Abnormal DNS Query Traffic from IPv6 based DNS Clients

Hirofumi Nagatomi,[†] Dennis A. Ludeña R.,[†] Yasuo Musashi[††]
Ryuichi Matsuba, [††] and Kenichi Sugitani [††]

[†]Graduate School of Science and Technology
Kumamoto University, 860-855, JAPAN
E-mail: {nagatomi,dennis}@st.cs.kumamoto-u.ac.jp
Phone +81-96-342-3013

[††]Center of 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

Abstract

We have investigated statistically on the abnormal traffic of the DNS query packets that have an IPv6-based source IP address in a university campus network through 2005. The following three interesting results are found, as follows: (1) In the DNS query access traffic on April 20th, 2005, the A and PTR records based DNS query packets were observed including 4 keywords like hostdomain names and IP addresses in the university. (2) In the traffic at August 30th, 2005, the abnormal PTR record based DNS query packet traffic mainly includes a lot of IP addresses of the university, as their query contents. And (3) the abnormal A record based DNS query packet traffic including the six keywords like “mx”, “ns”, “mail”, “gate”, “smtp”, and “relay” were observed through August 5th to December 10th, 2005. From these results, we can reasonably concluded that we should pay much attention not only IPv4 address based packet traffic but also IPv6 address based one when detecting the security incident in the campus or enterprise network system.

Introduction

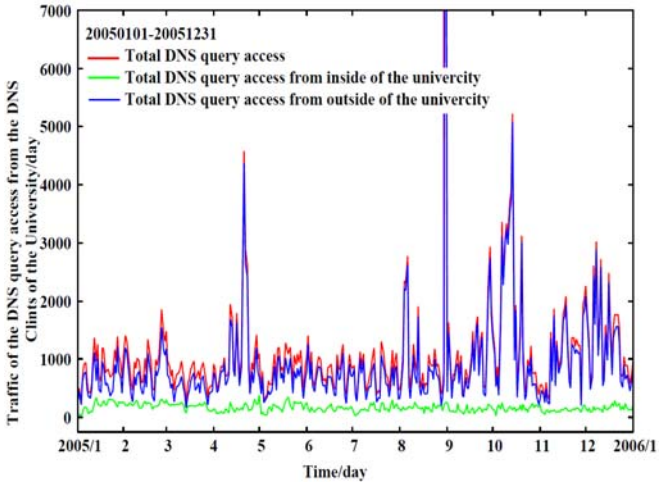


Figure 1 Traffic of the DNS query packets to the top domain DNS server and the traffic from the inside- and the outside-DNS clients in a university through January 1st, 2005 to December 31st, 2005.

The total DNS query traffic from the IPv6-based DNS clients is mainly driven by that from the outside of the university.

- 2 -

1. Introduction

It is of considerable importance to keep security of a domain name system (DNS) server in the information and communication technology (ICT)-based societies since the almost network application strongly depends on the domain name resolution services at their initial stages like, for example, a host domain name for a web site in the Web browser (a standard name resolution), the IP addresses of the PC clients for several network application servers (a reverse name resolution), and a host domain name of the E-mail servers by a simple mail transfer protocol (SMTP; E-mail) server daemon program (a mail exchange name resolution). The DNS service is requested by DNS clients with a DNS query packet such as A (Address), PTR (Pointer), or MX (mail exchange) record based UDP packet mainly and they correspond to standard, reverse, and mail exchange name resolution accesses, respectively. If the DNS stops, the almost the network applications will crash.

One of the attractive solutions to keep security of the DNS server is to employ an intrusion detection system (IDS) [1-6]. The IDS surely provides a plenty of useful alert messages, however, it provides too much alert ones to analyze in real time (false positive or negative). In order to develop a new useful 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, we observed traffic of the DNS query packets that have an IPv6 based source IP address in the top domain name system (tDNS) server of a university (Figure 1). Interestingly, the total traffic is mainly driven by the traffic from the outside of the university and several peaks can be found in Figure 1. These peaks are categorized into three groups. The first is a peak at April 20th, 2005, the second is a peak for August 30th, 2005, and the last is a group for April 20th, August 5th, September 28th, October 13th, and December 10th, 2005.

