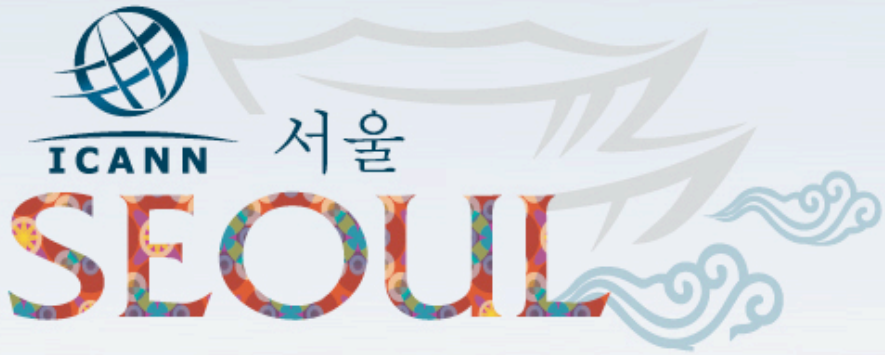
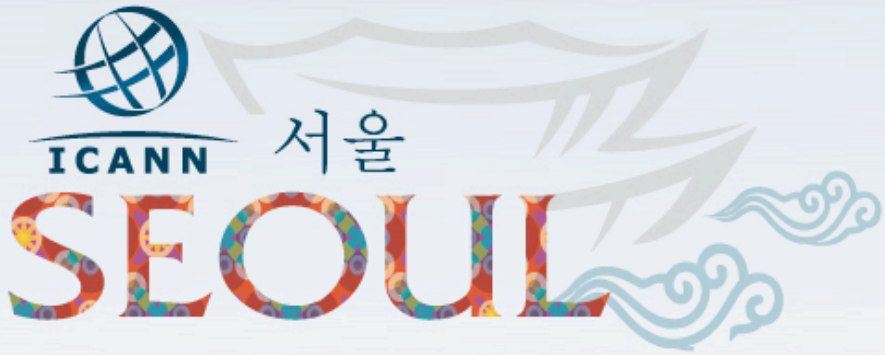


SSAC Meeting with ccNSO on Redirection

28 October 2009



Redirection & Synthesized DNS Responses in Top Level Domains – What Breaks?

Ram Mohan

October 2009

Redirection of DNS Responses @ TLDs

- **Issue**
  - Wildcarding of DNS records at TLDs
  - Provides "valid" address and routing even when domain names do not exist
- **Consequences**
  - Breaks core DNS systems & legacy applications
  - Erodes trust relationships
  - Creates new opportunities for malicious attacks, without ability of affected parties to mitigate problem

Reference Document: SAC041

SSAC Advice:

Clear & Significant danger to security & stability of the DNS

Board Resolution (June 2009):

Take all available steps with appropriate entities to prohibit such use

Prohibit redirection/synthesis for all TLDs (gTLD & ccTLD, including IDN TLDs)

- Revise new gTLD Guidebook
- Consult with ccTLD community/GAC for new ccTLDs
- Revise existing gTLD agreements
- Add appropriate guidelines to existing ccTLD arrangements

Reference Document: SAC041

Problems Caused

- Architectural violation
- Impact on Internet protocols
- Single point of failure
- Reserved and blocked domains ‘appearing’ alive
- Privacy concerns
- Lack of choice for Internet users
- Poor user experience
- Impact on IDN TLDs

References: See list at end of presentation

Architectural Violation

- Redirection at the TLD level violates fundamental principles
  - DNS Protocol is neutral about what protocols to answer
  - Redirection assumes HTTP protocol (web browsing)
- All future protocols dependent on DNS affected by redirection
  - Unacceptable invasion of protocol boundaries
    - For example, HTTP could use DNS even though HTTP is a recent invention, due to clear layering

Every Current & Future Internet Application Is Affected

Impact & Side-Effects on:

- Every mail server, mail agent
- Every instant message program and agent
- Every VOIP server, proxy and user agent
- Every parental control system
- Every anti-virus system
- Every license management system
- Every software update system

i.e., Every Application On The Internet

Most Basic Internet Tools Break

- Systems that test for “existence” of a host fail
  - Spam filters stop working (all forged addresses now appear to be real)
  - URL link checkers will fail (all links appear to be valid)
- Systems that believe a host name is valid break
  - Mail to a mis-typed address will not bounce anymore
  - And, the mail is delivered to a different address, without any notification or choice by the e-mail sender
  - Search engines won’t be able to function as normal
- Applications that root operators, IANA and other organizations use to monitor TLD name service & zone composition might break

Impact on IDN TLDs

IDN TLD are deployed in <language>, but are represented on the DNS in ASCII

Wildcards for IDN TLD can cause unexpected behavior:

- Localization of content could break
  - User may request a web page in <language A> and get a different page in <language B>, with no choice

Reference document s

http://www.icann.org/committees/security/ssac-report-09jul04.pdf

http://www.iab.org/documents/docs/2003-09-20-dns-wildcards.html

http://www.icann.org/committees/security/sac041.pdf

http://www.icann.org/en/registries/rsep/tralliance_report.pdf

QUESTIONS?

감사합니다

Thank you!