ICANN
POLICY FORUM
74
THE HAGUE

Joint Session: SSAC/ALAC

ICANN74 | Tuesday, 14 June 2022

Agenda

SSAC Topics:

- SAC121 Routing Security (SSAC lead: Russ Mundy)
- SAC120 Input on IDN Variants (SSAC lead: Patrik Fältström)
- Addendum to SAC114 (SSAC lead: Rod Rasmussen)
- SSAD (SSAC lead: Steve Crocker)
- NCAP (SSAC lead: Jim Galvin and Matt Thomas)

ALAC Topics:

- Response to DNS Abuse Questions (ALAC)

Recent SSAC Publications

SAC121: SSAC Briefing on Routing Security

SAC121: SSAC Briefing on Routing Security

- As the Internet has grown and the number of networks has increased, the number of routing incidents has also increased.
- SAC121 examines the security and stability implications of insecurities in the Internet's routing system, and areas network operators should be aware of.
- It provides a tutorial on this space in an effort to help the larger ICANN and Internet policy communities understand these technologies and the issues surrounding them.
- The target audience for it is the non-technical ICANN Community, with a focus on DNS operators.

SAC121: SSAC Briefing on Routing Security

- SAC121 provides information on:
    - The Internet’s routing system,
    - routing security challenges for DNS infrastructure operators and their implications,
    - the role of network operators in securing the Internet's routing system,
    - security extensions of the border gateway protocol.
- Contains extensive references to other material on routing security.
- Contains no recommendations to the ICANN Board

Recent SSAC Publications

SAC120: SSAC Input to GNSO IDN EPDP on Internationalized Domain Name Variants
(Patrik Faltstrom)

SAC120: Input to GNSO IDN EPDP on IDN Variants

- An IDN variant is an alternate code point (or sequence of code points) that could be substituted for a code point (or sequence of code points) in a candidate label to create a variant label that is considered the “same” in some measure by a given community of Internet users. There is no general agreement of what that sameness requires.
- In the DNS two variants are distinct domain names. It is users of specific communities that will recognize variants as equivalent.
- To ensure security and stability of IDNs with variants, an IDN and its variants must be treated as a single package from a domain provisioning and life cycle management perspective.

SAC120: Input to GNSO IDN EPDP on IDN Variants

- This report includes an excerpt of relevant IDNs EPDP charter questions, questions asked by the EPDP team, and the SSAC's response
- A variant management mechanism serves two purposes:
  - Enhance security of IDNs that have variants
  - Promote an acceptable experience that meets the user expectations for those IDNs
- Balancing Security and Usability:
  - IDN and its variants must be treated as a single package from a domain provisioning and life cycle management perspective
  - Variants of an IDN that are in actual use can be delegated.

SAC120: Input to GNSO IDN EPDP on IDN Variants

- Important Limitations:
  - There is no protocol solution in the DNS or other protocols (e.g., HTTP, SMTP, TLS) to enforce equivalence of variant domains.
  - Management of variant domains can introduce a combinatorial explosion for registries, registrars and registrants and need to managed carefully
- These limitations call for a conservative approach in the delegation and management of variant domain names.
- The Root Zone must use the ICANN Root Zone Label Generation Rule to determine variants for all current and future TLDs.

Recent SSAC Publications

Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References (Rod Rasmussen)

Addendum to SAC114: Background

- SSAC published SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report on 11 Feb 2021
- SAC114 contains commentary on both the final report of the GNSO Subsequent Procedures Working Group and observations and recommendations on wider issues tied to increasing future delegations of new gTLDs
- SSAC reconvened a work party to consider the community’s feedback and provide additional context for the language and recommendations in SAC114
- Overall, SSAC remains concerned that the gTLD Subsequent Procedures have been crafted without adequate learning from the prior expansion round

Addendum to SAC114: Context for Rec. 1

Looking forward, the SSAC has short- and long-term concerns regarding the future of the root zone:

Short-term Concerns	Long-term Concerns
● SSAC finds substantial evidence that some new gTLDs have amplified the already considerable challenges with **domain name abuse** ● SSAC agrees that a holistic solution is needed to handle such abuse ● However, **waiting** until efforts to mitigate DNS abuse can be equally applied to all existing and new gTLDs **effectively cedes the ground to malicious actors**	● ICANN community is continuing with another round of root zone expansion without agreeing to an **overall, long-term strategy** for the root zone ● Without a documented long-term strategy it appears that ICANN intends to continue to approve root zone expansion in an ad hoc manner ● The root zone is complex and i**t is difficult to predict failure of the root zone** before it occurs ● It is therefore advisable from a security, stability, and resiliency perspective to take a **conservative approach** in expanding the root zone

