Detection- and Prevention-System of DNS query-based Distributed Denial-of-Service Attack

Yasuo Musashi,† Seiji Hayashida,† Ryuichi Matsuba,†
Kenichi Sugitani,† and Kai Rannenberg††

†Center for Multimedia and Information Technologies
Kumamoto University 860-8555, JAPAN
E-mail: {musashi,matsuba,sugitani}@cc.kumamoto-u.ac.jp
Phone +81-96-342-3915 Fax +81-96-342-3829

††Lehrstuhl für M-Commerce uud Mehrseitige Sicherheit
Institut für Wirtschaftsinformatik
Johann Wolfgang Goethe Universität Frankfurt am Main
Gräfstr. 78 D-60054 Frankfurt/Main, GERMANY
kai.rannenberg@m-lehrstuhl.de
Phone +49-69-798-25301 Fax +49-69-798-25306

Abstract

The syslog messages of the top domain DNS (tDNS) servers in a university were statistically investigated when having receiving a large amount of DNS query packets like a distributed denial-of-service (DDoS) attack. Three types of DNS query-based DDoS attacks are found and summarized as follows: (1) In the term of February to April, 2004, the DNS-DDoS attack is mainly dominated by the PTR record-based DNS query packets from the outside of the university in which the content of the packet include an unused IP address (a dark address) in the university. (2) In the term of April of 2005, it is significantly driven by the A record based DNS query packets from the inside of the university and the contents of the packets have IP addresses directly. And (3) in the April 20th, 2005, it is surely contributed by the DNS query packets that include a fully qualified domain name (FQDN) of a subdomain E-mail sever, an FQDN of the tDNS, and two kinds of IP addresses that are related with the PC clients in the subdomain, respectively. These results are useful information for us to develop the detection and prevention systems against the DDoS attack to the DNS server and to understand what kinds of security incidents take place. Also, we have partially developed and implemented detection- and prevention-system and evaluated how it works.

Introduction

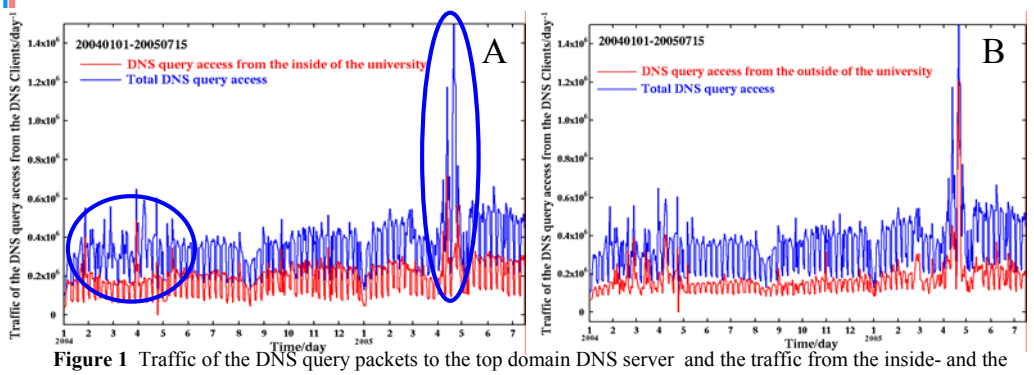


Figure 1 Traffic of the DNS query packets to the top domain DNS server and the traffic from the inside- and the outside-DNS clients in a university through January 1st, 2004 to July 15th, 2005.

The traffic of the DNS query packets in the top domain DNS server of a university was abnormally increased during both two terms in which one is the early days of February to the late days of April, 2004, and in that the other is the days of April, 2005.

The former term is mainly driven by the traffic from the outside and then the other one is dominated by both in- and outsides.

1. Introduction

It is of considerable importance to keep security of a DNS server since the DNS server 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 an E-mail server (SMTP/POP3) and/or Web browsing network applications. From this point, it is required to protect firmly the DNS server.

One of the attractive solutions to keep security of the DNS server is to employ an intrusion detection system (IDS) [1-9]. There are two types of IDSs; one is a misuse type [3,4], scanning a database of the remote attack signature and the other is an anomaly type[3-7], getting statistical profile of network packet access or anomaly use of network protocol. The IDS surely provides a plenty of useful alert messages, however, it provides too much alert ones to analyze in real time. Furthermore, the IDS is only to do detection, and we need to develop an intrusion prevention system (IPS) that automatically detects and prevents the security incidents in no distance future.

In order to develop a new useful misuse/aid-hybrid IDS/IPS against future remote attack on the DNS server, it is of considerable importance to get more detailed information for access traffic of network applications like DNS query packets between a DNS server and its DNS clients.

Recently, the top domain name server of a university has been under several DNS query packets-based distributed denial-of-service (DNS-DDoS) attacks like transmitting a lot of DNS query packets, probably because in order to crash the DNS server (Figure 1). Especially, the DNS query access traffic of the top domain DNS server of the university was abnormally increased during both two terms in which one is early days of February to the late days of April, 2004, and in that the other is the days of April, 2005. The former is mainly driven by the traffic from the outside and then the other is contributed by both inside and outside.

The present paper discusses (1) on the investigation of three different kinds of DDoS attacks through February 1st to April 30th, 2004 (the former term), April 7th to 30th, 2005 (the latter term), and April 20th, 2005 (the special day), (2) on correlation analysis of DNS query traffic between DNS server and DNS clients that especially transmit query contents including unused (dark) IP addresses [11] and several fully qualified domain names, (3) how to implement a DNS query-based DDoS attack detection system by analyzing syslog messages of the DNS server, and (4) how to prevent the DNS-DDoS attack, effectively.

