DNS 解決 PTR レコード分散型サービス妨害攻撃の自動検知と自動阻止システムの開発

武藏 泰雄 † 松葉 龍一 † 杉谷 賢一†

概要: 我々の大学のトップドメイン DNS サーバが大量の DNS 解決パケット送りつけられる分散型サービス妨害攻撃 (DDoS) を受けている時、DNS サーバの syslog を統計的に解析したところ次のような結果を得た: (1)DNS 解決 DDoS 攻撃パケットは主に逆引 (PTR) レコードで構成されている。(2) その PTR レコードで解決する IP アドレスは、主として本大学の未使用の IP アドレスである。従って、未使用 IP アドレスの PTR レコードを監視すれば、DNS 解決型 DDoS 攻撃検知すること可能である。またその DDoS 攻撃を自動的に検知し、自動的に阻止するシステム (IPS) を開発した。

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

Yasuo Musashi,† Ryuichi Matsuba,† and Kenichi Sugitani†

Abstract: The syslog messages of the top domain DNS servers in Kumamoto University were statistically investigated when having a distributed denial-of-service (DDoS) attack like receiving a large amount of DNS query packets. The interesting results are: (1) Contents of the DNS query-based DDoS attack packets mainly consist of reverse (PTR) records. (2) The PTR records include a lot of unused IP addresses of our university. Therefore, we can detect the DNS query-based DDoS attack by only monitoring the contents of DNS query PTR record packet traffic having unused IP addresses. Also, we developed and implemented a simple intrusion prevention system (IPS) for the DNS query-based DDoS attack on the our top domain DNS servers.

1. Introduction

It is of considerable importance to keep security of a DNS server because the DNS provides very important information such as a host domain name (an A record), an IP address (a PTR record), and mail exchange (an MX record), to DNS clients like E-mail server (SMTP/POP3) and/or WWW browsing network applications. In other words, these network applications strongly depend on the DNS server. From this point, we need to protect the DNS server, firmly.

One of the attractive solutions to keep security of the DNS servers is to employ an intrusion detection system (IDS).[1−10] There are two types of IDSs; one is a misuse intrusion detection (MID) type,[3,4] scanning a database of the remote attack signature, and the other is an anomaly intrusion detection (AID) type,[3−8] getting statistical profile information of network packet traffic and/or an anomaly use of network protocol. Recent IDS includes both models like the former and the latter. Surely, the IDS provides a lot of useful alert messages, however, 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.

In order to develop a new useful MID/AID-hybrid IDS with an IPS against future remote attack on the DNS servers, it is of considerable im-

†熊本大学総合情報基盤センター・Center for Multimedia and Information Technologies, Kumamoto University.

portance to get more detailed information for traffic of network applications like DNS query packets between a DNS server and a DNS client.

Recently, our top domain name system (DNS) server has 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 server.

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 unused 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

2.1 Network Systems

We investigated traffic of DNS query accesses between the top domain DNS server (**tDNS**) † and the DNS clients. Figure 1 shows a schematic diagram of a network observed in the present study. **tDNS** is one of the top level domain name (kumamoto-u) system servers and plays an important role of subdomain delegation and domain name resolution services for many PC terminals.

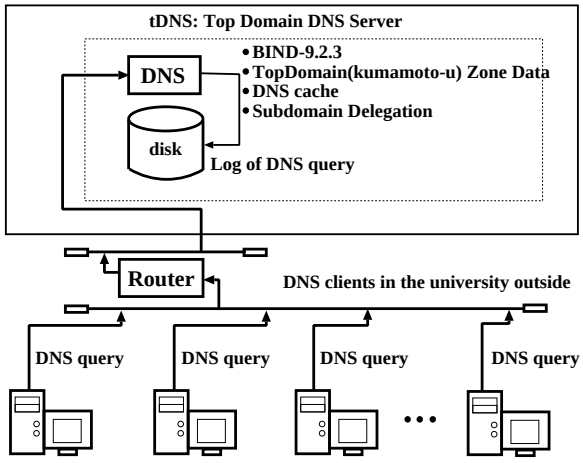

Figure 1. A schematic diagram of a network observed in the present study.

