Mathematical Problems of Computer Science 42, 107--112, 2014.

Methods of Limiting the Domain Name Service Traffic Against Distributed Denial of Service Attacks

Arthur S. Petrosyan and Eugene B. Prohkorenko

Institute for Informatics and Automation Problems of NAS RA
e-mail: arthur@sci.am, eugene@sci.am

Abstract

The goal of the research described in this paper is to find methods of limiting the Domain Name Service (DNS) traffic against Distributed Denial of Service (DDoS) Attacks.

Since DNS is a core network service, the protection of DNS servers is vital for the whole network infrastructure. In view of the different forms of DDoS attacks on DNS servers (like the DNS Amplification Attack), the implementation of effective preventive methods becomes very important.

This article describes the research work done in the Academic Scientific Research Computer Network of Armenia (ASNET-AM) managed by the Institute for Informatics and Automation Problems (IIAP) of the National Academy of Sciences of the Republic of Armenia (NAS RA), targeted to the deployment of the improved methods of limiting the DNS traffic against DDoS attacks. Special attention was given to User Diagram Protocol (UDP)-based Amplification Attacks resulting in Distributed Reflective Denial of Service (DRDoS) attack. This paper includes a description of best practice configuration of protection methods for the most widely used Name Server Software - "Berkeley Internet Name Domain" (BIND9) package.

Keywords: DNS, Denial of Service, DDoS, Amplification Attack, BIND.

1. Introduction

DDoS attacks today use DNS reflection and amplification to achieve attack data bit rates up to 300 gigabits per second (Gbps) and even more.Underlying many of these attacks is packet-level source address forgery or spoofing, a well-knownvulnerability in which an attacker generates and transmits User Diagram Protocol (UDP) packetspurporting to be from the victim's IP address. Attackers often use query-response protocols, such as DNS toreflect or amplify responses to achieve attack data transfer rates exceeding the victim's network capacityeither in bits per second, packets per second, or both.

DNS is especially suitable for such attacks because the response is typically larger, and in some cases,much larger than the query.

2. DRDoS UDP Attacks

A Distributed Reflective Denial of Service (DRDoS) attack is an emerging form of Distributed Denial of Service (DDoS) that relies on the use of publicly accessible UDP servers, as well as bandwidth amplification factors, to overwhelm a victim system with UDP traffic.
UDP [1], by design, is a connection-less protocol that does not validate the source IP addresses. Unless the application-layer protocol uses countermeasures such as session initiation [2], it is very easy to forge the IP packet datagram to include an arbitrary source IP address. When many UDP packets have their source IP address forged to a single address, the server responds to that victim, creating a reflected Denial of Service (DoS) Attack.

Recently, certain UDP protocols have been found to have particular responses to certain commands that are much larger than the initial request. If previously the attackers were limited linearly by the number of packets directly sent to the target to conduct a DoS attack, now a single packet can generate tens or hundreds of times the bandwidth in its response. This is called an amplification attack, and when combined with a reflective DoS attack on a large scale it makes it relatively easy to conduct DDoS attacks.

3. DNS Amplification Attack

A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS), in which attackers use publically accessible open DNS servers to flood a target system with DNS response traffic. The primary technique consists of an attacker sending a DNS name lookup request to an open DNS server with the source address spoofed to be the target's address. When the DNS server sends the DNS record response, it is sent instead to the target. Attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. In most attacks of this type observed by US-CERT, the spoofed queries sent by the attacker are of the type "ANY," which returns all known information about a DNS zone in a single request. Because the size of the response is considerably larger than the request, the attacker is able to increase the amount of traffic directed at the victim. By leveraging a botnet to produce a large number of spoofed DNS queries, an attacker can create an immense amount of traffic with little effort.

Additionally, because the responses are legitimate data coming from valid servers, it is extremely difficult to prevent these types of attacks. While the attacks are difficult to stop, network operators can apply several possible mitigation strategies.