The present paper discusses on the abnormal IPv6 address based DNS query traffic consisting of (1) the A and PTR records based DNS query packets at April 20th, 2005, (2) the PTR record based DNS query packets at August 30th, 2005, and (3) the A record based DNS query packets at August 5th, September 28th, October 13th, and December 10th, 2005 (see Figure 1).

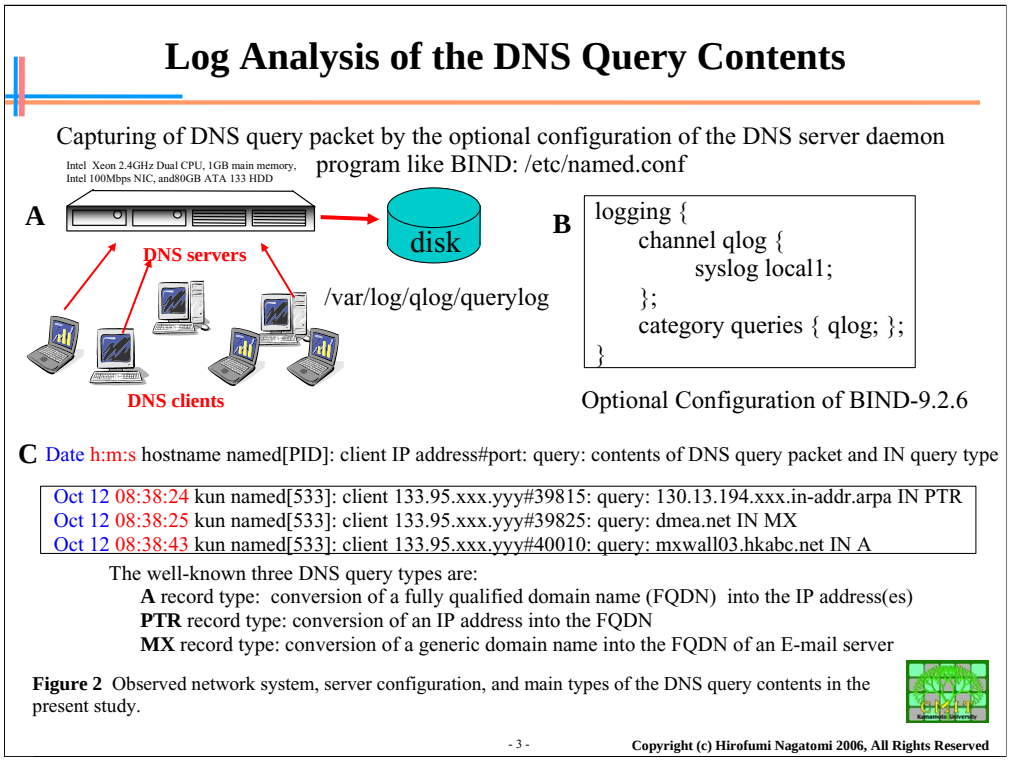


Figure 2 Observed network system, server configuration, and main types of the DNS query contents in the present study.

2. Observations

2.1 Network System

We investigated traffic of the IPv4/IPv6 address based 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-9.2.6 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 in the university, respectively, and the operating system is Linux OS and is currently employed kernel-2.4.32.

2.2 Capturing of DNS Query Packets

In tDNS, BIND-9.2.6 program package has been employed as a DNS server daemon [7]. 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.

