

DNS Hijacking

Inappropriate domain name management causes DNS Hijacking

IEPG Meeting
Nov. 6, 2005

Kazunori Fujiwara, JPRS
<fujiwara@jprs.co.jp>

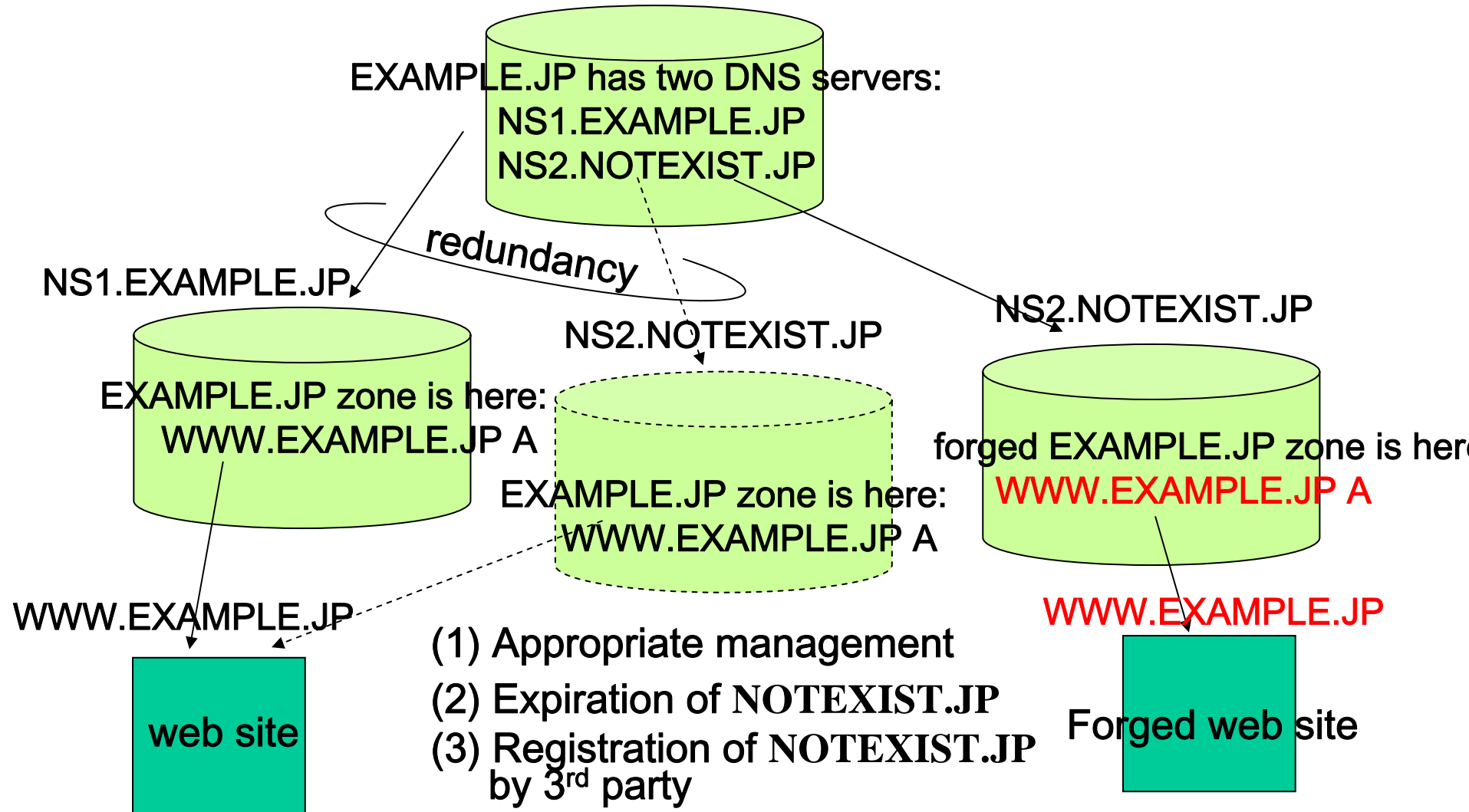
What is 'inappropriate domain name management'?

- Registrants have to manage
 - DNS servers that provide zone information (Child)
 - Contains DNS servers' information
 - DNS servers' information that is registered to registry (Parent)
- Child and Parent should be synchronized
 - If not, it causes lame delegation
 - If not, it is in one of inappropriate states
- Typical inappropriate states
 - Registering incorrect name (typo)
 - Leaving expired (non-existing) domain name in Parent
 - Leaving non-working DNS server as Child
- These states may cause DNS hijacking.

How 'domain name hijack' can happen?

- Suppose DNS server's domain name exists no more
 - EXAMPLE.JP has NS1.EXAMPLE.JP and NS2.NOTEXIST.JP as its name servers, but NOTEXIST.JP was expired and not existent any more
 - Anyone can register NOTEXIST.JP and setup NS2.NOTEXIST.JP as a DNS server of EXAMPLE.JP
 - Then he/she can forge zone information so that DNS responses from NS1.EXAMPLE.JP and from NS2.NOTEXIST.JP are different
- This situation easily happen
 - If domain name registration manager and DNS operation manager in registrant organization are different and their activities are not synchronized

How 'domain name hijack' can happen?



Case study : in Japan (1/2)

- One domain name had two DNS servers
 - A famous credit card company's domain name
 - One DNS server kept working but the other stopped its operation (April 2005)
- Stopped DNS server's domain name was expired. One month after, anyone could register expired domain name. (May 2005)
 - An attacker could register the domain name and run malicious authoritative DNS server.
 - In this situation, forging to DNS and phishing is very easy
- One person warned this situation to Japanese community
- Now, it has been fixed

Case study : in Japan (2/2)

- IPA (a governmental organization) announced a security advisory about this issue
- After that, JPRS, JPCERT, and Ministries announced their advisories
- Articles about this were published on various web sites
- National newspaper Asahi-Shimbun wrote it up.
 - <http://www.asahi.com/english/Herald-asahi/TKY200510030127.html>

Who is responsible?

- **Registrant of the domain name is responsible for its management**
 - Registrant should confirm and keep the configuration appropriate
 - TLD registries sets and modifies the zone data reflecting the instructions given by Registrants or Registrars
- **On the other hand, registries/registrars can check and find inappropriately managed domain names**
 - What roles should registries play?
 - Education
 - Check & individual notification

What TLD registry can do

- **Promote Registrants' understanding about DNS**
 - Through web pages of registries/registrars/ISPs/...
 - Through news from media
 - Through public lectures
- **Check the status of domain names and warn the registrants/registrars about the inappropriateness**
 - Only TLD registries can check all the domains
 - But it is difficult to check the appropriateness if registered DNS server name is not under the TLD
 - Therefore, cooperation between registries is required
- **Disable DNS delegation if the domain name is exposed to significant danger**
 - With or without any consent/notification to the registrar

What JPRS did

- Expressed public warning on its Web site
- Checking appropriateness of DNS setting under .JP
 - Not checked if DNS servers are not under .JP
- Sending warning mails to registrars (monthly)
- Sending warning to registrants (monthly)
 - E-mail
 - Postal mail
- Start implementing to disable inappropriate DNS delegation

Consideration and inquiries □

- What should we do as TLD registry ?
 - LAME delegation check and disabling delegation includes this
- Collaborative checking among TLDs is required
 - It is difficult to check the appropriateness
if registered DNS server name is not under the TLD
- Do you cope with inappropriate domain name management ? If you will do, please let me know!
 - Do you face such domain name hijacking?
 - What kind of measures have you taken to address this issue?
 - Results

Questions/Comments?