A Customize Approach for Detection and Protection for DNS Amplification Attack

[1]Margi Patel, [2] Pooja Modi
[1] M. Tech Student, [2]Assistant Professor,
[1] Department of Computer Engineering, MEC, Basna. India.
[2] Department of Computer Engineering, MEC, Basna. India.
[1]margipatel2222@gmail.com,[2]pooja0391@gmail.com

Abstract - Internet is huge and prominent source of data, information, and different type of services. The Domain Name System (DNS) is a critical component of the Internet infrastructure, provides the translation of easy to remember domain name to IP address, for network services and applications. Denial of Service (DoS) attack usually either involves attackers sending messages to exploit certain vulnerabilities leading to the abnormality or paralysis of business systems, or sending a massive amount of regular messages quickly to a single node to run out the system resources resulting in business system failure. A DNS amplification attack is a type of distributed denial of service (DDoS) attack that takes advantage of the fact that a small DNS query can generate a much larger response. Our proposed approach achieves accuracy for use different types of query and also using this combine approach to detecting and protecting DNS Amplification attack.

Index Terms - Domain Name System (DNS), Distributed Denial of service (DDoS), DNS amplification attacks

I. INTRODUCTION

Denial of service (DoS) attacks has become a major threat to current computer networks. A Denial of Service (DoS) attack usually either involves attackers sending messages to exploit certain vulnerabilities leading to the abnormality or paralysis of business systems, or sending a massive amount of regular messages quickly to a single node to run out the system resources resulting in business system failure.In general, DDoS attacks can be divided into the bandwidth based attack, application based attack, traffic based attack. Denial of service attacks is difficult to detect and mitigate [9].
Domain Name System (DNS) amplification attacks are a type of powerful distributed denial-of-service (DDoS) reflection attack that have a long history dating back to the "Smurf" attack in 1997. Today's DNS amplification attacks are even stronger, can slow down Internet access and cause significant damage to the intended target. [10].
DoS attacks can be roughly classified into three types, based on their targets and layers:

- Network layer - attacks on network bandwidth resources
- Transmission layer - attacks on connection resources
- Application layer - attacks on computing resources

II. BACKGROUND THEORY

DNS Amplification Attack

These DDoS attacks are becoming more sophisticated, making it hard for packet filters to catch the traffic. This urges to push the filtering towards the name server, so that the defence mechanisms can also become more sophisticated.

In order to launch a DNS amplification reflection attack the attacker needs to perform two tasks. First the attacker spoofs the address of the victim. This is the reflection part; it will cause all the replies from the DNS server to be directed to the victim's server. This can easily be done since in UDP no handshake (like in TCP) is being done between the client and the server. Secondly the requester searches for responses that are several times bigger than the request. The attacker achieves an amplification factor because the response is many times larger than the request. The amplification can even be larger when DNSSEC is used, because of the signatures used the size of the response increases.

Now the attacker is ready to perform the attack. The attacker sends a stream of small queries originating from a group of infected computers to one or multiple authoritative DNS servers. The DNS servers will then reply to the resolver. However, because the attacker spoofed the address of the victim, all the traffic is directed to the victim.

