宇治市の住民情報データ流出事件を経験して

――― 住民情報データ流出事件の教訓 ―――

木村 修二

はじめに

宇治市では、９９年５月に２１万件の住民情報データが流失していたことが発覚した。古典的で幼稚な不正行為であったので、発覚から約１週間で、流失ルートの解明からデータの回収・消去までを行うことができた。市では再発防止策をまとめ、制度的な保障としての個人情報保護条例の改正と、実態的な保障としての情報セキュリティシステムの構築に取り組んだ。

この事件発覚直後から再発防止策をまとめ推進してゆく過程で考え続けた。一体何に失敗したのか？どう対応すべきか。

１．「情報セキュリティ」への疑問

（１）事件発覚直後からマスコミは、「個人情報のずさんな管理で流出」という表現が跋扈した。また識者のコメントとして「信頼できる事業者の選定」に失敗とか、「本番の生データの持ち出し」を批判されることが多数見受けられた。しかしこれらは、事件が起こったという結果から原因を語っている結果解釈でしかなく、再発防止策にはならないことに気づかされた。同じことを行っている数多くの自治体では事故が発生していないのだから。

宇治市が全国最下位のセキュリティ水準であったなら、事件発生は自業自得と納得もいくが、悪くても全国平均値程度ではあったと思っている。世界最高の堅牢さを誇るところでも事件は発生の報道も目にすることがある。情報セキュリティの水準と事故の発生とは相関関係があるかと考えれば、相関関係を見出すことができない。情報セキュリティの向上に努めても事故は防止できないことになる。

事件のあと当然のごとく再発防止策に取り組むが、しかし情報セキュリティを向上させれば事件は防止できるのか、という基本的な疑問を抱いていた。

（２）再発防止策は対症療法的であってはならないし、事件はなぜ発生したのか、なぜ事故が起きたのか、因果関係を解明しつつ、普遍化することを通じて、根源的な再発防止策を構想することを想定した。しかし、事件発生の個別具体的な、因果関係のある根拠は見出せなかった。結局、くだけた言い方になるが、「悪い奴がいた」「悪いことができる環境だった」という、ごく一般的な２つの条件がそろえば事件はどこででも起こると理解せざるを得なかった。だから再発防止策はこの条件を排除することが課題となった。「悪い奴」を排除できればいいが、職員だけでなく委託業者の社員その他

多くの人が関わるのであるから、また職員研修が全職員すべてに浸透して意思改革を達成できると想定することは不可能としか思えないことから、たった１人の「悪い奴」を排除する手法たりえない。だから、「悪いことができない環境」を技術的セキュリティで最大限に構築し、やむを得ない部分だけ、強力な抑止力で対応することを再発防止策の基本とした。マネジメント系の情報セキュリティを後景に退け、技術的セキュリティに前面に力を傾注した。

（３）情報セキュリティの水準と事故の発生とは相関関係がないし、情報セキュリティの向上に努めても事故は防止できないのは、事件は管理者側の対策よりも攻撃者側の要素、つまり「攻撃者の執着心と技術力」によると理解した。だから、攻撃を「できなくする」ことが可能であるならば、事件を防止することができる。それが「悪いことができない環境」ということである。

システム管理者が自らの権限だけで整備できる領域が唯一対応可能な領域である。それ以外の領域には無限の脅威が存在する。だからこの領域を完全に分離することからはじまる。だから一般に語られる情報セキュリティの体系ではなく、実効性のある別の体系を模索せざるを得なかった。

２．「情報セキュリティ」の理念の再確認と直後の対応

自治体の情報管理の原則は、情報公開制度と個人情報保護制度である。これらと無関係に情報セキュリティといわれるものがあるわけがない。

被害者（情報主体）の意思を考慮せずに、加害者（情報保有者）だけで対策を考えることにはならないし、情報セキュリティは、情報主体の権利保障を内包しなければならない。だから、情報公開条例・個人情報保護条例の下に情報セキュリティを構築すべきであると再確認した。