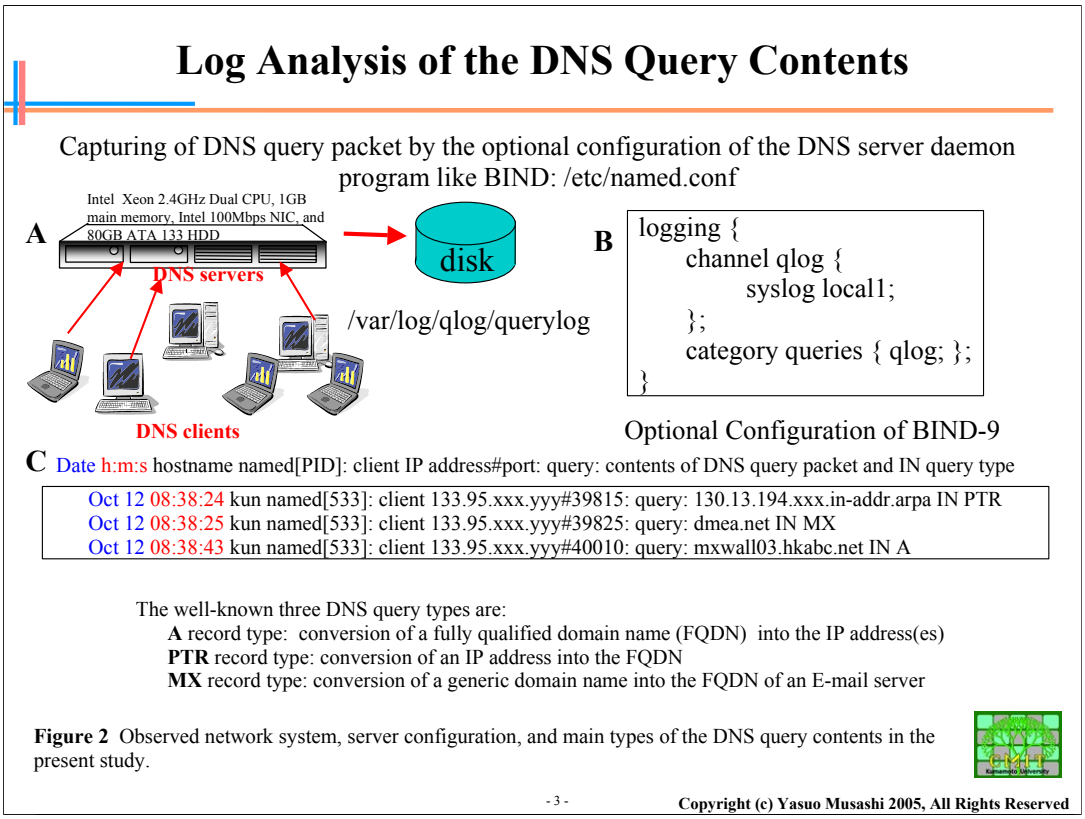


Figure 2 Observed network system, server configuration, and main types of the DNS query contents in the present study.

2. Observations

2.1 Network System

We investigated traffic of the DNS query access between the top domain DNS server (tDNS) and the DNS clients. Figure 2 shows an observed network system in the present study, an optional configuration of the BIND-9.2.3 server program daemon in tDNS, the structure of syslog messages, and the three typical DNS query types. The DNS server, tDNS, is one of the top level DNS (kumamoto-u) servers and plays an important role of domain name resolution and subdomain delegation services for many PC clients and the subdomain network servers, respectively, and the operating system is Linux OS and is currently employed kernel-2.4.30 (Intel Xeon 2.40GHz Dual CPU, 1GB main memory, Intel 100Mbps NIC, and 80GB ATA 133 hard disk drive).

2.2 Capturing of DNS Query Packets

In tDNS, BIND-9.2.3 program package has been employed as a DNS server daemon [10]. The DNS query packets and their contents have been captured and decoded by a query logging option (Figure 2B, see % man named.conf in more detail). The log of DNS query access has been recorded in the syslog files. All the syslog files are daily updated by the crond system. The line of syslog message mainly consists of the content of DNS query packet like a fully qualified domain name (an A record type), an IP address (a PTR record type), and a mail exchange (an MX record type), as shown in Figure 2C.

