Security and Stability Advisory Committee

Activities Update
ICANN Beijing Meeting
April 2013

Agenda

1. SSAC Overview and Activities – Patrik Fältström
2. SAC057: SSAC Advisory on Internal Name Certificates – Patrik Fältström
3. SAC058: SSAC Report on Domain Name Registration Data Validation – Don Blumenthal

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

2013 Work Plan: Committees/ Working Groups

- SSAC Membership
- DNSSEC Workshop Program
- Domain Name System (DNS) Security and Stability Analysis Working Group (DSSA-WG)

2013 Work Plan: Work Parties

- Identifier Abuse Metrics
- Root Key Rollover
- SSAC Meetings with Law Enforcement
- IGF Workshop
- New gTLD Success Metrics
- Abuse of the DNS for DDoS Attacks
- MDNS, Complexity/Challenges in the DNS

2012-2013 Publications by Category

Domain Name System (DNS) Security and Abuse

- [SAC058] SSAC Report on Domain Name Registration Data Validation Taxonomy—Mar 2013
- [SAC057] SSAC Advisory on Internal Name Certificates—Mar 2013
- [SAC053] SSAC Report on Dotless Domains—Feb 2012

Internationalized Domain Names (IDNs)

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

2012-2013 Publications by Category, Cont.

Registration Data (WHOIS):

- [SAC055] SSAC Comment on the WHOIS Review Team Final Report—Sep 2012
- [SAC054] SSAC Report on the Domain Name Registration Data Model—Jun 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 advises that ICANN should take immediate steps to mitigate the risks.

Findings

1. The SSL observatory data shows that at least 157 CAs have issued internal name certificates.
2. The exact number of internal name certificates that end in an applied for new gTLD cannot be known unless CAs voluntarily disclose the list.
3. Enterprises use internal name certificates for a variety of reasons.

Findings, Cont.

4. The practice for issuing internal name certificates allows a person, not related to an applied for TLD, to obtain a certificate for the TLD with little or no validation, and launch a man-in-the-middle attack more effectively.
5. **The CA / Browser (CA/B) forum is aware of this issue and requests its members to stop this practice by October 2016. The vulnerability window to new gTLDs is at least 3 years.**

Recommendation

- **The ICANN Security Team should immediately develop and execute a risk mitigation plan.**

Outcome

- **Following the SSAC advice, ICANN took immediate mitigation actions to reduce the risk:**
  - ICANN alerted the CA/Browser (CA/B) Forum Chairperson (23 Jan 2013)
  - ICANN briefed the CA/B Forum at its annual meeting (5 Feb 2013)
  - Ballot 96 on new gTLDs was brought forward and passed by the CA/B Forum (20 Feb 2013), which implies:
    - CAs will stop issuing certificates that end in an applied-for-gTLD string within 30 days of ICANN signing the contract with the registry operator.
    - CAs will revoke any existing certificates within 120 days of ICANN signing the contract with the registry operator.

SAC058: SSAC Report on Domain Name Registration Data Validation Taxonomy

Don Blumenthal

Description

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.

Findings

1. Data quality is relative to registrants and their purposes.
   - Identify potential providers (customers) of data and purposes.
2. Certain verification measures can be automated, some with only a small amount of investment, and would improve the quality of registration data.
   - Use a formal data structure and strong data typing to reduce unintentional errors.
3. Different contact data elements have different validation cost structures.
   - May be large upfront cost in the beginning as nothing is validated.
   - Ongoing costs might be related to the frequency of data revalidation.
   - Economies of scale for validation as more contacts are validated.

Recommendations

1. The ICANN community should consider adopting the terminology outlined in this report in documents and discussions.
   - **Syntactic Validation** - the assessment of data with the intent to ensure that they satisfy specified syntactic constraints, conform to specified data standards, and are transformed and formatted properly for their intended use.
   - **Operational Validation** - the assessment of data for their intended use in their routine functions.
   - **Identity Validation** - the assessment that the data corresponds to the real world identity of the entity.

Recommendations

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:
   - What data elements need to be added or validated to comply with requirements or expectations of different stakeholders?
   - Is additional registration processing overhead and delay an acceptable cost for improving accuracy and quality of registration data?
   - Is higher cost an acceptable outcome for improving accuracy and quality?
   - Would accuracy improve if the registration process were to provide natural persons with privacy protection upon completion of multi-factored validation?

Recommendations

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.

Thank You & Questions?