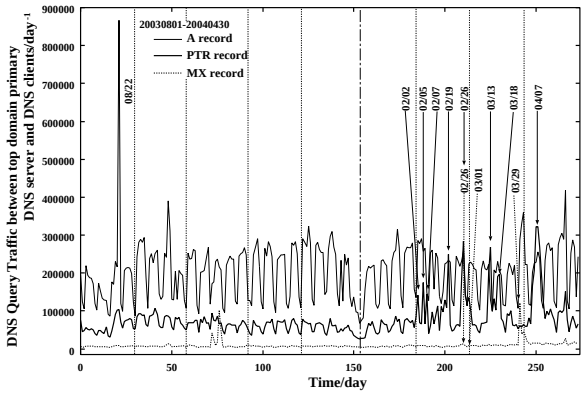

Figure 2. The DNS query traffic between the top domain DNS server and the DNS clients through August 1st, 2003 to April 30th, 2004. The thin solid line shows the A record based DNS query traffic, the thick solid line indicates the PTR record based DNS query traffic, and the dotted line demonstrates the MX-record based DNS query traffic (day^{-1} unit).

2.2 DNS Query Packet Capturing

In **tDNS**, BIND-9.2.3 program package has been employed as a DNS server daemon.[11] The DNS query packets and their contents have been captured and decoded by a query logging option (see man named.conf), as follows:

```
logging {
        channel qlog { syslog local1; };
        category queries { qlog; };
}
```

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. The syslog message consists of DNS query contents like mainly a host domain name (an A record), an IP address (a PTR record), and mail exchange (an MX record).

2.3 Abnormal PTR Traffic

We observed traffic of DNS query request packet from DNS clients to the top domain DNS server

†**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.

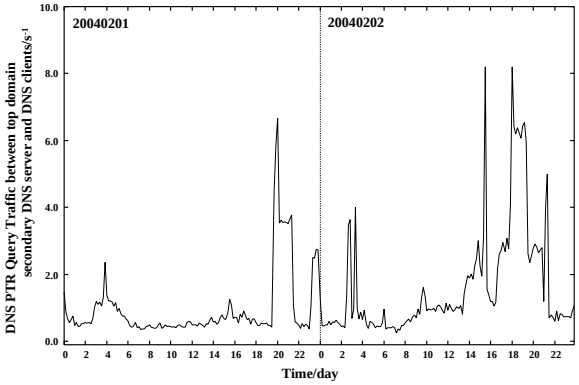

Figure 3. The DNS query PTR record traffic between the top domain DNS server and the DNS clients at February 1st to 2nd, 2004 (s^{-1} unit).

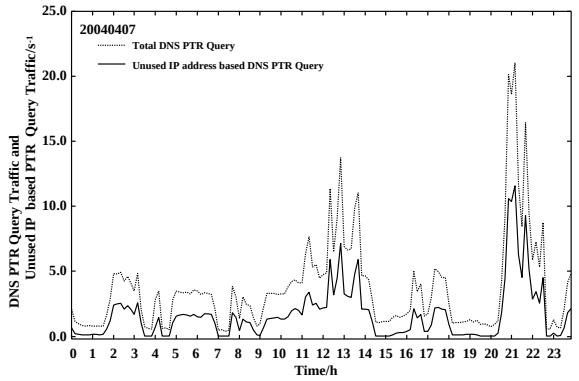

Figure 4. The DNS query PTR record traffic between the top domain DNS server and the DNS clients at April 7th, 2004 (s^{-1} unit).

(**tDNS**) through August 1st, 2003 to April 30th, 2004 (Figure 2). In Figure 2, the DNS query normal name-resolution (an A record) request packet curve changes weekly within an almost averaged value of 250,000, and the DNS query mail-exchange (an MX record) request packet curve keeps almost the same value upon going from August 1st, 2003 to April 30th, 2004.

On the other hand, the DNS query reverse (PTR record) request packet curve changes in 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 19:30 at February 1st, 2004 (Figure 3), and after this day, its value frequently exceeds the values of the other DNS query A or MX record request packets (Figure 2). Especially, the abnormal DNS query PTR record request packet traffic becomes very much high at April 7th, 2004.

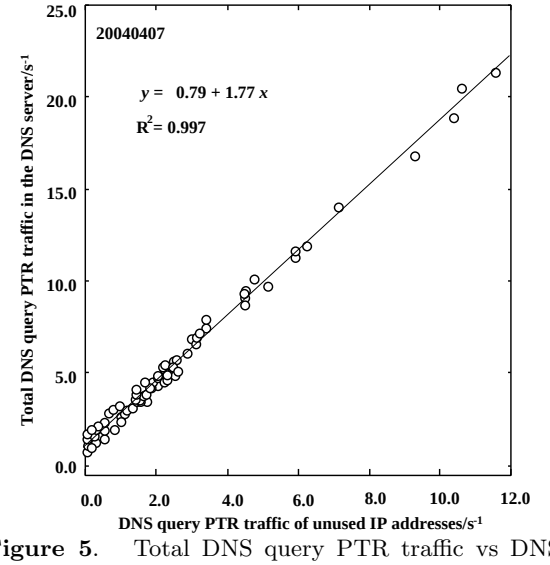

Figure 5. Total DNS query PTR traffic vs DNS query PTR traffic of unused IP addresses (April 7th, 2004). (s^{-1} unit).

