Kurdistan Journal of Applied Research (KJAR)
Print-ISSN: 2411-7684 | Electronic-ISSN: 2411-7706

Website: Kjar.spu.edu.iq | Email: kjar@spu.edu.iq

Efficient Authentication Mechanism For Defending Against Reflection-Based Attacks on Domain Name System

Dana Hasan
Computer Science Department
College of Science
University of Garmian
Kalar, Sulaimania, Iraq
dana.hasan@garmian.edu.krd

Rebeen R. Hama Amin
Network Department
Computer Science Institute
Sulaimani Polytechnique University
Sulaimania, Iraq
rebeen.rebwar@spu.edu.iq

Masnida Hussin
Department of Communication Technology and Network
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Serdang, Selangor, Malaysia
masnida@upm.edu.my

Article Info

Volume 5 – Issue 1 – June 2020

DOI:
10.24017/science.2020.1.12

Article history:

Received: 08 April 2020
Accepted: 07 June 2020

Keywords:

DNS, Reflection,
Amplification attacks,
Amplification factor,
CHAP,
Source Authentication.

ABSTRACT

Domain Name System (DNS) is one of few services on the Internet which is allowed through every security barrier. It mostly depends on the User Datagram Protocol (UDP) as the transport protocol, which is a connectionless protocol with no built-in authentication mechanism. On top of that, DNS responses are substantially larger than their corresponding requests. These two key features made DNS a fabulous attacking tool for cybercriminals to reflect and amplify a huge volume of requests to consume their victim's resources. Recent incidents revealed how harsh DNS could be when it is abused with great complexity by attackers. Moreover, these events had proven that any defense mechanism with single point deployment couldn't accurately and efficiently overcome an attack volume with high dynamicity. In this paper, we proposed the Efficient Distributed-based Defense Scheme (EDDS) to overcome the shortcomings of a centralized-based defense mechanism. By using an authentication message exchange, which is a Challenge-Handshake Authentication Protocol (CHAP)-based authentication mechanism. It is deployed on multiple nodes to determine the legitimacy of the DNS request. Moreover, it significantly reduces the impact of the amplification factor for the fake DNS requests without having any side effects on legitimate ones. Then, a Stateful Packet Inspection (SPI)-based packet filtering is proposed to distinguish legitimate requests from fake ones by considering the results of the

authentication procedure. Both authentication-message exchange and SPI-based filtering are introduced to provide detection accuracy without reducing the quality of service for legitimate users. As the simulation results show, the proposed mechanism can efficiently and accurately detect, isolate, and discard the bogus traffic with minimal overhead on the system.

Copyright © 2020 Kurdistan Journal of Applied Research.
All rights reserved.

1. INTRODUCTION

Domain Name System (DNS) is a distributed, hierarchical naming system that forms the most vital part of the internet's structure which translates Internet Protocol (IP) addresses into names and vice versa. DNS relies mostly on the User Data Protocol (UDP) as the transport protocol. It transmits a name resolution request using port 53 in a single UDP packet [1][2][3][4]. DNS existence goes back to the time when the Internet was first introduced. It was commended when protocols were modeled with no security concerns. DNS is based on Internet Protocol (IP) does not provide any authentication mechanism. Furthermore, the transport protocol that has been used by DNS is mostly UDP. Lack of authentication and connection-less transportation in DNS transactions makes DNS an easy task for the attacker. Besides, DNS response packets are significantly larger than their corresponding requests and the ratio is called Amplification Factor. The higher the amplification factor, the easier the attacker can disrupt the victim's network, and consume its resources. High amplification factor and absence of source authentication makes DNS an elegant attack tool to perform massive Reflection/Amplification attack and take down important network infrastructure of their victim [5][6][7].

The main issue with current defense mechanisms is that they cannot distinguish legitimate traffic from malicious traffic accurately. The most recent studies confirm that these types of attacks are mostly performed against primary Internet components using DNS servers as the main tool of the attack. For example, as reported in [8] and [9], in March 2013, an amplification attack was launched against Spamhaus (non-profit anti-spam organization). The attack has been identified as a DNS-based attack with approximately 300 Gbps of traffic volume at its peak. It was the most severe flooding attack recorded using DNS as an attacking resource. Knowing that the majority of the defense mechanisms are helpless against an attack with such magnitude.

To have a successful defense mechanism there are three essential requirements, first, accurately detect attack's traffic. Second, stop the incoming traffic flood by quickly responding to the attack traffic. Finally, it is equitably necessary to differentiate the legitimate traffic that shares the attack signature and delivers without reducing the quality of service. Unlikely, there is no single defense mechanism that can meet all three requirements because they depend on single-point deployment. Detecting the attack traffic is most accurate near the victim. Meanwhile, the response is most successful near to the attack source. By taking these factors into account, it becomes clear that countering Distributed Denial of Service (DDoS) attacks requires distributed cooperative solutions [5][10].