（１）情報セキュリティの理念

情報主体のプライバシーの権利を保障すること、それに市民の知る権利を保障すること、これが情報セキュリティの目的である。だからプライバシー保護制度から情報セキュリティシステムに要請される課題は、機密性・完全性・可用性といわれる自己完結的な内部統制系統だけでなく、これに、外部にいる情報主体（市民）の自己情報コントロール権を貫徹し、その意思・コンセサスに基づいて内部統制をさせることである。さらに外部の情報主体が、自らのどんな個人情報が蓄積され、どう管理され、どう利用されているかを、自らが監視できなければならないと考えた。

（２）だから、情報主体が安心して自らの個人情報を提供できるためには、情報主体が自ら安全性を判断するための情報（セキュリティ情報）をすべて開示しなければならない。また、情報主体がセキュリティの水準を決定し、情報保有者は、情報主体の意思に従って、それを実現する。これがデータ保護からプライバシー保護への転換であると考えている。

DNS Query Access and Backscattering SMTP Distributed Denial-of-Service Attack

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

†Center for Multimedia and Information Technologies, Kumamoto University,
2-39-1 Kurokami, Kumamoto-City, 860-8555, JAPAN

Abstract: We statistically investigated DNS query access from an E-mail server when having a backscattering SMTP distributed denial-of-service (DDoS) attack. The interesting results are summarized, as follows: (1) In usual, the DNS query access from the E-mail server is cached by the E-mail server and includes only expired generic/fully qualified domain name (FQDN), (2), however, it includes a lot of unresolved FQDNs that consist of host/FQDN and a local domain name. Therefore, we can detect the E-mail server having a backscattering SMTP DoS attack by only watching the DNS query access from the E-mail server.

1. Introduction

One of the attractive solutions to keep security of the E-mail 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. Surely, the IDS provides a lot of useful alert messages, however, it generates too much alert ones to analyze in 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 E-mail servers, it is of considerable importance to get more detailed information for traffic of network applications like DNS query packets between a DNS server and an E-mail server as a DNS client.

Recently, a subdomain E-mail server has started to be under a backscattering SMTP distributed denial-of-service (DDoS) attack like transmitting a plenty of E-mails, probably, in oder to crash the E-mail server.

The present paper discusses (1) on correlation analysis on DNS query traffic between DNS server and the subdomain E-mail server that especially transmits query contents including unresolved fully qualified domain name (FQDN) of local network segments, and shows (2) how to implement an indirect detection system of a backscattering SMTP DDoS attack by only analyzing syslog messages of the DNS server.

2. Observations

2.1 Network systems

We investigated traffic of DNS query accesses between the top domain DNS server (**tDNS**) † and a subdomain E-mail server (**sdEMS**).[11] Figure 1 shows a schematic diagram of a network observed in the present study. **tDNS** is one of the top level domain name system servers and plays an important role of subdomain delegation and domain name resolution services for many PC terminals.

†Center for Multimedia and Information Technologies, Kumamoto University.
†**tDNS** is a top domain DNS server in a certain university and the OS is Linux OS (kernel-2.4.26), and hardware is an Intel Xeon 2.40GHz Dual SMP machine.

2.2 DNS Query Packet Capturing

In **tDNS**, BIND-9.2.3 program package has been employed as a DNS server daemon.[12] 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 DNS Query Traffic

We observed traffic of DNS query request packet from the E-mail server (**sdEMS**) to the top domain DNS server (**tDNS**) through March 25th to September 4th, 2004 (Figure 2). In Figure 2, the DNS query access traffic from the E-mail usually mainly consists of an A record packet, a PTR record packet, and an MX record packet. Usually, the A record packet traffic is considerably larger than those of PTR and MX record packet ones and we can see two duration that indicate abnormal DNS query traffic through March 30th to April 2nd and August 31st to September 1st, 2004.

