# Search Engine Based Investigation on Misconfiguration of Zone Transfer

Yin Minn Pa Pa, Katsunari Yoshioka, Tsutomu Matsumoto

Yokohama National University

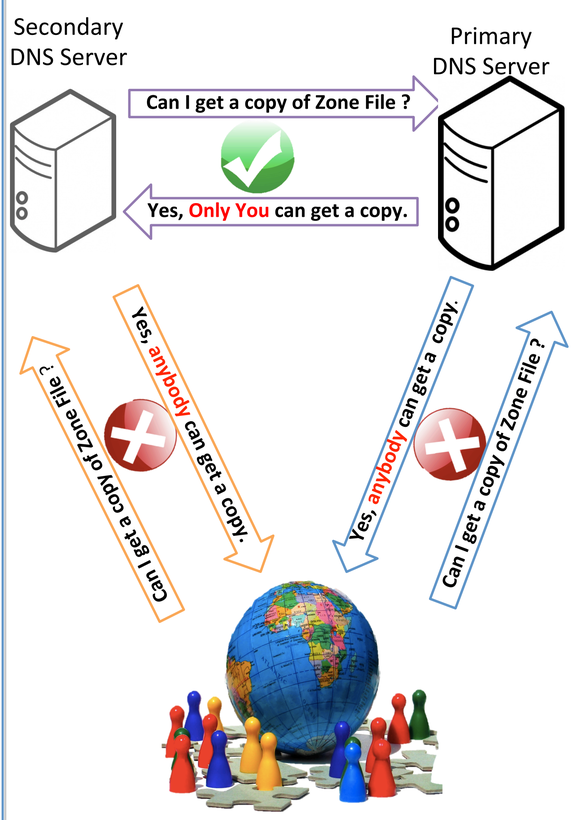
## Introduction

- **Proposed Study**
  - How to investigate the existence of misconfigurations of zone transfer using search engine
- **Problem Statement**
  - 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.
- **Contribution**
  - Unlike previous studies, the proposed method does not require actual download of zone files for investigation.
  - By the investigation, 55 misconfigured TLD and 6,234 SLD are found including one serious case in which zone files for the entire country were exposed to the public.(fixed on 2012/ June/22).

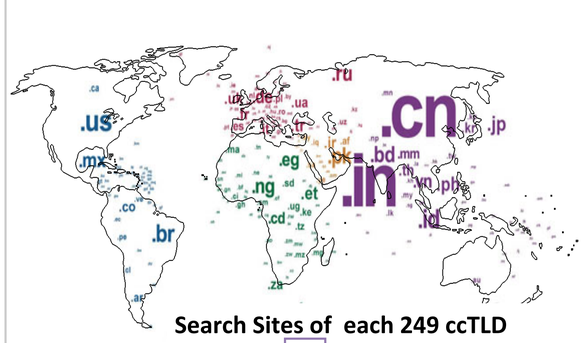
## Background

- **Zone Transfer**
  - Zone transfer is one of the critical operations of Domain Name System(DNS) in which the contents of a zone file are copied from primary DNS server to secondary DNS server(s).
- **Normal Operation of Zone Transfer**
  - Primary DNS server should allow zone transfer only to trusted secondary DNS server(s).
- **Misconfiguration of Zone Transfer**
  - Either of primary or secondary DNS server allows zone transfer to anybody.

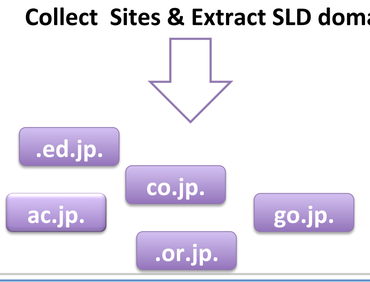
### Misconfiguration of Zone Transfer ?




