Statistical Analysis in Log Files of Electronic-Mail Server and Domain Name System Server. SPAM Mail Generates Many DNS Query Packets

YASUO MUSASHI,† RYUICHI MATSUBA,† and KENICHI SUGITANI†

†*Center for Multimedia and Information Technologies*
Kumamoto University
Kumamoto-City, 860-8555, JAPAN
E-mail: musashi@cc.kumamoto-u.ac.jp

Recently Security Incidents in the University

(1) W32.Blaster/W32.Welchia
(2) W32.Sobig.F
(3) W32.Slammer
(4) Falsifying "From: " addresses by KLEZ MMW
(5) Hi-jacking the network server
(6) Defacing of Home Pages
(7) Flamming in the BBS
(8) .....

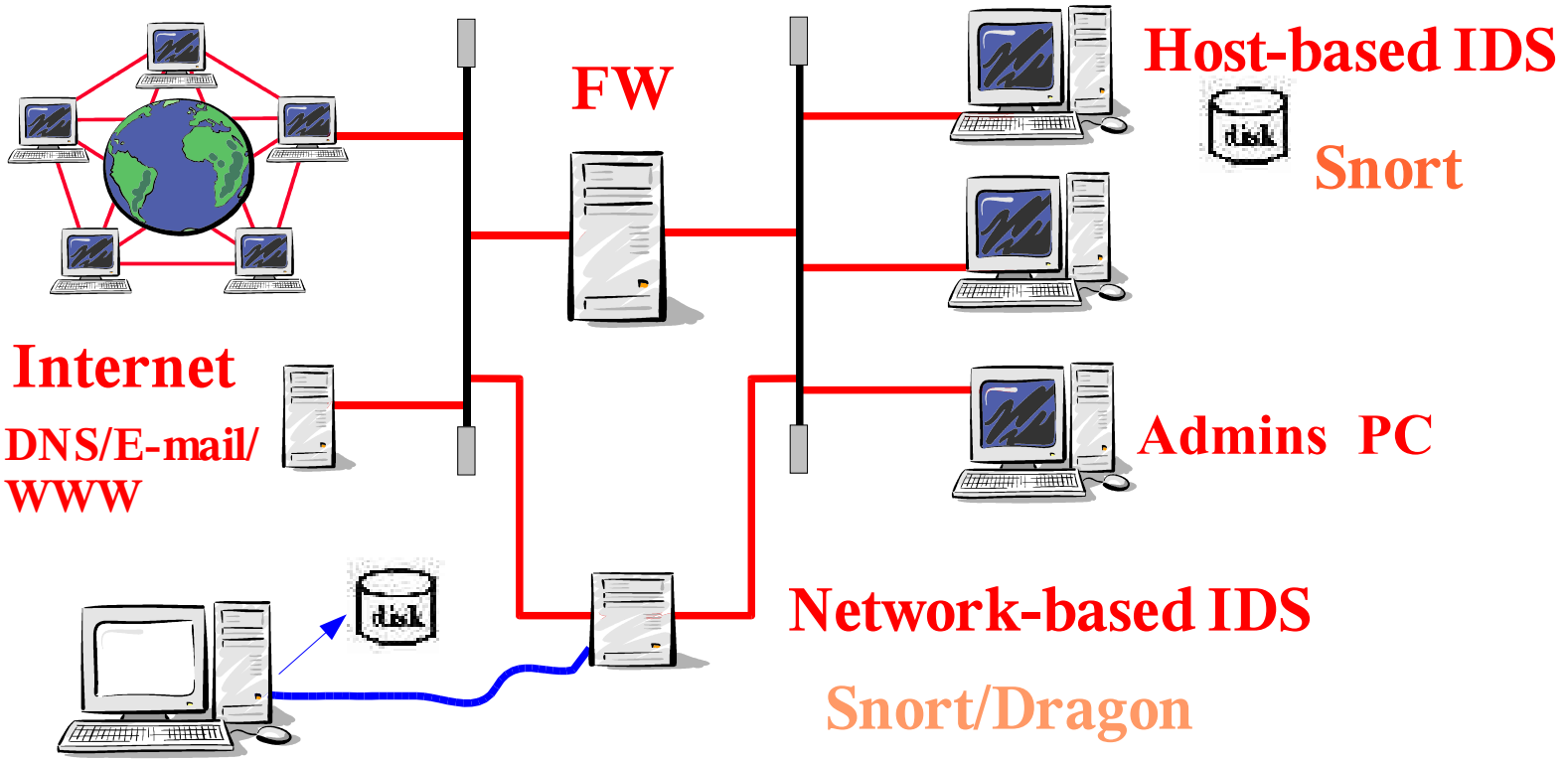
W32/Blaster worm

W32/Welchia worm

W32/SobigF worm

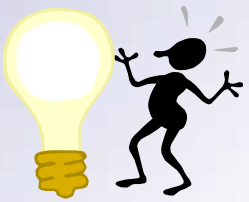
Intrusion Detection System (IDS)

The conventional IDS detects attack with signatures (pattern-matching).



Misuse Intrusion Detection Model → Signature Based
Anomaly Intrusion Detection Model → Protocol Based?

Domain Name System (DNS)



The DNS is a very important network service in the internet.

The other network applications like SMTP, POP3, FTP initially call name-resolving APIs, such as gethostbyaddr(), gethostbyname(),...

If the DNS stopps, the almost the network services of the internet will be in dead

We need to protect the DNS server from the network security incidents.

An Installation of the IDS is one of the solutions.

DDoS Attack to DNS ROOT servers 20021021

- An attack started at October 21st, 2002
- 9 root servers were sent considerably large amount of ICMP packets
- In fact, 13 root servers were included as a target

DNS server is a target for DDoS

Packets for DNS server in Our University

A large amount of DNS query packets from an E-mail server (1MX) is observed to be considerably larger than the others when logging UDP packets to port 53 of a DNS server (1DNS).

- **This means that the E-mail server shoud be a big DNS query packet generator.**

We have investigated on the correlation between DNS and SMTP/POP3 accesses.

Previous Our Works

- **DNS and SMTP/POP3**

  Musashi, Y., Matsuba, R, Sugitani, K.: **Traffic Analysis on a Domain Name System Server. SMTP Access Generates Many Name-Resolving Packets to a Greater Extent than Does POP3 Access,** *J. Academic Computing and Networking*, Vol. 6, No. 1, pp.21-28 (2002)

- **Mass Mailing Worm and DNS query access**

  Musashi, Y., Sugitani, K., Matsuba, R.: **Traffic Analysis on Mass Mailing Worm and DNS/SMTP**, *IPSJ SIG Notes, Computer Security 19th*, Vol. **2002**, No. 122, pp.19-24 (2002)