In a Standard DNS Reflection/Amplification attack, the attacker forges DNS query packets and sends them to a DNS server. In the process, the attacker spoofs the packet's address with the targeted victim's IP address, rather than the actual sender of the packet. Upon receiving the query and processing it, the DNS server obediently sends back the response to the source address which is indicated by the request query (which is the victim's address). When the response packet arrives at its target, the victim processes the packet finds out it is an unrequested packet, and discards it. At this point, the attack's goal is accomplished, since the response consumed some of the victim's bandwidth and computational resources. To maximize the response size, the attacker looks for Resource Records (RR) with the highest response size (i.e. TXT, ANY). Also using DNS Security Extension (DNSSEC) can increase the size of the responses more because of the signature that imported in DNS responses. This results in a high amplification factor leading to the victim's resources suffer exhaustion quickly [4][11][12][13]. The vulnerability mentioned in DNS shows the need for a defense mechanism to be capable of detecting spoofed requests queries and reduce the impact of the amplification factor when the attack occurred. In this work, we present Efficient Distributed-based Defense Scheme (EDDS) that keeps the Quality of Service (QoS) intact and expeditiously detects the attack occurred before the network resources suffer exhaustion. By implementing modified CHAP-based authentication, we grant authentication to all legitimate DNS queries. Then, our classification packet filtering distinguishes all legitimate request queries and discards the fake ones.

The paper is organized as follows. Section 2 surveys previous works for mitigating DNS Reflection/Amplification attacks. Section 3 the proposed defense mechanism is described in detail with illustrations of the experiment design. Section 4 demonstrates the simulation of our work and results. Section 5 concluded the paper.

2. RELATED WORK

Amplification attacks demonstrate a significant danger to network security because of their clear advantages of amplification without exposing the attacker's anonymity. Amplification attacks detections are pulling more and more attention [14]. Many researchers worked on finding and giving solutions to solve the weaknesses in DNS protocol and how it operates along with counter measurements and some known defense mechanisms to face Reflection/Amplification attacks. When the attack occurs, the target should be disconnected from the network then solve the problem manually, which is a resource-consuming process. Therefore, every defense mechanism aims to detect the attack as quickly as possible and counter it as the nearest possible to the source of the attack [5] [10].

Centralized are mono-point deployments mechanisms, which are subdivided into Source, Destination, and intermediate based defense mechanisms. On the other hand, distributed mechanisms depend on more than a deployment node. These nodes are scattered through a network or multiple networks and cooperating to counter the attack volume. [15] Suggested a source-based mechanism to reduce the amplification factor by increasing the size of the request queries and deactivating the ANY resource record. The advantage is that it can reduce the amplification factor by a certain level. However, it also increases undesirable traffic on the networks. Also, by disabling some RR, all services related to that record will stop functioning. On top of lowering the amplification factor, the amplifiers (i.e. DNS Authoritative Servers) may need to send a limited response back to each IP address within a pre-defined time frame. This technique is called Response Rate Limiting (RRL), it is an intermediate-based defense mechanism. The drawback is that it can only use for authoritative name servers. Also, it is not much help when attack complexity is increased [15][16][17].

Another defense mechanism is proposed in [12]. They proposed a destination-based mechanism intends to distinguish between legitimate and spoofed DNS responses. The advantage is that it can separate attack traffic with good accuracy. However, during an attack, the path to the victim is flooded with bogus traffic and the upstream network suffers heavy congestion. To protect systems from DNS flooding attacks, it is necessary to design a distributed defense mechanism to mitigate the attack torrent. Also, it should be able to prevent reflecting and amplifying DNS responses before it reaches the victim.

In [14] the authors proposed their work which applies a sketch technique to uncover amplification attacks and mitigate it. their work uses an algorithm to directly collect and monitor network traffic in search of any disruption in the network traffic. their method is simple and efficient because it does not require to collect and examine the traffic feature and check the characteristics of amplification attacks. their experiment is conducted using simulations and real-world testbed. their results can accurately detect and mitigate amplification attacks on occurrence. However, this method cannot prevent amplification attacks from taking place, to begin with. Also, a large number of slow-rated amplifiers can overwhelm this mechanism easily.

The authors in [18] proposed a system that tends to monitor any change in the amplification factor and Time to Live (TTL) header to establish mitigation and enable the victim to further endure the traffic volume during DNS reflection/amplification attacks. their system secures the safety of legitimate packets in the process. Using centralized properties of SDN-based networks, they can generate alarms followed by the mitigation process by immediately writing metrics into a time-series database. as the experiments showed, their work can also be used for other forms of UDP-based attacks. However, the proposed system can only work with an SDN-based network and any legacy network outside the SDN-network is unprotected.

3. METHODS AND MATERIALS

In this section, we are going to discuss the proposed mechanism in detail. Since spoofing is the main requirement for an attacker to launch DNS Reflection/Amplification attack. Therefore, we studied how spoofed packets behave during the attack. While it is under attack, the local DNS server in the Internet Service Provider (ISP) sends out DNS requests multiple ports. However, it receives responses from ports which it didn't send out requests from that create an anomaly. Based on this fertile fact, we can build a distributed mechanism to counter DNS Reflection/Amplification attack with good accuracy and acceptable efficiency.