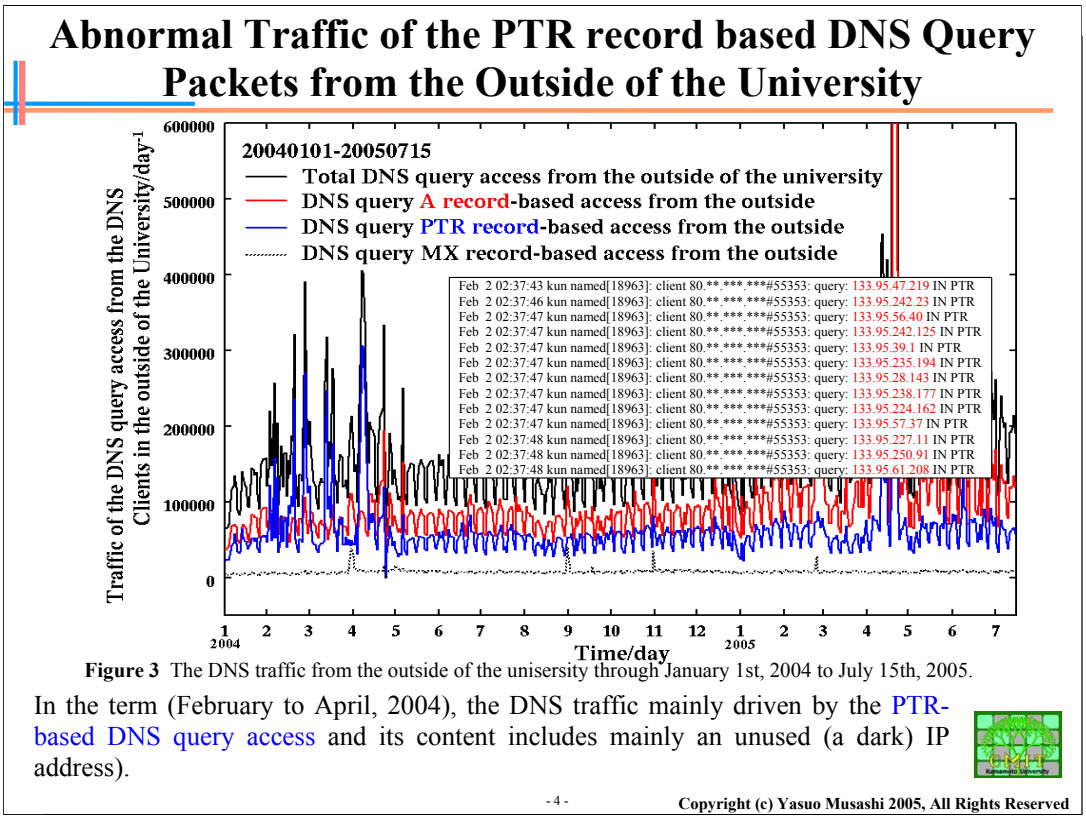


Figure 3 The DNS traffic from the outside of the uniersity through January 1st, 2004 to July 15th, 2005.

In the term (February to April, 2004), the DNS traffic mainly driven by the PTR-based DNS query access and its content includes mainly an unused (a dark) IP address).

3. Results and Discussion

3.1 Abnormal Traffic of PTR-record based DNS Query Packets

We observed traffic of DNS query packets from DNS clients in the outside the university to the top domain DNS server (tDNS) through January 1st, 2004 to July 15th, 2005 (Figure 3). In Figure 3, the A record-based DNS query traffic curve changes weekly within an averaged value of *ca.* 70,000 packet/day and the MX record based DNS query traffic curve keeps almost the same value upon going from January 1st to 31th, 2004.

On the other hand, the traffic curve of the PTR record based DNS query packets changes in almost the same manner as that of the A record based one upon going from January 1st, 2004, however, it begins to fluctuate drastically on February 1st, 2004 (Figure 3), and after this day, its value frequently exceeds the values of the other DNS query traffic curves. This situation was continued to be until April 30th, 2004 and we called as the former term. Furthermore, the total DNS query traffic from the outside of the university is mainly driven by the PTR record based DNS query traffic. Especially, the abnormal PTR record based DNS query traffic becomes very much high at April 7th, 2004.

Interestingly, the source IP addresses of these PTR record based DNS query traffic are mainly to be sent from the outside the university, and their source IP addresses changes quickly when filtering their access, in other word, the source IP addresses are variable like almost the same as a distributed denial-of-service (DDoS) attack and/or a DDoS attack itself. Hereafter, we have named this type of DDoS attack as a DNS query PTR record based DDoS attack .

Usually, the contents of PTR based record DNS query packets include an IP address in which the IP address is registered or actually used in the network. It is, however, very interesting that the abnormal PTR record based DNS query traffic includes many packets that have unused internal IP addresses of the university as their contents. From this feature, we can obtain an important information and we should investigate correlation between the total PTR record based DNS query packet traffic and the unused IP addresses-included PTR record based DNS query packet traffic.

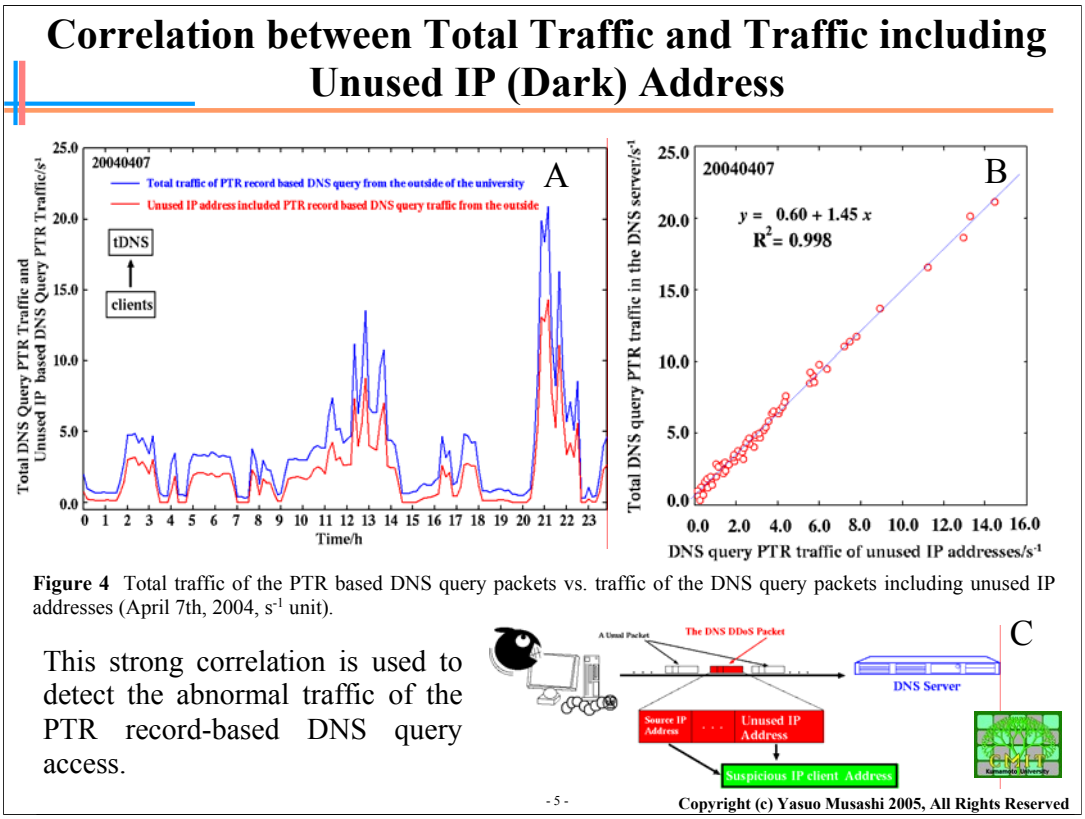


Figure 4 Total traffic of the PTR based DNS query packets vs. traffic of the DNS query packets including unused IP addresses (April 7th, 2004, s^{-1} unit).

