Secure and Stable Introduction of New gTLDs

Introduction

ICANN's mission and core values call to preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet's system of unique identifiers (names, IP numbers and protocol parameters). Consistent with these goals and in concert with the ICANN community, ICANN has undertaken a number of measures to assess and, where necessary, mitigate potential security and stability risks associated with the launch of new gTLDs.

This information sheet summarizes some of these measures that will allow ICANN to introduce new gTLDs into the Domain Name System (DNS) in a secure and stable manner. It also discusses measures to address situations in which a "live" (or delegated) new gTLD might compromise the security and stability of the DNS.

It is important to note that while the launch of new gTLDs is an important event in the history of the Internet's Domain Name System (DNS), the community has successfully introduced significant changes without compromising the security and stability of the DNS. For example, 45 Internationalized Domain Names (IDNs) have been added to the DNS since 2008 and Domain Name System Security Extensions (DNSSEC), a massive upgrade to the DNS infrastructure, was successfully deployed in 2010.

Addressing the Potential for Name Collisions

In a study published in January 2013, ICANN's Security and Stability Advisory Committee (SSAC) indicated that some certificate authorities issue X.509 certificates for names are not resolvable in the public DNS. Organizations use these certificates to verify the identity of a resource or to encrypt communications within their private networks. SAC 057 noted that certain organizations have adopted names for use within their private network name spaces assuming that these would not duplicate and thus conflict with top-level domains. Queries of these name spaces may "leak" into the public DNS, either through configuration error or as a result of the use of older software. When such a leak occurs, a DNS query for a resource on a private network would be resolved by querying the public DNS, resulting in a "collision" with the same top-level label as a new TLD. SSAC had identified this behavior in an earlier report, but the list of applied-for new gTLDs was not known until June 2012.

Following the direction of the ICANN Board of Directors and the advice of SSAC, ICANN commissioned an in-depth study on the potential impacts of the applied-for new gTLD strings. The study, released on 5 August 2013, considers the likelihood and impact of name collisions between applied-for new gTLD strings and non-delegated TLDs. The study also reviewed the possibility of collisions arising from the use of X.509 digital certificates.

The study identifies three categories of strings according to the potential name collision risk they represent. It also identifies options that could be undertaken to mitigate the associated risks.

The study concludes that for nearly 80% of the distinct applied-for new gTLDs, the impact of name collision is sufficiently low to permit ICANN to continue with contracting and delegation of those gTLDs. Nevertheless, to minimize the likelihood of any impact, ICANN proposes that new gTLD registries implement two additional mitigation measures as described in a recommendation paper accompanying the release of the report. These measures will help mitigate the potential impact related to name collisions in general as well as those arising from internal name certificates. ICANN does not expect a material impact to the timeline for the delegation for these strings.

The study identifies approximately 20% (or 279) of the distinct applied-for new gTLDs for which the impact of name collision warrant additional investigation. The proposed classification of the strings can be found here. ICANN, in consultation with the community, will undertake further study to better assess the risk factors associated with these strings and any necessary mitigating action. ICANN proposes not to proceed to contracting and delegation of these strings until that study is concluded. Concurrently, an applicant may provide evidence of the results from the steps taken to demonstrate or mitigate the name collision impact to fall within an acceptable level. We anticipate that this study will take 3-6 months to complete once started.

Finally, the name collision report identifies two strings as carrying a potentially high risk of name collision – home and corp. ICANN proposes not to proceed to contracting and delegation for these strings unless and until an applicant can demonstrate that its proposed string should be classified as low risk. ICANN will work with the applicants and the community to determine a course of action for this category of strings.

Additional Security and Stability Measures

As an added step, ICANN has undertaken updating its already robust risk management procedures for improved response to any unforeseen issues arising from the delegation of new gTLDs.

ICANN's existing coordinated vulnerability disclosure process has been updated to include elements related to the emergency escalation process, from monitoring TLD registry operators for service level agreement performance to use of the emergency backend registry operator (EBERO) process and emergency measures to temporarily transition or remove a TLD that presents a significant risk to the secure and stable operation of the DNS.

Root Server System Monitoring

ICANN's Root Server Stability Advisory Committee (RSSAC) is drafting recommendations on measurement of the Root Server System, including a set of parameters for measuring

and monitoring the root servers. The RSSAC is expected finalize the recommendations in the near future.

In addition, ICANN as the L-root operator publishes a companion report on its website that focuses on the DNS protocol effects when the root zone changes. The data for this report is collected from the L-root instances.

ICANN also publishes on its website historical root zone data from 1999. This information includes:

The size of the overall root zone
The number of delegations (TLDs)
The root zone size per delegation
The number of resource records in the root zone

Further Information for the Community

The community is invited to provide comment on ICANN's recommendation. In addition, a Webinar is being planned with the community to provide further information.