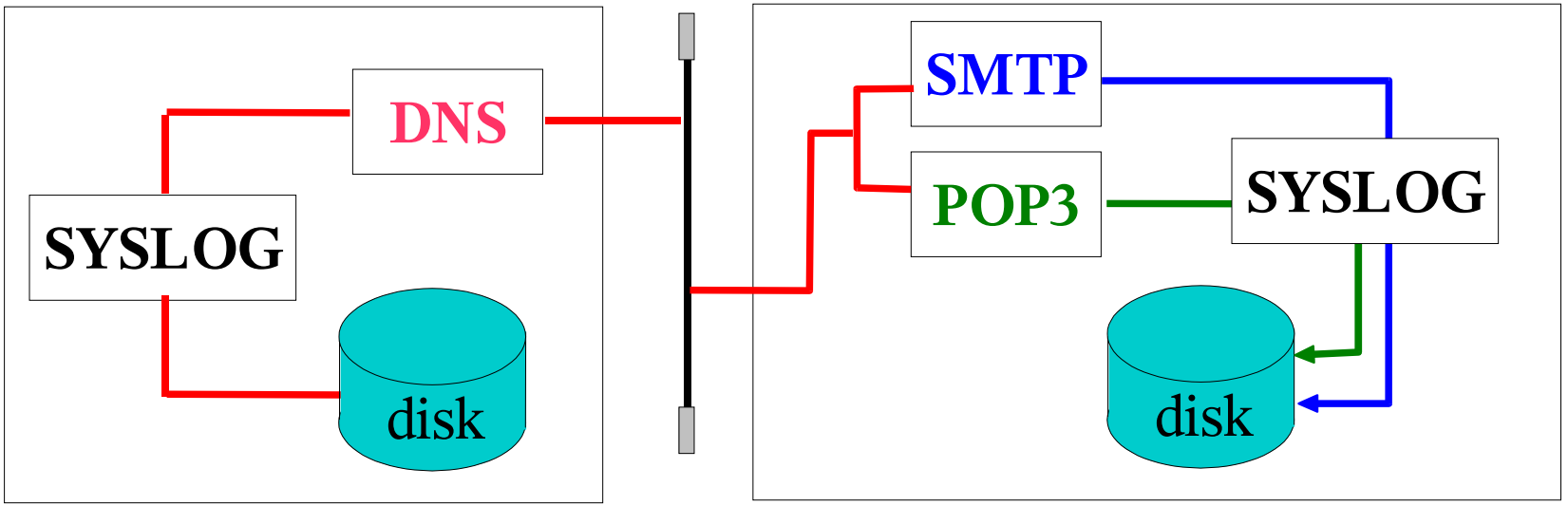
- **SMTP: "from=" and "to=" lines, DNS-active or not**

  Musashi, Y., Matsuba, R., Sugitani, K.: **Statistical Analysis in Logs of DNS Traffic and E-mail Server.** *IPSJ SIG Notes, Computer Security 20th*, Vol. **2003**, No. 18, pp.185-190 (2003)

The Present Investigated Network Servers

DNS cache server

SMTP/POP3 server



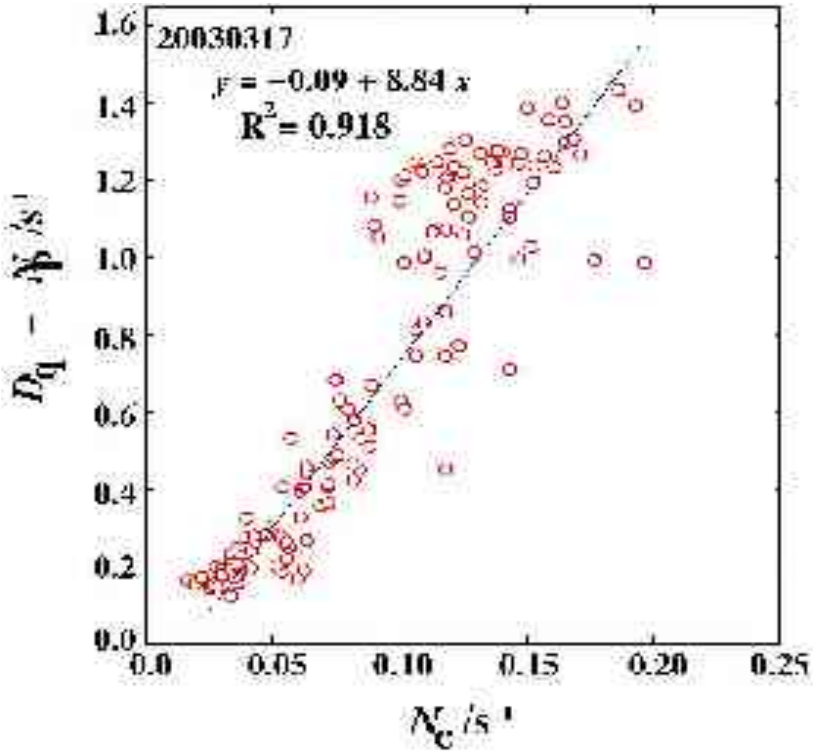
1DNS

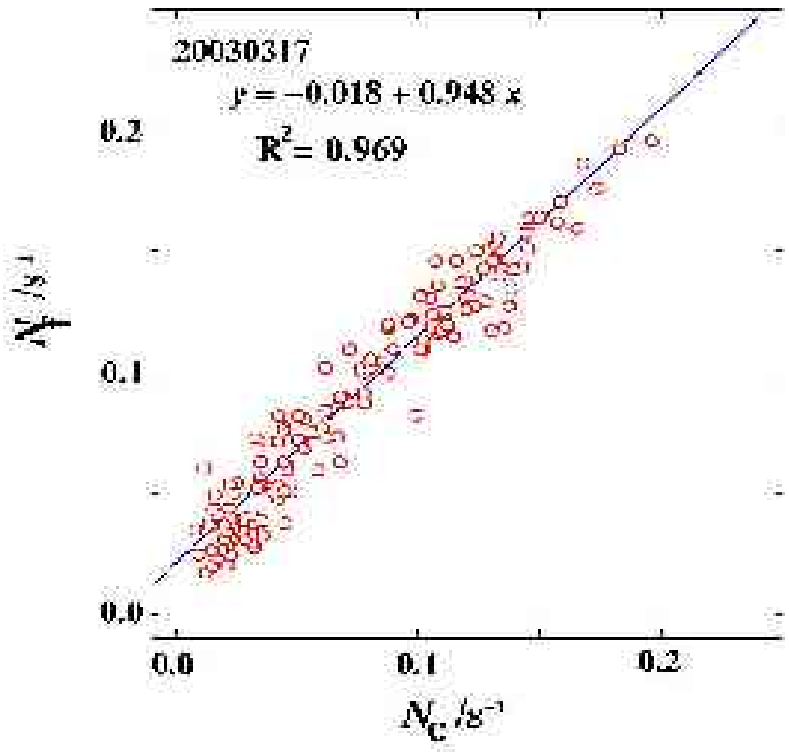
- AMD Athlon 1.1GHz
- Linux-2.4.21
- BIND-9.2.2
- iplog-2.2.3

