Public Meeting of the Security & Stability Advisory Committee

Cartagena, Colombia

07 December 2010

CARTAGENA no. 39 5 - 10 December 2010 DE INDIAS

11:00 am to 12:30 pm

Comision 2A/B

Agenda

1. Introduction, Steve Crocker, SSAC Chair
2. Root Scaling Update, Steve Crocker, SSAC Chair
3. Registrant's Guide to Protecting Domain Name Registration Accounts (SAC044), Rick Wilhelm, Network Solutions
4. Orphaned Name Servers, Jim Galvin, Afilias

CARTAGENA
no. 39 5 - 10 December 2010
ICANN DE INDIAS

Agenda, Cont.

5. Invalid TLD Queries at the Root Level of the Domain Name System, Dave Piscitello, ICANN
6. SSAC Review: Registry Transition Program, Jim Galvin, Afilias
7. Internationalized Registration Data Working Group (IRD-WG) Interim Report: Brief Update Steve Sheng, ICANN
8. Implementation of SSAC Improvements, Steve Crocker, SSAC Chair

SSAC Current Activities

Root Scaling

Registrant's Guide

Orphaned Name Servers

Invalid TLD Queries

SSAC Review: Registry Transition Program

IRD-WG

SSAC Improvements

High Security TLDs

Member Recruitment

Registrar Failure: DNS Zone Risk Analysis

CARTAGENA DE INDIAS
no. 39 5 - 10 December 2010
ICANN

Root Scaling Update

Steve Crocker,
Chair, SSAC

Background

- The SSAC has been considering two reports: the Root Scaling Study Team’s (RSST) Report and the TNO Report on the potential impact on the stability of the root when adding:
  - DNSSEC;
  - IPv6 address records;
  - Internationalized Domain Name top level domains (IDN TLDs); and
  - New TLDs.
- December 2010: SSAC has discussed these issues and has developed recommendations.

Recent Developments

- The root zone is now DNSSEC-signed, and root-level DS records have been accepted and published.
- 291 IPv6 address records and 15 new IDN TLDs (representing 12 countries/territories) have been added to the root zone.
- There are no known reports of significant outages in DNS.

Recent Developments, Cont.

- ICANN commissioned a study on gTLD scenario planning that showed that root zone growth is currently limited by scaling human factors. Currently ICANN can handle a maximum of around 1000 new gTLD applications a year.
- ICANN has asked the root operator if they can handle the above growth and they said yes.

CARTAGENA DE INDIAS
no. 39 5 - 10 December 2010
ICANN

Simplified Questions

- Can the root system sustain a maximum growth of 1000 new gTLDs per year for the first round of new gTLD applications?
- If ICANN subsequently increases its capacity to approve more applications, what should the process be to handle this increase?

Recommendations

1. Formalize and publicly document the interactions between ICANN and the root server operators with respect to root zone scaling.
2. ICANN, National Telecommunications and Information Administration (NTIA), and VeriSign should publish statements, or a joint statement, that they are materially prepared for the proposed changes.

Recommendations, Cont.

3. ICANN should publish estimates of expected and maximum growth rates of TLDs, including IDNs and their variants, and solicit public feedback on these estimates.
4. ICANN should update its SSR plan to include actual measurement, monitoring, and data sharing capability of root zone performance.

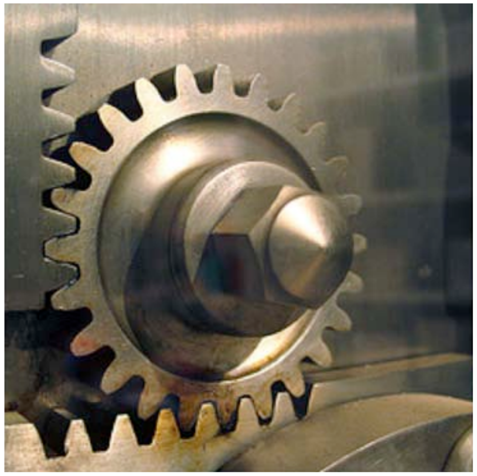
Recommendations, Cont.

5. ICANN should commission and incent interdisciplinary studies of security and stability implications from expanding the root zone more than an order of magnitude, particularly for enterprises and other user communities.