This strong correlation is used to detect the abnormal traffic of the PTR record-based DNS query access.

3.2 Unused IP Address in the University

We illustrate the observed traffic of the PTR record based DNS query packets between the top domain DNS server (tDNS) and its clients of the outside the university in Figure 4A at the days of April 7th, 2004. In Figure 4A, the traffic curve of the PTR-record based DNS query packets and the traffic curve of the PTR based record DNS query packets that includes unused IP addresses change simultaneously. This result indicates that both traffic curves are strongly correlated each other.

Figure 4B shows regression analysis on the total traffic of the PTR record based DNS query packets versus the traffic of the PTR record based DNS query packets including unused IP addresses. The data are April 7th, 2004. In Figure 4B, the correlation coefficient (R^2) is 0.998. This also means that the total traffic of the PTR record based DNS query packets considerably correlates to the traffic of the PTR record based DNS query packets including unused IP addresses. Recently, unused IP address has been reported as a dark address or a dark address space [11], and these IP addresses are generated by the result of misconfiguration of network device such as routers, servers, and PCs, backscatter from spoofed source addresses, or scanning from mass mailing/service attack worms and other probing before attack.

As a result, it is clear that (1) the DNS query packet traffic including unused IP addresses as their contents can be clearly suspicious and then (2) we can detect the abnormal PTR record based DNS query packet traffic whether or not the DNS query contents include unused IP addresses (Figure 4C). Therefore, we developed the detection- and prevention-system against the PTR record based DNS query DDoS attack and implemented it into the top domain DNS server (tDNS).

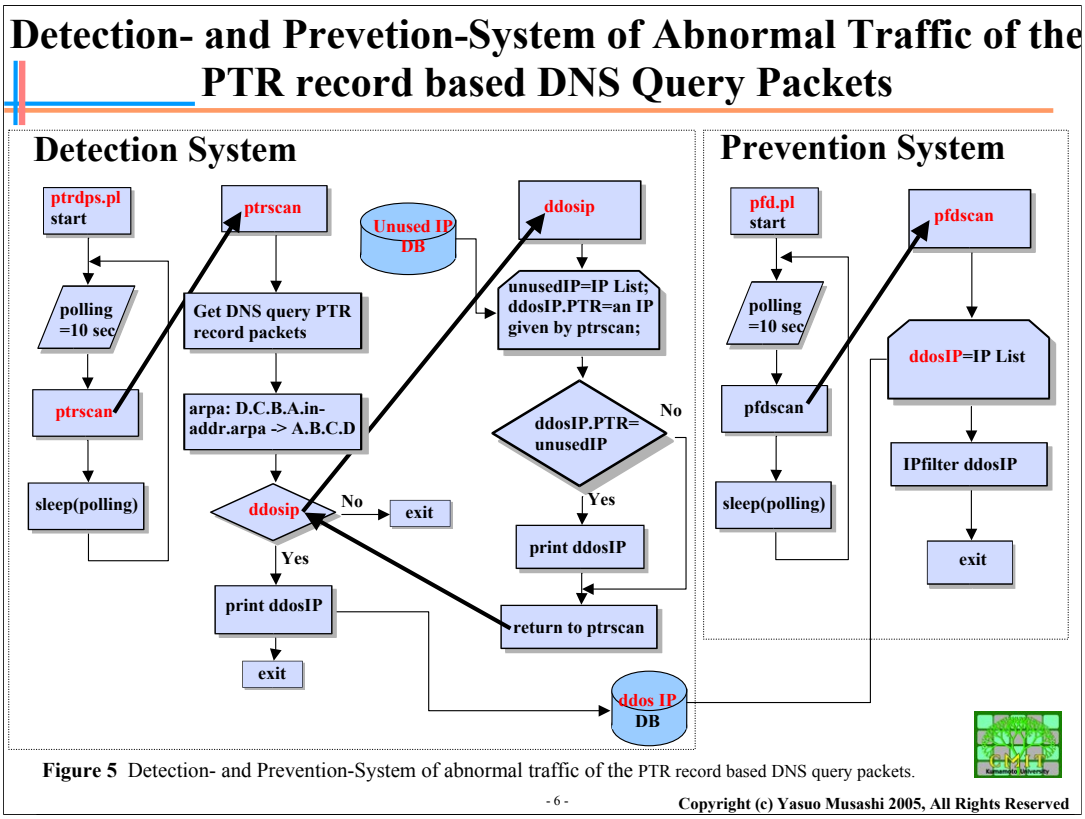


Figure 5 Detection- and Prevention-System of abnormal traffic of the PTR record based DNS query packets.

3.3 Development of PTRDPS

We designed and developed new detection and prevention systems against the PTR record based DNS query DDoS attack (PTRDPS). Figure 5 shows a procedure and program diagrams of the system. This system consists of a PTR record based DNS query packets capture, a PTR record preprocessor “arpa”, a detection engine for the DDoS attack “ptrscan”, and a prevention (filtering) 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 10 seconds.

In the PTR record capture, the PTR record based DNS query packets and their contents are decoded and recorded with the query-logging system of BIND-9.2.3[10].

In the preprocessor “arpa”, it extracts lines describing DNS query packets only including PTR records from the syslog file (/var/log/qlog/querylog) in the DNS server. After discarding IP addresses of the DNS clients in the university, the preprocessor “arpa” changes a description format of an IP address in the content of a 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 contents of the PTR record based DNS query packet is complicated for the detection engine. This “arpa” senses 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 converted contents of the PTR record based packets into a “newdb” file and the old “newdb” file is renamed as an “olddb” one.

