Search Engine Based Investigation on Misconfiguration of Zone Transfer

Yin Minn Pa Pa, Katsunari Yoshioka, Tsutomu Matsumoto
Graduate School of Environment and Information Sciences
Yokohama National University
Yokohama, Japan
(yin-pa-dx,yoshioka,tsutomu@ynu.ac.jp)

***Abstract*—This study proposes how to investigate the existence of misconfigurations of zone transfer in any level of domain name system hierarchy using search engine based approach without the need to look at the zone file. The analysis has been conducted on 1,284 authoritative name servers of 314 top-level domains and 46,416 authoritative name servers of second level domain of 249 country code top-level domains. In case of top-level domains investigation, 84 name servers authoritative to answer for 53 top-level domains are misconfigured and allow zone transfer to us. In case of second level domains investigation, 5,394 authoritative name servers authoritative to answer for 6,234 second-level domains allow zone transfer. In particular, we found a serious misconfiguration case where the misconfigured DNS server was authoritative for not only its TLD but also SLD and lower level, exposing 83 % the DNS related information of the country to the public.**

Keywords—misconfiguration of zone transfer

I. Introduction

Domain Name System (DNS) plays an important role in the Internet. Zone transfer is one of the critical operations of DNS in which the contents of a zone file are copied from primary DNS server to secondary DNS server(s). Primary DNS server should allow zone transfer only to trusted secondary DNS server(s). If zone transfer is misconfigured in either of primary or secondary DNS server(s), all the resource records (RR) of zone file can be leaked on the Internet. Individual RR is not sensitive. But, a copy of entire zone including different types of RR(s) may be sensitive. If a malicious entity receives a copy of entire zone file, domains existing in zone, total number of directly accessible hosts (public IPs) of targeting organization, services running in an organization, operating systems and hardware information, IP address of routers and servers may be obtained easily from zone file. Up to 84 different types of resource information may be disclosed from zone file.

The deeper the level of DNS hierarchy, the more different types of RR may be contained in a zone file. That is why, it is important to investigate the existence of misconfiguration of zone transfer in DNS hierarchy. To start investigation on misconfiguration of zone transfer, it is necessary to obtain the list of existing domains in an investigated DNS hierarchy. Without looking at the zone file of upper level domain, it is difficult to get the entire list of lower level domains. Because of such difficulties, previous studies had been done only on second level domain (SLD) of one to two top-level domain (TLD) for which zone file access is permitted for the research. There is a possibility to receive the list of SLD from misconfigured zone file of TLD. However, downloading zone file rather than secondary name server can raise a legal issue. These conditions make many constraints to investigate the existences of misconfiguration of zone transfer in lower level of DNS hierarchy.

This study proposes how to investigate the existence of misconfigurations of zone transfer in any level of DNS hierarchy using search engine based approach without the need to look at the zone file. With the proposed approach, the existence of misconfiguration of zone transfer has been investigated for all 314 TLD and SLD of 249 country code top-level domains (ccTLD).

In TLD investigation, the analysis has been conducted on 1,284 authoritative name servers of 314 TLD. From this, 84 name servers authoritative to answer for 53 TLD are found misconfigured on zone transfer. One ccTLD of a country is noticed in which misconfigured name servers are authoritative to answer not only for the ccTLD but also most of its SLDs. Moreover, NS RRs of lower level domains are existed in the same zone. Consequently, 83% of DNS infrastructure information of the entire country was exposed to the Internet. (The information regarding this serious misconfiguration has been provided to the authoritative personnel of that ccTLD and the misconfiguration was fixed on June 22, 2012).

In case of SLD investigation, the analysis has been done only on second level domains of 249 ccTLD. Using Google advanced site search, it is possible to look for the web pages of the ccTLD. From this, the list of existing SLD for each of the 249 TLD can be obtained. For example, different SLDs existing under .jp ccTLD like co.jp, gov.jp, ac.jp, etc. After receiving the list of SLDs, the authoritative name servers are looked for and investigated. Out of 46,416 authoritative name servers of 34,164 investigated SLD, 5,394 authoritative name servers of 6,234 SLD allow zone transfer.