Addendum to SAC114: Context for Rec. 1

SAC114 Recommendation 1: *The SSAC recommends that the ICANN Board initiate a fundamental review to determine whether continuing to increase the number of gTLDs is consistent with ICANN's strategic objective to "evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base." This review should be considered an input towards updating ICANN's strategic goals in conjunction with implementing the CCT Review Team's recommendations. Such a fundamental review should include at least the following areas of study based on prior rounds of the New gTLD program: Impacts on root server operations; Impacts on SSR issues; Impacts on overall DNS operations; Analysis of how all metrics for success were met; Risk analysis*

- The SSAC would like to see the ICANN Board and Community document a long-term strategy for root zone expansion
- Recommendation 1 is intended to provide the impetus to have the ICANN Board consider the short- and long-term concerns related to continuous root zone expansion
- The review mentioned in Recommendation 1 would be a useful starting place for developing the strategy

Addendum to SAC114: Context for Recs. 3 & 7

SAC114 Recommendation 3: *The SSAC recommends that the ICANN Board, prior to launching the next round of new gTLDs, commission a study of the causes of, responses to, and best practices for mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations. The best practices should be incorporated into enforced requirements, as appropriate, for at least all future rounds.*

SAC114 Recommendation 7: *The SSAC recommends that the ICANN Board, prior to authorizing the addition of new gTLDs to the root zone, receive and consider the results of the Name Collision Analysis Project, pursuant to Board Resolution 2017.11.02.30.*

- Community feedback revealed some confusion as to the intended timing of Recommendations 3 and 7 - these recommendations could be addressed concurrently with other necessary work to plan for, support, and enable a program to introduce additional gTLDs to the root zone
- The constraint that motivated the timing included in Recommendation 3 is that proceeding without documenting best practices, baseline contract provisions, and policies prior to the launch of the application window leads to transactions where applicants are committing to contracts without essential information
- While it would be best to have NCAP completed before the launch of the application window, it seems essential to have it completed before delegation of such gTLDs

SSAD

Steve Crocker

EPDP- Temp Spec

- SSAC published SAC118v2 on 17 November
- Steve Crocker participated in the GNSO's:
    - SSAD Operational Design Assessment (ODA)
    - Accuracy Scoping Team
    - EPDP Phase 2 Implementation Review Team (IRT)
- SSAC has responded to ICANN org's understanding request on SAC118v2
- SSAC currently awaiting for ICANN Board and GNSO Council's decision

Name Collision Analysis Project

Jim Galvin and Matt Thomas (Co-Chairs)

NCAP Background

- ICANN Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board on name collisions
    - Specific advice regarding .home/.corp/.mail
    - General advice regarding name collisions going forward
- Studies to be conducted in a thorough and inclusive manner that includes other technical experts
    - 25 discussion group members, including 14 SSAC work party members
    - 23 community observers
    - Chaired by James Galvin and Matt Thomas

NCAP - Recent Publications

- Case Study of Collision Strings
  - Studies of .corp, .home, .mail, .internal, .lan, and .local using DNS query data from A and J root servers.
  - Highlight changes over time of the properties of DNS queries and traffic alterations as a result of DNS evolution.
- A Perspective Study of DNS Queries for Nonexistent Top-Level Domains
  - Aims to understand the distribution of DNS name collision traffic throughout the DNS hierarchy
  - Provide insights into where and how DNS data can be collected and assessed.

NCAP - Key Findings so far

- Name collisions are and will continue to be an increasingly difficult problem; case study indicates impact has increased
  - DNS service discovery protocols and suffix search lists are a continuing problem
- Critical diagnostic measurements (CDMs) are defined as a way to measure name collisions by informing the assessment of the risk of delegation
- Any root server identifier is representative of the CDMs seen in the root server system (RSS)
- Mitigation and remediation is problematic, increasingly difficult as the volume and diversity of CDMs increases
- Existing measurement platforms could be extended to help inform applicants

NCAP - Critical Diagnostic Measurements

- Query Volume
- Query Origin Diversity
  - IP address distribution
  - ASN distribution
- Query TYPE Diversity
- Label Diversity
- Other characteristics
  - Open-Source Intelligence (OSINT)

- **Impact (or Harm) is determined by evaluating both Volume and Diversity across all CDMs**

NCAP - Work in Progress

- The NCAP discussion group is developing a framework to assess name collisions
  - How the Board is going to assess name collisions
  - Guidance on how to consider the risks of delegation given the existence of name collisions

- The initial framework, along with findings from other studies, will be published for public comment in 2Q2022
  - Initial draft publication date is likely to slip

NCAP - How to Participate

- Review the report as soon as it is released for public comment
- Attend or review recording
    - NCAP Update (14 June 13:00 UTC)
    - NCAP Discussion Group (14 June 14:30 UTC)
- Join the discussion group

ALAC Questions

Response to DNS Abuse Questions (ALAC)

Thank you