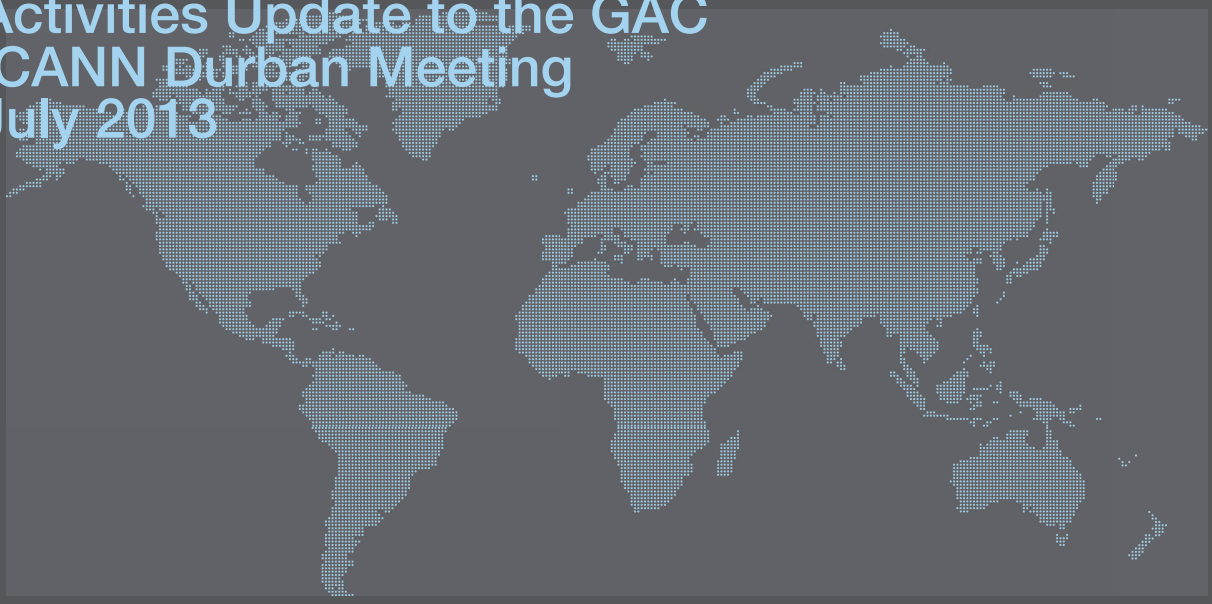
Security and Stability Advisory Committee

Activities Update to the GAC
ICANN Durban Meeting
July 2013



Agenda

1. SSAC Overview and Activities – Patrik Fältström
2. SAC057: SSAC Advisory on Internal Name Certificates
3. SAC058: SSAC Report on Domain Name Registration Data Validation Taxonomy
4. SAC059: SSAC Letter to the ICANN Board Regarding Interdisciplinary Studies
5. Variants Work Party Update – Patrik Fältström
6. Root Key Rollover Work Party Update – Russ Mundy
7. Abuse of the DNS Work Party Update – Merike Kaeo

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: 39; appointed by ICANN Board for 3-year terms.

2013 Work Plan: Current Activities

- SSAC Membership
- DNSSEC Workshop
- Identifier Abuse Metrics
- Root Key Rollover
- SSAC Meetings with Law Enforcement
- IGF Workshop
- New gTLD Success Metrics
- Abuse of the DNS for DDoS Attacks
- Comment on Variant TLDs Report
- Namespace Collisions
- Response to Expert Working Group on gTLD Directory Services

2012-2013 Publications by Category

Domain Name System (DNS) Security and Abuse

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

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

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

Registration Data (WHOIS):

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

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

SAC057: SSAC Advisory on Internal Name Certificates

Patrik Fältström

Overview

- Advisory identifies a Certificate Authority (CA) practice that, if widely exploited, could pose a significant risk to the privacy and integrity of secure Internet communications.
- This CA practice could impact the new gTLD program.
- The SSAC recommended that ICANN should take immediate steps to mitigate the risks.

Status

- Following the SSAC advice, ICANN took immediate mitigation actions to reduce the risk.
- However, residual risks remain and much more work needs to be done to address them.

SAC058: SSAC Report on Domain Name Registration Data Validation Taxonomy

Jim Galvin

Overview

Various studies that assessed the quality of domain name registration data have collectively shown that the accuracy of the data needs to be improved. In this report, the SSAC examines the feasibility and suitability of improving registration data accuracy through validation. Specifically, the SSAC:

- Proposes validation taxonomy for community consideration;
- Explores the suitability and efficacy of various techniques of validating registration data elements in light of the taxonomy.

