within intermediate networks at Autonomous Systems (AS). The advantage is it can detect and respond to the attack flow at the intermediate networks where it close to the source as possible with better acceptable accuracy. However, it causes high storage and processing overhead at the AS routers (Zargar *et al*., 2013). Also, the detecting procedure is difficult to implement due to the challenge in determining the accurate communication traffic that resides by the network attack.

The distributed defense mechanism is the approach that use defensive strategies from various distributed components in the network (i.e., source, destination and intermediate network). Same as the target in the centralized defense mechanism where is to monitor the incoming fraud in the communication network. It is required cooperation between the multiple nodes to achieve better monitoring policy to protect against the attack. Furthermore, a trust communication among nodes is needed to gain accurate information on traffic and fraud that are currently running in the network. Resources are available at various levels (source, destination, intermediate networks). Therefore, distributed mechanisms are more robust against flood attacks. However, since the nodes are distributed and scattered all over in the network, it raises processing overhead and computational complexity during communication among them. Table 1 describes mechanisms based on deployment point from different perspectives (Zargar *et al*., 2013).

Table 1: Defense mechanism according to deployment point

| Type | Deployment point | Accuracy | Scalability | Performance | Complexity |
|---|---|---|---|---|---|
| Centralized | Source | Low | Low | Moderate | Low |
| | Destination | High | Low | Good | Low |
| | Intermediate | Low | Medium | Moderate | Medium |
| Distributed | Hybrid | Medium | Medium-high | Poor-moderate | Medium-high |

## MATERIALS AND METHODS

**Our approach:** Our system model consists of several components. It is made up of two servers and several clients. The Local Recursive Server (LRS) provides answers for DNS request queries stored in its cache to the User machine. If the answer is not there, it forwards a name resolution request to Authoritative Name Server (ANS) asking for that record. ANS provides DNS response query to incoming requests according to the information stored in its configuration. User machine asks for name resolution for a website or a service and attacker machines utilizing ANS to perform reflection/amplification attack and targeting LRS. The detail about system model is shown in Fig. 1.

we propose defense mechanism through authentication message exchange. It aims to provide authenticity to all legitimate DNS queries. The classification-based filtering strategy is developed to facilitate the defense strategy by classifying the legal and illegal requests. Specifically we designed different query structure (i.e., request, response) to identify the packet that coming into the DNS and the packet that outgoing from the DNS. For the request and response packets we introduced two extra small-sized packets are validation request packet for investigating the source of the request, and confirmation response packet to determine the request legitimacy. Then our designed filtering strategy drops all illegitimate requests and only keeps the real ones before such bogus request overwhelmed the communication path to the user/victim.

The information on outgoing DNS request (i.e., source IP, source port, destination IP and destination port) is stored in a table in LRS. The request is sent to the ANS for applying IP address of the respective website or service. ANS stores the request in its table while preparing the validation packet that exchanges the source IP of the request to destination IP. The LRS received the validation packet to check the request's information (i.e., destination IP and source port) with its record. If the information is correct, then the request is considered valid. Next, the confirmation packet sent back to informs ANS on such result. It considered the request query as "Real" and sends back the DNS response. Also, the confirmed record is removed from LRS database. The idea is to prevent the request information misused by the attacker. Such strategy also can increase the accuracy of our work even if the attacker knows the outgoing port of the request query. However, if the information in the validation packet is not similar as in the LRS record, then it sent a false response packet to notify the ANS on the illegal request. Such bogus request is considered as "Spoofed" and it will be dropped from the system.

**Experimental design:** As mentioned before, our simulation model is made-up from two primary servers are ANS and LRS. Both ANS and LRS run using microsoft windows server 2008 32-bit. We installed microsoft SQL server 2008 on both servers to store DNS traffic information. In order to run all machines we used VM ware workstation 12.0×64 for designing the defense mechanism and Kali Linux 1.1.c with DNS Flooder 1.1 used to generate the attacking network traffic. We developed a packet sniffer tool to store the generated attack traffic. The Java programming language is used to code the authentication and classification processes. The simulation program started with 5000 packets and increased by 5000 for every replication. We organized the experiment in a way in which 99% is "Spoofed" packets, and 1% is "Real" packets. The size of the validation packet is randomly selected between 8-20 bytes. Meanwhile, the confirmation packet and false response packet is no >1 byte.

