Detection and Prevention of DNS Query PTR record-based Distributed Denial-of-Service Attack

Yasuo Musashi, Ryuichi Matsuba, and Kenichi Sugitani

Center for Multimedia and Information Technologies, Kumamoto University,
Kumamoto-City, 860-8555, JAPAN

musashi@cc.kumamoto-u.ac.jp

Abstract

The syslog messages of the topdomain DNS servers in Kumamoto University were statistically investigated when having receiving a large amount of DNS query packets like a distributed denial-of-service (DDoS) attack. The interesting results are: (1) The DNS query-based DDoS attacking packets considerably include reverse (PTR) records. (2) The PTR records include a lot of unregistered IP addresses of our university as their query contents. Thus, we can detect the DNS query-based DDoS attack by only watching the traffic of unregistered IP address-based DNS query PTR record packets. Also, we developed and implemented an intrusion prevention system (IPS) for the DNS query-based DDoS attack on the our top domain DNS servers.

Keywords: Intrusion Detection, Intrusion Prevention, IDS, IPS, PTR record, DDoS attack

1. Introduction

One of attractive solutions to keep security of the DNS servers is to employ an intrusion detection system (IDS)[1-3]. Although the IDS provides a lot of useful alert messages, it generates too much alert ones to analyze in a real time. Furthermore, the IDS detects only security incidents and does not prevent a remote attack automatically. Therefore, we need to develop an intrusion prevention system (IPS) in no distant future. Recently, our top domain name system (DNS) servers have started to be under a DNS query-based distributed denial-of-service (DNS-DDoS) attack like transmitting a plenty of DNS query packets, probably, in oder to crash the DNS servers. The present paper is to discuss (1) on correlation analysis on DNS query traffic between DNS server and DNS clients that especially transmit query contents including unregistered IP addresses of our university network segments, (2) how to implement a DNS query-based DDoS attack detection system by analyzing syslog messages of the DNS server, and (3) how to prevent the DNS-DDoS attack.

2. Observations

We investigated traffic of DNS query access between the top domain DNS server (**tDNS**) [*] and DNS clients. In **tDNS**, BIND-9.2.3 program package has been employed as DNS server daemon[4]. The DNS query packets and their contents have been captured by a query logging option (see man named.conf). The log of DNS query access has been recorded in the syslog file. All of the syslog files are daily updated by the crond system.

[*] **tDNS** is a secondary top domain DNS server in Kumamoto University (kumamoto-u). The OS is Linux OS (kernel-2.4.26), and hardware is an Intel Xeon 2.40GHz Dual SMP machine.

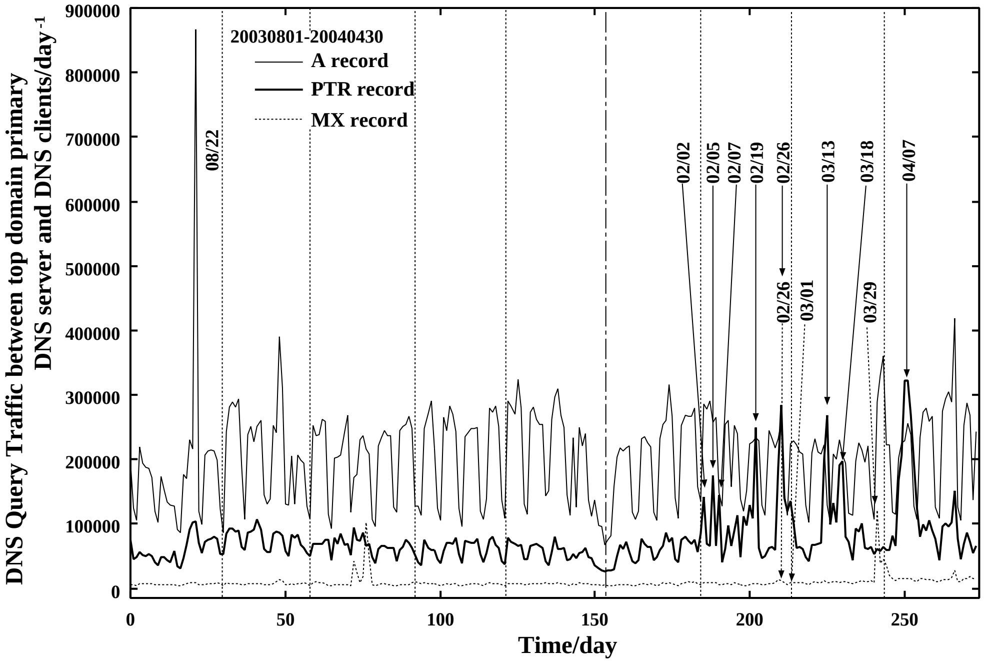

Fig. 1. The DNS query traffic between the top domain DNS server and the DNS clients through August 1st, 2003 to April 30th, 2004. The thin solid line shows the A record based DNS query traffic, the thick solid line indicates the PTR record based DNS query traffic, and the dotted line demonstrates the MX-record based DNS query traffic (day^{-1} unit).