Interestingly, almost request packet IP addresses of DNS clients providing the abnormal DNS query PTR record request packet traffic, belong to outside IP addresses of our university *i.e.* the numbers of both outside and inside IP addresses are calculated to be 305,358 and 17,052 packets, respectively, in the day of April 7th, 2004.

Also, the outside IP addresses of the DNS clients are variable, in other word, the clients IP address changes frequently like a distributed denial-of-service (DDoS) attack and/or DDoS attack itself. Furthermore, the DNS query content of the abnormal PTR record request packet contains unused internal IP addresses of our university.

From this point, we investigated further on the traffic of the DNS query PTR record-based DDoS attack and developed detection and prevention systems for the DDoS attack.

3. Results and Discussion

3.1 Detection of DNS query PTR record-based DDoS attack

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 4 at April 7th, 2004. In Figure 4, the total traffic

curve of the DNS query PTR record request packet and the traffic curve of the DNS query PTR record request packet changes, simultaneously. The latter traffic includes the DNS query PTR packets that contain unused IP addresses of our university as their contents. This result indicates that the abnormal DNS query PTR record-based traffic is correlated with the DNS query PTR record-based traffic in which the DNS query packet includes an unused IP address of our university network. Figure 5 shows regression analysis between total DNS query PTR record traffic versus total DNS query PTR record traffic of unused IP addresses. The data are April 7th, 2004. In Figure 5, the correlation coefficient (R^2) is 0.997. This also means that the abnormal total DNS query PTR traffic considerably correlates to the traffic of DNS query PTR packets including unused IP addresses.

It is clear that a DNS query content including an unused 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 unused IP addresses.

3.2 Development of PTRDPS

We designed and developed a new detection and prevention system for a DNS query PTR record DDoS attack (PTRDPS). This system consists of PTR record packet capture, PTR record preprocessor "arpa", a detection engine for the DDoS attack "ptrscan", and a prevention system for the DDoS attack "pfd.pl". The procedures for the detection system are properly worked out to a Perl "ptrds.pl" script that executes "ptrscan" in a time per 10 seconds.

In the PTR record packet capture, DNS query PTR record request packets and their contents are recorded and decoded with the query-logging system of BIND-9.2.3.[11]

In the preprocessor "arpa", it extracts lines describing DNS query packets only including PTR records from the syslog file in the DNS server. After discarding IP addresses of the DNS clients in

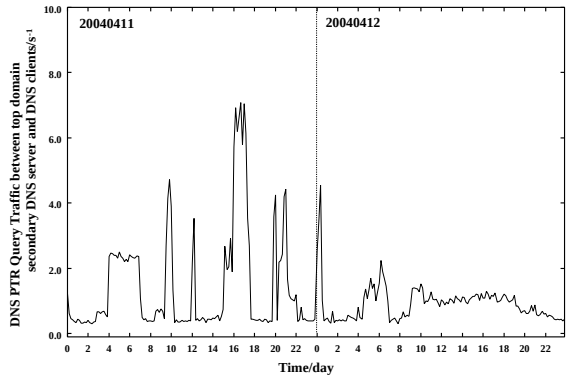

Figure 6. The DNS query PTR record traffic between the top domain DNS server and the DNS clients at April 11th to 12th, 2004 (s^{-1} unit).

our university, the preprocessor "arpa" changes a description format of an IP address in the content of PTR record packet, like sorting "D.C.B.A.in-addr.arpa" to "A.B.C.D", where A, B, C, and D indicate 8 bits unsigned integer (0-255) values. This is because the described IP address in the content of PTR record is complicated for the detection engine. This "arpa" is a packet filter to be sensitive only for a string that includes a key word as "in-addr.arpa" and it is compiled with the gcc-3.2.3 C compiler. The preprocessor is called in the following detection engine and prints out the filtered contents of the PTR record packets into a "newdb" file and the old "newdb" file is renamed as an "olddb" file.