In the following sections, the background concerning with zone transfer operation, data collection and analysis methodologies, results and analysis on results are explained.

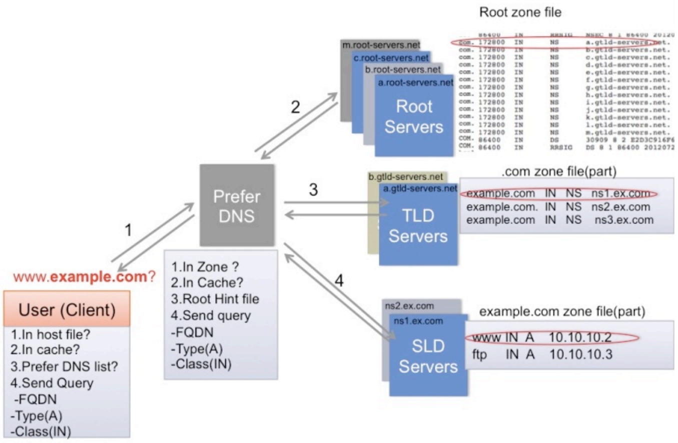
II. Background

In this section, the overview of domain name system, domain delegation, zone file, zone trasfer process and misconfiguration of zone transfer are explained.

A. Domain Name System

The main function of DNS is to map domain name to IP address and vice-versa. Root DNS, top-level DNS and users level DNS servers operate according to delegated domain name space hierarchy. The delegation of domain at users' level name server can be up to 127 levels below. Name servers authoritative for each level of domain name operate with their own authority control.

The typical name resolving process starts from the browser of the user's computer. Fig. 1 shows the typical name resolving process. The requested domain is checked in the host file of user's computer. If the corresponding IP is found, the name resolving process is finished. If the IP is not found, the DNS query will be sent to the local DNS server. The local DNS server can be set manually by user or set automatically by DHCP. The user can select open DNS servers instead of the local server. These local or open DNS servers that resolve domains recursively instead of clients are recursive DNS servers. If the answer is still not found, the recursive DNS server sends query to root DNS servers.



```
     86400   IN     RRSIG    NSEC 8 1 86400 20120
com. 172800  IN     NS       a.gtld-servers.net.
com. 172800  IN     NS       b.gtld-servers.net.
com. 172800  IN     NS       c.gtld-servers.net.
com. 172800  IN     NS       d.gtld-servers.net.
com. 172800  IN     NS       e.gtld-servers.net.
com. 172800  IN     NS       f.gtld-servers.net.
com. 172800  IN     NS       g.gtld-servers.net.
com. 172800  IN     NS       h.gtld-servers.net.
com. 172800  IN     NS       i.gtld-servers.net.
com. 172800  IN     NS       j.gtld-servers.net.
com. 172800  IN     NS       k.gtld-servers.net.
com. 172800  IN     NS       l.gtld-servers.net.
com. 172800  IN     NS       m.gtld-servers.net.
COM. 86400   IN     DS       30909 8 2 E2D3C916F6
COM. 86400   IN     RRSIG    DS 8 1 86400 2012072
```

```
example.com   IN  NS  ns1.ex.com
example.com.  IN  NS  ns2.ex.com
example.com   IN  NS   ns3.ex.com
```

```
www IN  A    10.10.10.2
ftp    IN  A    10.10.10.3
```

1.In Zone ?
2.In Cache?
3.Root Hint file
4.Send query
-FQDN
-Type(A)
-Class(IN)

1.In host file?
2.In cache?
3.Prefer DNS list?
4.Send Query
-FQDN
-Type(A)
-Class(IN)

Fig. 1. Typical name resolving process

The IP address of the root DNS server is already known in the recursive DNS server through root hint file. The root DNS servers give referral answer to the TLD DNS servers for top-level domain and its corresponding IP address. The DNS servers to which recursive DNS server contacts in order to resolve domains are called authoritative DNS servers.