A, PTR, and MX records based DNS Query Traffic (IPv6)

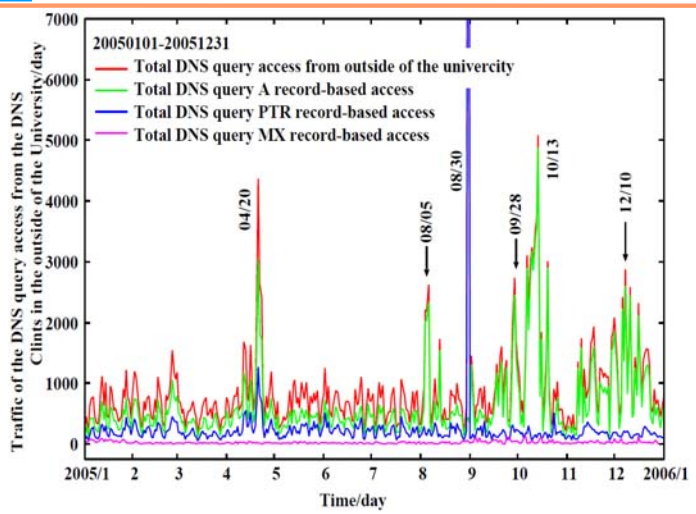


Figure 3 Traffic of the DNS query packet access from the outside of the university.

Several interesting peaks can be found: (i) April 20th, (ii) August 5th, (iii) August 30th, (iv) September 28th, (v) October 13th, and (vi) December 10th, 2005.

3. Results and Discussion

3.1 Abnormal IPv6 based DNS Query Packet Traffic

We observed traffic of IPv6 source IP address-based DNS query packet from DNS clients in the outside the university to the top domain DNS server (tDNS) through January 1st to December 31st, 2005 (Figure 3). In Figure 3, the A and PTR records based DNS query traffic curves change weekly within averaged values of *ca.* 400 and 270 packet/day, respectively, and the MX record based DNS query traffic curve keeps almost the same value of *ca.* 20 packet/day. In Figure 3, we can find several interesting peaks of (i) April 20th, (ii) August 5th, (iii) August 30th, (iv) September 28th, (v) October 13th, and (vi) December 10th, 2005.

In the first peak (i), the both traffic curves of the A and PTR records based DNS query packets changes simultaneously and the total DNS query traffic from the outside university is dominated by the both A and PTR record based DNS query packet traffics. In the other peaks (i)-(vi), we can observe the traffic curves are mainly driven by the A record based DNS query packet traffic ones. Exceptionally, the third peak (iii) is mainly contributed by the PTR record based DNS query packet traffic. Therefore, the peaks (i)-(vi) should be categorized into three groups, as follows: (1) The first group consists of (i), (2) the second group is assigned to (iii), and (3) the third group includes (ii), (iv), (v) and (vi). Therefore, we investigated furthermore on the three groups.

Abnormal A and PTR records based DNS Query Traffic

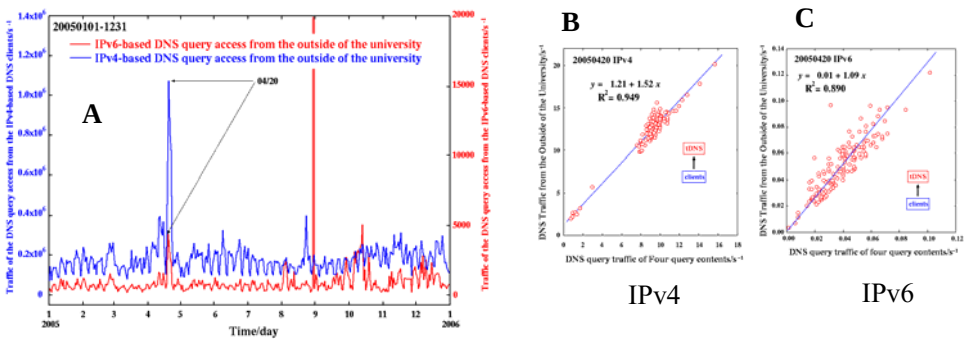


Figure 4 Total DNS query traffic from the outside of the university vs. DNS query traffic of four query contents (April 20th, 2005, s^{-1} unit)

In the query contents of the DNS query packets in the peak at April 20th, 2005, 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 PC clients in the subdomain, respectively. Since the E-mail server is claimed as a spam-sender through the day of 20th April, 2005, the top DNS server are severely accessed by the spam-mail detection system/spam filter world-widely at the day.