Registrant's Guide to Protecting Domain Name Registration Accounts (SAC044)

Rick Wilhelm,
Network Solutions

Protecting Registration Accounts



- A guide for registrants
- A complement to SAC040
- Overview of threats
- Best practices to follow
- Making informed decisions when choosing a registrar

CARTAGENA no. 39 5 - 10 December 2010 DE INDIAS ICANN

A Dynamic Threat Landscape

- Unauthorized access
- Malicious DNS changes
- Contact info changes
- Unauthorized DNS transfer
- Renewal interference

CARTAGENA
no. 39 5 - 10 December 2010
ICANN DE INDIAS

Account Protective Measures

- Protect account credentials
- Use correspondence to trigger internal checks
- Maintain ownership proof
- Diversify points of contact
- Implement change controls

Proactive Monitoring Measures

- WHOIS and DNS changes
- Contact data accuracy
- Nameserver accuracy
- “Last change” timestamps
- Registry & registrar status codes

CARTAGENA
no. 39 5 - 10 December 2010
ICANN
DE INDIAS

Research Prospective Registrars

- Account management features
- Correspondence schedule
- Security measures
- Reputation and references

Orphaned Name Servers

Jim Galvin,
Afilias

What is an Orphaned Name Server Record?

1. A name server (NS) record that exists in a delegation;
2. The parent domain does not exist:
   - Subcase 1: Parent domain is *temporarily* removed from the zone file, i.e., the parent domain exists in the registry but is not otherwise visible. This will ordinarily happen when a domain is placed in a “hold” status or enters certain “grace” periods.

What is an Orphaned Name Server Record?

- Subcase 2: Parent domain is *permanently* removed from the registry database. This will ordinarily happen when a domain is deleted.

2. These cases can not be distinguished with public information.

SSAC Research So Far

1. Across all 13 gTLDs, there are a total of 20.4K orphan name servers;* this accounts for 0.8% of all gTLD glue records (May 26, 2010 data).
2. 28% - 31% of domains that utilize orphan name servers have appeared on one or more abuse lists.

* Defined as name servers whose records exists in a delegation but the parent domain name no longer exists in the zone, i.e., it is not known which of the two sub cases previously defined applies.

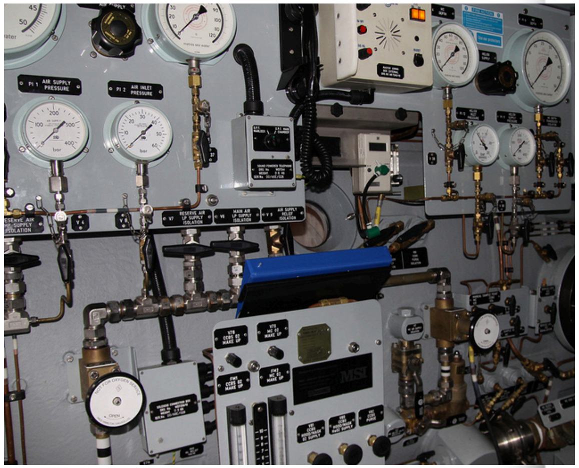
Next steps

1. The SSAC Work Party is deliberating on open issues and recommendations.
2. The SSAC Work Party will prepare a report;
3. The SSAC members will review the report;
4. The report will be published.