4. Attack Mitigation Techniques

The Internet Corporation for Assigned Names and Numbers (ICANN) has issued specific recommendations on mitigation of such attacks [3]. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) also has addressed the same

issue providing a number of recommendations [4--7]. These recommendations together with *research work done in ASNET-AM can be summarized in the following* best practice configuration of protection methods for the most widely used Name Server Software - "Berkeley Internet Name Domain" (BIND9) package [8].

First of all the network infrastructure must give high quality (smallest delay and reliability) of DNS traffic, to provide customers with comfortable browsing and downloading. Next DNS system must be divided into two subsystems [9]:

1. Local non-recursive authoritative DNS servers, serving own domains zones to the outside world.
2. Local recursive DNS resolvers for customers.

Restricted access to the outside public DNS servers must also be provided (accounting that their response time is much longer than that of local DNS resolvers).

5. Local Non-recursive Authoritative DNS Servers

Asthe DNS queries being sent by the attacker-controlled clients must have a source address spoofed to appear as the victim's system, the first step to reducing the effectiveness of DNS amplification is for Internet Service Providers to reject any DNS traffic with spoofed addresses. The changes recommended below would substantially reduce the potential for the most popular types of DDoS attacks.

5.1 Disabling Recursion on Authoritative Name Servers

Authoritative Name Servers are deployed to provide name resolution for hosted domains. As stated above DNS resolution for private client systems should be provided by a separate server and the authoritative name server should act only as a DNS source of zones information to external clients. Thus, these systems do not need to support recursive resolution of other domains on behalf of a client, and should be configured with recursion disabled.

It is strongly recommended for BIND9 global options to contain the following lines:

```
allow-query-cache { none; };
recursion no;
```

5.2 Response Rate Limiting (RRL)

A very important feature available in recent versions of BIND9 allows an administrator to limit the maximum number of responses per second being sent to one client from the name server [11][12]. This functionality named Response Rate Limiting (RRL) is intended to be used on authoritative domain name servers only when it affects the performance on recursive resolvers. To provide the most effective protection, it is strongly recommended for BIND9 global options to contain the following lines to implement RRL:

```
rate-limit {
   responses-per-second 5;
   window 5;
};
```

6. Defending the Local Recursive DNS Resolvers

Local recursive DNS resolvers preferably should be located inside LAN of each organization not to cross the border routers with customers' requests.
Local non-recursive authoritative DNS servers preferably should be located in a demilitarized zone (DMZ) [10].

Each DNS server should have SNMP support enabled, to monitor DNS traffic activity. Average normal activity must be calculated and used for local firewall setting.

Since customers' PCs, infected with botnet agents create DNS requests to local DNS servers and further to victims or directly to victims, the router's firewalls must be activated to filter the outgoing external DNS traffic. Limiting a Query Per Second (QPS) locally helps to distribute the load and not to overload border routers in case of massive attack. ASNET-AM practice shows that local DNS requests filtering for customers has a good effect. We have estimated that in normal situation each customer's PC generates not more than 100 QPS. Whereas each botnet agent infected customer PC can create up to 20 000 QPS.
It is strongly recommended for BIND9 global options to contain the following lines:

```
acl INT_IP_RANGE { [INTERNAL-IP-RANGE] };
allow-query { INT_IP_RANGE; };
allow-query-cache { INT_IP_RANGE; };
allow-recursion { INT_IP_RANGE; };
rate-limit {
   responses-per-second 100;
   window 5;
};
```

7. Conclusion

To provide the most effective protection, it is recommended that authoritative and recursive name servers run on different systems, with RRL implemented on the authoritative server and access control lists implemented on both servers. This will reduce the effectiveness of DNS amplification attacks by reducing the amount of traffic coming from any single authoritative server while not affecting the performance of the internal recursive resolvers. Each DNS server should have SNMP support enabled, to monitor DNS traffic activity. Average normal activity must be calculated and used for local filter setting arrangement.