To design such a mechanism, we constructed a network as in figure 1. Two DNS servers used to provide answers to the name resolution queries sent by users. The first server is the Authoritative Name Server (ANS), which provides name resolution according to its configuration. The other is Local Recursive Server (LRS) which forward name resolution requests to ANS if the name is not previously stored in its cache. Two types of end-users are installed on the system model, the User device asks for resolving a name from LRS. However, the Attacker machines used to send bogus traffic to ANS using the fabricated IP address of LRS as their source address. Then ANS reflects and amplifies the responses and sends it back to the victim (i.e. LRS).

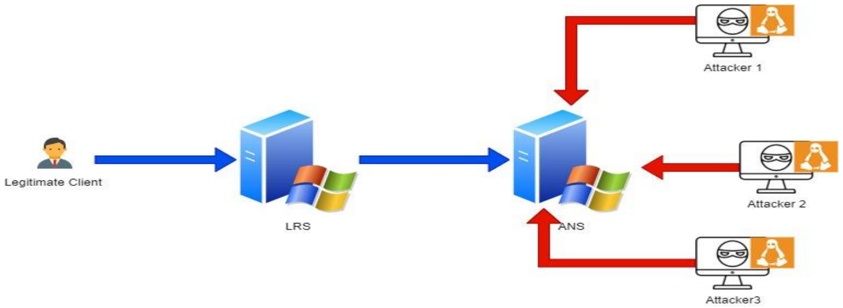


Figure 1: Proposed Test-Bed Scheme

In this scheme, we suggested a defense mechanism using modified CHAP-based authentication. CHAP is an authentication method introduced to prevent identity spoofing in DNS [19]. It is used to provide authentication to all legitimate DNS requests and mark the false ones as spoofed packets as shown in Figure 2.

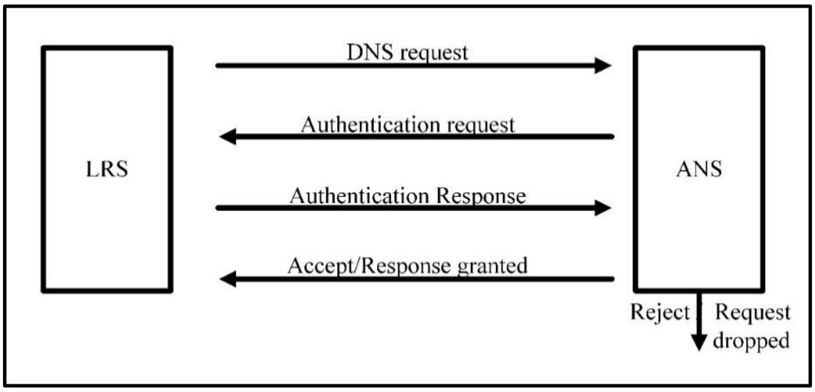


Figure 2: Challenge-Handshake Authentication Protocol (CHAP) for DNS

We intend to use this technique to determine the authenticity of DNS transactions. This authentication procedure establishes new DNS query arrangements by introducing two additional small-sized packets beside both DNS request and corresponding response, to conclude the request rightfulness. The two packets are named as authentication request and authentication response. The architecture of EDDS is illustrated in figure 3. Then, our Stateful Packet Inspection (SPI)-based filtration mechanism discards all bogus traffic and allows only legitimate ones to have a DNS response.