Invalid TLD Queries at the Root Level of the Domain Name System

Dave Piscitello,
ICANN

Root System Resolves TLD Strings as Follows

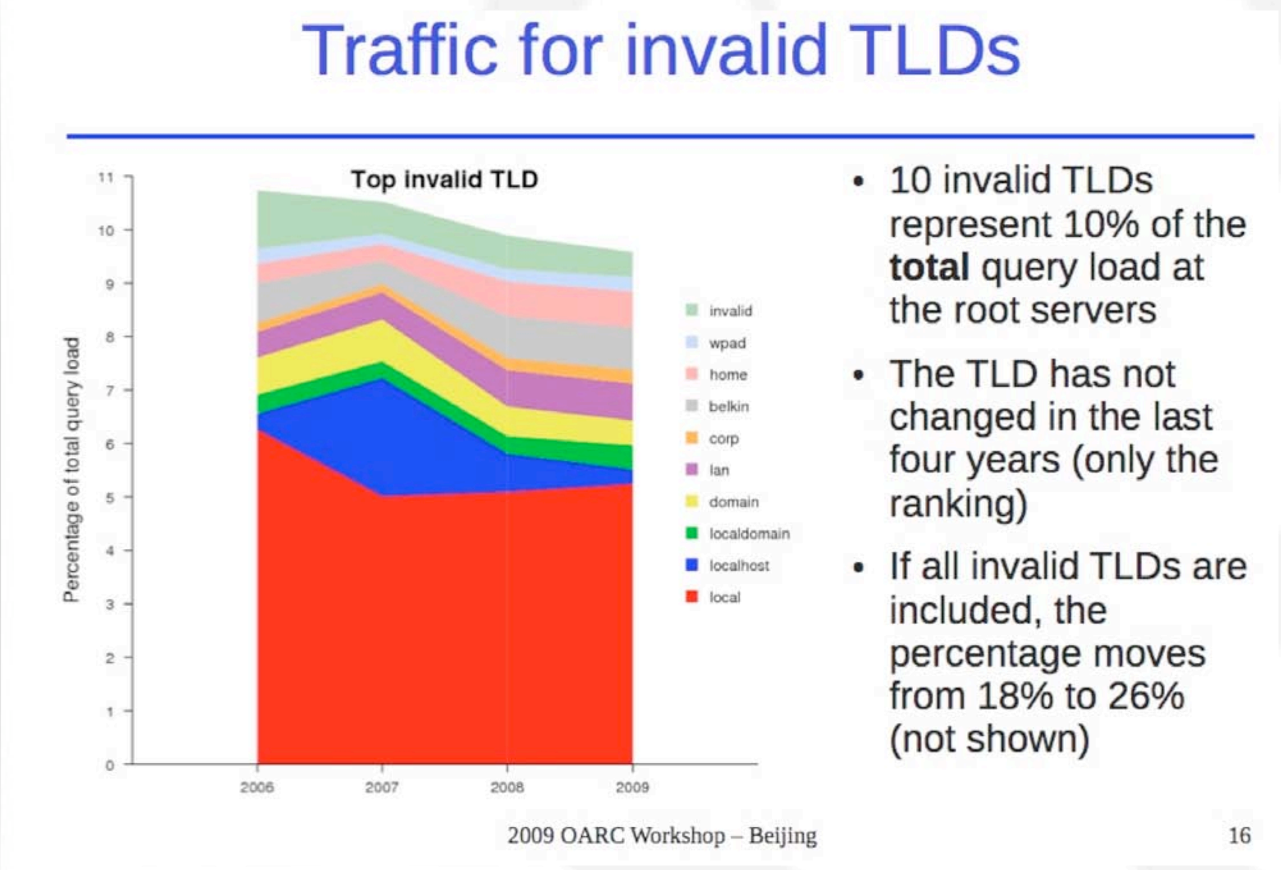


1. String exists in the root zone, return positive result.
2. String is not delegated and has not been queried.
3. String is not delegated but has been queried (return NXDOMAIN).
4. String was previously delegated but has been removed (return NXDOMAIN).

Conditions (2) and (3) are of interest to new TLD applicants

Non-Delegated TLD Strings Appear Routinely at the root

These queries are wrongly directed at root name servers as a result of configuration errors or incorrect query of DNS in networks where name spaces other than the DNS are used



Traffic for invalid TLDs

- 10 invalid TLDs represent 10% of the **total** query load at the root servers
- The TLD has not changed in the last four years (only the ranking)
- If all invalid TLDs are included, the percentage moves from 18% to 26% (not shown)

2009 OARC Workshop – Beijing 16

CARTAGENA
no. 39 5 - 10 December 2010
ICANN
DE INDIAS

Implications for New TLD Applicants

- Certain strings that have appeared at root with measurable (and meaningful) frequency:
  - A TLD operator inherits this traffic if it uses one such string; and
  - Conditions that cause invalid queries are likely to persist.

CARTAGENA no. 39 5 - 10 December 2010 ICANN DE INDIAS