In case of "www.example.com" the IP address of the authoritative DNS server for ".com" TLD is answered by a root server. Based on the received referral information, the recursive DNS server continues the name resolving process by sending the DNS query to the authoritative DNS servers of top-level domain (in this case '.com' servers). The top-level domain DNS servers ('.com' servers) provide the referral information for the lower level domains. The recursive DNS server continues querying till the final answer is received. This answer is sent back to the user's computer and the user can finally connect to the server of "www.example.com".

For multiple sub domain levels, all the queries will be directed to authoritative SLD name server. This name server is responsible to give the referral information for lower level domains.

B. Domain Delegation

Each node within the domain name hierarchy is assigned to an organization or person to administer the node. The authority of a particular node can be delegated to the lower level of that node. Fig. 2 shows the typical domain delegation.

The root-level domains are administered by Internet Corporation for Assigned Numbers and Names (ICANN). The generic Top-Level Domains (gTLD) are administered by ICANN and delegated to a series of accredited registrars. The ccTLDs are delegated by ICANN to individual countries for authoritative administration.

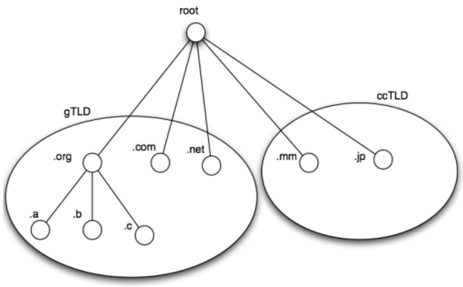


Fig. 2. Domain delegation

C. Zone File

The zone file is located in an authoritative DNS server that is responsible for a domain or zone. The zone file describes all the characteristics of a domain including services provided by the domain. The main contents of the zone file are Time To Live ($TTL) directive which defines how long the copy of the zone file should be kept in the other DNS servers, $ORIGIN directive which defines the domain name for the zone, Start of Authority (SOA) resource record which defines the global characteristics of the zone containing serial number, refresh time, retry time, expiry time and minimum time concerning with zone transfer process and Name Server (NS), resource records which define which domain is under which name server. The other main contents are IP Address (A) resource records that define IP address of the host in the domain and MX resource records that define the mail servers.

In authoritative DNS servers, there can be two types of zone files, master and slave zone files. Master zone file is stored in master DNS server and slave in slave DNS server. For example, if the zone file for "example.com" domain is stored in the DNS server called ns1, then, the DNS server is master DNS server for example.com domain. The DNS server, ns1, will answer the queries regarding with example.com authoritatively setting "aa" (Authoritative Answer) bit in the replying DNS packet header. If the zone file from DNS server ns1 is copied to DNS server ns2, then ns2 will also answer the queries for example.com authoritatively. The DNS server, ns2, is the slave DNS server for example.com zone. There will be no difference in answer from ns1 and ns2.

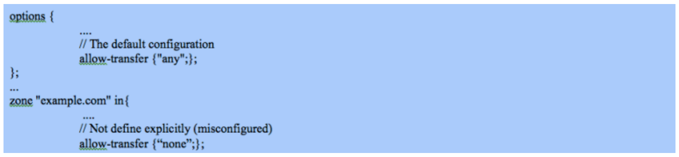
D. Zone Transfer Process

Zone transfer is the process of replicating the databases containing the DNS data across a set of DNS servers. The slave DNS server checks for changes in master zone file in every refresh time as defined in the SOA resource record by sending SOA query to Master DNS server. If updates or changes are made in the master zone file before defined refresh time, master DNS server will send NOTIFY message to slave DNS server to initiate SOA query. After receiving SOA record, the slave DNS server compares serial number of master DNS server's zone file with that of previously copied zone file. If the serial number in the received SOA RR is higher than the one currently stored in the slave, a zone transfer is initiated. If the slave server fails to make contact with the master during refresh cycle, it will reconnect to master server according the retry time defined in SOA RR. If the contact is made, both the refresh and expiry counts are reset. If the slave fails to make contact till it reaches the expiry time defined in SOA RR, the zone records in slave are assumed to be no longer authoritative.

