SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN62 | June 2018

Agenda

1. SSAC Overview
2. Name Collision Analysis Project (NCAP)
3. Advisory Regarding Access to Domain Name Registration Data
4. An IoT Security Lab for the DNS (work in progress)
5. KSK Roll (Work in progress)
6. Other Publications

Security and Stability Advisory Committee (SSAC)

Who We Are

- **38** Members
- Appointed by the ICANN Board

What We Do

Charter: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)
- Internet Service/Access Provider
- ICANN Policy and Operations

How We Advise

101 Publications since 2002

REPORTS ADVISORIES COMMENTS

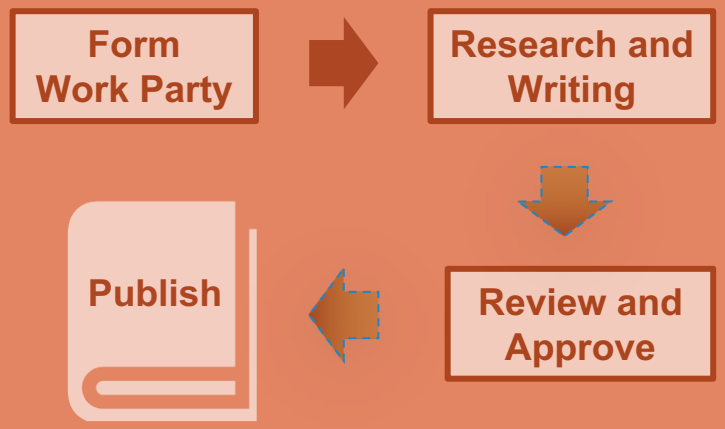
OUTREACH

Security and Stability Advisory Committee (SSAC)

ICANN's Mission & Commitments

- To ensure the stable and secure operation of the Internet's unique identifier systems.
- Preserving and enhancing the operational stability, reliability, security and global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process



Consideration of SSAC Advice

(to the ICANN Board)

Security and Stability Advisory Committee (SSAC)

Current Work Parties

Name Collision Analysis Project

SSAC Organizational Review

KSK Roll

Internet of Things

Emerging Security Topics (Ongoing)

DNSSEC Workshops (Ongoing)

Membership Committee (Ongoing)

Recent Publications

[SAC101]: SSAC Advisory Regarding Access to Domain Name Registration Data (18 June 2018)
[SSAC2018-16]: Draft Assessment Report of the Independent Examiner (13 June 2018)
[SSAC2018-15]: Review of IDN Implementation Guidelines (11 June 2018)
[SSAC2018-13]: Response Regarding the Actions of the ICANN Nominating Committee (09 May 2018)
[SSAC2018-12]: SSAC Comments on the Independent Review of the ICANN Nominating Committee Draft Final Report (07 May 2018)

ICANN | SSAC
Security and Stability Advisory Committee

Outreach

ssac.icann.org and SSAC Intro: www.icann.org/news/multimedia/621

www.facebook.com/pages/SSAC/432173130235645

SAC067 SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition and SAC068 SSAC Report on the IANA Functions Contract: www.icann.org/news/multimedia/729

Current Work in Progress

- Name Collision Analysis Project
- SSAC Organizational Review
- KSK Roll
- Internet of Things
- Emerging Security Topics (Ongoing)
- DNSSEC Workshops (Ongoing)
- Membership Committee (Ongoing)

Topics of Interest/Possible New Work

- Signing root NS Sets Analysis
- Challenges of Hosting Large Domain Portfolios
- Best Practices for Handling Takedown Requests
- Updating the SSAC Skills Survey

Current and Future Milestones

Q2 2018

- ✓ **[SAC101]: SSAC Advisory Regarding Access to Domain Name Registration Data (18 June 2018)**
- ✓ **[SSAC2018-16]: Draft Assessment Report of the Independent Examiner (13 June 2018)**
- ✓ **[SSAC2018-15]: Review of IDN Implementation Guidelines (11 June 2018)**
- ✓ **[SSAC2018-13]: Response Regarding the Actions of the ICANN Nominating Committee (09 May 2018)**
- ✓ **[SSAC2018-12]: SSAC Comments on the Independent Review of the ICANN Nominating Committee Draft Final Report (07 May 2018)**

Q3 2018

- ◉ SSAC Organizational Review
- ◉ Possible Advisory on the KSK Roll
- ◉ Possible Advisory on Internet of Things
- ◉ Continued work on Name Collision Analysis
- ◉ Emerging Security Topics (Ongoing)
- ◉ DNSSEC Workshops (Ongoing)
- ◉ Membership Committee (Ongoing)

Second Organizational Review of SSAC

- July 2017: The SSAC formed its own review party to review SSAC procedures and operations; the WP has made recommendations to change SSAC operational procedures

- February 2018: ICANN selected Analysis Group to conduct review of the SSAC

- March - May 2018: Independent Examiner starts review of SSAC through interviews and surveys

- June 2018 - Assessment report published for comment
  - https://www.icann.org/resources/reviews/org/ssac
  - https://www.icann.org/news/announcement-2018-06-21-en

- November 2018 - Final Report (with recommendations) published

Name Collision Analysis Project

James Galvin
Jay Daley

What are we dealing with?

