ICANN 48

Security and Stability Advisory Committee

Activities Update
ICANN Buenos Aires Meeting
November 2013

Agenda

1. SSAC Overview and Activities – Patrik Fältström
2. SSAC Advisory on Concerning the Mitigation of Name Collision Risk (SAC 062) – Patrik Fältström
3. SSAC Advisory on DNSSEC Key Rollover in the Root Zone (SAC 063) – Russ Mundy
4. SSAC Comment on ICANN's Initial Report from the Expert Working Group on gTLD Directory Services (SAC 061) – James Galvin
5. SSAC Comment on Examining the User Experience Implications of Active Variant TLDs Report (SAC 060) – Patrik Fältström and Ram Mohan

Security and Stability Advisory Committee (SSAC) Overview

- 2001: SSAC initiated; 2002: Began operation.
- Provides guidance to ICANN Board, Supporting Organizations and Advisory Committees, staff and general community.
- Charter: To advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.
- Members as of November 2013: 41; appointed by ICANN Board for 3-year terms.

2013 Work Plan: Current Activities

- SSAC Membership Committee
- DNSSEC Workshop
- Identifier Abuse Metrics
- SSAC Outreach to Law Enforcement
- IGF Workshop
- Large Scale Abuse Using the DNS Infrastructure

2012-2013 Publications by Category

DNS Security

[SAC063]: SSAC Advisory on DNSSEC Key Rollover in the Root Zone – 07 November 2013

[SAC062]: SSAC Advisory Concerning the Mitigation of Name Collision Risk – 07 November 2013

[SAC059]: SSAC Letter to the ICANN Board Regarding Interdisciplinary Studies – 18 April 2013

[SAC057] SSAC Advisory on Internal Name Certificates—March 2013

[SAC056]: SSAC Advisory on Impacts of Content Blocking via the Domain Name System —09 October 2012

[SAC053] SSAC Report on Dotless Domains—February 2012

2012-2013 Publications by Category

Internationalized Domain Names (IDNs)

[SAC060]: SSAC Comment on Examining the User Experience Implications of Active Variant TLDs Report—23 July 2013

[SAC052] SSAC Advisory on Delegation of Single-Character Internationalized Domain Name Top-Level Domains—January 2012

2012-2013 Publications by Category

Registration Data (WHOIS):

[SAC061] SSAC Comment on ICANN's Initial Report from the Expert Working Group on gTLD Directory Services—06 September 2013

[SAC058] SSAC Report on Domain Name Registration Data Validation Taxonomy—March 2013

[SAC055] SSAC Comment on the WHOIS Review Team Final Report—September 2012

[SAC054] SSAC Report on the Domain Name Registration Data Model—June 2012

SAC062: SSAC Advisory Concerning the Mitigation of Name Collision Risk

Patrik Fältström

Overview

- In the context of top level domains, “name collision” refers to the situation in which a name that is properly defined in the global DNS namespace may appear in a privately defined namespace where users, software, or other functions in that domain may misinterpret it.
- The SSAC provides advice in the areas of
  - High risk strings
  - Trial delegation
  - Root zone monitoring capability
  - Emergency rollback capability

High Risk Strings

- Strings with documented evidence of broad and significant private usage should be considered for permanent reservation for internal use to reduce security and stability issues
  - Similar to private IP address allocation (RFC 1918)
  - RFC 6761 and 6762 documented some strings for private use

Trial Delegation

- Types of trial delegation:
  - DNS Infrastructure Testing (Type I)
    - I-a: Log and return RCODE 3 for every request
    - I-b: Activate certain names under the TLD to measure name collision
  - Application and Service Testing and Notification (Type II)
    - Log queries and respond with wildcard and synthesized responses to application servers, application server provide a notification
- Benefits and risks associated with each option

Root Zone Monitoring Capability

- The SSAC supports the decision for ICANN to work with the community to develop a long-term plan to retain and measure root-server data.
- Such a capability must be defined and deployed promptly and be sufficiently flexible.

Emergency Rollback Capability

1. Emergency action may be needed, including the rapid reversal of the delegation of a TLD, in the case significant security or stability problems occur as a result of name collision following the formal delegation of a TLD
   1) the existing root zone management process needs to be updated to accommodate the potential need to rapidly reverse the delegation of a TLD
   2) document the set of conditions that make it evident that the only mitigation option available is the complete removal of the delegation of a TLD

Recommendations

See the document, pages 7, 11, and 12 at: http://www.icann.org/en/groups/ssac/documents/sac-063-en.pdf for the complete text of the recommendations.

1. **ICANN should work with the wider Internet community, including at least the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF), to identify**
   1) what strings are appropriate to reserve for private namespace use and
   2) what type of private namespace use is appropriate (i.e., at the TLD level only or at any additional lower level).

Recommendations, Cont.

2. **ICANN should explicitly consider the following questions regarding trial delegation and clearly articulate what choices have been made and why as part of its decision as to whether or not to delegate any TLD on a trial basis:**
   - Purpose of the trial
   - Operation of the trial
   - Emergency Rollback
   - Termination of the trial

Recommendations, Cont.

3. ICANN should explicitly consider under what circumstances un-delegation of a TLD is the appropriate mitigation for a security or stability issue.
4. Finally, ICANN should work in consultation with the community, in particular the root zone management partners, to create additional processes or update existing processes to accommodate the potential need for rapid reversal of the delegation of a TLD.

SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone

Russ Mundy

Overview

- The SSAC has published an advisory on issues relating to the rollover of the Domain Name System Security Extensions (DNSSEC) Key-Signing Key (KSK).
- The Advisory explores the following topics:
  - Terminology and definitions relating to DNSSEC key rollover in the root zone
  - Key management in the root zone
  - Motivations for root zone KSK rollover
  - Risks associated with root zone KSK rollover
  - Available mechanisms for root zone KSK rollover
  - Quantifying the risk of failed trust anchor update
  - DNS response size considerations.