E. Misconfiguration of Zone Transfer

While zone transfer is important for the efficient operation of DNS, it can be source of information leakage. The master DNS server should allow zone transfer only to the slave or trusted DNS servers. If the zone transfer is not restricted at all, all the resource information of the zone file can be accessible by unauthorized persons. Not only master DNS server but also slave DNS server should specify exactly which IP address or network to allow and which to restrict the zone file download.

In Berkeley Internet Name Daemon (BIND), *allow-transfer* specifies which hosts are allowed to receive zone transfers from the server. Administrators can specify the *allow-transfer* option in the *zone* statement in order to override the *options*' *allow-transfer* statement in the configuration file of BIND DNS server (/etc/name.conf). If not specified, the default is to allow transfers from all hosts. Fig. 3 shows an example of misconfiguration of zone transfer setting.



```
options {
                ....
                // The default configuration
                allow-transfer {"any";};
};
...
zone "example.com" in{
                ....
                // Not define explicitly (misconfigured)
                allow-transfer {“none”;};
```

Fig. 3. An example of misconfiguration of zone transfer

III. Methodology

The methodologies for data collection and analysis are discussed in the following two sub-sections. The scripts based on Google Search Engine and Perl module, Net::DNS::Resolver, are used for the collection and analysis of the data.

A. Data Collection

The analysis is conducted based on two data sets, TLD and SLD lists. TLD list is collected from IANA [1] at July 20 07:07:01 2012 UTC. In TLD list, there are total of 314 TLD domains including 249 ccTLD, 22 gTLD and 43 internationalized domain names (IDN). The second data set is the list of SLD of each ccTLD in which total of 34,164 SLD are consisted. There are two steps in collection of second data set. Firstly, Uniform Resource Locator (URL) of each of the ccTLD is collected using Google Site Search. Google gives 1,000 URL for each ccTLD. The total 156,648 URLs are collected for ccTLD of 249 countries. In collection of URLs from Google site search result, multi-link add-on on Mozilla Firefox is used. Then, the collected URLs are treated by Perl script to receive the required data set of SLD. Fig. 4 shows the data collection steps for second data set.

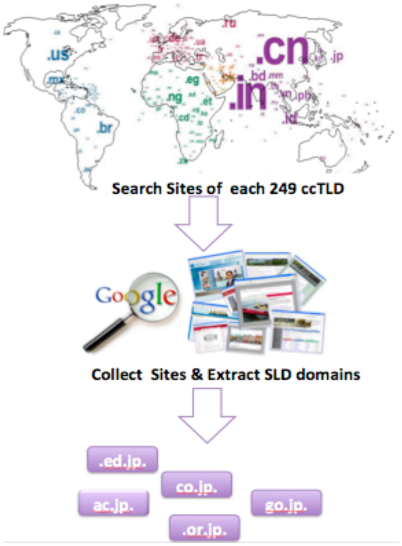


Figure. 4. Data collection steps for second data set

B. *Data Analysis*

Zone transfer misconfiguration is investigated for two data sets, TLD and SLD lists. The same data analysis steps are applied for both TLD and SLD data sets.