References

[1] UDP: User Datagram Protocol,[Online]. Available: http://tools.ietf.org/html/rfc768
[2] SIP: Session Initiation Protocol, [Online]. Available: http://tools.ietf.org/html/rfc3261

[3] (February, 2014), SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure, (An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)), [Online]. Available: https://www.icann.org/en/system/files/files/sac-065-en.pdf
[4] (March 07, 2014), UDP-based Amplification Attacks Alert (TA14-017A), [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA14-017A
[5] (July 22, 2013), DNS Amplification Attacks Alert (TA13-088A),[Online]. Available: https://www.us-cert.gov/ncas/alerts/TA13-088A
[6] G. Kambourakis, T. Moschos, D. Geneiatakis and S. Gritzali,"Detecting DNS amplification attacks", Available:http://www.dgeneiatakis.com/papers/conferences/conference-08.pdf
[7] (March 17, 2006), Randal Vaughn, Gadi Evron, "DNS Amplification Attacks", [Online]. Available: http://crt.io/DNS-Amplification-Attacks.pdf
[8] "Berkeley Internet Name Domain", BIND,[Online]. Available: http://www.isc.org/downloads/bind/
[9] A.Petrosyan and E.Prokhorenko, "Улучшенная модель распределенной системы DNS для сети ASNET-AM", *Proceedings of the Conference CSIT'2013*, pp. 387-388, Yerevan, 2013.
[10] Strengthen network defenses by using a DMZ, [Online]. Available: http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/
[11] (February 14, 2013), T. Rozekra and J. de Koning, "Defending against DNS reflection amplification attacks", [Online]. Available: http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf
[12] "Response Rate Limiting with BIND", Eddy Winstead (Internet Systems Consortium (ISC)), APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies), Asia Pacific's Premier Regional Internet Summit 2014, [Online]. Available: https://conference.apnic.net/data/37/apricot-2014-rrl_1393309768.pdf

Submitted 15.08.2014, accepted 28.11.2014 .

Դոմենային տիրույթների ծառայության հոսքերի սահմանափակման մեթոդներ՝ ծառայության խափանման տարաբաշխված հարձակումներից պաշտպանությանհամար

Ա. Պետրոսյան, Ե. Պրոխորենկո

Ամփոփում

DNS ծառայությունն առանցքային դեր ունի ներկայիս ցանցային տեխնոլոգիաների ոլորտում, և DNS սերվերների պաշտպանությունը կենսական նշանակություն ունի ողջ ցանցային ենթակառուցվածքի անխափան աշխատանքի

համար: Հաշվի առնելով վերջին տարիներին լայն տարածում ստացած DNS սերվերներին ուղղված ծառայության խափանման տարաբաշխված հարձակումների տարբեր տեսակները, շատ կարևոր է դառնում դոմենային տիրույթների ծառայության հոսքերի սահմանափակման և պաշտպանության արդյունավետ մեթոդների մշակումն ու ներդրումը:

Հոդվածում նկարագրված են ASNET-AM Հայաստանի ակադեմիական գիտահետազոտական կոմպյուտերային ցանցում կատարված ուսումնասիրության արդյունքները, որոնց նպատակն է՝ մշակել դոմենային տիրույթների ծառայության հոսքերի սահմանափակման և պաշտպանության արդյունավետ մեթոդներ:

Методы ограничения сетевого трафика услуги доменных имен для защиты от распределенных атак, направленных на отказ в обслуживании сетевых услуг

А. Петросян, Е. Прохоренко

Аннотация

Услуга DNS является ключевой в современном мире сетевых коммуникаций, поэтому защита DNS-серверов имеет жизненно важное значение для всей сетевой инфраструктуры в целом. В связи с различными формами DDoS атак на DNS серверы (например, DNS Amplification атаки), внедрение эффективных методов защиты и ограничения становится очень важным.

В статье описаны исследования, направленные на определение эффективных способов ограничения сетевого трафика для защиты от распределенных атак направленных на отказ в обслуживании сетевых услуг (DDoS-атаки), в частности услуги Domain Name Service (DNS). Представлены результаты научно-исследовательской работы, проделанной в Академической научно-исследовательской компьютерной сети Армении (ASNET-AM), направленные на применение улучшенных методов ограничения DNS трафика для защиты от DDoS атак. Особое внимание уделено защите от атак усиления на основе протокола UDP. Статья включает в себя описание рекоменудуемой конфигурации DNS серверов на основе пакета "Berkeley Internet Name Domain" (BIND9).