There are two peaks: One peak is at March 31st. In the day, **sdEMS** is likely to be abnormal so that a manager of **sdEMS** sought us out to get a solution to prevent a backscattering SMTP distributed denial-of-service (DDoS) attack. The backscattering SMTP DDoS attack uses a bogus E-mail account and/or an E-mail address (forgery domain name). The other peak in August 31st is the same as that in March 31st.

We tried to check the DNS query contents of these two days and fortunately found interesting results, as follows: (1) The contents include unresolved fully qualified domain names (FQDNs) in

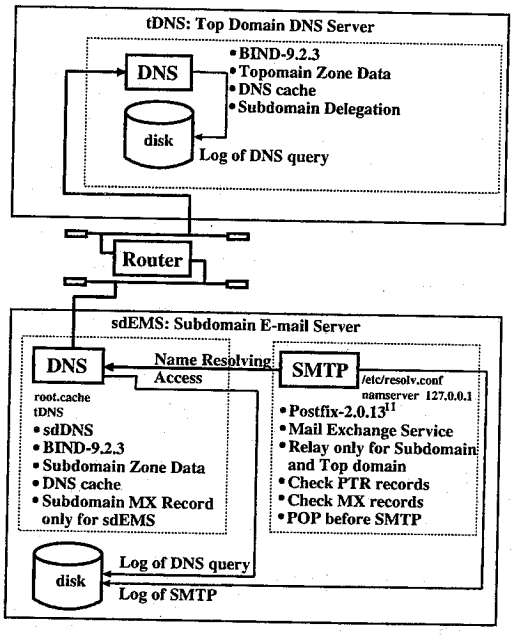

Figure 1. A schematic diagram of a network observed in the present study.

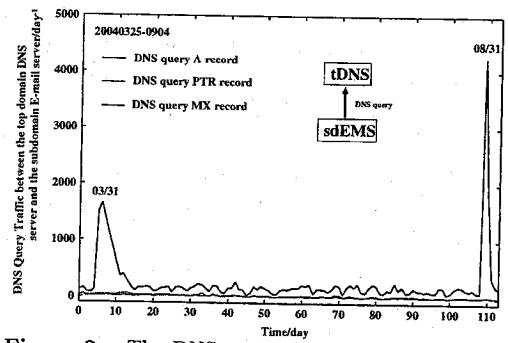

Figure 2. The DNS query traffic between the top domain DNS server and the E-mail server through March 25th to September 4th, 2004. The thick solid line shows the A record based DNS query traffic, the thin solid line indicates the PTR record based DNS query traffic, and the dotted line demonstrates the MX-record based DNS query traffic (day^{-1} unit).

a high probability, and (2) these FQDNs consist of a couple of a certain FQDN and the local generic domain name. The certain FQDN is unclear whether or not can be resolved and the generic local domain. From these results, it is worthwhile to investigate statistically correlation between the total DNS query traffic and the DNS

query traffic that includes unresolved FQDN. We have prepared the unresolved FQDN filtering C program (gcc-3.2.3) that senses a syslog message line including unresolved FQDN.

3. Results and Discussion

3.1 Unresolved FQDN

We illustrate the observed traffic of the DNS query traffic between the top domain DNS server (**tDNS**) and the E-mail server (**sdEMS**) in Figure 3 through March 29th to April 3rd, 2004. In Figure 3, the DNS query traffic including unresolved FQDN contributes in a small scaled manner to the total traffic through 00:00 March 29th to 08:30 March 30th, 2004. However, the DNS query traffic increases after 08:30 March 30th, and then both traffic curves of DNS query access including unresolved FQDN and the total DNS query access change, simultaneously. The DNS query traffic becomes to be calm temporally at 19:30 but it restarts to fluctuate severely after 08:30 April 1st. Reportedly, the **sdEMS** had an SMTP DoS attack through March 30th to April 3rd, 2004. Unfortunately, the syslog messages is lost when having a SMTP DoS attack so that it is unclear what kinds of SMTP DoS attacks took place in that day.