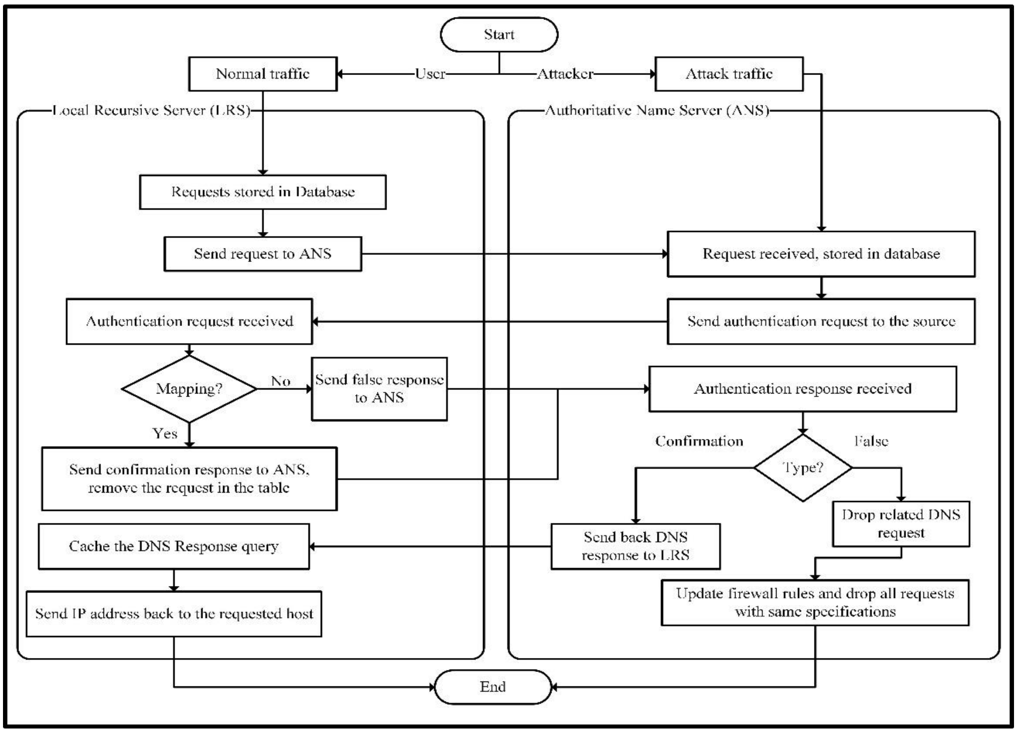

Start
User
Attacker
Normal traffic
Attack traffic
Local Recursive Server (LRS)
Authoritative Name Server (ANS)
Requests stored in Database
Send request to ANS
Request received, stored in database
Send authentication request to the source
Authentication request received
Mapping?
No
Yes
Send false response to ANS
Authentication response received
Confirmation
False
Type?
Send confirmation response to ANS, remove the request in the table
Drop related DNS request
Send back DNS response to LRS
Cache the DNS Response query
Update firewall rules and drop all requests with same specifications
Send IP address back to the requested host
End

Figure 3: EDDS architecture

To implement this scheme, we used several tools. The User-machine is running on Microsoft Windows 7 Home Premium x86. Attacker machines operate on Kali Linux 1.1c, both servers using Microsoft Windows Server 2008 X86. The attacking tool which is used is DNS Flooder 1.1, which is a very powerful tool written in C language. It can generate highly organized, dynamic, and spoofed packets using ANY records to provide a high amplification factor. The database tool we used in both systems is Microsoft SQL Server 2008 X86. The components of the system model are running in a virtual machine environment using VMWare Workstation 12.0 Pro.

The system model is operating on a Lenovo Thinkpad T420 laptop with Core i5 2.5GHz CPU, 10 GB RAM, 256 GB SSD, and the operating system is Microsoft Windows 10 X64. The DNS Servers (i.e. ANS and LRS) specifications are Core i5 2.5 GHz CPU, 3 GB RAM, 50 GB Virtual Storage. The User-machine features are Core i5 2.5 GHz CPU, 1 GB RAM, 30 GB Virtual Storage. Finally, the attacker's machines hardware specifications are Core i5 2.5 GHz CPU, 512 MB RAM, 15 GB Virtual Storage.

The information about packets is stored in tables using Packet Capture 1.0 which is a tool we developed for that purpose. Every operation in our mechanism, on both servers (Authentication transactions, mapping process, classification filtering, and discarding the spoofed packets) is done using Java programming language. The experiment is performed in five different replications with five different duration. We organized the experiments on every simulated mechanism in a way in which the legitimate requests would be the only %1 of the total traffic, and the rest of requests are spoofed traffic generated by the attacker.

LRS table stores information about every request packet which is sent out to ANS. While ANS stores information about every incoming DNS packet (from LRS and the attacker). After receiving and storing the DNS request, the authentication procedure is initiated by ANS through sending an authentication request to the source of the requests (LRS in this case) which are stored in its table. The authentication request is a small packet (maximum 20 bytes). It contains the destination IP address and the source port of the incoming DNS request which is stored in the ANS table. LRS receives this authentication request packet, compares the packet content with its table, returns the authentication response to ANS. The authentication response is a tiny packet (only 1 byte) indicate the DNS request's legitimacy.

If the mapping is successful, then the authentication packet contains a confirmation message that informs ANS about the packet legitimacy followed by removing the mapped record from LRS. Removing the record is to protect LRS records from being abused by cybercriminals to trick the system even if they know the outgoing port of DNS requests which significantly improves detection accuracy. However, in case of unsuccessful mapping, LRS sends an authentication response which warns ANS about the spoofed request. Then the SPI-based filtering at the ANS side removes every similar incoming packet (i.e. packet with the same port and IP) from its table without performing further authentication for similar packets.

The performance metrics which are used to calculate the effectiveness and efficiency of EDDS include defense strength, efficiency, and Amplification factor. The defense strength is measured in terms of four different outcomes which are true positive (TP), which is the total number of malicious traffic that the system detects as malicious. False-positive (FP) is the total number of legitimate traffic that the system detects as malicious. False-negative (FN) is the total number of malicious traffic that the system detects as legitimate. True negative (TN) is the total number of legitimate traffic that the system detects as legitimate.

Based on the defense strength outcomes, we can calculate three other criteria that every defense mechanism should have which are Accuracy, Sensitivity, and False-negative rate. Accuracy is the ratio of true outcomes to total outcome in the system which can be calculated according to equation 1.

$$Accuracy = \frac{TN+TP}{TN+TP+FN+FP} \quad \text{........(1) [5]}$$

Sensitivity is the ratio of true positive to the total of positive outcomes. It is calculated using equation 2.

$$Sensitivity = \frac{TP}{FN+TP} \quad \text{........(2) [5]}$$

The false-negative rate is the ratio of false-negative outcomes to the total of negative outcomes. The calculation is done using equation 3.