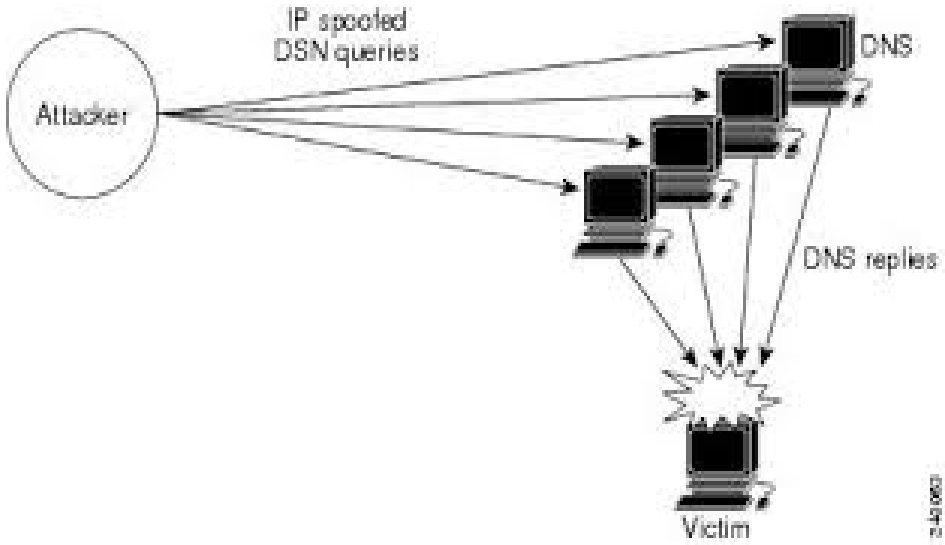

Fig: 1 DNS Amplification Attack [11]

III. RELATED WORK

Georgios Kambourakis, Tassos Moschos et al [1] present a novel, simple, and practical scheme that enable administrators to distinguish between genuine and falsified DNS replies. Its monitoring in real time DNS traffic and altering security supervisors when necessary. Use firewall by automatically updating rules to ban bogus packets. They argue that the solution based on one –to –one mapping of DNS requests and responses. They also used the DNS amplification attacks detector (DAAD) detection logic.

Marios Anagnostopoulos, Stefanos Gritzalis et al [2] proposed a model in which DNSSEC-powered amplification attack which use benefits of more number of DNS forwarders. For their proposed scheme they argue that compared to normal amplification attack the method don't need revocation of need of aggressor for the botnet and elimination of virtually traces that used towards disclosing the attacker action for true identification.

The experimental result they have shown based on the data from three countries and the forwarder from these countries might be easily recruited by attacker. They also show that with the help of legacy PC equipment and a certain degree of reconnaissance one is able to achieve an amplification factor that between 37 and 44.

Amir Herzberg, Haya Shulman et al [3] provides model for the defense against DNS amplification attack. They argue that their proposal effectively prevent DNS based amplification. They present the theoretic model analysis and predicating that the model is adopted vastly. The propose model also gives enough support to reduce the threats of dns amplification attack. In the proposed scheme they also suggest the way to reduce the cost and provides the additional defense for the dns server. Their mechanism also produces a list of `good' DNS resolvers and resolvers' platforms as well as potentially compromised (suspect) hosts. The model is of independent interest and can be used to analyze defenses against different types of DoS attacks.

Tassos Moschos, Dimitris Geneiatakis [4] proposed model present and evaluate a novel and practical method that is able to distinguish between authentic and bogus DNS replies. The proposed scheme can effectively protect local DNS servers acting both proactively and reactively. The argue that in its current pilot stage the proposed solution is practical and easy to implement in any network realm. Moreover, test results showed that is effective and can be easily parameterized to fit properly into any network domain. The futures work the mentioned that they shall investigate alternative and more efficient data stores like Bloom Filters. This would not only improve the performance of the DAAD tool, but make it scalable as well.

Muhammad Yesir, Feroz Ahmed at el [22] proposed scheme which can effectively protect DNS servers acting both proactively and reactively. Authors shown DNS DDoS attack and also suggest a mechanism that can protect a DNS server from amplifying DDoS attacks especially the attacks targeting the bandwidth consumption of the victim server. They also propose a new defense based on IP tables and routine fail2ban detection. The attack flow detection mechanism detects attach flows based on the indication or stress at the server, since it is getting more difficult to identify bad flows only based on the incoming traffic patterns.

The proposed mechanism is based on three key ideas. The first one is an IP table's scheme in the first stage, which protects the servers from a sudden surge of attack flows. In second one is to stop unauthorized recursion by trusted network list allow in bind. They also set response rate limit in bind. The amplification of illegitimate responses can be limited by implementing RRL on authoritative name servers. RRL can prevent false positives by setting SLIP. Authors also investigated the condition to detect the victim servers and freeze the white list based on the server response time in detail. The third key idea is to detect attack flows based on the concept of a white list based admission control defined for each pair of client and server IP addresses in the second stage.

COMPARISON OF VARIOUS RESEARCH SCHEMES

The table below shows a short comparison about the various schemes proposed by a researcher by taking different parameters. The table gives the description about the basic technique used with the benefits that researcher gets the limitations found in schemes.