1MX

- Ultra-SPARC 300MHz
- Solaris 2.6
- Postfix-2.0.6
- Qpopper-4.0.5

Correlation between DNS and SMTP/POP3 accesses





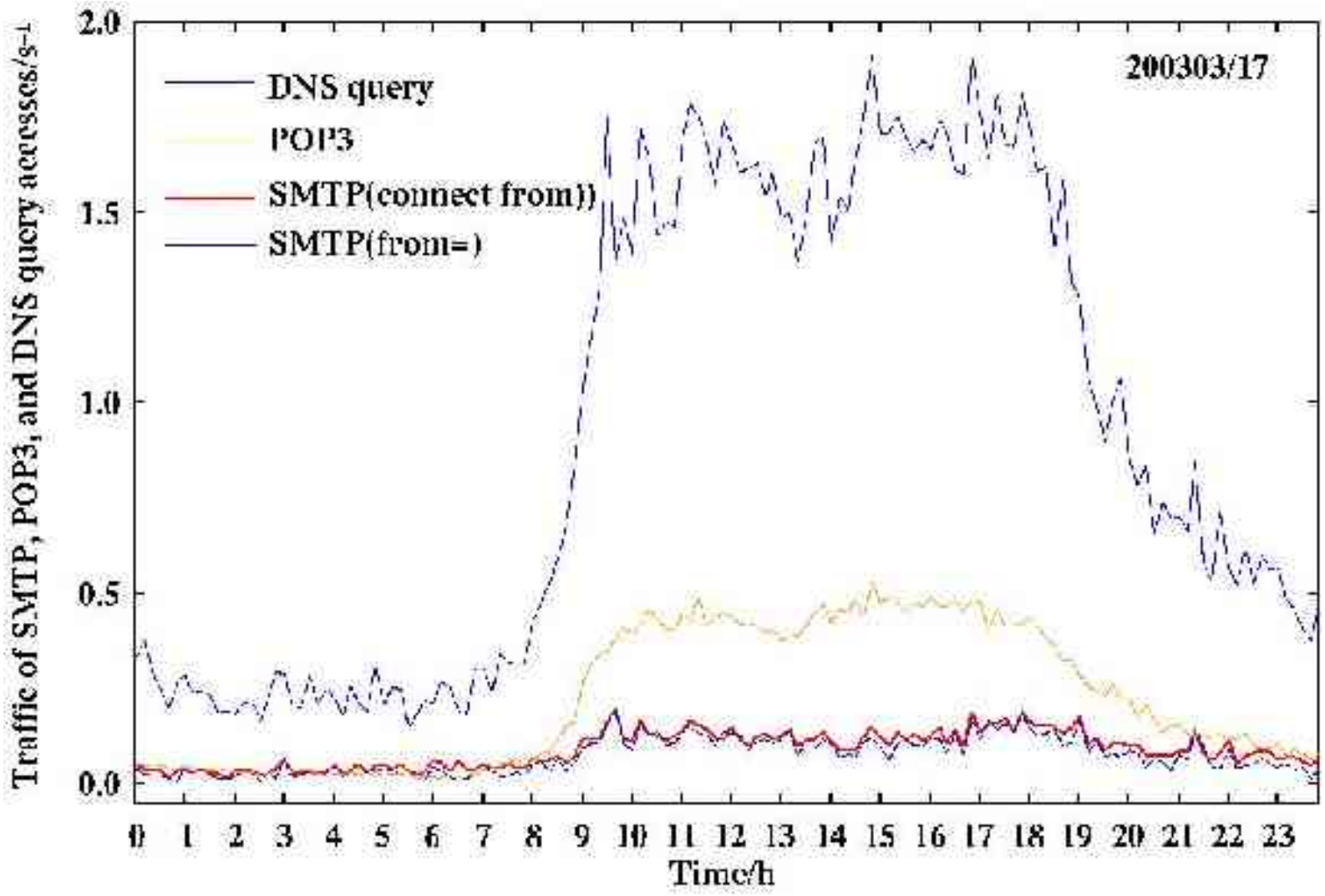
- D_q means the number of DNS query access from 1MX
- N_S/N_f show the numbers of SMTP/"qmgr: from=" lines
- N_c diplays the number of "smtpd: connect from" line
- N_P represents the number of "popper:" line.

$$D_q = 8.8\,N_C + N_P$$

$$N_f = 0.95\,N_C$$

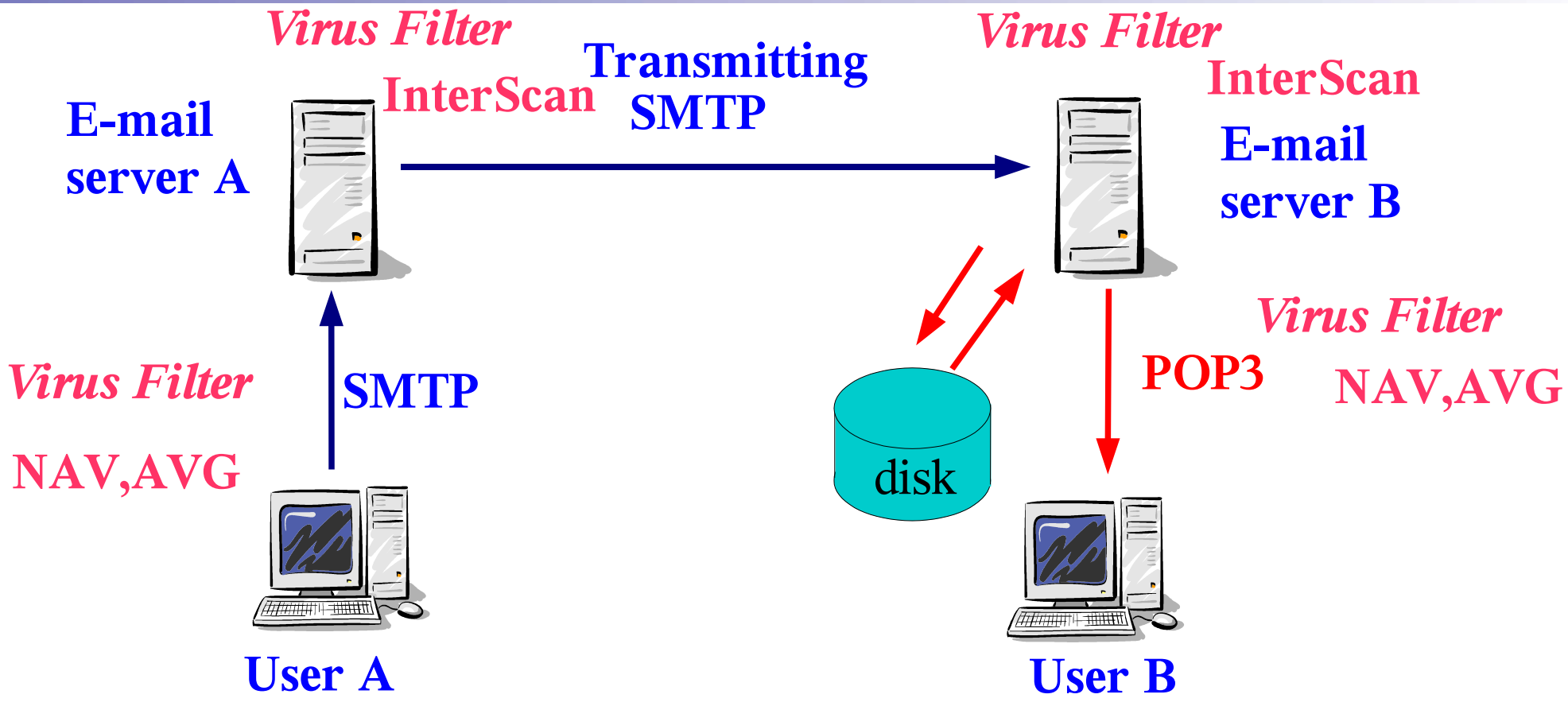
Both "connect from" and "from=" lines correlate to DNS access

DNS, SMTP, and POP3 in a week day



Both "smtpd: connect from" and "qmgr: from=" lines correlate to DNS query accesses from its E-mail server.