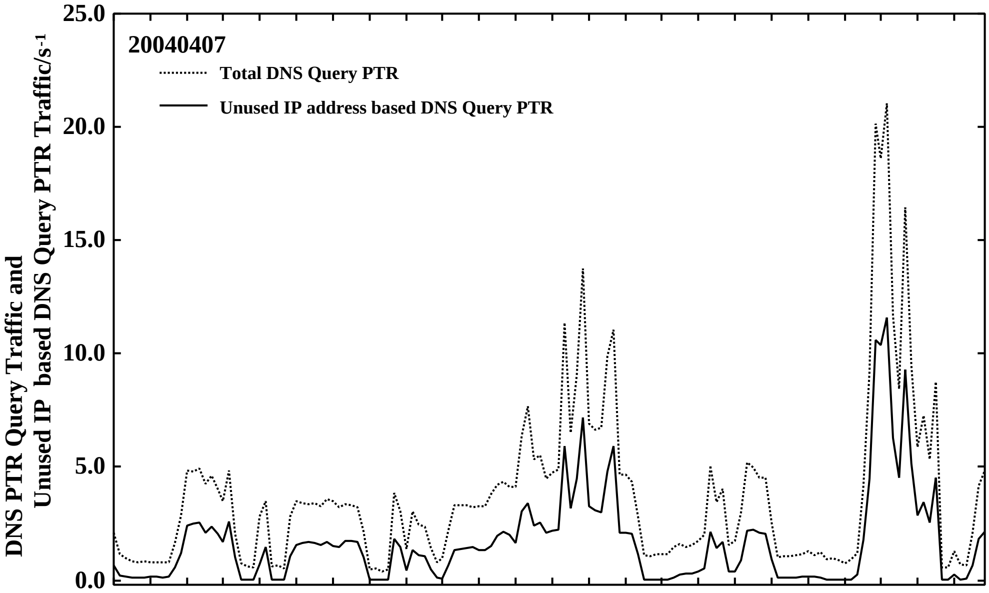

Fig. 2. The DNS query PTR record traffic between the top domain DNS server and the DNS clients at April 7th, 2004 (s^{-1} unit).

We observed traffic of DNS query request packet from DNS clients to the top domain name server (**tDNS**) through August 1st, 2003 to April 30th, 2004 (Figure 1). In Figure 1, the DNS query reverse (PTR record) request packet curve changes in an almost the same manner as that of the A record curve upon going from August 1st, 2003 to January 31st, 2004, however, it starts to fluctuate drastically on February 1st, 2004, and after this day, its value frequently exceeds the values of other DNS query A or MX record request packet. Especially, the abnormal DNS query PTR record request packet traffic becomes very much high at April 7th, 2004.

We illustrate the observed traffic of the DNS query PTR record packets between the top domain DNS server (**tDNS**) and its DNS clients in Figure 2 at April 7th, 2004. In Figure 2, the total traffic curve of the DNS query PTR record request packet changes in a simultaneous manner with that of the DNS query PTR record request packet including unregistered IP addresses as their contents.

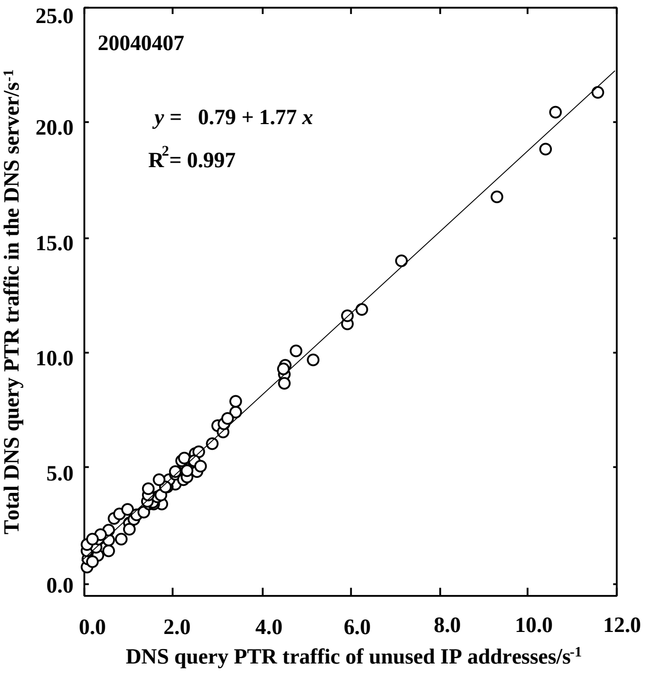

Fig. 3. Total DNS query PTR traffic vs DNS query PTR traffic of unregistered IP addresses (April 7th, 2004). (s^{-1} unit).