Data analysis is based on two main steps. The data analysis steps are shown in Fig. 5. Perl script based on Net::DNS [2], Net::IP, Net::Domain::TLD and List::MoreUtils is used for both steps. In the first step, authoritative name servers of investigated domains are searched. For example, if the investigated domains are TLD, authoritative name server of each of TLDs is searched. In this step, for each of investigated domain, NS, A RR of name servers and SOA are queried programmatically to receive list of authoritative name servers. When NS query is failed, the domain is put into "No Name Server List". When queries on A and SOA RRs are failed, the domain is put into "A Fail" and "SOA Fail" respectively. When there is no authority answer bit ("aa" bit) in the reply of SOA query, the name server is assumed as not authoritative for investigated domain. These name servers are put into "Lame Delegation Error" list. In domain name system, a lame delegation, also known as a lame response, is a type of error that results when a name server is designated as the authoritative server for a domain name for which it does not have authoritative data [3].

In the second step, zone transfer misconfiguration for each of authoritative name server is investigated by sending asynchronous full zone transfer (AXFR) queries. If the name server allows zone transfer to Internet, we put it in the misconfigured list.

In managing AXFR replies from misconfigured name server, we use methods called *axfr_start* and *axfr_next* of Perl Net::DNS::Resolver module. In contract with normal *axfr* method in which AXFR replies are returned as Net::DNS::RR object, we try to manage the packets in the socket level with *axfr_start* and *axfr_next* methods in which the replies are IO::Socket:INET objects. The method, *axfr_start,* performs zone transfer query. If zone transfer is allowed, axfr_next reads one packet at a time by using the socket object. We read the first packet of zone transfer that is SOA RR if the zone transfer is allowed and other packets are truncated. From TLD investigation, 1,284 authoritative name servers are investigated. For SLD investigation, 46,416 name servers are investigated. The results on each of the investigation are discussed in next section.

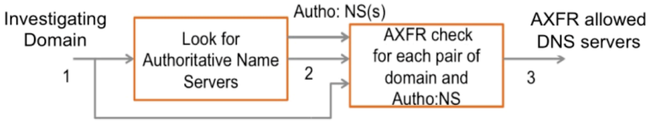

Investigating Domain
1
Look for Authoritative Name Servers
2
Autho: NS(s)
AXFR check for each pair of domain and Autho:NS
3
AXFR allowed DNS servers

Fig. 5. Data analysis method

IV. Results

A. *TLD Investigation Results*

TLD data set includes 314 domains. Two analysis steps are applied for each of TLDs.

From the first step of looking for authoritative name server, total of 1,284 name servers (1,140 IP addresses) are found. Four top-level domains, gb., pw., sj., bv., are not in active as there are no NS RR replies for these domains. These four domains are put into the "No Name Server " list. There are 5 name servers in the "A Fail" list as A query for NS RR of these name servers fail. There are 11 name servers in the "SOA Fail" list as SOA query for these name servers fail. There are 22 name servers in the lame delegation error list. The domain .kh has 7 authoritative name servers and 3 out of 7 are lame delegations.

From the second step of AXFR check to all these 1,284 name servers, 84 name servers (82 IP addresses) allow zone transfer. In terms of domains, 55 TLD domains out of 314 TLD domains (17%) allow zone transfer. Top-level domains that allow zone transfer are: [AERO. AN. AO. ARPA. AW. BB. BD. BI. BM. BV. CI. CR. CW. CY. DO. ER. ET. FO. GD. GE. GP. GQ. GT. GY. INT. IQ. KM. KW. MC. MG. ML. MM. MO. MP. MW. NI. NP. PF. PG. PK. PW. SC. SJ. SL. SV. TC. TJ. TO. UK. VG. XN--FZC2C9E2C. XN--XKC2AL3HYE2A. XN--YGBI2AMMX. YE. ZW.] The countries whose TLD's zone transfer is misconfigured are shown in Fig. 6.