- Board Resolution: https://www.icann.org/resources/board-material/resolutions-2017-11-02-en#2.a

- SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board regarding:
  - A proper definition for name collision
  - Suggested criteria for determining whether an undelegated string should be considered a string that manifests name collisions, i.e., is a “collision string”
  - Suggested criteria for determining whether a Collision String should not be delegated
  - Suggested criteria for determining how to remove an undelegated string from the list of “Collision Strings” (aka mitigations)

- Studies to be conducted in a thorough and inclusive manner that includes technical experts (such as members of IETF working groups, technical members of the GNSO, and other technologists)

Current Status

- SSAC published a draft project plan for public comment, ten comments received
- SSAC had meetings with Office of CTO and ICANN Board Technical Committee to clarify the proposal and advance the work in a collaboratively manner
- SSAC Work Party finalizing the proposal taking into consideration all the inputs for submission to the Board for final consideration
- At ICANN 62, five hours of working sessions planned, including 90 minutes of an open working group meeting for community engagement
  - Tuesday, 26 June, 10:30am-12pm, Metropolis 3

Call for participation

- The SSAC NCAP Work Party will function as an ordinary SSAC Work Party but in an inclusive and open manner
  - Membership will be extended to non-SSAC technical experts (SSAC Invited Guests) by invitation from the NCAP WP based on data contributions, relevant skills, experience, and participation on the open discussion group mailing list
  - There will be some open work party meetings
- SSAC NCAP Discussion Group for open discussion will be opened
  - Anyone completing an Statement of Interest (SOI) can join the discussion group
  - All work party members will be subscribed
- Cross Community Session at most ICANN meetings
- A form will be available for open contribution of any data or material that anyone believes the work party should consider

SAC101: Advisory Regarding Access to Domain Name Registration Data

Greg Aaron

Published 13 June 2018

https://www.icann.org/en/system/files/files/sac-101-en.pdf

SAC101: Advisory Regarding Access to Domain Name Registration Data

- Registration Data Directory Services (RDDS): WHOIS now, RDAP later.
- Reliable, consistent, and predictable access to domain name registration data is essential for a variety of legitimate purposes.
- Access to the data for legitimate users has been diminished, and availability is more constrained and more restricted than ever.
- This has happened for two main reasons: legal/policy developments (especially GDPR), and rate limiting.
- ICANN has an obligation to ensure the continued availability of gTLD registration data to the greatest extent possible.
- ICANN's new Temporary Specification for gTLD Registration Data does not deliver on that need.
- SAC101 provides background on the policy and technical issues.
- SAC101 includes 7 detailed recommendations designed to get past these problems.

SAC101: Advisory Regarding Access to Domain Name Registration Data

- *Rate-limiting* is imposed by registrars and registries. It limits the amount of data a requestor can obtain, and/or how quickly the requestor can obtain it.
- Rate limiting is imposed for some legitimate reasons: preventing denial-of-service and misuse of data.
- Problem is, it's applied to everyone, indiscriminately.
- ICANN should develop a program to identify legitimate users and give them tiered/gated access. Such a program will mitigate the problems that rate-limiting causes.
- Rate-limiting is separate from, but related to, the policy issue of which parties are allowed to see what registration data.

SAC101: Advisory Regarding Access to Domain Name Registration Data

- SSAC believes that law enforcement and security practitioners have a legitimate need to access the real identity of the responsible party(ies) for a domain name. Such access must comply with legal requirements.
- ICANN's new Temporary Specification allows RDDS (WHOIS) operators complete freedom to choose when to redact domain contact data from publication, whether or not a domain contact is protected by GDPR or by any other local privacy law. The result has been blanket redactions, hiding more data than is legally called for. A more balanced and justified approach is needed.
- No mechanisms for law enforcement and security practitioners to retrieve data on a predictable and reliable basis.