E-mail Exchaging (SMTP/POP3)



(1) MMW will be stopped
(2) Updating the Signature Pattern
(3) Many Virus Alert were generated with To:, From:, Reply-To:..

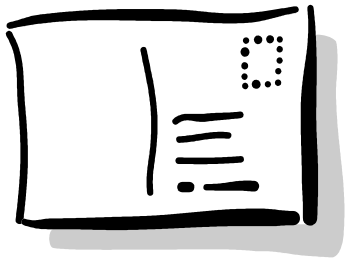
- **Increase of Undesirable E-mail Traffic**

E-mail Address includes Domain Name

Both E-mail and Web hosts addresses contain domain names

account_name@domain.name

http://www.domain.name/



The Domain Name System (DNS) is one of the database systems that translates between domain names and IP addresses, and provides information to controle E-mail exchanging.

(1) **Domain Name to IP address (A record)**

(2) **IP address to Domain Name (PTR record)**

(3) **Mail exchanging (MX record)**

DNS and SMTP/POP3 (I)

$$D_q = \sum_i R_i = R_{SMTP} + R_{POP3} + R_{FTP} + \cdots \quad (1)$$

$$R_i = m_i N_i$$

D_q = the DNS query access numbers between 1DNS and 1MX

R_i = the access numbers the fromDNS clients

i = network protocols like SMTP, POP3, FTP, ···

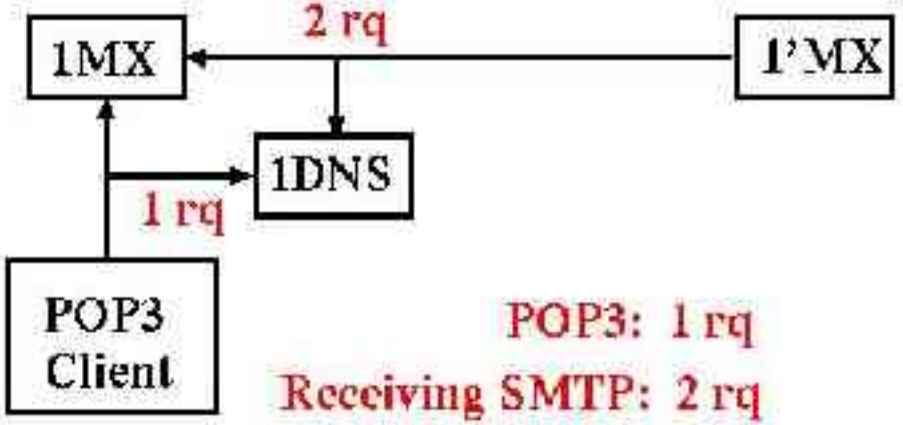
N_i = the access numbers of network applications

$$R_{SMTP} + R_{POP3} \gg R_{FTP} + \cdots \quad \text{(1MX)} \quad (2)$$

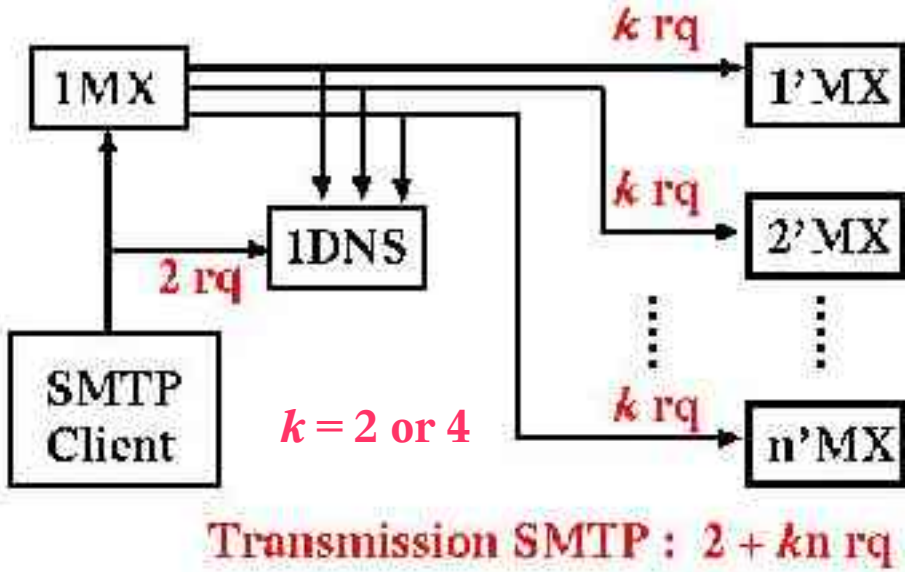
$$D_q = m_{SMTP} N_{SMTP} + m_{POP3} N_{POP3} \quad (3)$$

DNS and SMTP/POP3 (II)

(A) POP3 access and Receiving SMTP access



(B) Transmission SMTP access



1 rq = 1 request of DNS query packet

$$R_{\mathrm{POP3}} = m_{\mathrm{POP3}}\, N_{\mathrm{POP3}} \qquad (4)$$

$$R^{\mathrm{rec}}_{\mathrm{SMTP}} = 2\, N^{\mathrm{rec}}_{\mathrm{SMTP}} \qquad (5)$$

$$R^{\mathrm{tr}}_{\mathrm{SMTP}} = (2 + kn)\, N^{\mathrm{tr}}_{\mathrm{SMTP}} \qquad (6)$$

DNS and SMTP/POP3 (III)

$$D_q = m_{SMTP} N_{SMTP} + N_{POP3}$$

$$m_{SMTP} = 2 + kn(1-q)$$

$$k = 2 \text{ or } 4$$

$$R_{SMTP} = R_{SMTP}^{rec} + R_{SMTP}^{tr} \tag{7}$$

$$q = \frac{N_{SMTP}^{rec}}{N_{SMTP}^{rec} + N_{SMTP}^{tr}} \tag{8}$$

$$m_{SMTP} N_{SMTP} = 2qN_{SMTP} + (1-q)(2+kn) N_{SMTP} \quad (N_{SMTP} > 0)$$

$$\begin{aligned} m_{SMTP} &= 2q + (1-q)(2+kn) \\ &= 2 + kn(1-q) \end{aligned} \tag{9}$$

Evaluation of E-mail Exchanging

The syslog messages of the Postfix-2.0.6 mainly consist of the following three lines(contents).