The detection engine “ptrscan” is a C-shell script program consisting of four componets, a DDoS IP detector “ddosip”, a difference checker, an E-mailer without a local MTA “smail”, and a registra for an IP address-based access-control-list (ACL) database file. The “ddosip” program compiled by the gcc-3.2.3 C compiler checks whether or not unused IP addresses are included in the contents of the DNS query packets and shows source IP addresses of the DNS clients when detecting unused IP addresses in the university (private dark addresses).

The difference checker is a “diff” command with an option “-c” to check difference between “olddb” and “newdb” files. Before this difference checker, the proprocessor “arpa” is called. After this checker, if the “newdb” file differs from the “olddb” one, and then this difference is e-mailed to network manages by the “smail” command. The “ptrscan” script, in the last stage, registers the suspicious IP addresses of DNS clients into the ACL database file for the prevention system for the PTR record based DNS query packet DDoS attack.

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” script scans the ACL database file and executes IP filtering with an “iptables” command of the Linux system on the top domain DNS server (tDNS). The ACL database file is flushed hourly not to meet memory overflow of the “iptables”.

Results of the Detection and Prevention System: PTRDPS

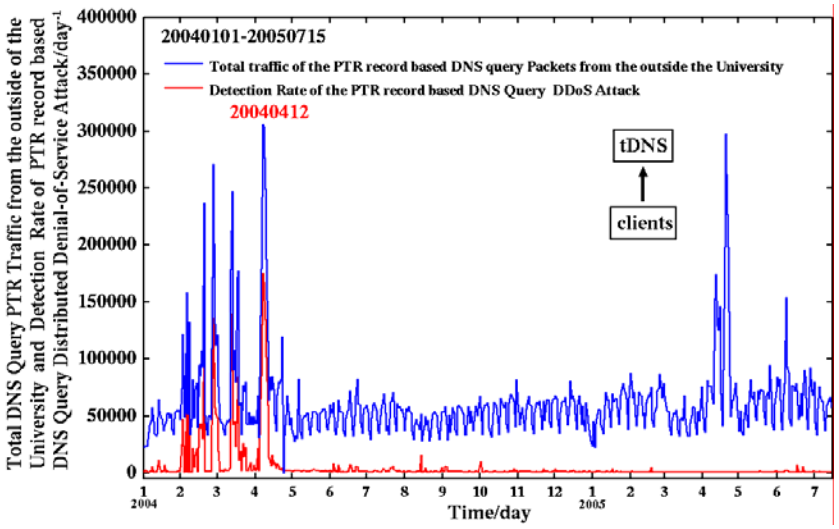


Figure 6 The total traffic of the PTR record based DNS query packets and Detection Rate of the PTR record based DNS query packets including unused IP addresses through January 1st, 2004 to July 15th, 2005 (day^{-1} unit).

- 7 -

3.4 Evaluation of PTRDPS

We installed the detection- and prevention-system of the PTR record based DNS query packet DDoS attack (PTRDPS) into the top domain DNS (tDNS) server and evaluated detection rate through January 1st, 2004 to July 15th, 2005. The machine in the evaluation has the following configuration: Intel Xeon 2.40 GHz Dual CPU, 1GB main memory, Intel 100Mbps Ethernet NIC, and 80 GB ATA 133 hard disk drive. The linux kernel is currently to be a version of 2.4.30.

As shown in Figure 6, the total traffic curve of the PTR record based DNS query packets changes severely before installing PTRDPS, while after the installation, the total traffic curve drastically to be mild (April 12th, 2004). Figure 6 also demonstrates the detection rate of the PTR record based DNS query packets DDoS attack. Before detection rate is observed to be 48,584/day in the day of April 11th, 2004. However, after the installation of PTRDPS, the detection rate decreases and it is finally observed to be ca. 1,500/day the day of April 25th, 2004. Therefore, it can be said that the detection-prevention system (PTRDPS) has been preventing the abnormal traffic of the PTR record based DNS query packets from the outside of the university.

However, the total traffic curve of the PTR record based DNS query packets severely changes through the last week of February and through the early three weeks of April, 2005. Especially, we can observe the most largest peak in April 20th, 2005 (294,287/day). At the day, the traffic of the PTR record based DNS query packets including unused IP addresses is observed to be only 573/day. This small value of the rate means that the DNS server has been attacked by the another traffic type of the PTR record based DNS query packets. Also, at this day, the A record based traffic from the outside of the university is estimated to be 889,019/day (75,000/day in usual) and this is the most largest recordable value of the total traffic A record based DNS query packets from the outside of the university in the DNS server. From these results, we investigate further on the latter term (from April 1st to July 15th, 2005) of the DNS query based DDoS attack against the top domain DNS server of the university.

Traffic of the DNS Query Packets from the In- and Outsides of the University

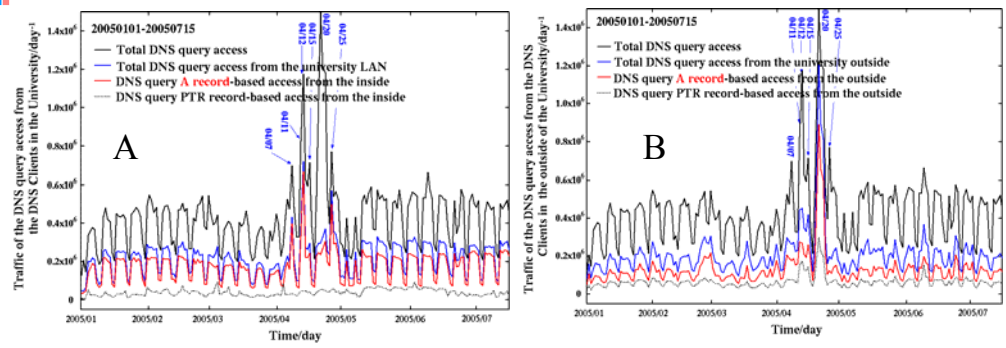


Figure 7 Traffic of the DNS query access to the top domain DNS server and the traffic from the inside- and the outside-DNS clients through January 1st, 2005 to July 15th, 2005.