SAC101: Recommendation 1

1. The ICANN Board, ICANN Organization, and ICANN community must solve long-deferred problems regarding domain registration data and access to it. SSAC recommends that the ICANN Board [execute] a plan that accomplishes the following [..].
    a. ICANN policy-making should result in a domain registration data policy, including statements of purposes for the collection and publication of the data.
    b. The ICANN Board and the ICANN Organization should require contracted parties to migrate from using the WHOIS protocol to using the RDAP protocol.
    c. The ICANN Board and the ICANN Organization should require the remaining thin gTLD registries to move to thick status per the Thick WHOIS Consensus Policy and Board Resolution 2014.02.07.08.
    d. The ICANN Board should support the creation of an accredited RDDS access program, with the ICANN Organization ensuring the creation, support of, and oversight of the supporting technical access mechanism.
    e. The ICANN Board should arrange updates to the Registrar Accreditation Agreement and registry contracts as necessary to ensure compliance with A through D above.

SAC101: Recommendations 2, 3

2. The ICANN Board should direct the ICANN Organization to incorporate the following principle into its contracts with gTLD RDDS service providers: Legitimate users must be able to gain operational access to the registration data that policy says they are authorized to access, and must not be rate-limited unless the user poses a demonstrable threat to a properly resourced system. This recommendation is also made to policy-makers participating in the EPDP.

3. The ICANN Board and EPDP policy-makers should ensure that security practitioners and law enforcement authorities have access to domain name contact data, via RDDS, to the full extent allowed by applicable law.

SAC101: Recommendations 4, 5

4. The ICANN Board and the ICANN Organization should not allow a fee to be imposed for RDDS access unless such a decision is made via a formal Policy Development Process (PDP).

5. The SSAC reiterates Recommendation 2 from SAC061: "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. A separate security risk assessment should also be conducted regarding the implementation of the policy." These assessments should be incorporated in PDP plans at the GNSO.

SAC101: Recommendations 6, 7

6. The ICANN Board should direct the ICANN Organization to amend registry and registrar contracts to clarify that if a data field is required to be published, the registry or registrar must publish it in RDDS server output, not just in Web-based output.

7. The ICANN Board should direct the ICANN Organization to amend registry and registrar contracts to ensure that RDDS access is provided in a more measurable and enforceable fashion, which can be understood by all parties.

Please see SAC101 for the rationales and background for these recommendations.

https://www.icann.org/en/system/files/files/sac-101-en.pdf

An IoT Security Lab for the DNS (Work In Progress

Cristian Hesselman

DNS challenges in the IoT

- Further improve mitigation of IoT-powered DDoS attacks on the DNS
  - Many widely distributed vulnerable IoT devices, 24/7 available
  - Large amounts of attack traffic, multiple attack vectors
  - Devices remain infected longer and infections spread quickly
  - Booter operators moving into the “IoT business”