DNS query contents	IPv4	IPv6
*********.**.kumamoto-u.ac.jp	230,729	1,345
133.95.***.**	216,798	265
***.kumamoto-u.ac.jp	180,298	999
133.95.***.**	152,548	377

- 5 -

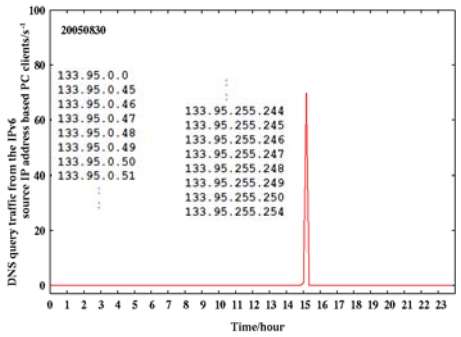
3.2 Abnormal Traffic of A and PTR records based DNS Query Packets

Firstly, we illustrate the observed IPv4/IPv6 address based DNS query packet traffic between the top domain DNS server (tDNS) and the DNS clients from the outside the university in Figure 4A through January 1st to December 31st, 2005. In Figure 4A, we can find a couple of peaks at April 20th, 2005, in the IPv4 and IPv6 addresses based traffic curves. The both IPv4 and IPv6 addresses based DNS query traffic consist of the A and PTR records based DNS query packets (see Figure 3). Unexpectedly, we failed statistically to find out the suspicious source IP addresses of the abnormal DNS query traffic at April 20th, 2005, and then we noticed that the abnormal traffic would be a large-scale IP address distributed denial of service (DDoS) attack.

We can also demonstrate statistics of the contents for the A and PTR record based DNS query traffic at April 20th, 2005. the top-four keywords for query contents are shown in table of Figure 4. Interestingly, the same keywords can be observed in the top keywords for query contents of the IPv4 and IPv6 addresses based DNS query traffics. The four keywords are related with two fully qualified domain names (FQDNs) of a subdomain E-mail server and the top domain DNS (tDNS) server, respectively, and the other two different IP addresses in the subdomain.

In order to confirm this result, we performed Figures 4B and 4C show regression analysis on the total traffic of the 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. The data are April 20th, 2005. In Figures 4B and 4C, the correlation coefficients of the IPv4 and IPv6 addresses based DNS traffics (R^2) are calculated to be 0.949 and 0.890, respectively. This also means that the total DNS query traffic from the outside of the university considerably correlates to the traffic of the A and PTR records based DNS query packets including the four keywords at April 20th, 2005. 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 check filter or the manager of E-mail servers in the internet and we have also found the same subdomain name, FQDNs, and IP addresses of the four keywords in the E-mails.

Abnormal PTR based DNS Query Traffic



DNS client IP address	Top access clients
2001:1***:10**::2	22,001
2001:1***:10**::4	20,538
2001:2f8:14:**::64	229
3ffe:8200:0:10:250:****:fe00:****	135
3ffe:8200:0:10:250:****:fe00:****	67

Figure 5 Traffic of the DNS query packets from the IPv6 based DNS clients.

The abnormal DNS query traffic is observed in the short period of time through 15:09-15:19 at August 30th, 2005. In the traffic, the two top DNS clients are found and they belong to the same site. The traffic mainly consists of the PTR record based DNS query packets including internal IP addresses of the university. Probably, the DNS clients tried to scan the hosts in the university.