$$False\ negative\ rate = \frac{FN}{TN+FN} \quad \ldots\ldots(3)\ [5]$$

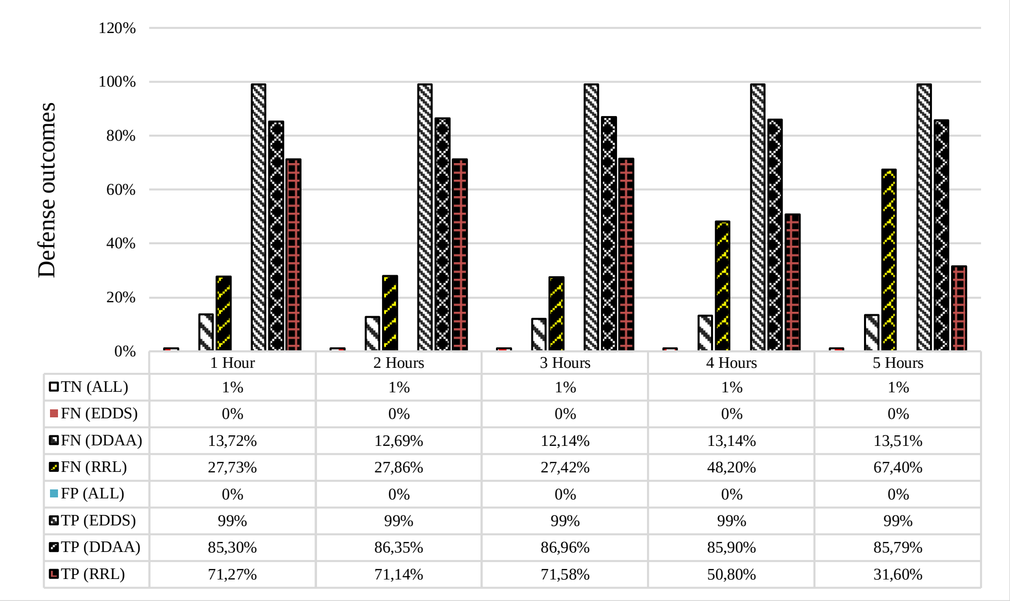
To measure efficiency, the number of processed transactions (i.e. legitimate and Spoofed) per replication are recorded by each simulation. We measured efficiency to show the number of name-resolution transactions that each defense mechanism can handle within a pre-defined time interval. We also can determine the amplification factor Af by measuring the ratio of response size ResS to corresponding request size ReqS [3][5][12] as shown in equation 4.

$$Amplification\ factor\ = \frac{Response\ size}{Request\ size} \quad \ldots\ldots\ldots.\ (4)$$

The results of the proposed mechanism are compared with two previously suggested solution by previous researches which are Detecting DNS Amplification Attack (DDAA) which is proposed by [12] and Response Rate Limiting (RRL) which is proposed by [16][17] and currently implemented in Bind 9.

4. RESULTS AND DISCUSSIONS

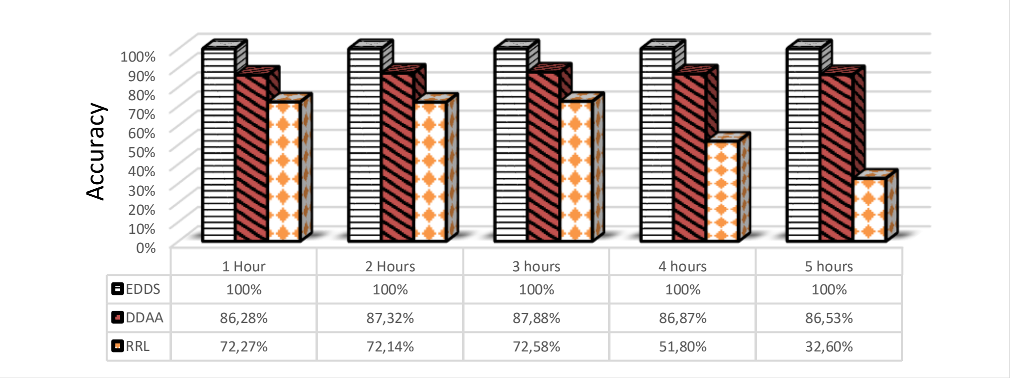
The results of our experiments are calculated and analyzed thoroughly to extract the outcome of this work. Base on the given equations in the methodology of this article, we demonstrate the impact of using a distributed-base defense scheme to protect DNS from reflection/amplification attacks. One of the criteria we showed is defense strength, which is one of the most important criteria used to measure the strength of any defense mechanism. In this work, three simulations are tested in five different tests with different parameters (i.e. the period of testing, and traffic). Testing simulations for different periods and different traffic types is important to know how the defense mechanism is working under different attack volumes and durations. The period of tests starts with 1 hour and it is increased by 1 hour for each replication (i.e. first replication is for one hour, second replication is for 2 hours, and so on). Four outcomes are shown which are True Negative (TN), False Negative (FN), False Positive (FP), and True Positive (TP). These outcomes are illustrated in Figure 4 for each defense mechanism (The outcomes with similar results are combined).