However, it is clearly said that the DNS query contents including unresolved FQDN is useful to detect an unknown SMTP DoS attack.

3.2 Backscattering SMTP Attack

We observed abnormal DNS traffic from the E-mail server **sdEMS** to the top DNS server **tDNS** through August 31st to September 1st, 2004 (see Figure 4). In Figure 4, the total DNS query traffic suddenly increases after 02:00 August 31st. Simultaneously, traffic curve of the DNS query access changes in almost the same manner as that of the DNS query access including unresolved FQDN. This feature has already observed in Figure 3 and means that it is worthwhile to investigate the syslog messages of **sdEMS**.

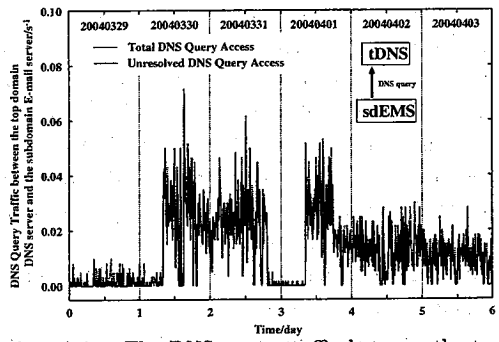

Figure 3. The DNS query traffic between the top domain DNS server and the E-mail server through March 29th to April 3rd, 2004. The solid and dotted lines show the DNS query traffic including unresolved FQDN and total DNS query traffic, respectively (s^{-1} unit).

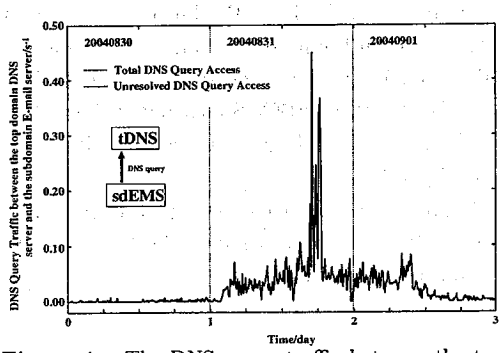

Figure 4. The DNS query traffic between the top domain DNS server and the E-mail server through August 30th to September 1st, 2004. The solid and dotted lines show the DNS query traffic including unresolved FQDN and total DNS query traffic, respectively (s^{-1} unit).

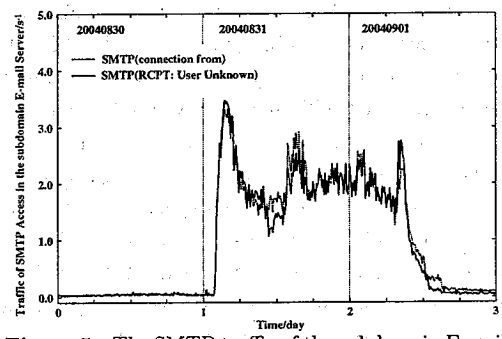

Figure 5. The SMTP traffic of the subdomain E-mail server (**sdEMS**) through August 30th to September 1st, 2004. The solid and dotted lines show the access number of "RCPT: User Unknown" and the access number of "connect from" line, respectively (s^{-1} unit).

As shown in Figure 5, the SMTP client connection traffic suddenly increases after 02:00 August 31st. Simultaneously, the SMTP RCPT: User Unknown traffic curve changes in almost the same manner as that of the SMTP client connection traffic one. Furthermore, the IP addresses of SMTP clients are variable when the abnormal DNS query traffic takes place. From these results, it is clear that **sdEMS** had a backscattering SMTP distributed denial-of-service (DDoS) attack *i.e.* we can conclude that the DNS query traffic from **sdEMS** is kicked by the backscattering SMTP DDoS attack.