- 6 -

3.3 Abnormal PTR based DNS Query Traffic

We observed the abnormal IPv6 address based traffic of the DNS query packets from the outside of the university to the top domain DNS server through the day of August 30th, 2005 (Figure 5). In Figure 5, the main traffic starts from 15:09 and almost ends after 15:19, *i.e.* it takes a short period of time, as only 10 minutes. Surprisingly, the IPv6 address based DNS query traffic takes a rate of 43,151 packet/day (the usual rate; *ca.* 700 packet/day). The traffic rate consists of the A, A6, AAAA, PTR, MX, and TXT records based DNS query traffic ones of 257, 109, 75, 42,659, 47, and 4 packet/day, respectively. This feature indicates that the abnormal DNS query traffic is surely driven by the PTR record based DNS query traffic.

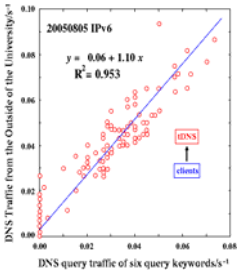
As shown in a table in Figure 5, the top two DNS query access clients can be found. We can also detect the IP addresses of the university (from 133.95.0.0 to 133.95.255.255) in the query contents of the abnormal PTR record based DNS query packet traffic. As a result, it can be clearly said that the abnormal PTR record DNS query packet traffic is generated as the pre-scanning and/or pre-investigation to search the next victim PC clients in the university before security attack against the university.

Abnormal A record based DNS Query Traffic

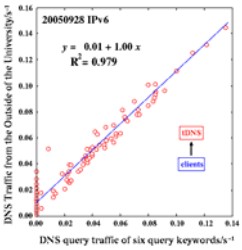
A

1 Character		2 Character		3 Character		4 Character		5 Character	
1041	m	682	mx	339	mai	339	mail	233	gate.
285	g	345	ma	233	gat	233	gate	207	relay
222	n	259	ga	231	mx.	226	mx1.	194	mail1
207	r	215	ns	226	mx1	225	mxs.	172	smtp.
202	s	207	re	225	mxs	207	rela	145	mail.
114	k	172	sm	215	ns.	172	smtp	73	kun.k
51	h	111	ku	207	rel	73	kun.	51	hpx.m
36	w	51	hp	172	smt	51	hpx.	32	kuc-
24	a	35	ww	73	kun	32	kudc	27	mxs.a

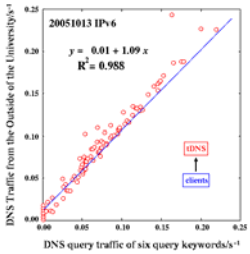
B



C



D



E

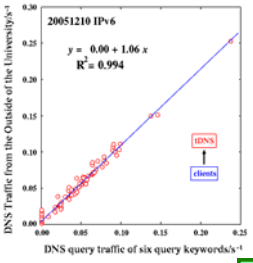


Figure 6 Total DNS query traffic from the outside of the university vs. DNS query traffic of four query contents at August 5th, September 28th, October 13th, and December 10th, 2005(s^{-1} unit)