	1 Hour	2 Hours	3 Hours	4 Hours	5 Hours
□ TN (ALL)	1%	1%	1%	1%	1%
■ FN (EDDS)	0%	0%	0%	0%	0%
▨ FN (DDAA)	13,72%	12,69%	12,14%	13,14%	13,51%
▨ FN (RRL)	27,73%	27,86%	27,42%	48,20%	67,40%
■ FP (ALL)	0%	0%	0%	0%	0%
▨ TP (EDDS)	99%	99%	99%	99%	99%
▨ TP (DDAA)	85,30%	86,35%	86,96%	85,90%	85,79%
▨ TP (RRL)	71,27%	71,14%	71,58%	50,80%	31,60%

Figure 4: Shows the outcome of each defense mechanism based on the TN, FN, TP, FP outcomes

One of the main criteria to measure the strength of any defense mechanism is accuracy. Figure 5 shows that regardless of how sophisticated the attack is going to be, EDDS still detects the attack traffic with extreme accuracy.

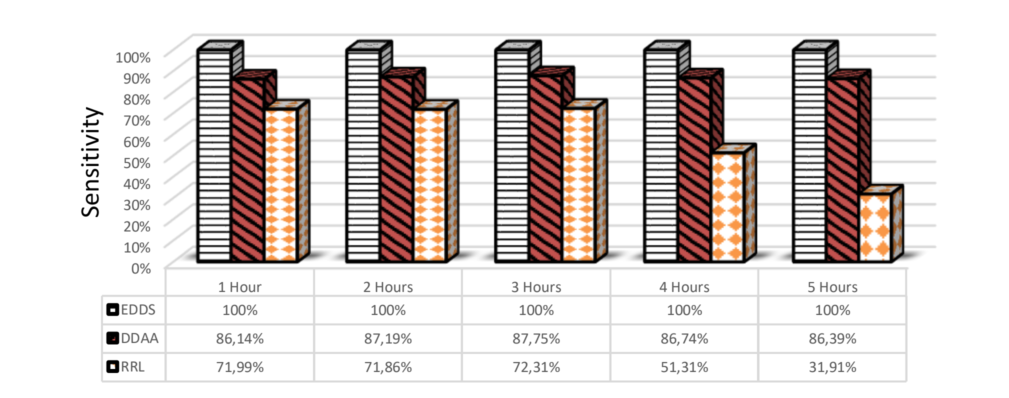


	1 Hour	2 Hours	3 hours	4 hours	5 hours
▤ EDDS	100%	100%	100%	100%	100%
▨ DDAA	86,28%	87,32%	87,88%	86,87%	86,53%
▨ RRL	72,27%	72,14%	72,58%	51,80%	32,60%

Figure 5: Accuracy

It also provides a significant detection rate which practically reached %100 (lost packets are ignored). On the other hand, DDAA has difficulties detecting all incoming spoofed responses compared to EDDS, because DDAA can be manipulated by the attacker by generating traffic similar to the victim's traffic. Therefore, the detection accuracy of DDAA is downgrading. Also, RRL lacks any detection mechanism due to the RRL design that concentrates on reducing DNS traffic instead of detecting malicious traffic and distinguish them. Response rate limiting can restrict misuse against a single amplifier and cannot hold against multiple amplifiers at a low request rate.

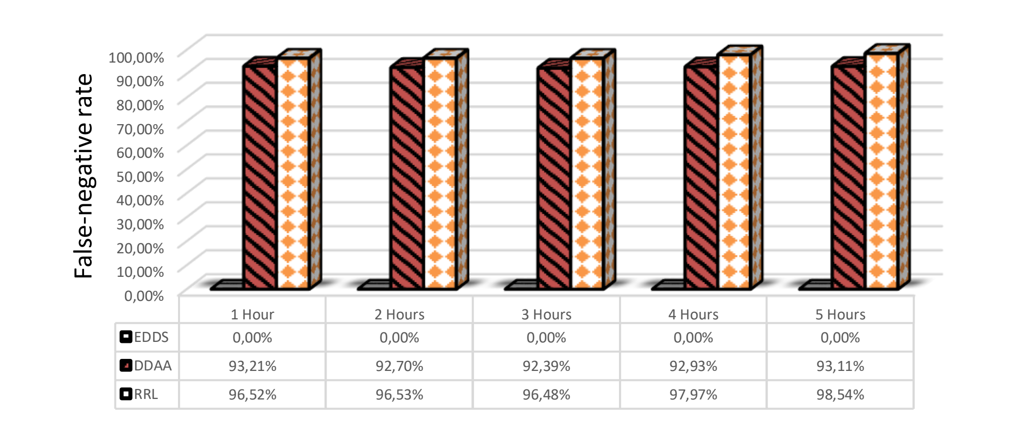
Sensitivity is the measurement ratio of true positives over total desired positive outcomes. Figure 6 shows the sensitivity of each defense mechanism. EDDS was highly sensitive in detecting malicious traffic. Because EDDS relies on inspecting and authenticating every incoming DNS request. However, it can be observed from the figure that DDAA is less sensitive. Knowing that this contraction in sensitivity occurs when the legitimate and attack traffics share the same features. As the attack traffic gets more sophisticated the RRL sensitivity degrades.