Paper	Accuracy	Performance	Authentication	Searching	Overhead	Rectification	Method/ Technique
Georgios et. al [1]	✓	x	✓	✓	✓	x	DAAD MODEL
Marios et. al [2]	x	x	✓	x	x	x	FIRE WALL
Amir et. al [3]	x	✓	✓	x	x	x	RRL MECHANISM
Tassos et. al [4]	X	✓	✓	x	x	✓	DAAD MODEL

Table 1. Comparison study

IV. CONCLUSION

DNS amplification attack majorly affects the network usage as well client. By working at both the side client and server we can achieve greater security against attack. As server also support to stop attack client work with fewer burdens. So, by customizing security methods and by working on more than one type of attacks as well parameters we can achieve greater security with less overhead.

V. REFERENCES

[1] Kambourakis, Georgios, et al. "A fair solution to dns amplification attacks."Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on. IEEE, 2007.

[2] Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., & Gritzalis, S. (2013). DNS amplification attack revisited. Computers & Security,39, 475-485.

[3] Herzberg, Amir, and Haya Shulman. "DNS authentication as a service: preventing amplification attacks." Proceedings of the 30th Annual Computer Security Applications Conference. ACM, 2014.

[4] Kambourakis, Georgios, et al. "Detecting DNS amplification attacks." Critical Information Infrastructures Security. Springer Berlin Heidelberg, 2008. 185-196.

[5] Microsoft Corporation, 2013, "Domain Name System [online]"; Available:http://technet.microsoft.com/en-us/network/bb629410.aspx.

[6] Network Working Group, "Domain Name- Concepts and Facilities [online]";Available: https://www.ietf.org/rfc/rfc1034.txt.

[7] http://www.nsfocus.com/uploadfile/Product/ADS/DDoS%20FAQ/What%20is%20DDoS%20Attack.pdf.

[8] Kawaljit, K., Navreen, K. B., and Gurpreet, K. "A Study of DNS Amplification Attack Defence Methods", IEEE-2014.

[9] http://www.excitingip.com/1500/an-introduction-to-ddos-distributed-denial-of-service-attack

[10] http://www.nsfocus.com/SecurityView/DNS%20Amplification%20Attacks%20on%20the%20Rise.pdf

[11] Arukonda, Srinivas, and Samta Sinha. "The Innocent Perpetrators: Reflectors and Reflection Attacks." (2015).

[12] A. Herzberg and H. Shulman. DNSSEC: Security and Availability challenges. In Communications and Network Security (CNS),2013.

[13] Deshpande, Tushar, et al. "Formal analysis of the DNS bandwidth amplification attack and its countermeasures using probabilistic model checking." High-Assurance Systems Engineering (HASE), 2011 IEEE 13th International Symposium on. IEEE, 2011.

[14] Eastlake, Donald E. "Domain name system security extensions." (1999).

[15] Arends, Roy, et al. DNS security introduction and requirements. No. RFC 4033. 2005.

[16] MacFarland, Douglas C., Craig A. Shue, and Andrew J. Kalafut. "Characterizing Optimal DNS Amplification Attacks and Effective Mitigation." Passive and Active Measurement. Springer International Publishing, 2015

[17] Arukonda, Srinivas, and Samta Sinha. "The Innocent Perpetrators: Reflectors and Reflection Attacks." (2015).

[18] Microsoft Corporation, 2013, "Domain Name System [online]"; Available:http://technet.microsoft.com/en-us/network/bb629410.

[19] P. Vixie and V. Schryver, "DNS Response Rate Limiting,"2012. [online]. Available: http://ss.vix.com/~vixie/isc-tn-2012-1.txt

[20] T. Rozekrans and J. de Koning, "Defending against DNS reflection amplification attacks," University of Amsterdam, February 2013.

[21] M. Anagnostopoulos et al., "DNS amplification attack revisited,"ELSEVIER Computers and Security, Vol.39, pp. 475-485,2013.

[22] Muhammad Yea sir Arafat, Muhammad Morshed Alam and Feroz Ahmed "Realistic Approach And Mitigation Techniques

for Amplifying DDOS Attack on DNS ” Proceedings of 10th Global Engineering, Science and Technology Conference 2-3 January, 2015, BIAM Foundation, Dhaka, Bangladesh, ISBN: 978-1-922069-69-6.