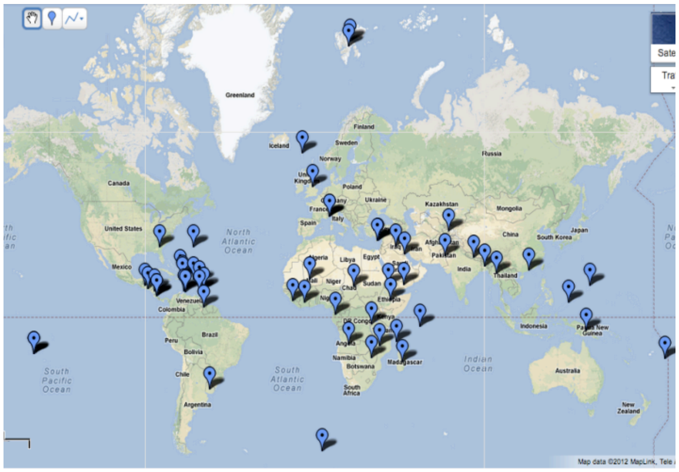


Fig. 6. Zone transfer misconfigured countries (TLD)

B. *SLD Investigation Results*

SLD data set includes 34,164 domains. Two analysis steps are applied for each of TLDs.

From the first step of looking for authoritative name server, total of 46,416 name servers are received. There are 436 name servers in the "A Fail" list as A query for NS RR of these name servers fail. There are 936 name servers in the "SOA Fail" list as SOA query for these name servers fails. There are 1,375 name servers in the lame delegation error list.

From the second step of AXFR check to all the 46,416 name servers, 5,394 name servers (4,973 IP addresses) allow zone transfer. In terms of domains, 6,234 SLD domains out of 34,164 investigated domains are misconfigured for their zone transfer.

In ccTLD domains, ck., fj., fk., gn., gt., jm., lr., sv., their second level domains do not have NS records. That is why, SLD investigation fails for these 8 countries.

The summarized table on all of the results of TLD and SLD investigation sets is shown in Table 1.

TABLE I. SUMMARY OF RESULTS

Level	Investigated Domains	Mis-configured Domains	%	Name Servers	Mis-configured Name Server (by domain)	Mis-configured Name Server (by IP)	%
Top Level	314	55	17	1,284	84	82	7
Second Level	34,164	6,234	18	46,416	5,394	4,973	12

C. *Other findings*

- Zone transfer misconfiguration in TLD reveals zone information of its SLD. Accordingly zone transfer misconfiguration in SLD reveals zone information of its sub domains. From the analysis, it shows that 7 % of TLD name servers and 8% of SLD name servers are misconfigured.

- For a particular TLD, there can have 2 to 10 authoritative DNS servers. These servers' domain names can be in the same TLD zone or different TLD zone. For example, the authoritative name servers of .com TLD can be ns.example**.com** or ns.example**.net.** In case of ns.example.com, the name server exits in the same TLD zone as .com TLD. Our TLD investigation results show that misconfigured name servers are mostly name server existing in the same zone as its TLD.

- As the zone information contained in one name server is the same as others, revealing of zone file information from one name server can be as serious as revealing from all.

- We found cases where misconfiguration is propagated. Namely, a particular name server is found authoritative for both TLD and its SLD and a single point of misconfiguration affects both. For example, if a name server called ns.example.com is authoritative not only for .com TLD but also for example.com SLD, misconfiguration of zone transfer can be found in both TLD and its SLD zones.

V. ANALYSIS ON RESULTS

In order to understand the percentage of misconfiguration of name servers in each level of TLD and SLD, we calculate the ratio of misconfigured name servers to existing name servers for each TLD and SLD. The percentage of misconfiguration for TLD is marked blue and for SLD is marked red in Fig. 7.

According to the data shown in Fig. 7, we notice three countries (circled with red), in which both TLD and SLD misconfiguration is more than 40%. The ccTLD of these countries are bd., er., and mm. The .bd domain has 100% misconfiguration in both TLD and SLD. This is because of the fact that there are three authoritative name servers for bd. TLD and three out of the three allow zone transfer. When, SLD domains of the bd. domain are investigated, we notice that there are three SLD domains such as com.bd, org.bd and gov.bd. Again, when we check on the name servers of these bd.' existing SLD, the same three authoritative name servers are found. That is why, in such a case, we can say that these three name servers are not only authoritative for bd. TLD but also for its SLD and are misconfigured for both TLD and SLD.