Recommendations

1. **The ICANN community should consider adopting the terminology outlined in this report in documents and discussions.**
2. **As the ICANN community discusses validating contact information, the SSAC recommends that the following meta-questions regarding the costs and benefits of registration data validation should be answered.**
3. **The SSAC recommends that the ICANN community seek to identify validation techniques that can be automated and to develop policies that incent the development and deployment of those techniques. The use of automated techniques may necessitate an initial investment but the long-term improvement in the quality and accuracy of registration data will be substantial.**

SAC059: SSAC Letter to the ICANN Board Regarding Interdisciplinary Studies

Patrik Fältström

Overview

- On 13 September 2012 the Board of Directors asked the SSAC to provide advice on how “interdisciplinary studies of security and stability implications from expanding the root zone more than an order of magnitude should be carried out and whom else should be consulted.”
- SAC059 provides the SSAC’s advice on the composition of the interdisciplinary study team, broad topics and specific examples the team may wish to consider, and suggestions on how the studies should be performed.

Recommendations

The goal of the studies should be two fold:

- **Engage with communities that may not have been fully consulted by previous investigations on the impacts of the new gTLD program; and**
- **Explore areas of concern relating to expansion of the root zone that either derive from those communities or which have been identified by previous studies but that may not have been fully resolved.**

IDN Variant TLD Work Party Update

Patrik Fältström

Overview

- This SSAC Work Party is commenting the reports produced by the ICANN IDN Variant TLD programs
- The SSAC Report comments on the following:
  - Label Generation Rules (LGR) Procedure for the root zone
  - LGR's Repertoire & Variant Generation Rules
  - LGR's change process
  - Other User experience report recommendations

Issues

The SSAC provides comments on the following issues:

- **Conservatism principle with respect to allowable code points, and number of active variants**
- **Process to handle situations in which the community disagrees with ICANN's variant calculation**
- **Backward compatibility of LGR 2.0 with LGR 1.0**
- **Root LGR's applicability to second level and higher levels**
- **Operation Readiness of ICANN's new TLD functions with respect to variants**

Next Steps

- The Work Party has produced a document for the full SSAC review till 17 July.
- After that the Work Party will finalize the document for publication.

Root Key Rollover Work Party Update

Russ Mundy

Overview

- This SSAC Work Party is considering issues relating to the rollover of the Domain Name System Security Extensions (DNSSEC) Key-Signing Key (KSK).
- This work is not meant to result in a definitive advisory, but will provide an inventory and study of the issues related to a key rollover.
- The Work Party is exploring:
  - Possible root zone KSK rollover scenarios; and
  - Complications and complexities unique to the handling of root zone keys.
- IANA also held a recent public consultation on the contract requirement to perform a scheduled root zone KSK rollover. The Public Comment period ended on 31 May. Further consultation with the community is expected in the next few months.

Issues

- The Work Party is considering the following issues:
  - Key Management in the Root Zone
    - Zone-Signing Key (ZSK) Operational Role; and
    - Key-Signing Key (KSK) Operational Role.
  - Motivations for KSK Rollover.
  - Risks Associated with Key Rollover
  - Available Mechanisms for Key Rollover:
    - RFC 5011 Rollover;
    - Non-RFC 5011 Rollover; and
    - Common Resolver Rollover Requirements.
  - DNS Response Size Considerations.

Next Steps

- The Work Party will produce a document for the review of the full SSAC.
- The SSAC will decide whether and/or when to publish the final document.

Abuse of the DNS Work Party Update

Merike Kaeo

Objective

- Targeted audience is primarily DNS operators:
  - Authoritative DNS operators;
  - Recursive DNS operators; and
  - Both ISPs and Enterprises.
- Goal is to highlight current ongoing problems and provide scope of malicious/criminal activities that utilize the DNS infrastructure.
- Reference existing SSAC work that has not been widely implemented.
- Enumerate irresponsible behaviors which are causing Internet instability through not following past SSAC recommendations.
- Provide updated recommendations to foster greater DNS infrastructure stability.

Issues

- Increased scale and impact of attacks.
- Factors that make these amplification attacks possible.
- Prior work on mitigation techniques.
- Recommended steps to address unresolved critical issues.

Questions for Discussion

1. What steps should DNS and network operators take:
   - to resolve the issues that make such large scale DDoS attacks possible?
   - to prevent network spoofing to the greatest extent possible?
   - to identify unmanaged and inadvertently open recursive resolvers and close them?
   - to detect networks that deploy spoofable networks and run unmanaged open recursive resolvers?

Next Steps

- Send to the SSAC for review.
- Once approved and published, renew effort to evangelize and socialize the importance of security BCPs for overall Internet health and stability.

Thank You & Questions?