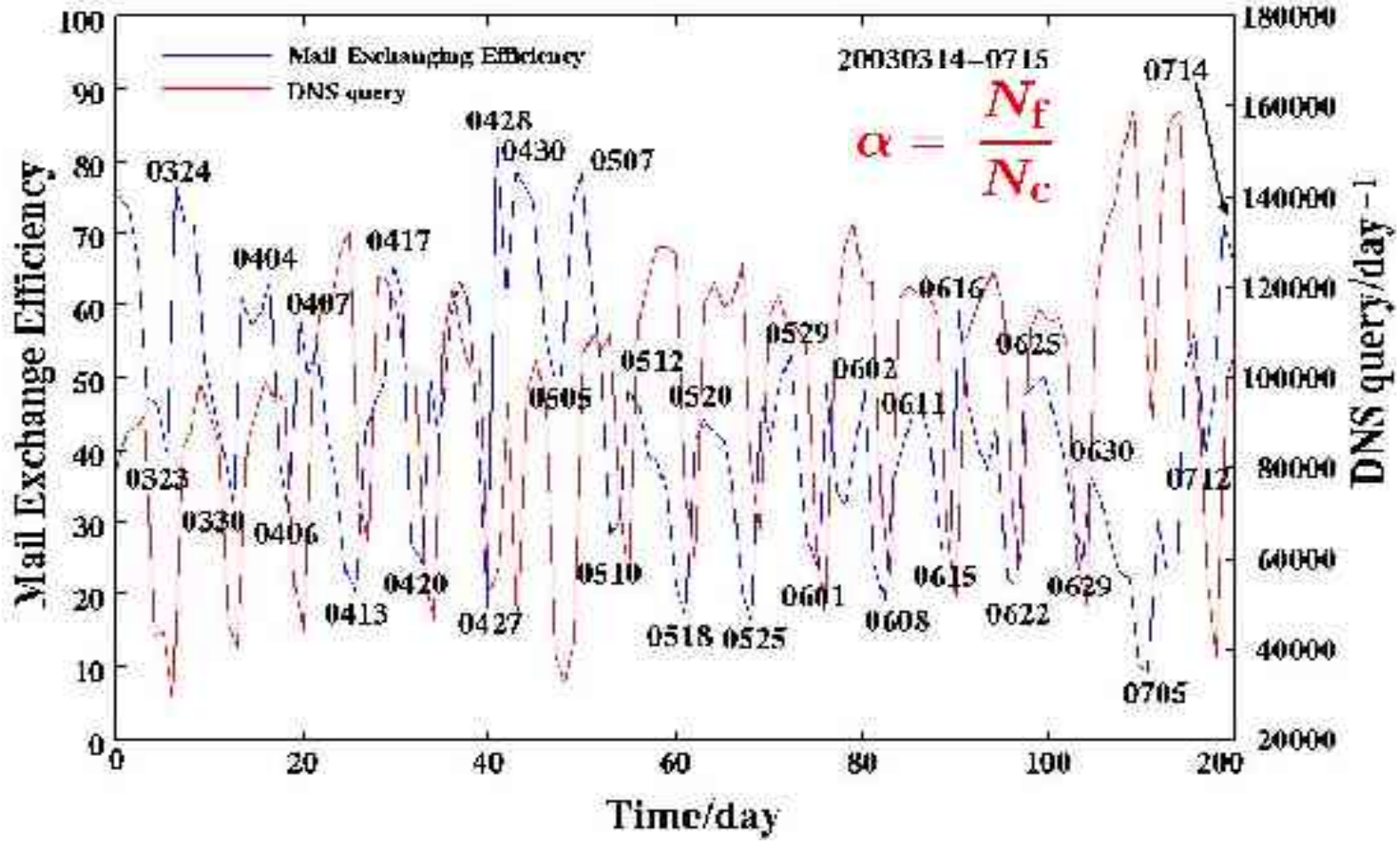
(1) "smtpd: connect from" lines: the connections of SMTP clients
(2) "qmgr: from=" lines: the E-mail exchanges and their from addresses
(3) "qmgr: to=" lines: the destination addresses of E-mails

Here, we define the Mail Exchanging Efficiency (MEE),

$$\mathrm{MEE} = \alpha = \frac{N_f}{N_c}$$

- N_f shows the numbers of SMTP/"qmgr: from=" lines
- N_c diplays the numbers of "smtpd: connect from" lines

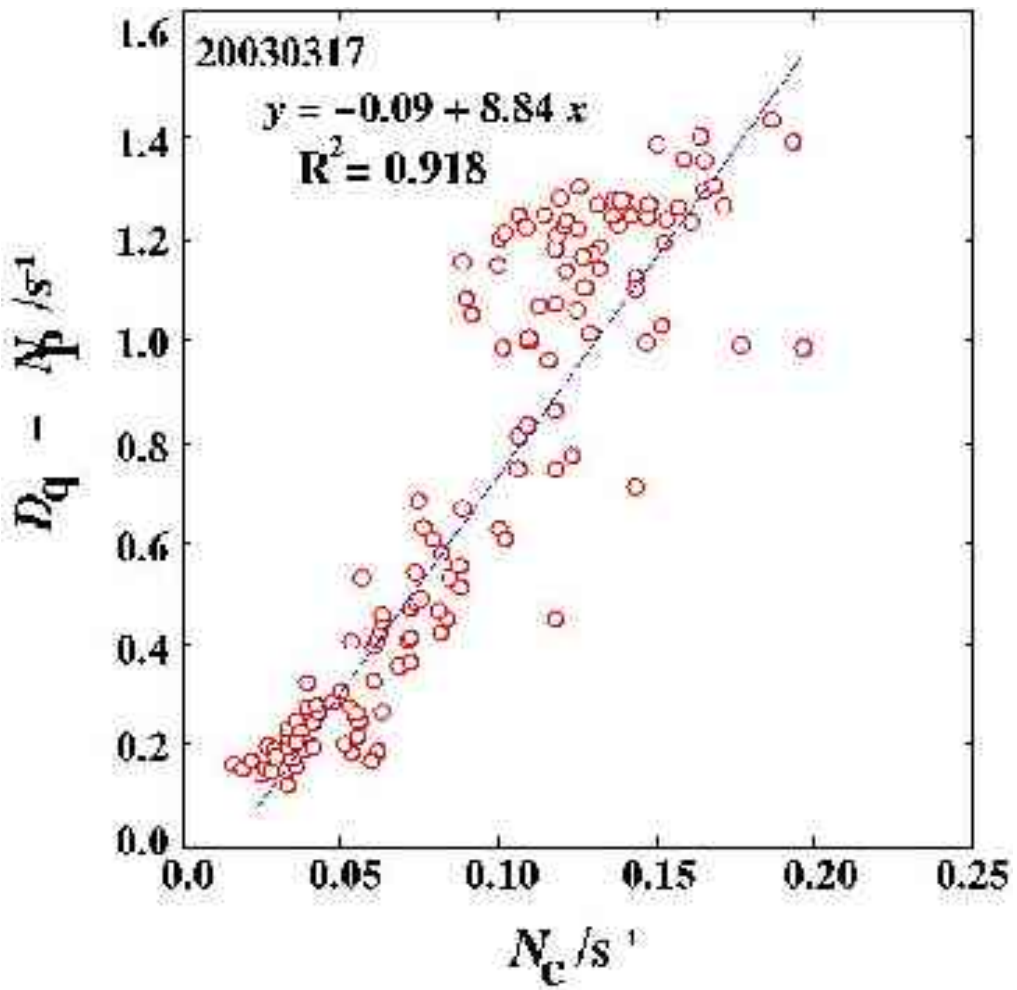
Changes in MEE value of 1MX(20030314-0715)