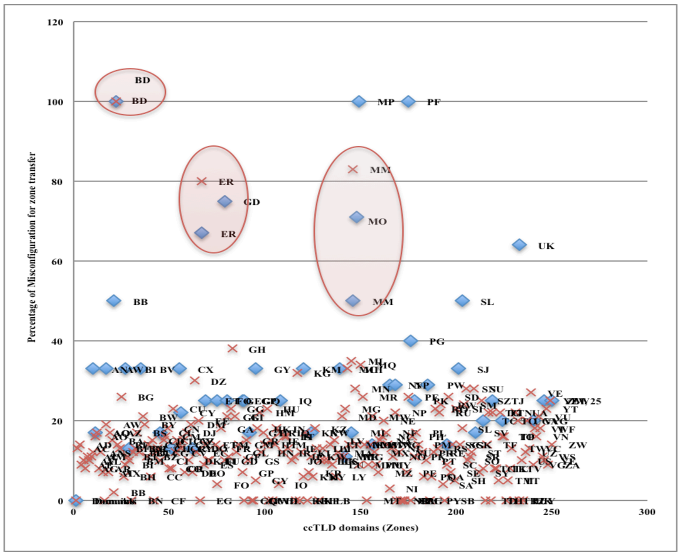


Fig. 7. Misconfiguration in ccTLD and SLD

In case of er. ccTLD, it has three authoritative name servers and two out of the three authoritative name servers have misconfiguration on zone transfer. In case of SLD of er. ccTLD, from our search engine based domain search, it has three SLDs, edu.er com.er and gov.er.. When we check the name servers of these er.'s SLD, we notice that four out of five authoritative name servers allow zone transfer. When the name servers of er. ccTLD and its SLD are checked , like bd.

case, two misconfigured name servers of er. ccTLD are also functioning as authoritative name servers of its SLD.

For the mm. ccTLD, two out of four (50%) authoritative name servers allow zone transfer. In case of SLD investigation, mm. ccTLD has six SLDs. Five out of six authoritative name servers for mm. SLDs allow zone transfer. Out of these five misconfigured name servers, two misconfigured name servers of mm. ccTLD are again included. It means that these two misconfigured name servers are responsible for mm. ccTLD and some of its SLD.

The misconfiguration can be more serious if the misconfigured DNS servers are authoritative for lower level. In the worst case, DNS infrastructure information of the whole country can be exposed if name servers' domain name for delegated zones exists in the same zone whose authoritative server is misconfigured. For example, example1.com domain of .com TLD has authoritative name servers whose domain name is ns1.dns.com. In such a case, name server domain name is existed in the same .com zone. That is why we continue the investigation on third level domains of these three countries (bd., er., mm. domains). We look for the third level domains of these three countries and then check the authoritative name servers and zone transfer. The results for er. and mm. show that misconfigured name servers are authoritative to answer not only for that ccTLD but also for most of its SLDs and third level domains. In mm. domain, authoritative name server's domain names of all SLD and third level domains existed in the same zone. Consequently, 83% of the DNS infrastructure information of the country is exposed to Internet. (Notice: The information regarding this misconfiguration has been provided to the authoritative personnel of that ccTLD and the misconfiguration was fixed on June 22, 2012.)

VI. Related Works

To start investigation on misconfiguration of zone transfer, it is necessary to obtain the list of existing domains in an investigated DNS hierarchy. Without looking at the zone file of upper level domain, it is difficult to get the entire list of lower level domains. Because of such difficulties, previous studies had been done only on second level domain (SLD) of one to two top-level domain (TLD) for which zone file access was allowed. There is a possibility to receive the list of SLD from misconfigured zone file of TLD. But, downloading zone file rather than secondary name server can raise legal issue. These conditions make many constraints to investigate the existence of misconfiguration of zone transfer in lower level of DNS hierarchy.