  → Makes these attacks more difficult to handle

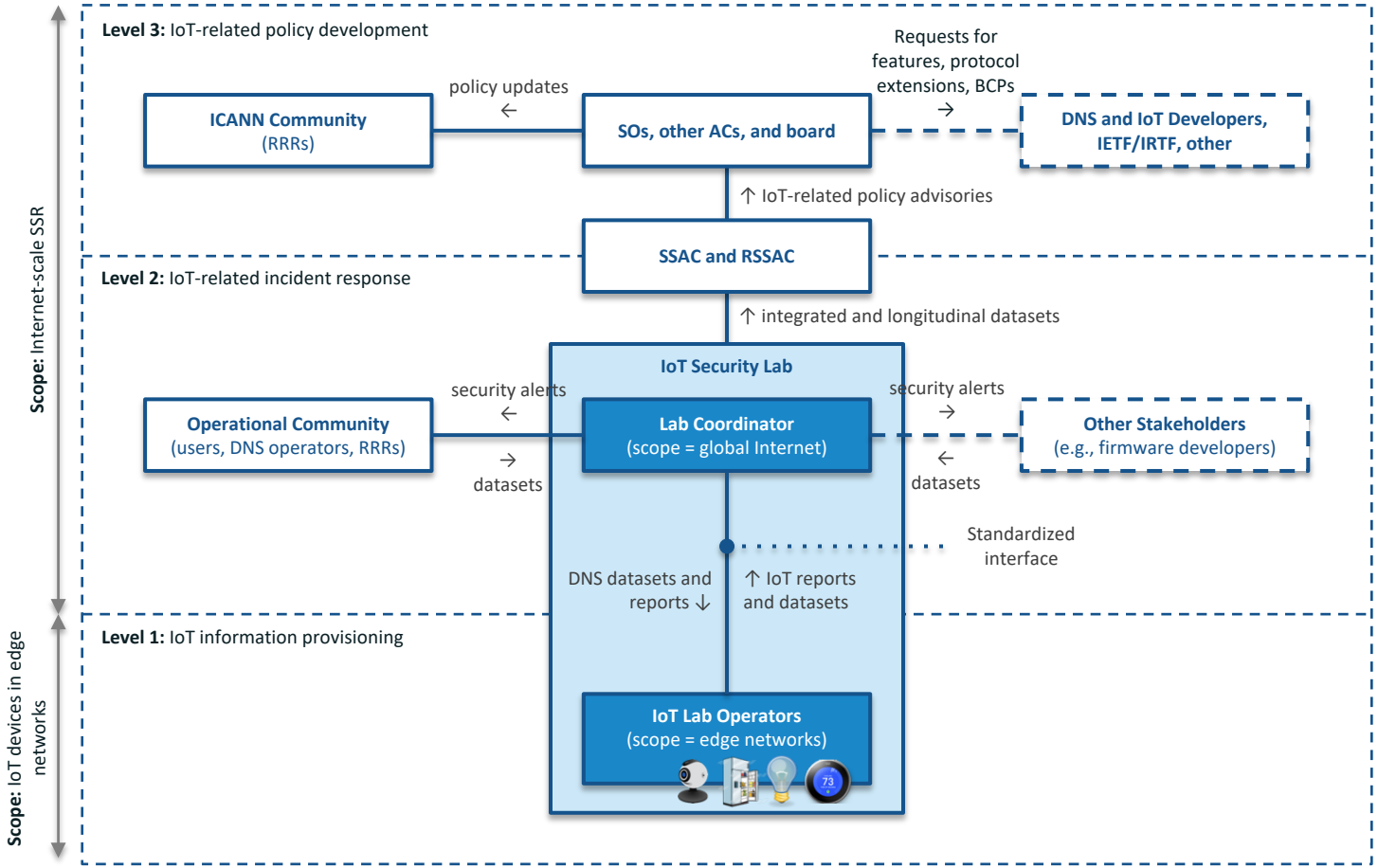
- Preserve the stability of the DNS as the IoT grows
  - IoT devices might use the DNS differently, for instance because software quality varies across operating systems
  - IoT devices may have on board validating resolvers but no update capabilities → KSK keyrolls get more difficult

Potential Proposal: IoT security lab

- Currently just a concept under discussion in the WP
- Goal: improve IoT-related policy development and DNS incident response by bringing relevant IoT security information into the DNS ecosystem
- Longitudinal measurements of:
  - DNS behavior of IoT devices
  - Vulnerabilities of IoT devices to remote compromise
  - Behavior of botnets that use the DNS
  - Device concentrations on the Internet

Concept of an IoT Security Lab also suggested in [5]

IoT security lab overview



This is the end goal, it will require multiple intermediate steps to get there!

Q&A

Work Party Members

Cristian Hesselman
Don Blumenthal
Jim Galvin
Jacques Latour
Rod Rasmussen
Andrew de la Haye
Jaap Akkerhuis
Julie Hammer
Tara Whalen
Robert Guerra
Lyman Chapin
Warren Kumari
Ondrej Filip

Coordinator

Cristian Hesselman
+31 6 25 07 87 33
cristian.hesselman@sidn.nl

KSK Roll

Joe Abley and Russ Mundy

KSK Work Party

- Board requests SSAC, RSSAC, RZERC to provide feedback on ICANN's updated KSK Roll Plan by 10 August
- SSAC work party exploring issues in the following areas:
  - outreach and communication
  - data and analysis
  - risk assessment
  - post roll issues
- SSAC aims to provide advice by 10 August to ICANN Board

Other Publications

Julie Hammer

Recent Publications

- [SSAC2018-16]: Draft Assessment Report of the Independent Examiner (13 June 2018)
  - Response to the Analysis Group on their Draft Assessment Report for the SSAC Review

- [SSAC2018-15]: Review of IDN Implementation Guidelines (11 June 2018)
  - SSAC Review of the Proposed Internationalized Domain Name (IDN) Implementation Guidelines Version 4.0
  - Did not identify any major issues

Recent Publications

- [SSAC2018-13]: Response Regarding the Actions of the ICANN Nominating Committee (09 May 2018)
  - Expressed concerns about the process that led to the removal of the SSAC Member from the NomCom.
  - Acknowledges that the NomCom acted within its remit and rights, but that doesn't make it necessarily right.

- [SSAC2018-12]: SSAC Comments on the Independent Review of the ICANN Nominating Committee Draft Final Report (07 May 2018)
  - The SSAC concurs with the full set of findings and recommendations and hopes the NomCom leadership will act quickly on them.

Questions to the Community

- What topics would you like SSAC to consider as a work item?
- What would you like SSAC to comment on?

Thank you