The detection engine "ptrscan" is a C-shell script program consisting of four components, a DDoS IP detector "ddosip", a difference checker, an E-mailer without a local MTA "smail", and a registrar for an IP address-based access-control-list "ip2f". The "ddosip" program compiled by the gcc-3.2.3 C compiler is a DNS query content matcher to detect and/or sort suspicious DNS client IP addresses that contain contents as unused IP addresses of out university. The difference checker is a "diff" command with an option "-c" to check difference between "olddb" and "newdb" files. Before this difference checker, the preprocessor is called. After the checker, if the "newdb" file differs from the "olddb" one, and then this difference is e-mailed to a network manager by the "smail" command. The C-shell script "ip2f" registers the suspicious DNS client IP addresses to a

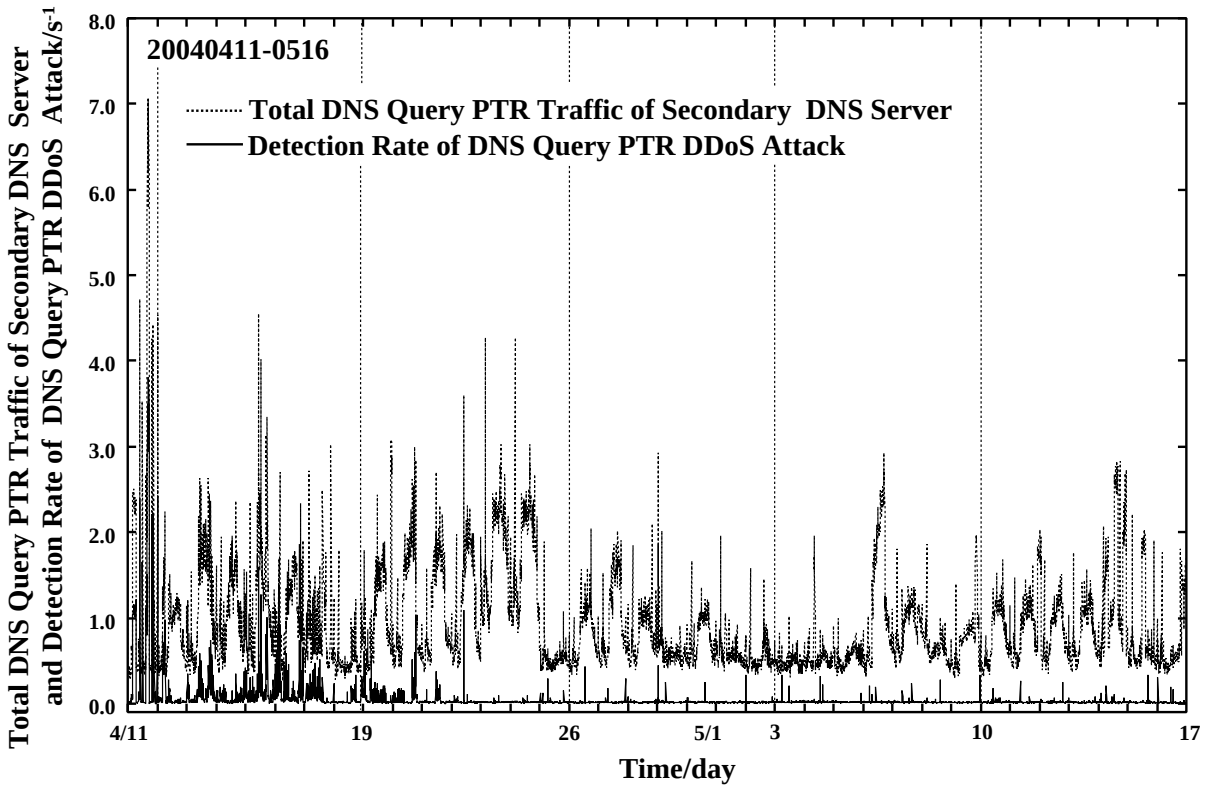

Figure 7. The DNS query PTR record traffic between the top domain DNS server and the DNS clients and the detection rate of DNS query PTR record based DDoS attack through April 11th to May 16th, 2004 (s^{-1} unit).

filtering table (an "ip2f.list" file) of the prevention system for the DDoS attack "pfd.pl".