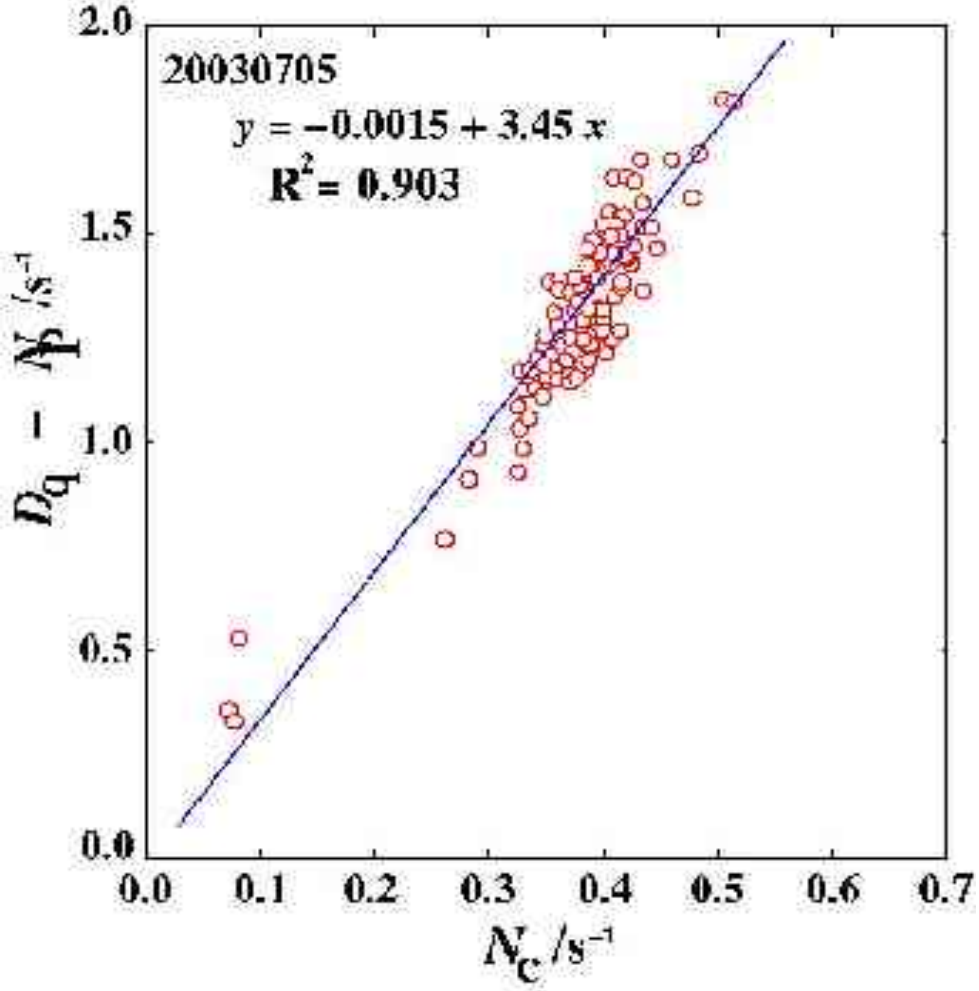


- Normally, the DNS curve follows the MEE curve (0.70av:weekday, 0.35av:holiday).
- However, several abnormal parts were found (0.21 for 20030413, 0.11 for 20030705).

- The mass "connect from" and "RCPT" lines were observed in the syslog files

Correlation Analysis between DNS and SMTP





The linear coefficient of SMTP is given in a smaller value than that in a normal value when the MEE value is small but the mass DNS query access is observed.

SPAM Signatures in the syslog files of Postfix

The mass "connect from" and "reject:RCPT" lines were observed in the syslog files

Relay access denied:

Apr 13 18:55:06 gpo postfix/smtpd[25182]: 6B7275F30: reject: RCPT from unknown[211.202.51.252]: 554 <mh4495.@co.kr>: Relay access denied; from=<test1@test1.com> to=<mh4495.@co.kr> proto=SMTP helo=<test1.com>

Recipient address rejected:

Apr 13 00:47:54 gpo postfix/smtpd[16733]: D0FAE5F34: reject: RCPT from unknown[2xx.216.xyy.2zz]: 504 < @ .com>: Recipient address rejected: need fully-qualified address; from=<tbillion@indot.com> to=<??????@??.com> proto=SMTP helo=<XaP0paHgf>

User unknown:

Apr 28 23:13:59 mailserver postfix/smtpd[19610]: 9A48C5F34: reject: RCPT from mailer.xxxx.com [192.168.1.50]: 450 <xxxx@mailserver.kumamoto-u.ac.jp>: User unknown in local recipient table; from=<getyou87@gehehe.com> proto=SMTP helo=<mailer.xxxx.com>

"User Unknown" is dominant in the Syslog Messages

	20030413[a)]	20030705[b)]
Relay access denied	16	7
Recipient address rejected	2	0
User Unknown	13505	32028

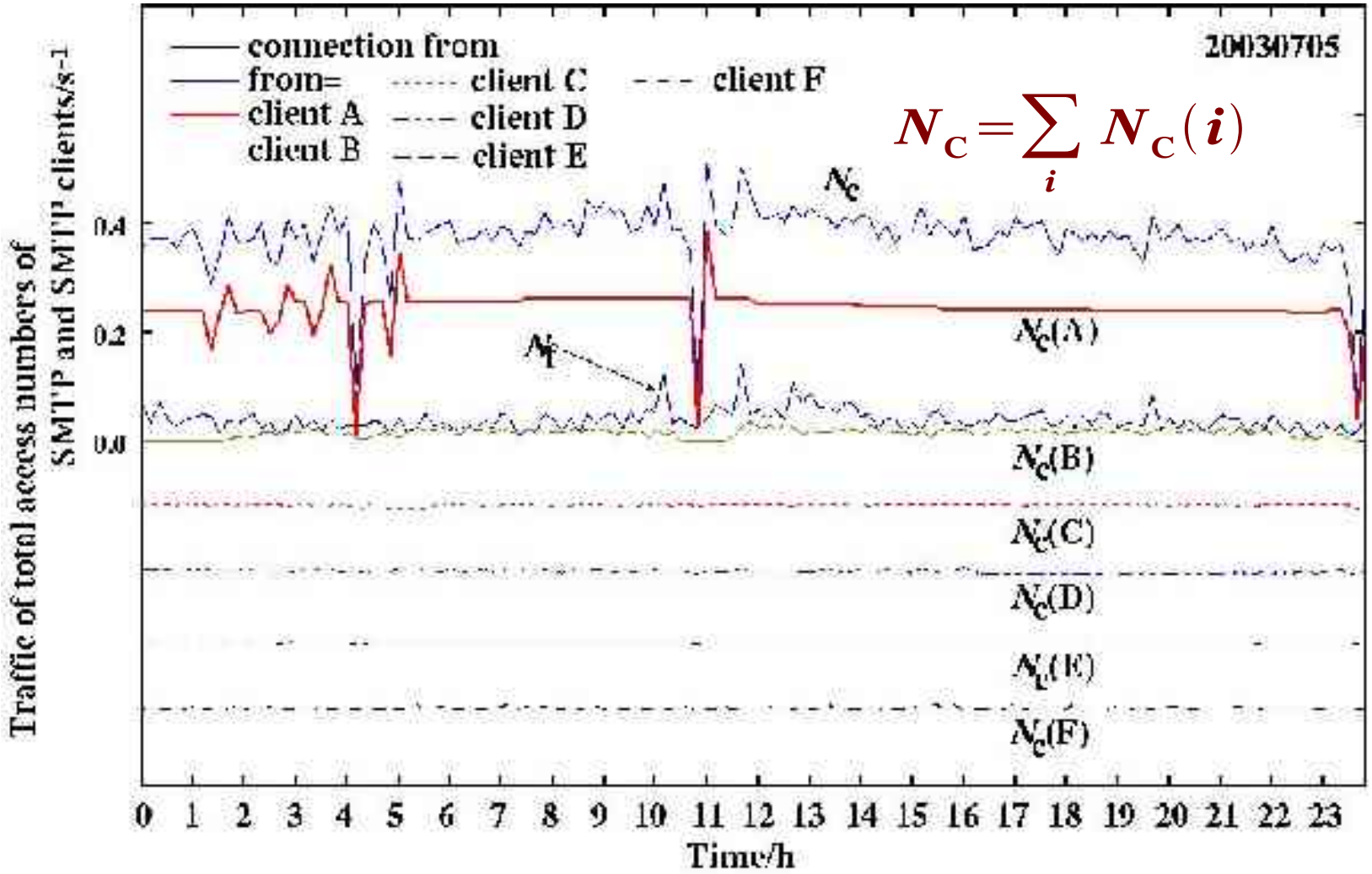
a) Several E-mail accounts were removed.