Figure 6 shows regression analysis between total DNS query traffic versus the DNS query traffic including unresolved FQDN. The data are August 31st, 2004. In Figure 6, the correlation coefficient (R^2) is 0.999. This also means that the total DNS query traffic from **sdEMS** considerably correlates to the traffic of DNS query access including unresolved FQDN.

Therefore, we can detect a backscattering SMTP DDoS attack whether or not the DNS query traffic includes unresolved FQDN.

4. Concluding Remarks

We statistically investigated syslog files in the top domain DNS server (**tDNS**) and the E-mail server (**sdEMS**). By monitoring the DNS query accesses on **tDNS**, we have found information about detection of abnormality in **sdEMS**: (1) Usually, the DNS query access from the E-mail server like (**sdEMS**) includes an unresolved fully qualified domain name as a query content. This is because the /etc/resolv.conf is configured to be a loop back address (127.0.0.1) so that the DNS query access is cached in **sdEMS** itself. (2) However, when having a scattering SMTP DDoS attack, the E-mail server like **sdEMS** cannot cache the DNS query access from itself and it starts to access to the upper DNS server like the top DNS server (**tDNS**). (3) And then the DNS query access from the E-mail server having the backscattering SMTP DDoS attack includes an unresolved FQDN.

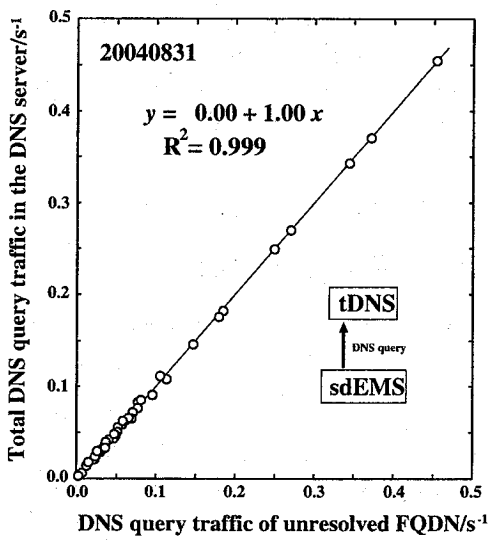

Figure 6. Total DNS query traffic vs DNS query traffic of unresolved FQDN (August 31st, 2004). (s^{-1} unit).

From these results, it is reasonably concluded that we can detect whether or not the E-mail server has a backscattering SMTP DDoS attack by only observing the DNS query access from the E-mail server.

We continue further investigation in order to get more information to develop an automated detection- and prevention-system for the E-mail server having a SMTP DDoS attack, DNS query DDoS attack, and the internet worm infection.[13-17]

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.postfix.org/

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

13) Matsuba, R., Musashi, Y., and Sugitani, K.: Statistical Analysis in Syslog Log Files ins DNS and Spam SMTP Relay Servers, *IPSJ Symposium Series*, No.2004, pp.31-36 (2004).

14) 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 Mangement 32nd*, Vol. 2004, No.37, pp.67-72 (2004).

15) Musashi, Y., Matsuba, R., and Sugitani, K.: Development of Automatic Detection and Prevention Systems of DNS Query PTR record-based Distributed Denial-of-Service Attack, *IPSJ SIG Technical Reports, Distributed System and Mangement 34th*, Vol. 2004, No.77, pp.43-48 (2004).

16) Musashi, Y., Matsuba, R., Sugitani, K., and Moriyama, T.: Workaround for Welchia and Sasser Internet Worms in Kumamoto University, *Journal for Academic Computing and Networking*, No.8, pp.5-8 (2004)

17) Musashi, Y., Matsuba, R., and Sugitani, K.: Indirect Detection of Mass Mailing Worm-Infected PC terminals for Learners, *Proc. the 3rd International Conference on Emerging Telecommunications Technologies and Applicatications (ICETA2004)*, Košice, Slovakia, pp.233-237, (2004).