In this research we measured our defense mechanism using two different metrics are amplification factor, $amp_F$ and detection accuracy, $D_A$. The amplification factor, $amp_F$ is the ratio between response size and request size given as in Eq. 1:

$$amp_f = \frac{res_s}{req_s} \quad (1)$$

Higher amplification factor means there is a greater chance the attacker can consume the user/victim's resources. We also measured the detection accuracy in term of how accurate the classification-based filtering able to detect the right request (or "Real") during DNS transaction. Specifically, the detection accuracy, $D_A$ represents as Eq. 2:

$$D_A = \frac{\sum_p \text{Real}}{\text{Total no. of packet}} \quad (2)$$

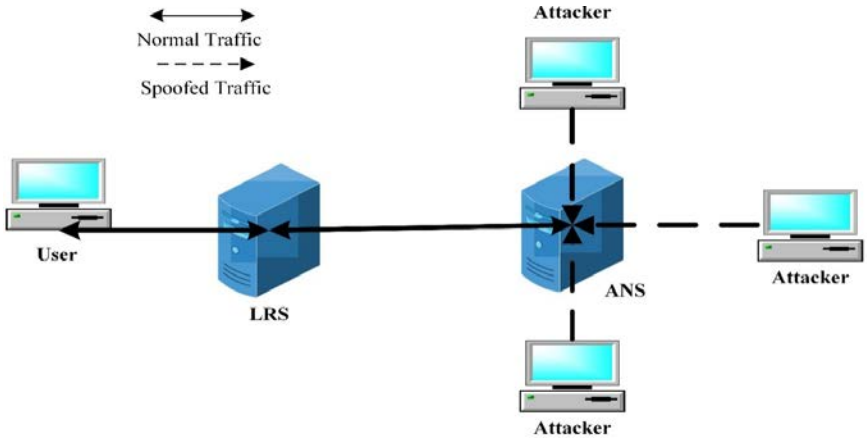



Fig. 1: System model

## RESULTS AND DISCUSSION

The output results from simulations show how significant DDS can reduce amplification factor during the attack. We calculated the amplification factor DDS, DAAD (Destination-base defense mechanism) (Zargar *et al*., 2013), Response Rate Limiting (RRL) (Intermediate network-based defense mechanism) (Rossow, 2014) and compared them together. The request query data length is (70) bytes. In DAAD and RRL mechanism, the response is (501) bytes. If we calculate Eq. 1 we can observe that the amplification factor is more than (7). However, when DDS is operating, there are two cases. The first case is if the request a legitimate one, the total bandwidth usage per request is the sum of validation request, confirmation response and DNS response. The minimum response size is (512) bytes and the maximum is (522) bytes that make the amplification factor more than (7.4) (Fig. 2). Shows the influence of amplification factor within different mechanisms.

The second case is if the system under attack and it receives a huge load of bogus traffic. In this case, the size of the response is the total of validation request and false response. The minimum size of the entire response is (11) bytes and the maximum is (21) bytes. It puts the maximum amplification factor in less than (0.27) while the system is under attack. Throughout our simulation if we take every transaction operation (request/authentication/response) into consideration and take their average bandwidth consumption for all legitimate and fake DNS requests we observed that the amplification factor is more than (0.36). The most interesting feature of authentication message strategy is the minimum overhead on the network bandwidth with very significant accuracy and bandwidth protection during an attack.

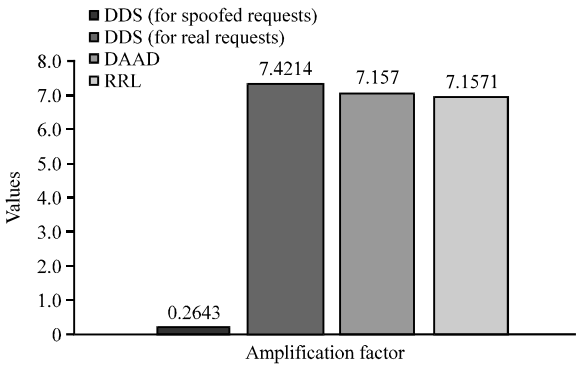
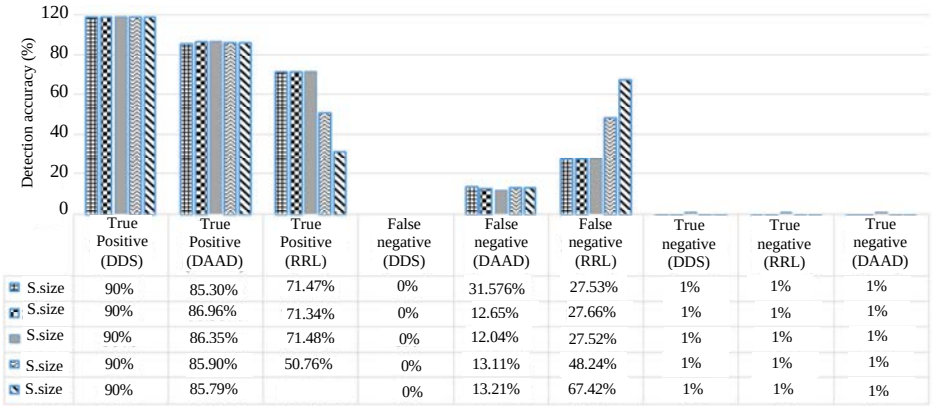



Fig. 2: Amplification factor in various scenarios

Our analysis indicates that the amplification factor becomes <1 when the system put in attack traffic which is caused by utilizing authentication-message exchange. However, the both other centrilized defense mechanisms (DAAD and RRL) showed that the amplification factor is >(7) during an attack. The reason is that DDS is a mechanism which is distributed through multiple nodes, and there is more than a deployment point. This feature allows DDS to have access to more resources and better protect against flooding attacks before the traffic reach the targeted system.