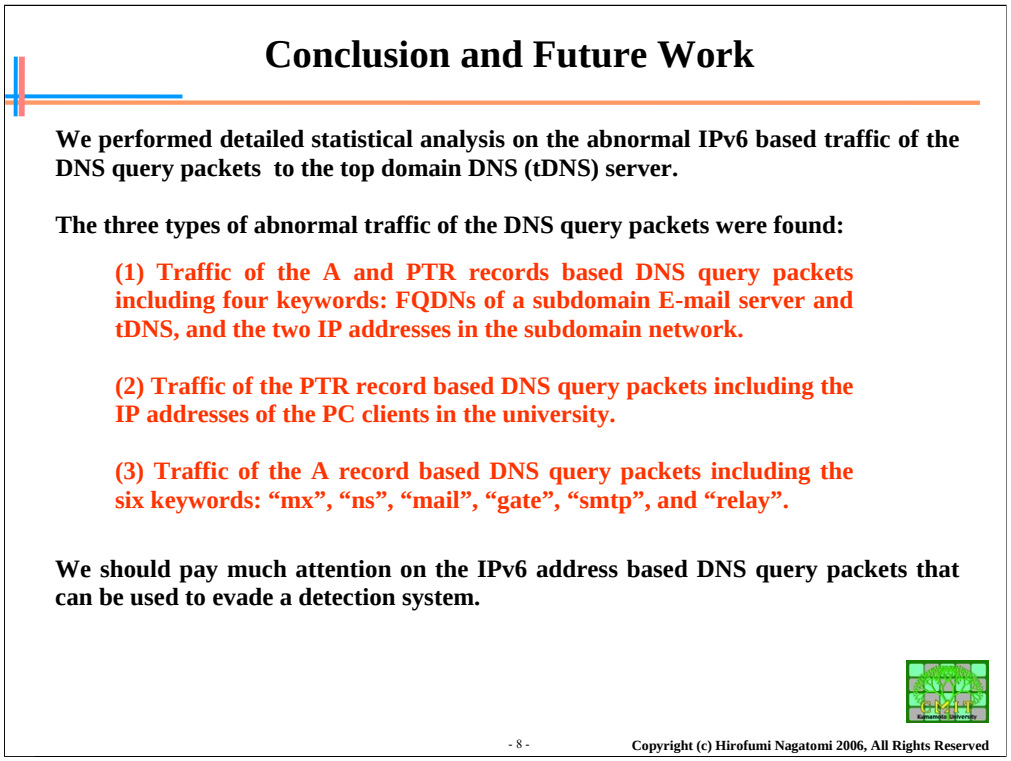
- 7 -

3.4 Abnormal Traffic of the A record based DNS Query Packets

We can demonstrate statistics of the query contents for the A record based DNS query packets in the IPv6 address based DNS traffic from the outside of the university through the day of August 5th, 2005, shown in Figure 6A. In Figure 6A, several interesting six keywords of "mx", "ns", "mail", "gate", "smtp", and "relay", are found. The six keywords are typically included in the DNS query packets that are transmitted from a mass mailing worm (MMW) and/or a bot worm (BW)-infected PC clients, such as W32/Mydoom MMW, W32/Mytob BW, and/or several W32/Zotob BW variants. Musashi *et al.* reported that the W32/Mydoom MMW and the W32/Mytob BW transmit the A record DNS query packets when attacking on the next vulnerable victim PC terminals [8].

Figures 3B-3E show 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 the six keywords. The data are August 5th, September 28th, October 13th, and December 10th, 2005 In Figure 3B, 3C, 3D, and 3E, the correlation coefficients (R^2) are calculated to be 0.953, 0.979, 0.988, and 0.994, respectively. This also means that the total traffic of the A record based DNS query packets correlates that of the A record based DNS query packets including the six keywords.

As a result, it is clear that the abnormal A record DNS query traffic in the days of August 5th, September 28th, October 13th, and December 10th, 2005, are mainly transmitted from the PC clients infected with the W32/Mydoom MMW, or W32/Mytob and W32/Zotob BW variants.



4. Conclusion and Future Work

We statistically investigated syslog files in the top domain DNS server (tDNS) in a university when observing abnormal IPv6 address based traffic of DNS query packets. These abnormal traffic are categorized with the following three types: (1) First is abnormal traffic of the A and PTR records based DNS query packets including the four keywords, (2) Second is abnormal traffic of the PTR record based DNS query packets that include the IP addresses in the university, and (3) Last is the abnormal traffic of the A record based DNS query packets including the six keywords that related to a simple mail transfer protocol (SMTP) engine of the mass mailing worm (MMW) and/or a bot worm (BW). From these results, we should pay much attention on the IPv6 address based DNS query packets that can be used to evade a detection system and implement this first knowledge in the IDS of our University as a first step of a future study.

References

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

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

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

[4] 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.

[5] 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.

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

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

[8] Y. Musashi, R. Matsuba, and K. Sugitani, “Detection, Prevention, and Managements of Security Incidents in a DNS Server”, *Proceeding for the 4th International Conference on Emerging e-learning Technologies and Applications (ICETA2005)*, Košice, Slovakia, 2005, pp.207-211.