



SSAC Activity Report June 2011

What is the SSAC?

The Security and Stability Advisory Committee (SSAC) advises the ICANN community and Board of Directors on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.

Introduction

This **Activity Report** is divided into the following sections: **Work Plan for 2011** and **Work Completed in 2011**.

The first section, **Work Plan for 2011**, presents the ideas and preliminary work to develop specific project plans. This is perhaps the most important section of this report because it provides notice of issues on the horizon. The Work Plan may include activities that have been carried over from the previous year.

The SSAC generates three types of work products: Reports, Advisories and Comments. Reports examine a topic in substantial detail. Advisories are issued in response to a problem or incident in a timely manner. Comments are usually responses to queries from staff or to ICANN documents posted for formal response. SSAC reports, advisories and comments are generally available for distribution to the community. Those work products that were produced in 2011 are described in the **Work Completed in 2011** section. For a list of SSAC documents see: <http://www.icann.org/en/committees/security/ssac-documents.htm>. For previous Work Plans and Activities see: <http://www.icann.org/en/committees/security/ssac-workplan.htm>.

The SSAC often considers security incidents or matters disclosed in confidence to committee members (e.g., a security vulnerability, an emerging threat to the Domain Name System (DNS), or information relating to a security incident). Discussions and ongoing work within the SSAC are thus typically conducted in private until complete, or until the need for confidentiality has lapsed. SSAC members participate in an individual capacity and do not represent the organizations that employ them. SSAC member biographies and statements of interest are posted here: <http://www.icann.org/en/committees/security/biographies-27jun11-en.htm>.

Feedback on this content, process, and format are welcome. Full information on the Committee and its completed reports is on the ICANN web site at <http://www.icann.org/en/committees/security/>. This report is suitable for general distribution and will also be available on the SSAC web site.

Patrik Fältström,
Chair, Security and Stability Advisory Committee

Work Plan for 2011

Source Address Validation – Source address validation refers to techniques that are used to verify the origin of Internet Protocol (IP) traffic as it enters the Internet. The purpose of such validation is to thwart impersonation or ‘spoofing’ at the IP level. Several source address validation techniques have been available for over a decade yet studies have shown that global deployment percentages of these techniques are very low. The SSAC has formed a Work Party to study current trends in using spoofed IP addresses for malicious traffic, determine techniques available for mitigating threats associated with this spoofed IP traffic, and provide recent incidents that would have been mitigated with more widespread source address validation deployment.

Orphaned DNS Records – Orphaned DNS records are name server records that exist in a delegation, but whose parent domain names no longer exist. The issue of concern is that orphaned DNS records can be maliciously abused. The SSAC has formed a Work Party to study this issue and develop possible recommendations in addition to those presented in [SAC048]: SSAC Comment on the Orphan Glue Records in the Draft Applicant Guidebook (12 May 2011) (see below).

WHOIS Taxonomy – The SSAC has developed a Work Party to consider findings and recommendations relating to the WHOIS. In particular, a taxonomy of elements of a domain registration system is essential to scope discussions and facilitate consensus on the various registration data related issues facing domain registration systems. The SSAC is considering a proposal to recommend that a taxonomy be developed and adopted for use in all documents, discussions, and events. The taxonomy includes: 1) a data model; 2) a directory service; and 3) a directory protocol(s). Recommendations may include that solutions be developed separately for each element in the taxonomy.

Internationalized Registration Data Working Group (IRD-WG) – SSAC members are participating in a joint Generic Names Supporting Organization (GNSO)-SSAC Working Group to study the feasibility and suitability of introducing response and display specifications to accommodate registration data that cannot be represented using US-ASCII. In 2010 the Working Group published an Interim Report. See: <http://gns0.icann.org/issues/ird/ird-wg-final-report-15nov10-en.pdf>. The WG is developing a Final Report to be published by the ICANN meeting in Dakar, Senegal in October 2011.

SSAC Public Meetings at ICANN Meetings in 2011 – The SSAC held public meetings at the ICANN meetings in Silicon Valley, California in March and Singapore in June (see below). It also will hold a public meeting at the ICANN meeting in Dakar, Senegal in October. At these meetings the SSAC will provide briefings on recently published and ongoing work.

Workshops on DNSSEC at ICANN Meetings in 2011 – The SSAC held DNSSEC Workshops in coordination with the DNSSEC Deployment Initiative at the ICANN meetings in San Francisco, California in March and Singapore in June. A workshop is planned for Dakar, Senegal in October. These workshops have been a part of ICANN meetings for several years. They provide a forum for both experienced and new people to meet, present and discuss current and future DNSSEC deployment issues. A new session has been added that provides an introduction to DNSSEC basics intended for people who are not yet familiar with DNSSEC.