The prevention system for the DNS query DDoS attack "pfd.pl" is a Perl script program that kicks a C-shell script program "pfdscan" in a time per 30 seconds. The "pfdscan" program scans the "ip2f.list" file and executes IP filtering with an "iptables" command of the Linux system. The "ip2f.list" table file is flushed hourly.

3.3 Evaluation

We implemented PTRDPS into the top domain DNS (**tDNS**) server and evaluated detection rate (April 12th, 2004). The machine in the evaluation has the following configuration: Intel Xeon 2.40GHz Dual CPU, 1GB main memory, Intel 100Mbps Ethernet NIC, and 80 GB ATA133 hard disk drive. The Linux kernel is currently to be a version of 2.4.26.

As shown in Figure 6, the total DNS query PTR record traffic curve changes severely before installing PTRDPS, while after the installation, the traffic curve drastically becomes mild. In Figure 7, we show observed the total DNS query PTR traffic and detection rate of the DNS query PTR record-based DDoS attack. Before installation of PTRDPS, the detection rate is observed to be 48,584 IP/day (April 11th, 2004). However, after the installation, the detection rate gradually decreases day by day, and finally is estimated to be *ca.* 1,500 IP/day after April 25th, 2004.

4. Concluding Remarks

We statistically investigated system log (syslog) files in the top domain DNS server (**tDNS**) when receiving a lot of abnormal DNS query PTR record-based packets like a denial-of-service (DDoS) attack by DNS clients from the outside of

our university. The IP addresses of the DNS clients are variable so that this DoS attack is considered to be a distributed DoS (DDoS) attack. By monitoring the DNS query accesses on **tDNS**, we have found information about detection of an IP address of a strange DNS client: (1) Usually, a DNS query PTR record packet includes only a registered and/or authorized IP address of a client, since the DNS query PTR record packet is requested to get a fully qualified domain name (FQDN) corresponding to the IP address of the client by a server daemon program when logging access of the client. Unfortunately, it can be clearly said that the DNS query PTR record packet is sent to get detailed inside information of network domain range like our university. Furthermore, in a sense, it should be a good tool for crackers to check computer security of a large scaled organization (to allow information leakage). (2) In this situation, the PTR record packet probably includes an unregistered and/or unauthorized IP address. Reversely, this fact is considerably useful for detecting an IP variable DNS query PTR record-based DDoS attack. From these points, we have developed and implemented a detection and prevention system of the DNS query PTR record-based DDoS attack (PTRDPS) into our top domain DNS server. Successfully, we have been preventing the current DDoS attack.

We continue further investigation to get more detailed information on the DDoS attack against DNS and E-mail servers.[12]

Acknowledgement. All the calculations and investigations were carried out in Center for Multimedia and Information Technologies (CMIT), Kumamoto University. We gratefully thank to all the CMIT staffs and system engineers of MQS (Kumamoto) for daily supports and constructive cooperations.

References and Notes

1) Northcutt, S. and Novak, J., *Network Intrusion Detection*, 2nd ed; New Riders Publishing: Indianapolis (2001).

2) Yang, W., Fang, B. -X., Liu, B., Zhang, H. -L., Intrusion detection system for high-speed network *Comp. Commun.*, Vol. 27, 2004 in press.

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

4) Laing, B.: How To Guide-Implementing a Network Based Intrusion Detection System, http://www.snort.org/docs/iss-placement.pdf, ISS, 2000.

5) Mukherjee, B., Todd, L., and Heberlein, K. N.: Network Intrusion Detection, *IEEE Network*, Vol. 8, No.3, pp.26-41 (1994).

6) Warrender, C., Forrest, S., and Pearlmutter, B.: Detecting Intrusions Using System Calls: Alternative Data Models, *Proc. IEEE Symposium on Security and Privacy*, No.1, pp.133-145 (1999).

7) Hofmeyr, S. A., Somayaji, A., and Forrest, S.: Intrusion Detection Using Sequences of System Calls, *Computer Security*, Vol. 6, No.1, pp.151-180 (1998).

8) Ptacek, T. H. and Newsham, T. N.: Insertion, Evasion, and Denial os Service: Eluding Network Detection, January, 1998, http://www.robertgraham.com/mirror/Ptacek-Newsham-Evasion-98.html

9) Anderson, D., Lunt, T. F., Javitz, H., Tamaru, A., and Valdes, A.: Detecting unusual program behavior using statistical component of the Next-generation Intrusion Detection Expert System (NIDES), *Computer Science Laboratory SRI-CSL-95-06*,1995.

10) http://www.snort.org/

11) http://www.isc.org/products/BIND/

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