In the second term (April, 2005), the DNS traffic is mainly driven by A recod-based DNS query access that is used to convert an FQDN (fully qualified domain name) into an IP address. There are five large peaks: The 04/07, 11-12,15, and 25 peaks and 04/20 one are different each other.

The former peaks are mainly dominated by the DNS query access from the DNS clients in the university, however, the latter one is contributed by the access from the outside DNS clients.

3.5 Abnormal Traffic of A Record Based DNS Query Packets

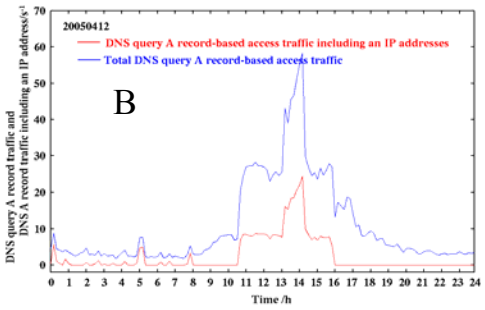
We observed the traffic of the DNS query packets from both inside and outside of the university through January 1st to July 15th, 2005 (Figure 7). In Figures 7A and 7B, we can see five large peaks of the total traffic curve of the DNS query packets in April, 2005, respectively. These peaks can be categorized the following two types: the former type of peaks at April 7th, 11-12th, 15th, and 25th, 2005, are mainly driven by the traffic of the DNS query packets from the inside the university (Figure 7A), and the latter type of peak of April 20th, 2005, is mainly dominated by the traffic from the outside of the university (Figure 7B).

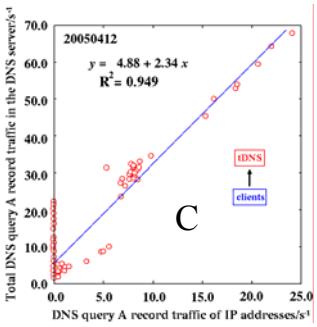
Interestingly, although the former type of peaks is almost driven by only traffic of the A record based DNS query packets, the latter one is dominated by both traffics of A and PTR records based DNS query packets, as shown in Figures 7A and 7B, respectively. We have already found that the traffic of the PTR record based DNS query packet in the latter type does not correlated with the traffic of the PTR record DNS query packets including dark IP addresses of the university (see the subsection of 3.4). Therefore, we investigated on the two different types of the five peaks.

Detection of Unusual Traffic of the A record based DNS Query Packets

A

```
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**0 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**1 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**2 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**3 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**4 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**5 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**6 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**7 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**8 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**9 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**0 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**1 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**2 IN A
Apr  7 20:03:33 kun named[678]: client 133.95.**.**#32769: query: 133.95.**.**3 IN A
```





The query contents of the DNS query access packets in the former four peaks, the IP address is directly included. Normally, only FQDN should be included in the contents of the A record based DNS query packets, however, the DNS query packets of the former peaks have IP addresses themselves as their contents. This feature is useful for detection of abnormal traffic of the A record based DNS query packets.

Figure 8 Total traffic of the A record based DNS query packets vs. traffic of the A record based DNS query packets including IP addresses (April 12th, 2005, s^{-1} unit).

3.6 Abnormal DNS Traffic of A record based DNS query packets

We observed traffic of the A record based DNS query packets between the top domain DNS (tDNS) server and the DNS clients in the university at the day of April 12th, 2005, as shown in Figure 8. This is because the traffic of the A record based DNS query packets becomes to be one of the largest peaks in the former type at this day in which the traffic is observed to be 666,261/day (about 120,000/day in usual). In Figure 8A, we can show the contents of the A record DNS query packets. Surprisingly, these contents include many IP addresses directly. Normally, only a fully qualified domain name (FQDN or host.domain name) should be included as contents in the A record based DNS query packets. These results can be also found in the contents of the other three peaks at April 7th, 15th, and 25th, 2005, respectively.

Hence, it is interesting to compare between both traffics: One is the total traffic of the A record based DNS query packets and the other is the traffic of the A record based DNS query packets that include IP addresses straightly as their contents.

Also, we illustrated the observed traffic of the A record based DNS query packet between tDNS and the DNS clients in the university in Figure 8B. Surely, the total traffic curve of the A record packets is similar to that of the A record packets including IP addresses. Figure 8C shows regression analysis on the total traffic of the A record based DNS query packets versus the traffic of the A record based DNS query packets including IP addresses as their contents. The data are April 12th, 2005 and the correlation coefficient (R^2) is 0.949. This means that the abnormal traffic of the A record based DNS query packets considerably correlates with that of the DNS query packets directly including IP addresses.

As a result, it is clear that (1) the contents of the abnormal A record based DNS query packets include directly IP addresses, (2) the total traffic of the A record based DNS query packets and the traffic of the A record based DNS query packets that include directly IP addresses considerably correlate each other, and (3) this feature can be useful for detecting abnormal traffic of the A record based DNS query packets and preventing it.