### Search Engine Based Investigation ?








## Data

- According to IANA(Internet Assigned Number Authority)
  - ccTLD -> 249
  - gTLD -> 22
  - IDN -> 43
- By the result of scripts
  - Total domains for the investigation -> 314
  - Authoritative Name Servers for 314 domains -> 1,284
- Google Site Search for SLDs
  - Sites of ccTLD -> 156,648
  - Extracted Second Level domains -> 34,164
  - Authoritative Name Servers for 34,164 domains -> 46,416

## Results

### Investigation on Top-Level Domains and Results

- The existence of misconfiguration of zone transfer has been investigated for all 314 TLD
- The following top-level domains allow zone transfer
  - [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. 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.] ( As of July 15 , 2012 )
  - 9 top-level domains (.bv,.cs,.dd,.eh,.gb,.pw,.sj,.ss,.yn) are not currently in active.
- **Zone Transfer Misconfigured ccTLD**

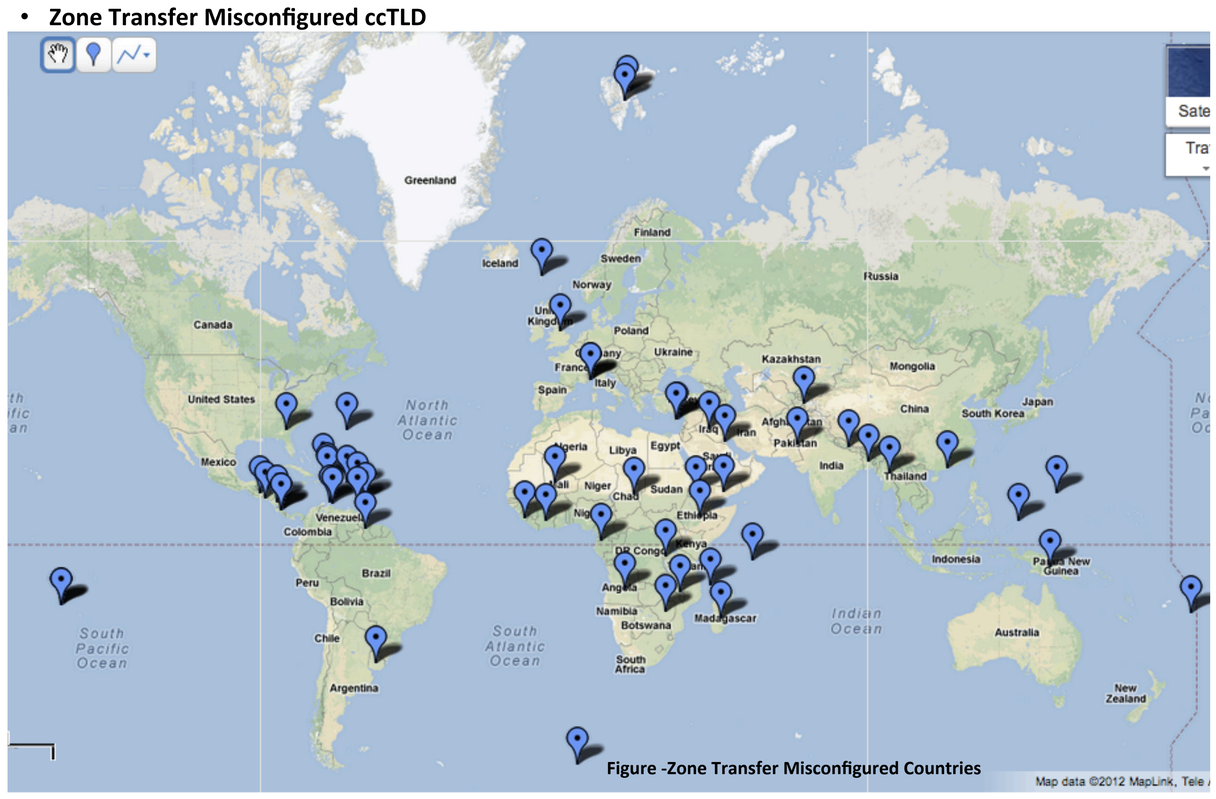



Figure -Zone Transfer Misconfigured Countries

### Investigation on Second Level Domains and Results

- The existence of misconfiguration of zone transfer has been investigated for 34,164 SLD domains of 249 ccTLD
  - ck,fj,fk,gn,gt,jm,lr,sv -> No Name Server for SLD
  - 27 ccTLDs ->Perfect configuration for both TLD & SLD
- Out of 46,416 authoritative name servers of 34,164 SLD, 5,394 authoritative name servers of 6,234 SLD allow zone transfer to anyone.
- One ccTLD of a country is noticed in which misconfigured name servers are authoritative to answer not only for that ccTLD but also its SLDs. Moreover, NS RRs of all lower level domains are existed in the same zone. Consequently, DNS infrastructure information of the whole country was exposed to the Internet. (Notice: 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.)