Recommendations

See the document, beginning on page 23, at: http://www.icann.org/en/groups/ssac/documents/sac-063-en.pdf for the complete text of the recommendations.

1. ICANN staff, in coordination with the other Root Zone Management Partners, should immediately undertake a significant, worldwide communications effort to publicize the root zone KSK rollover motivation and process as widely as possible.

Recommendations, Cont.

2. ICANN staff should lead, coordinate, or otherwise encourage the creation of a collaborative, representative testbed for the purpose of analyzing behaviors of various validating resolvers and their network environments that may affect or be affected by a root KSK rollover.
3. ICANN staff should lead, coordinate, or otherwise encourage the creation of clear and objective metrics for acceptable levels of “breakage” resulting from a key rollover.

Recommendations, Cont.

4. ICANN staff should lead, coordinate, or otherwise encourage the development of rollback procedures to be executed when a rollover has affected operational stability beyond a reasonable boundary.
5. ICANN staff should lead, coordinate, or otherwise encourage the collection of as much information as possible about the impact of a KSK rollover to provide input to planning for future rollovers.

SAC061: SSAC Comment on ICANN's Initial Report from the Expert Working Group on gTLD Directory Services

James Galvin

Overview

- **What is it:** The SSAC provides comments to ICANN EWG WG's initial report
- **Why the issue matters:**
  - Registration Data Directory service is an important service for the community
  - The current WHOIS service is not able to meet the community's need
  - The EWG proposed a model (ARDS) forward

Highlight of SSAC Comments

- Four areas:
  - Purpose of Registration Data
  - Availability Risks
  - Authentication and Access Control
  - Data Accuracy

Recommendations

See the document, beginning on page 14, at: http://www.icann.org/en/groups/ssac/documents/sac-061-en.pdf for the complete text of the recommendations.

1. **SSAC reiterates its recommendation from SAC055: The ICANN Board should explicitly defer any other activity (within ICANN's remit) directed at finding a 'solution' to 'the WHOIS problem' until the registration data policy has been developed and accepted in the community.**

Recommendations, Cont.

2. The ICANN Board should ensure that a formal security risk assessment of the registration data policy be conducted as an input into the Policy Development Process.
3. SSAC recommends that the EWG state more clearly its positions on data availability.
4. The SSAC suggests that the EWG address the recommendation from SAC058: “SSAC Report on Domain Name Registration Data Validation”.

SAC060: SSAC Comment on Examining the User Experience Implications of Active Variant TLDs Report

Ram Mohan

Overview

- The SSAC provides comments on ICANN's IDN variant TLD report
  - Examining the User Experience Implications of Active Variant TLDs
  - A Procedure to Develop and Maintain the Label Generation Rules for the root zone

- **Why the issue matters:** The root zone is shared by everyone on the Internet, and needs a set of label generation rules that ensures
  - minimal conflict
  - minimal risk to all users (independent of which language or script they are using, independent of gTLD or ccTLD)
  - minimal potential for incompatible change

Highlight of SSAC Recommendations

The SSAC Recommends ICANN to:

- **exercise the principle of conservatism with respect to allowable code points, and number of active variants**
- **ensure there is a secure, stable and objective process to handle situations in which the community disagrees with ICANN's variant calculation**
- **for the stability of root zone, make sure later versions of the LGR are backward compatible to avoid incompatible results with existing (historical) allocations**

Highlight of SSAC Recommendations, Cont.

- Focus the LGR on the root zone, but encourage its adoption at registry and other levels
- Ensure EBERO providers and TMCH support variant TLDs, and ensure that parity exists for variant support in all relevant systems and functions associated with new TLD components

Recommendations (1)

See the document, beginning on page 14, at: http://www.icann.org/en/groups/ssac/documents/sac-060-en.pdf for the complete text of the recommendations.

1. The root zone must use one and only one set of Label Generation Rules (LGR).
2. ICANN must maintain a secure, stable and objective process to resolve cases where some members of the community do not agree with the result of the LGR calculations.
3. ICANN should concentrate foremost on the rules for the root zone.

Recommendations (2)

4. ICANN should coordinate and encourage adoption of these rules at the second and higher levels as a starting point.
5. Be very conservative on code points allowed in the root zone.
6. Because the implications of removing delegations from the root zone can have significant non-local impact, new rules added to LGR must, as far as possible, be backward compatible.

Recommendations (3)

7. Should ICANN decide to implement safeguards, it should seek to distinguish two types of failure modes when a user expects a variant to work but it is not implemented: denial of service vs. misconnection.
8. Process needs to be developed to activate variants from allocable variants in LGR.
9. ICANN must ensure EBERO providers support variant TLDs, and that parity exists for variant support in all relevant systems and functions associated with new TLD components.

Recommendations (4)

10. In the current design of rights protection related to the TMCH process there is a risk of homographic attacks. The roles of the involved parties, specifically registrars, registries and TMCH, related to matching must be made clear.
11. When registries calculate variant sets for use in validation during registrations, such calculations must be done against all the implemented LGRs covering that script in which the label is applied for.

Recommendations (5)

12. The matching algorithm for TMCH must be improved.
13. The TMCH must add support IDN variant TLDs. Particularly during the TM Claims service a name registered under a TLD that has variant TLDs should trigger trademark holder notifications for the registration of the name in the TLD and all its allocated variant TLDs.
14. ICANN should ensure that the number of strings that are activated is conservative.

Thank you

ICANN 48 • 17-21 Nov 2013
Buenos Aires
ICANN