- A simple error

b) One specific SMTP client address drives SMTP accesses, totally.

- SMTP-DoS/A simple error

Detecting Strange SMTP Clients



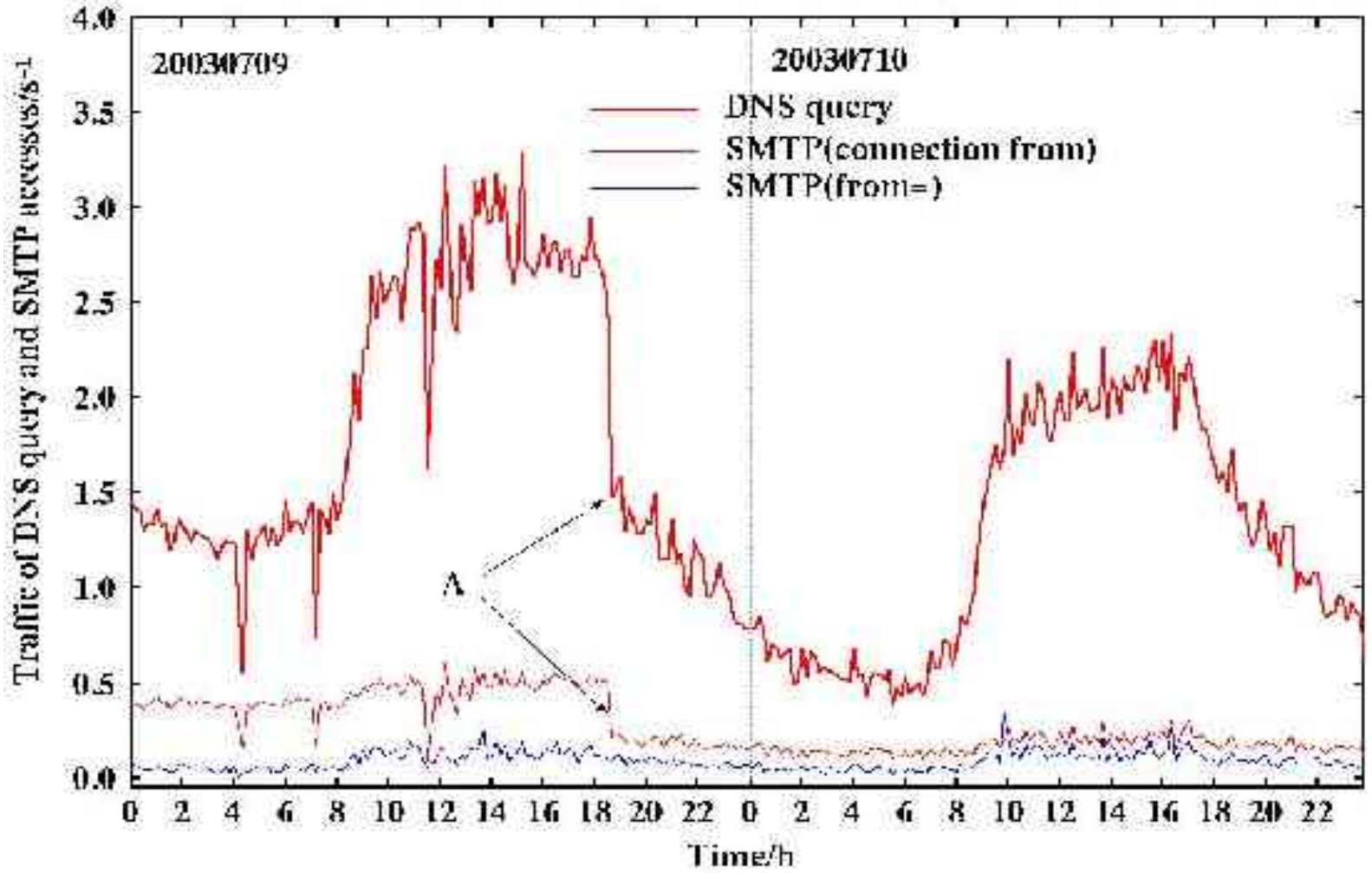
The client A (N_c(A)) curve dominantaly dirves the total N_c curve.

Access Controle List for Postfix

```
smtpc lientsc om          discard text
smtpc lientsc om          reject  text

smtpc lientsc om          ok      text
smtpc lientsc om          dunno   text
smtpc lientsc om          hold    text
smtpc lientsc om          filter  scan:dummy
```

Filtering by ACL for Postfix



The DNS traffic considerably decreases when employing "reject" option for an IP address of the SMTP client A.

Summary

1) Both “smtpd: connect from” and “qmgr: from=” lines in the syslog files for Postfix become the DNS clients.

$$D_q = 8.8\, N_C + N_P$$

$$N_f = 0.95\, N_C$$

2) The Mail Exchaging Efficiency, MEE and DNS query access from E-mail server provide very important information for the E-mail server.