Figure 3 shows regression analysis between total DNS query PTR record traffic versus total DNS query PTR record traffic of unregistered IP addresses. The data are April 7th, 2004. The correlation coefficient (R^2) is 0.997. This means that the abnormal total DNS query PTR traffic considerably correlates to the traffic of DNS query PTR packets including unregistered IP addresses. Furthermore, it is found that IP addresses of the DNS clients are significantly variable. These results clearly show that a DNS query content including an unregistered IP address in our university network is very suspicious. Therefore, we can detect a DNS query PTR record-based DDoS attack whether or not the DNS query contents include unregistered IP addresses.

3. Implementation and Evaluation

We designed and developed a new detection and prevention system for DNS query PTR record DDoS attack (PTRDPS). This system consists of PTR record packet capture, PTR record preprocessor (arpa), detection engine for the DDoS attack "ptrscan", and prevention system for the DDoS attack "pfd".

We implemented PTRDPS into the top domain name server **tDNS** and evaluated detection rate (April 12th, 2004). In Figure 4, we show observed the total DNS query PTR traffic and detection rate of DNS query PTR record-based DDoS attack. After installation of PTRDPS, the detection rate is observed to be 48584 IP/day, however, gradually decreases day by day, and finally is estimated to be *ca* 1500 IP/day after April 25th, 2004.

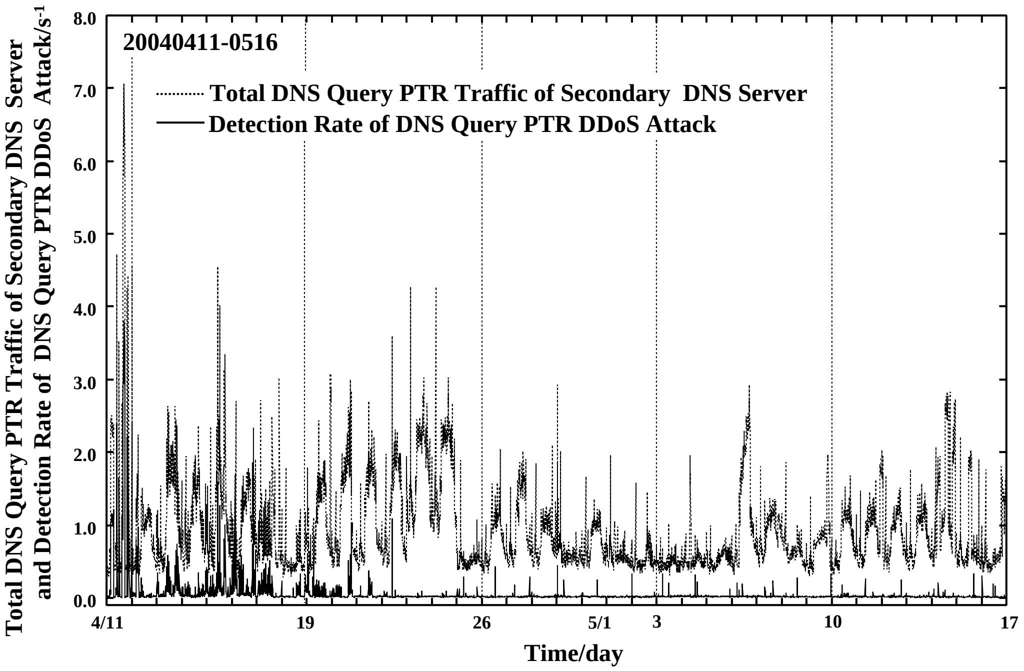

Fig. 4. The DNS query PTR record traffic between the top domain DNS server and the DNS clients and the detection rate of DNS query PTR record based DDoS attack through April 11th to May 16th, 2004 (s^{-1} unit).

4. Concluding Remarks

We implement a detection and prevention system of DNS query PTR record-based DDoS attack into our top domain name server. Successfully, we have been preventing the DDoS attack. We continue further investigation to get more detailed information on the DDoS attack against the DNS servers and E-mail servers[5].

References and Notes

[1] W. Yang, B. -X. Fang, B. Liu, and H. -L. Zhang, Intrusion detection system for high-speed network, *Comp. Commun.*, 27 (2004) in press.

[2] D. E. Denning, An Intrusion-detection model, *IEEE Trans. Soft. Eng.*, No.2, SE-13 (1987) pp.222-232.

[3] http://www.snort.org/

[4] http://www.isc.org/products/BIND/

[5] R. Matsuba, Y. Musashi, and K. Sugitani, Detection of Mass Mailing Worm-infected IP address by Analysis of Syslog for DNS server, *IPSJ SIG Technical Reports, Distributed System and Management 32nd*, No.37, 2004 (2004) pp.67-72.