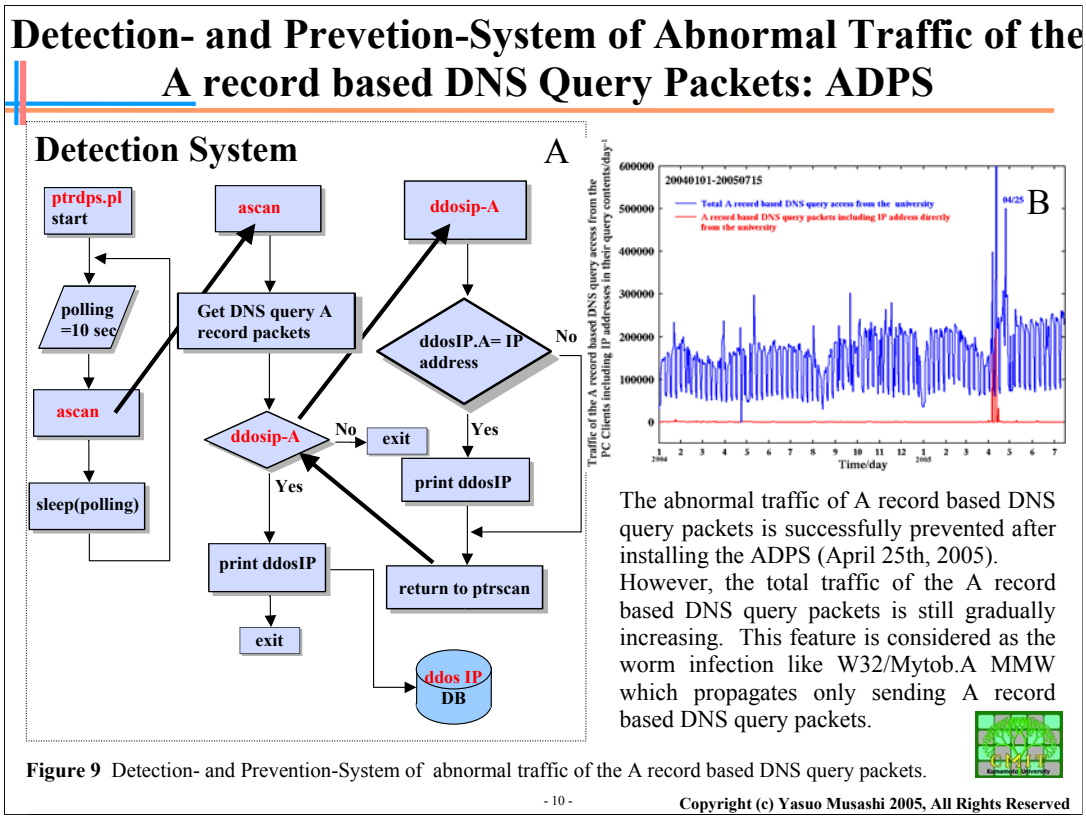


Figure 9 Detection- and Prevention-System of abnormal traffic of the A record based DNS query packets.

3.7 Developing of ADPS

We designed and developed new detection and prevention systems against the A record based DNS query DDoS attack (ADPS). Figure 9A shows a procedure and program diagrams of the system. This system consists of an A record based DNS query packets capture, a detection engine for the DDoS attack "ascan", and a prevention (filtering) system for the DDoS attack "pfd.pl". The procedures for the detection system are properly worked out to a Perl "ads.pl" script that executes "ascan" in a time 10 seconds. In the A record capture, the A record based DNS query packets and their contents are decoded and recorded with the query-logging system of BIND-9.2.3[10].

Preprocessing of the A record based DNS query packets is carried out with the "grep" command in the following detection engine and prints out the extracted contents of the A record based packets into a "newdb" file and the old "newdb" file is renamed as an "olddb" one.

The detection engine "ascan" is a C-shell script program consisting of four componets, a DDoS-A IP detector "ddosip-A", a difference checker, an E-mailer without a local MTA "smail", and a registra for an IP address-based access-control-list (ACL) database file. The "ddosip-A" program compiled by the gcc-3.2.3 C compiler checks whether or not IP addresses are included in the contents of the DNS query packets and shows source IP addresses of the DNS clients when detecting IP addresses in the contents.

The difference checker is a "diff" command with an option "-c" to check difference between "olddb" and "newdb" files. After this checker, if the "newdb" file differs from the "olddb" one, and then this difference is e-mailed to network manages by the "smail" command. The "ascan" script, in the last stage, registers the suspicious IP addresses of DNS clients into the ACL database file for the prevention system against the A record based DNS query DDoS attack. This ACL database file is the same one in PTRDPS *i.e.* the prevention system for ADPS shares the same prevention system in the previous one.

3.8 Evaluation of ADPS

The new system, ADPS, has been installed into the top domain DNS (tDNS) server from the day after April 26th, 2005. As shown in Figures 7A and 7B, after the day of April 26th, 2005, the total traffic of the A record based DNS query packets from the DNS clients in the university gradually decreases from 484,495/day in April 25th to 80,411/day in April 30th, 2005 (about 120,000/day in usual). However, the traffic of the A record based DNS query packets is smaller than those in April 7th and 15th, 2005, and the total traffic of the A record based DNS query packets from the university is still gradually increasing (Figure 9B). The former is caused by mistaken in the subdomain DHCP server and the latter maybe caused by the worm infection of W32/Mytob.A mass mailing worm (MMW). This is because the W32/Mytob.A propagate itself by mass mailing worm infection but it sends only A record based DNS query packets without a mail exchange (MX) resolution (no MX record based DNS query packet is send when propagating itself unlike W32/Netsky.P or W32/Sobig.C).