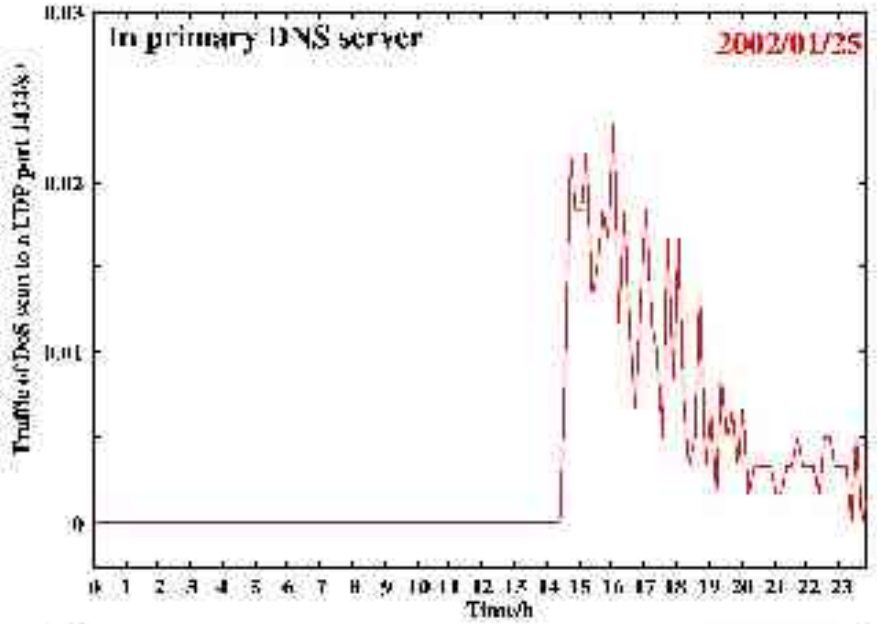
$$\mathrm{MEE} = \alpha = \frac{N_f}{N_c}$$

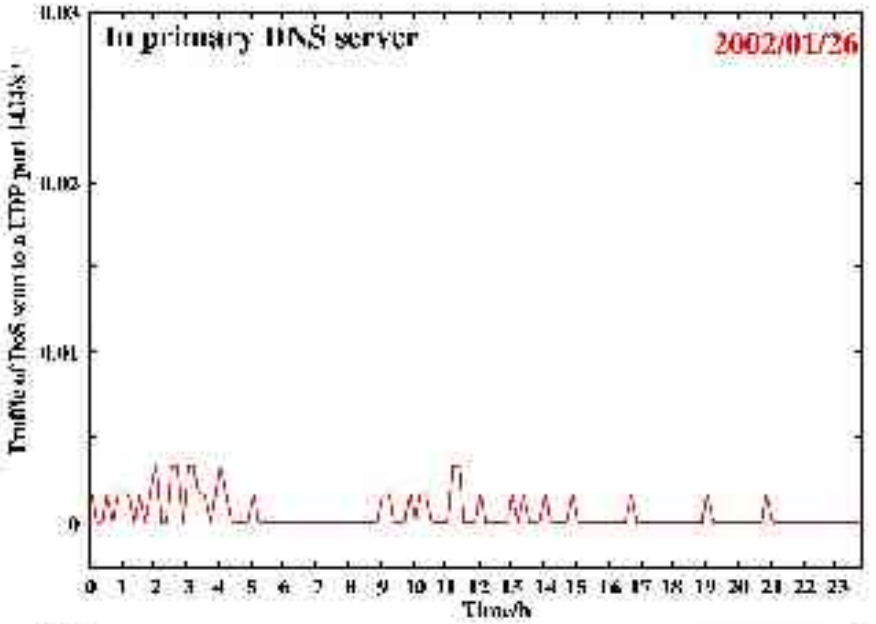
- N_f shows the numbers of SMTP/”qmgr: from=” lines
- N_c diplays the numbers of “smtpd: connect from” lines

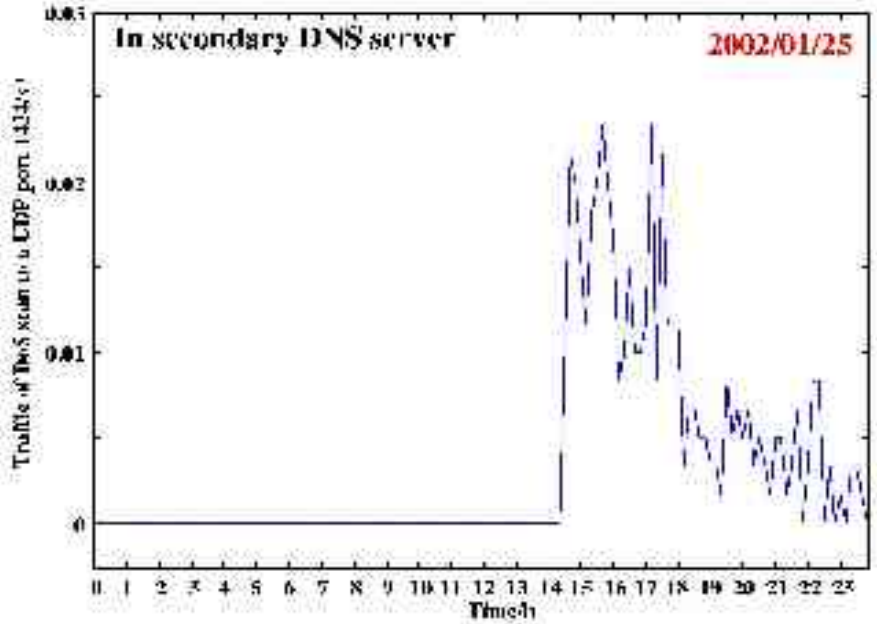
If α value decreases but DNS query access increses, the E-mail server should be abnormal.

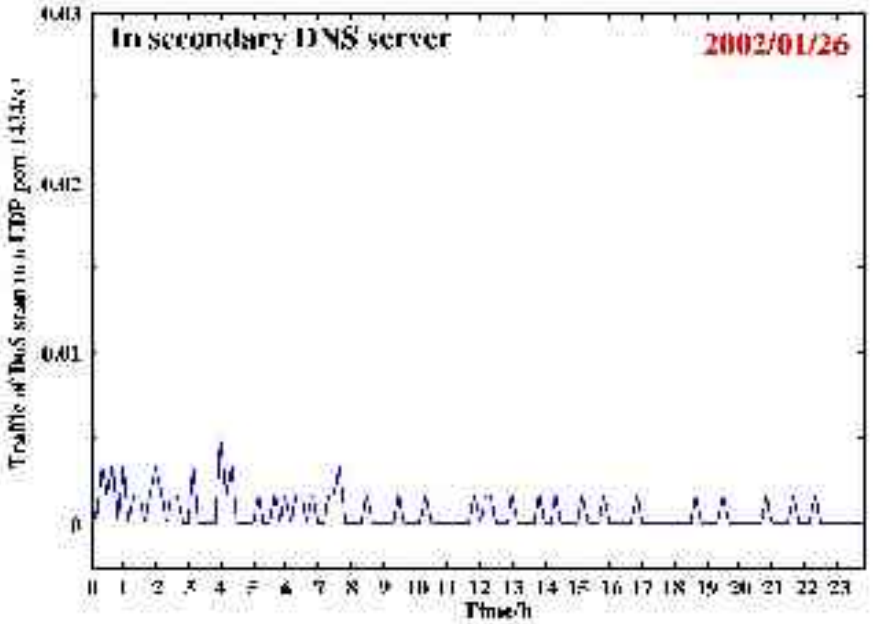
3) The "reject" option for ACL of Postfix is available to decrease the mass DNS query access from the E-mail server and the MEE value increases.

SQL Worm Attacks to the DNS Servers









W32.Welchia.Worm