A.J. Kalafut [4], attempted to transfer the zones listed in the .com and .net TLDs. They investigated zone transfer, zone diversity, deployment of new technologies and other configuration issues by downloading 6.6 % of zone file for second level domain names listed in .com and .net top-level domains.

Van Wanrooij [5] characterized misconfiguration on DNS from a sample of the (.nl) TLD. They did ANY queries of DNS on 10,000 randomly selected zones mentioned in the (.nl) zone.

The Measurement Factory [6] performed zone transfer on a small fraction of the .com and .net zones. They randomly sampled about 3.22% of .com and .net zones and attempted to transfer zone.

All the previous studies need to look at the zone file. The upper level of DNS name space needs to be seen in order to check misconfiguration in one level below. For example, in order to investigate SLD, it is necessary to get access the zone file of TLD's name server. In contrast with previous studies, this study proposes how to investigate the existence of misconfigurations of zone transfer in any level of DNS hierarchy using search engine based approach without the need to look at the zone file of upper level DNS name space.

Conclusion

Individual resource record in the zone file is not sensitive. But, a copy of entire zone file including different types of RR(s) may be sensitive. The deeper the level of DNS hierarchy, the more different types of RR may contain in a zone file. That is why, it is important to investigate the existence of misconfiguration of zone transfer in DNS hierarchy. To start investigation, it is necessary to obtain the list of lower level domains. So, it needs to look at zone file. Downloading zone file rather than secondary name server can raise legal issue. That is why in this study, we propose the search engine based method in order to investigate misconfiguration of zone transfer. Using the proposed method, misconfiguration of zone transfer in TLD and SLD are investigated. Our investigations do not need to look at the zone file of investigating DNS hierarchy. That is why, with our approach, the investigations can be done in any level of the DNS hierarchy in a broader way without the need to worry on legal issues that could happen by looking at the zone file.

In DNS hierarchical levels lower than SLD, there can be chances of revealing of DNS information from the misconfigured DNS servers authoritative for these lower level domains. That is why the investigations on the lower levels of DNS hierarchy should be done as future work.

Acknowledgements

A part of this study has been supported by PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) project by the Ministry of Internal Affairs and Communications, Japan.

REFERENCE

[1] "Internet Assigned Numbers Authority." [Online]. Available: http://www.iana.org/assignments/dns-parameters/. [Accessed: 17-Jul-2012].

[2] "Net::DNS." [Online]. Available: http://www.net-dns.org/. [Accessed: 21-Jan-2013].

[3] "Lame delegation - Wikipedia, the free encyclopedia." [Online]. Available: http://en.wikipedia.org/wiki/Lame_delegation. [Accessed: 21-Jan-2013].

[4] A. J. Kalafut, C. A. Shue, and M. Gupta, "Touring DNS open houses for trend and and configurations," *IEEE ACM Transactions on Networking*, vol. 19, no. 6, p. 1666, 2011.

[5] W. van Wanrooij and A. Pras, "DNS zones revisited," in Open EuropeanSummer School and IFIP WG6.4/6.6/6.9 Workshop (EU NICE), 2005.

[6] The Measurement Factory, "DNS survey: October 2007," http://dns.measurement-factory.com/surveys/200710.html.

[7] "Why is securing DNS zone transfer necessary ?" [Online]. Available: http://www.sans.org/reading_room/whitepapers/dns/securing-dns-zone transfer_868.

[8] "Whitehats.ca - Jeff Holland DNS/Bind Security." [Online].Available:http://www.whitehats.ca/main/members/Jeff/jeff_d_security/jeff_dns_security.html. [Accessed: 06-May-2012].

[9] " Pro DNS and BIND: Ron Aitchison", ISBN13: 978-1-59059-494-0

[10] "RFC 1035" [Online]. Available: http://www.ietf.org/rfc/rfc1035.txt [Accessed:29-Jan-2013].