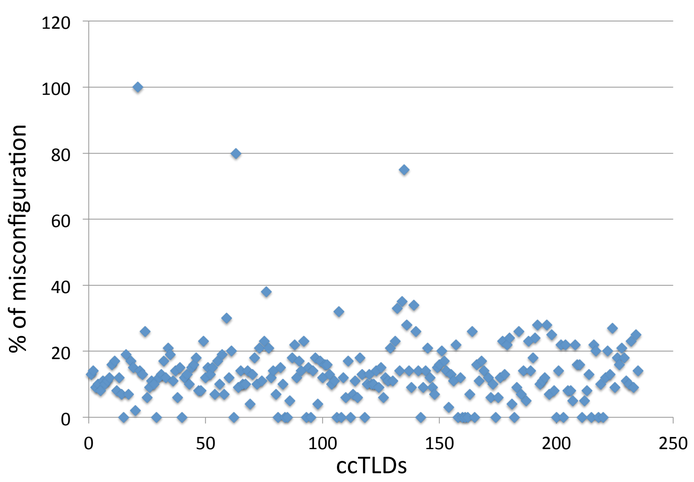



Fig-Percentage of Misconfiguration

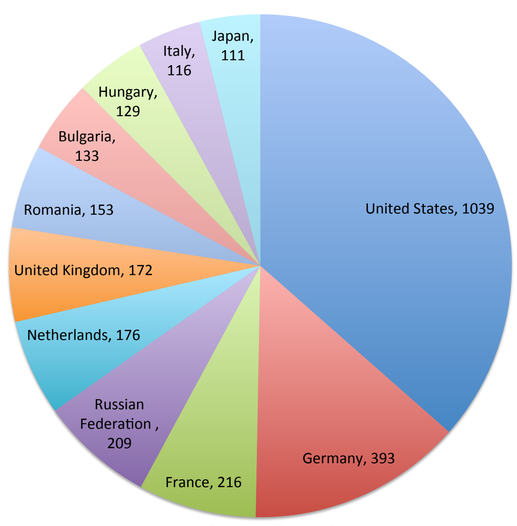



Fig-Location of Misconfigured Name Server

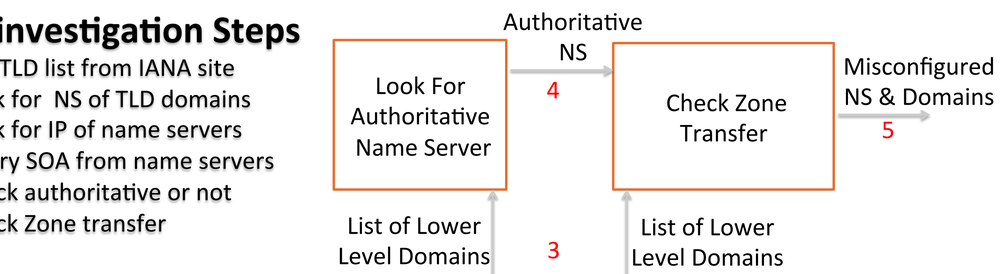
### Results Summary

| Level | Investigated Domains | Misconfigured Domains | % | Name Servers | Misconfigure Name Server (by domain) | Misconfigure 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 |

## Methodology

### TLD investigation Steps

- Get TLD list from IANA site
- Look for NS of TLD domains
- Look for IP of name servers
- Query SOA from name servers
- Check authoritative or not
- Check Zone transfer




### SLD Investigation Steps

- Look for sites of ccTLD Domains
- Collect Sites and Extract Domains
- Query NS of SLD domains
- Look for IPs of NS
- Query SOA from NS
- Authority Check
- Check Zone Transfer

## Conclusion

- Individual RR in 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 lower level of 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.
- THIS STUDY SOLVED THIS ISSUE

## Acknowledgement

This work was partially supported by the project "PRACTICE: Proactive Response Against Cyber-attacks Through International Collaborative Exchange" funded by the Ministry of Internal Affairs and Communications, Japan.

Contact: yinminpapa--xg@ynu.ac.jp