Collaboration with the ICANN Community – SSAC members are carrying forward work from various SSAC deliverables (SAC026, SAC033, SAC038, SAC040, SAC044, SAC049, and SAC050) into the GNSO through outreach efforts and via participation in various Working Groups. SSAC work products also are being considered by staff at GNSO request, including an inventory of WHOIS service requirements. SAC037 is the catalyst and basis for work on internationalizing registration data. See above. Recommendations from several SSAC documents are under consideration by the RAA WG. SAC044 has been singled out by the GNSO as an important report for registrars to make available to customers.

Collaboration with Affirmation of Commitment Review Teams – The SSAC has held informal meetings with two of the Review Teams formed as part of the Affirmation of Commitment: 1) The WHOIS Review Team, see: <https://community.icann.org/display/whoisreview/WHOIS+Policy+Review+Team> and 2) the Security, Stability, and Resiliency of the DNS Review Team, see: <https://community.icann.org/pages/viewpage.action?pageId=2950038>.

Work Completed in 2011

[SAC047]: SSAC Comment on the ICANN gTLD Registry Transition Processes Model (15 April 2011):

<http://www.icann.org/en/committees/security/sac047.pdf> – In conjunction with the anticipated introduction of new generic Top Level Domains (gTLDs) ICANN has published an Explanatory Memorandum to describe a model for the transition of a gTLD from one registry operator to another. The registry transition processes are intended to provide safeguards for registrants in cases where a registry ceases operation or in cases where a registry experiences prolonged technical outages. This SSAC Comment considers each of the circumstances where the transition processes are to be implemented. In particular, the SSAC considers the objectives, scope and application of the transition processes and recommends that the Explanatory Memorandum clearly identify risks that are mitigated by the proposed transition processes. The Comment asks whether matters such as emergency operator eligibility and regular auditing of emergency operators merit additional consideration. Given the real-time operational implications of a registry transition, the Comment pays particular attention to the security and stability of the Emergency Back-End Registry Operator Temporary Transition Process. Finally, the Comment asks that ICANN consider testing, retention of operational data from ex-registries, zone data escrow, and other information that will facilitate restoration of name resolution service for registrants.

[SAC048]: SSAC Comment on the Orphan Glue Records in the Draft Applicant Guidebook (12 May 2011):

<http://www.icann.org/en/committees/security/sac048.pdf> – In April 2011, ICANN published a draft guidebook for the new Generic Top Level Domain (gTLD) Applicants (Applicant Guidebook). This SSAC Comment considers a specific issue in the guidebook: the management and removal of orphan glue records. The Comment prepares a definition of orphan glue and recommends it be included for reference in the Applicant Guidebook. It also asks that ICANN considering refining the language of proposed policy regarding orphan glue.

[SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011):

<http://www.icann.org/en/committees/security/sac049.pdf> – This Report discusses circumstances that result in the loss or disruption of domain name resolution that can temporarily eliminate a domain name from the Internet. Without understanding the mechanisms underlying Domain Name System (DNS) operations and understanding the information necessary to construct DNS information, domain name registrants are at risk for long-term service interruptions. The Report provides an overview and background of the domain name registration process and how registration relates to domain name resolution. It considers technical or business circumstances that might result in loss or disruption of domain name resolution. The SSAC represents such circumstances as risks and recommends measures domain name registrants should take to reduce the impact to their businesses or organizations should any such circumstance affect their domain name(s).

[SAC050]: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System (14 June 2011):

<http://www.icann.org/en/committees/security/sac050.pdf> – This Advisory notes that all technical approaches to DNS blocking, and even more so attempts to circumvent the blocking, will have some impact on the security and/or stability of users and applications, and on the coherency or universal resolvability of the namespace. The Advisory offers four principles that organizations should apply regardless of the blocking mechanism that is used. In addition, the Advisory notes that when these principles are not applied, blocking using the DNS can cause significantly more collateral damage or unintended consequences with no remedy available to affected parties.

SSAC Public Report: Work Plan for 2011 (February 2011) See:

<http://www.icann.org/en/committees/security/ssac-activity-report-26feb10-en.pdf>. This report describes the SSAC Work Plan for 2011. It also includes a list of those work products that were produced in 2010. For Activity Reports see: <http://www.icann.org/en/committees/security/ssac-workplan.htm>. These reports describe SSAC activities and plans.

SSAC Public Meetings at the at the ICANN meetings in Silicon Valley, California (March 2011) see:

<http://svsf40.icann.org/node/22139> and Singapore (June 2011) see: <http://singapore41.icann.org/node/24597>.

Workshops on DNSSEC at the ICANN meetings in Silicon Valley, California (March 2011) see:

<http://svsf40.icann.org/node/22163> and Singapore (June 2011) see: <http://singapore41.icann.org/node/24553>.