	1 Hour	2 Hours	3 Hours	4 Hours	5 Hours
EDDS	100%	100%	100%	100%	100%
DDAA	86,14%	87,19%	87,75%	86,74%	86,39%
RRL	71,99%	71,86%	72,31%	51,31%	31,91%

Figure 6: Sensitivity

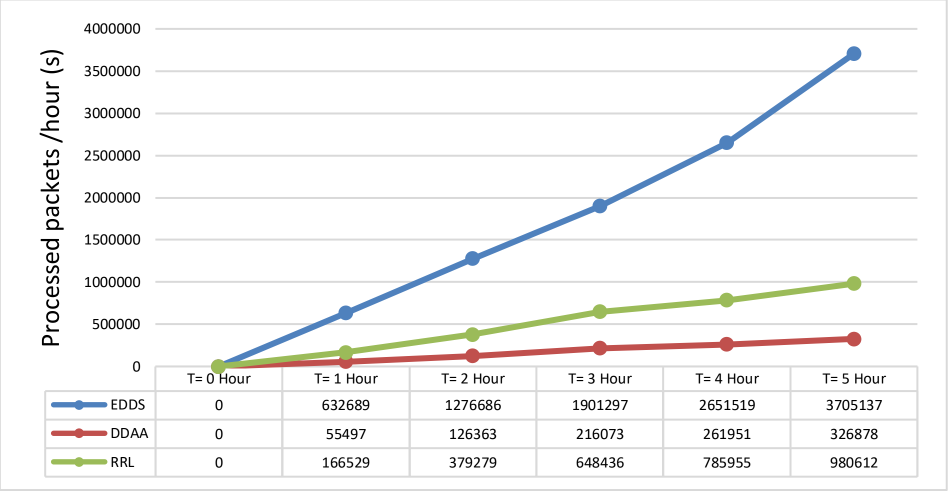
The false-negative rate can be obtained from the ratio of the defense mechanism over the total negative outcome. Figure 6 shows the false-negative rate of each mechanism, Due to its significant accuracy, EDDS has no false-negative ratio. However, as it appears from the results that both DDAA and RRL have a false-negative ratio. While DDAA can maintain a certain level, RRL continues to decrease as the traffic increases.



	1 Hour	2 Hours	3 Hours	4 Hours	5 Hours
EDDS	0,00%	0,00%	0,00%	0,00%	0,00%
DDAA	93,21%	92,70%	92,39%	92,93%	93,11%
RRL	96,52%	96,53%	96,48%	97,97%	98,54%

Figure 7: False-negative rate

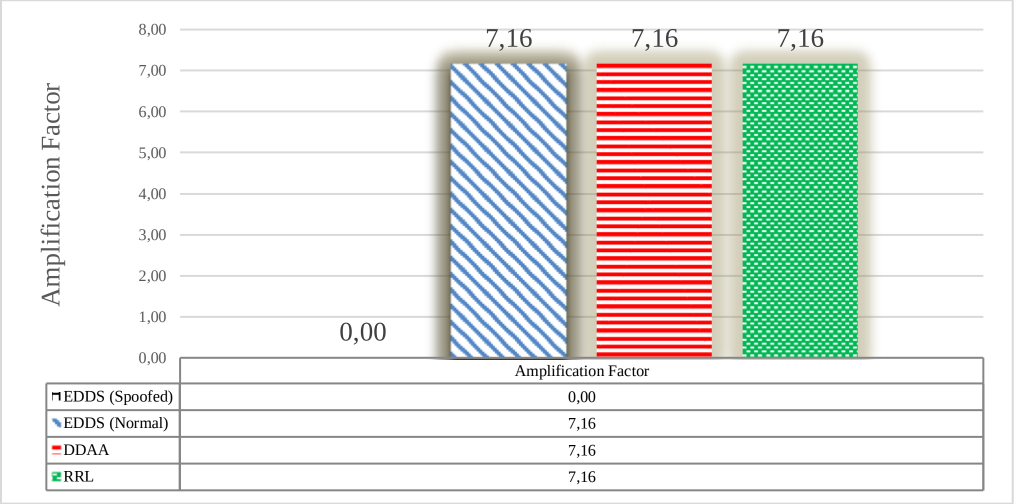
Even though the attack traffic is highly complex and sophisticated, EDDS was able to detect the attack traffic and protect the network from such attacks. Hence, by applying SPI-based packet filtering, we have successfully calculated the amount of time required for testing, filtering, and responding, or discarding each request query in a replication which increases the efficiency of EDDS. Figure 7 shows the efficiency of defense mechanisms.



	T= 0 Hour	T= 1 Hour	T= 2 Hour	T= 3 Hour	T= 4 Hour	T= 5 Hour
EDDS	0	632689	1276686	1901297	2651519	3705137
DDAA	0	55497	126363	216073	261951	326878
RRL	0	166529	379279	648436	785955	980612

Figure 8: Efficiency

The amplification factor is one of the major issues in DNS that can determine the significance of the malicious traffic generated for the attack. DNS requests size set to 70 bytes and DNS responses has 501 bytes for the experiment. Equation 4 has been applied and figure 8 shows the calculation of the amplification factor.



