ICANN Meeting 46 Beijing April 2013 – New gTLD SSR Update

General Points

- IANA is ready to process delegations wef 1May.
- Growth of traffic in the root zone is not really dependent on the no of TLDs. The change on the size of the root zone will not be as big as some previous changes (eg deployment of DNSSEC in 2010).
- L-root has been collecting some metrics (wef 3 Apr) so that long term trends can be observed i.e. they are establishing the baseline.

Discussion on SAC057 - Internal Name Certificates

Certificate Authorities (CAs)

- Not all CAs are members of the CA/Browser Forum and may not abide by Ballot 96. (See Supplementary Note)
- Even if they do, there will still exist a vulnerability window because of the 120 days (Ballot 96).
- We don't really know what certificates have been issued for these internal name servers.

Browser Vendors

- ICANN Security Team is working with Browser Vendors on this issue. Some browsers do not check for revocation of certificates.
- Part of Solution might be to use DANE and sign with DNSSEC.
- Options being considered by browser vendors to address this will only be applicable to latest versions and there will still be many older browser versions in use.

Other Applications

- Browsers are not the only applications used to connect to the internet. There are a number of other protocols that rely on Certificates. The traffic is not all web queries.
- Some applications don’t support renovation checking at all, or a man-in-the-middle attack can stop the revocation from happening.
- One mitigation is to ask server manufacturers to turn on OCSP Stapling by default (On-Line Certificate Status Protocol). This would ensure that revocation status would be checked.
- There may be other complex interactions between the DNS and other applications at the root level, cross application issues, which need to be explored. SSAC has been asking for interdisciplinary studies on these issues and ICANN may need to act as coordinator/facilitator/collaborator on these.

Other Issues and Concerns

- Irrespective of the case where certificates already exist for yet to be released gTLDs, there is also a problem associated with internal network configurations which utilise these names with or without certificates at the second or third levels eg example.com where .example is an applied for new gTLD. Queries to these new gTLDs may be directed to these internal networks, causing problems for businesses, consumers and end users. It was observed that ISPs will likely bear the brunt of complaints if this occurs and possibly incur significant costs in customer support that is unrelated to their core services.

Letter from Paypal

- Letter identified their concern about 'significant security issues related to delegating gTLDs that are currently in wide use as de facto private TLDs’. They state the top 10 of these represent 10% of the total query load at the root servers. The top 13 invalid queries some of which are gTLD suffixes identified in RFC6762 are:
  - .invalid .wpad .home .belkin .corp .lan .domain .localdomain .localhost .local .intranet .internal .private
- This was highlighted in SAC045 - Invalid Top Level Domain Queries at the Root Level. Recommendations were made in that report to mitigate this risk.

New Measurements

- SAC057 is based on data from August 2010. One member of the community has collected similar but not identical data since the release of SAC057. They examined only web queries in the .com and .net TLDs, looking for IPs that are pointed to by DNS names. Although the results are not comparable, they found that there are some 25 million certificates associated with 51 applied for new gTLDs, the biggest being .corp with 102 unique sub-domains.
- The top 4 in order of size were:
  - .corp .home .offline .inc
- Others that are also commonly found are:
  - .site .mail .bank .ads (active directory service)

Conclusion

There was a call to the community to identify any other issues and concerns which should be addressed in relation to new gTLDs.
Supplementary Note

Mozilla has a Network Security Services (NSS), a set of libraries designed to support cross-platform development of security-enabled client and server applications. This library provides a complete open-source implementation of the crypto libraries used by AOL, Red Hat, Sun, and other companies in a variety of products, including the following:

- The Mozilla client products, including Mozilla Suite, Firefox, and Thunderbird.
- The Netscape browsers
- AOL Communicator and AOL Instant Messenger (AIM)
- Open source client applications such as Evolution, Gaim, and OpenOffice.org 2.0.

At the SSAC Public Meeting in Beijing (0800-0900 Thursday 11Apr12), it was revealed by a member of the CAB Forum that recently Mozilla started the process to adopt the gTLD requirements (ballot 96). Once Mozilla adopts it, the requirement will be binding on all CAs (in NSS), regardless of whether they are CAB Forum members.