Another study on our work is about accuracy. We studied how classification filtering affects the detection accuracy. Accuracy in detection by a system mostly represented in four forms which are true positive, true negative, false positive and false negative. Where the true positive is the spoofed packets detected as spoofed. True negative is real packet detected as real. False positive is real packets detected as spoofed. Finally, false negative is spoofed packets detected as real. As Fig. 3 shows, when classification filtering in DDS is taken place, it shows higher accuracy results than other mechanisms.




| | True Positive (DDS) | True Positive (DAAD) | True Positive (RRL) | False negative (DDS) | False negative (DAAD) | False negative (RRL) | True negative (DDS) | True negative (RRL) | True negative (DAAD) |
|---|---|---|---|---|---|---|---|---|---|
| S.size | 90% | 85.30% | 71.47% | 0% | 31.576% | 27.53% | 1% | 1% | 1% |
| S.size | 90% | 86.96% | 71.34% | 0% | 12.65% | 27.66% | 1% | 1% | 1% |
| S.size | 90% | 86.35% | 71.48% | 0% | 12.04% | 27.52% | 1% | 1% | 1% |
| S.size | 90% | 85.90% | 50.76% | 0% | 13.11% | 48.24% | 1% | 1% | 1% |
| S.size | 90% | 85.79% | | 0% | 13.21% | 67.42% | 1% | 1% | 1% |

Fig. 3: Detection accuracy between different defense mechanisms

The reason behind such significant detection accuracy is that the proposed mechanism does not leave any information behind for the attacker to utilize after the end of the authentication process. The pattern alongside with the presented data in the table above shows the significant accuracy of classification filtering. DDS shows remarkable accuracy compared to centralized defense mechanisms. The effectiveness and robustness of the system are increased dramatically if the defense mechanism is distributed.

## CONCLUSION

Domain Name System (DNS) is one of the communication services on the network that used by hackers and other cyber criminals to perform several malicious operations. One of the fraud activities is DNS reflection/amplification attacks where it floods the user/victim's resources within a very short time. It is because DNS transactions (i.e., request and responses) are used UDP that does not support authentication procedure. It is a big challenge to monitor accurately and detect such attacks. In this research we proposed the authentication message exchange to tackle the amplification factor and protect the communication path from flooding with bogus traffic. Our authentication procedure incorporated into the classification packet filtering to classify the legitimate request while removing the fake requests from the DNS. The results show that our defense mechanism able to reduce amplification factor with better detection accuracy.

## RECOMMENDATIONS

In the near future we intend to enhance the efficiency of DDS. By enriching classification filtering with firewall, a new level of security can be achieved. The classification filtering sends updates to the firewall and the later block all DNS attack requests.

## REFERENCES

Anagnostopoulos, M., G. Kambourakis, P. Kopanos, G. Louloudakis and S. Gritzalis, 2013. DNS amplifievisited. Comput. Secur., 39: 475-485.

Bilge, L., E. Kirda, C. Kruegel and M. Balduzzi, 2011. Exposure: Finding Malicious Domains Using Passive DNS Analysis. Northeastern University, Boston, Massachusetts,.

Kambourakis, G., T. Moschos, D. Geneiatakis and S. Gritzalis, 2007. Detecting DNS Amplification Attacks. In: Critical Information Infrastructures Security, Lopez, J. and B.M. Hammerli (Eds.). Springer, Berlin, Germany, pp: 185-196.

Koc, Y., A. Jamakovic and B. Gijsen, 2012. A global reference model of the domain name system. Int. J. Crit. Infrast. Prot., 5: 108-117.

Liu, B., J. Li, T. Wei, S. Berg and J. Ye *et al.*, 2015. SF-DRDoS: The store-and-flood distributed reflective denial of service attack. Comput. Commun., 69: 107-115.

MacFarland, D.C., C.A. Shue and A.J. Kalafut, 2015. Characterizing Optimal DNS Amplification Attacks and Effective Mitigation. In: Passive and Active Network Measurement, Mirkovic J. and Y. Liu (Eds.). Springer, Berlin, Germany, pp: 15-27.

Marrison, C., 2014. DNS as an attack vector and how businesses can keep it secure. Network Secur., 2014: 17-20.

Rossow, C., 2014. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. University of Amsterdam, Amsterdam, Netherlands,.

Rozekrans T, M. Mekking and D.J. Koning, 2013. Defending Against DNS Reflection Amplification Attacks. University of Amsterdam, Amsterdam, Netherlands,.

Ye, X. and Y. Ye, 2013. A practical mechanism to counteract DNS amplification DDoS attacks. J. Comput. Inf. Syst., 9: 265-272.

Zargar, S.T., J. Joshi and D. Tipper, 2013. A survey of defense mechanisms against Distributed Denial of Service (DDoS) flooding attacks. IEEE. Commun. Surv. Tutorials, 15: 2046-2069.