	Amplification Factor
EDDS (Spoofed)	0,00
EDDS (Normal)	7,16
DDAA	7,16
RRL	7,16

Figure 9: Amplification Factor

EDDS drops any spoofed packets from getting responses. Therefore, the response size during an attack is equal to 0, as can be observed in figure 8. Thus, the amplification factor during attacks is considered to be 0. However, other defense mechanisms cannot distinguish and drop spoofed requests from getting responses which produce amplification factor for attack traffic.

5. CONCLUSION

Domain Name Service is an indispensable service on the Internet. It is because of it that everybody in the civilized world can tap into this global network and utilize its services. Through the use of a modified CHAP-based authentication method, we provided an authentication procedure for DNS request queries. Then our classification-based filtering distinguishes all requests that passed the authentication procedure and provided them with a DNS response query. It also discards all the spoofed addresses and prevents them from getting a DNS response. Our experimental results and analysis show how our mechanism can mitigate the amplification factor during an attack. It also effectively detects and discards all attack traffic on DNS servers with very good efficiency and less CPU usage per node. In the future, we designate to transform our mechanism into service and making it operational during an attack only. Thus, the total performance of the DNS service will not diminish. It can also reduce the latency due to the delivery timeframe which the authentication procedure requires during an attack. Also, it integrates very high-security features into the domain name itself. Meanwhile, we seek to try our mechanism within a testbed environment to test its defense capability and efficiency during heavy attack load.

REFERENCE

[1] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, “DNS Amplification Attack Revisited,” *Comput. Secur.*, vol. 39, pp. 475–485, 2013.

[2] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi, “EXPOSURE : Finding Malicious Domains Using Passive DNS Analysis,” in *Network and Distributed System Security (NDSS)*, 2015, pp. 1–17, doi: https://doi.org/10.1145/2584679.

[3] X. Ye and Y. Ye, “A Practical Mechanism to Counteract DNS Amplification DDoS Attacks ⋆,” *J. Comput. Inf. Syst.*, vol. 1, pp. 265–272, 2013.

[4] D. C. MacFarland and C. A. S. A. J. Jalafut, “Characterizing Optimal DNS Amplification Attacks and Effective Mitigation,” in *International Conference on Passive and Active Network Measurement*, 2015, vol. 1, pp. 15–27, doi: 10.1007/978-3-319-15509-8_2.

[5] S. T. Zargar, J. Joshi, and D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[6] S. Di Paola and D. Lombardo, “Protecting against DNS Reflection Attacks with Bloom Filters,” in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 1–16, 2011.

[7] C. Marrison, “DNS as an attack vector – and how businesses can keep it secure,” *Network Security*, vol. 2014, no. 6, Elsevier Ltd, pp. 17–20, 2014.

[8] Y. Takano, R. Ando, and T. Takahashi, “A Measurement Study of Open Resolvers and DNS Server Version,” *Internet Conf. IC2013*, pp. 23–32, 2013.

[9] F. J. Ryba, Matthew Orlinski, M. W¨ahlisch, C. Rossow, and T. C. Schmidt, “Amplification and DRDoS Attack Defense – A Survey and New Perspectives,” *arXiv Prepr. arXiv*, p. 19, 2015.

[10] P. Gulihar and B. B. Gupta, “Cooperative Mechanisms for Defending Distributed Denial of Service (DDoS) Attacks,” in *Handbook of Computer Networks and Cyber Security*, Cham: Springer International Publishing, pp. 421–443, 2020.

[11] B. Liu *et al.*, “SF-DRDoS : The store-and-flood distributed reflective denial of service attack,” *Comput. Commun.*, vol. 69, pp. 107–115, 2015, doi: 10.1016/j.comcom.2015.06.008.

[12] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, “Detecting DNS Amplification Attacks,” in *International workshop on critical information infrastructures security*, 2007, pp. 185–196.

[13] T. Rozekrans, J. de Koning, and M. Mekking, “Defending against DNS reflection amplification attacks,” University of Amsterdam, 2013.

[14] X. Jing, J. Zhao, Q. Zheng, Z. Yan, and W. Pedrycz, “A reversible sketch-based method for detecting and mitigating amplification attacks,” *J. Netw. Comput. Appl.*, vol. 142, no. June, pp. 15–24, 2019, doi: 10.1016/j.jnca.2019.06.007.

[15] C. Rossow and H. G¨ortz, “Amplification Hell : Revisiting Network Protocols for DDoS Abuse,” no. February, pp. 23–26, 2014.

[16] P. Vixie and V. Schryver, “DNS Response Rate Limiting (DNS RRL),” *Internet System Consortium*, 2012. https://ftp.isc.org/isc/pubs/tn/isc-tn-2012-1.txt.

[17] P. Vixie and Vernon Schryver, “Response Policy Zones,” *Internet Engenieering Task Force*, 2017. https://tools.ietf.org/html/draft-vixie-dns-rpz-00.

[18] K. Ozdincer and H. A. Mantar, “SDN-based Detection and Mitigation System for DNS Amplification Attacks,” *3rd Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2019 - Proc.*, no. Figure 2, 2019, doi: 10.1109/ISMSIT.2019.8932809.

[19] M. Inamura, “Expansions of CHAP Modificationless on Its Structures ofPacket and Data Exchange,” in *International Conference on Information Systems Security and Privacy*, pp. 1–8,.2015.