Abnormal Traffic of A and PTR records based DNS query access

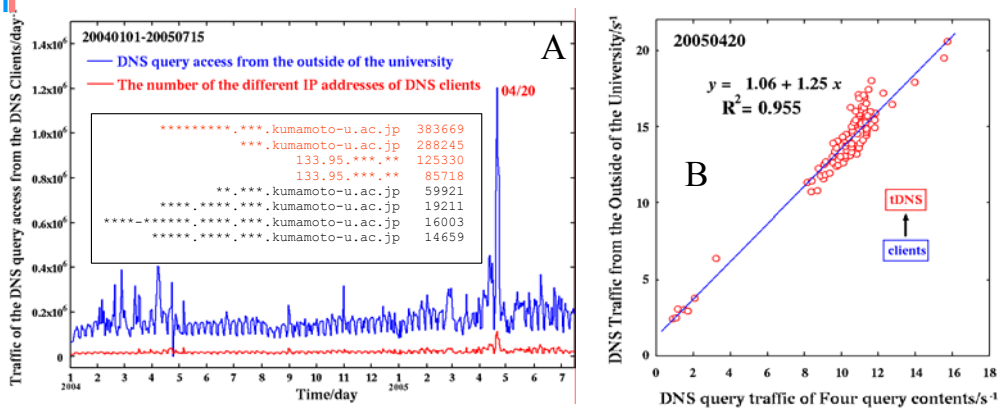


Figure 10 DNS Traffic from the Outside the University vs. DNS query traffic of Four-qeury contetns (April 20th, 2005, s^{-1} unit)

In the query contents of the DNS query packets in the latter peak, the most largest number of contents mainly consist of an FQDN of a subdomain E-mail server, an FQDN of top domain DNS server (tDNS), and two IP addresses that related with the subdomain, respectively. Since the E-mail server is claimed as a spam-sender through the the day of April 20th, 2005, the top DNS server are severely accessed by the spam-mail detection system/spam filter world-widely at the day.

3.9 Abnormal DNS Traffic of A and PTR records based DNS query packets

We observed both traffics of the DNS query packets and the kinds of source IP addresses of DNS query packets between the top domain DNS (tDNS) server and the DNS clients of the outside the university through January 1st, 2004 to July 15th, 2005, as shown in Figure 10A. This is because, firstly, we failed statistically to find out the suspicious source IP addresses of the abnormal traffic of the DNS query packets and then we noticed that the abnormal traffic would be a large-scaled source IP DDoS attack. In Figure 10A, we can see correlation between the total traffic and the traffic of the kinds of source IP addresses in the DNS query packets from the outside of the university. This feature seems to be a large-scaled DDoS attack.

We can also demonstrate statistics of the contents for the A and PTR records based DNS query packets at April 20th, 2005. Expectedly, it is found that contents statistically consist of two fully qualified domain names (FQDNs) for the A record DNS query packets and two different IP addresses for PTR record DNS query packets, respectively, *i.e.* the traffic of the A and PTR records based DNS query packets from the outside of the university mainly driven by these four keywords of query contents. These four keywords are an FQDN of an subdomain E-mail server, an FQDN of tDNS, and IP addresses of the PC clients in the subdomain.

In order to confirm this result, we performed regression analysis on the total traffic of the A and PTR records DNS query packets from the outside of the university versus the traffic of the A and PTR records based DNS query packets including the four keywords (Figure 10B). The data are April 20th, 2005 and the correlation coefficient (R^2) is 0.955. This result indicates that the abnormal traffic of the A and PTR record based DNS query packet considerably correlates to that of the DNS query packets including four keywords. Fortunately, the fact of this abnormal A and PTR records based DNS query traffic can be easily understood since we have received a lot of spam relay or claiming E-mails probably generated automatically and/or manually by the spam filter or the manager of the E-mail servers and we have also found the same subdomain name, FQDNs, and IP addresses in the four keywords.

As a result, it can be clearly concluded that (1) the query contents of the abnormal A and PTR records based DNS query packets at April 20th, 2005, statistically can be sorted as four keywords which mainly consist of two FQDNs of the subdomain E-mail server and the top domain DNS (tDNS) server, respectively, and the two different IP addresses in the subdomain, and (2) the abnormal traffic like a large-scaled DDoS attack is caused by a great large amount of the DNS resolution accesses from the spam filter of the E-mail servers in the internet.

Conclusion and Future Work

We performed detailed analysis on the syslog files in the top domain DNS (tDNS) server.

The three types of abnormal traffic of the DNS query packets were found:

Traffic of the PTR record based DNS query packets including unused IP addresses as their contents and from the outside of the university.

Traffic of the A record based DNS query packets including IP addresses and from the inside the university.

Traffic of the DNS resolution accesses from the spam filter of the E-mail servers on the internet.

We have developed and installed new DDoS attack detection- and prevention-system (PTRDPS/ADPS) into the top domain DNS server and we are just testing it.

- 12 -

Conclusion and Future Work

We statistically investigated systlog files in the top domain DNS server (tDNS) when observing abnormal traffic of DNS query packets. These abnormal traffic are categorized three types: (1) The first is abnormal traffic of the PTR record based DNS query packets including unused (dark) IP addresses as their contents from the outside of the university. (2) The second is abnormal traffic of the A record based DNS query packets that include directly IP addresses as query contents. And (3) the third is the a large-scaled DNS resolution access from the spam filter in the internet. We have developed and installed the detection- and prevention-system (PTRDPS/ADPS) into tDNS and we are currently testing it.

References

[1] S. Nothcutt and J. Novak, "Network Intrusion Detection," 2nd ed; New Riders Publishing: Indianapolis, 2001.

[2] W. Yang, B. –X. Fang, B. Liu, and H. –L. Zhang, "Intrusion detection system for high-speed network, Comp. Commun., Vol. 27, No. 13, 2004, pp.1288-1294.

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

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

[5] B. Mukherjee, L. Todd, and K. N. Herberlein, "Network Intrusion Detection," IEEE Network, Vol. 8, No. 3, 1994, pp.26-41.

[6] S. A. Hofmeyr, A. Somayji, and S. Forrest, "Intrusion Detection Using Sequences of System Calls," Computer Security, Vol. 6, No. 1, 1998, pp.151-180.

[7] T. H. Ptacek and T. N. Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Detection," January, 1998, http://www.robertgraham.com/mirror/Ptacek-Newsham-Evasion-98.html.

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

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

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

[11] E. Cooke, M. Bailey, Z. M. Mao, D, Watson, F. Jahanian, and D. McPherson, "Toward understanding distributed blackhole placement," Proc. the 11th ACM Conference on Computer and Communications Security (CCS'04), Washington DC, USA, 2004, pp.54-64.