SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN64 | March 2019

Agenda

1. SSAC Overview
2. SAC101v2: SSAC Advisory Regarding Access to Domain Name Registration Data
3. SSAC Input to Temporary Specification for gTLD Registration Data EPDP
4. Securing Your Domains Against Registration Hijacking
5. Update on Name Collision Analysis Project
6. SSAC IOT WP Update

Security and Stability Advisory Committee (SSAC)

Who We Are

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

What We Do

Role: 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

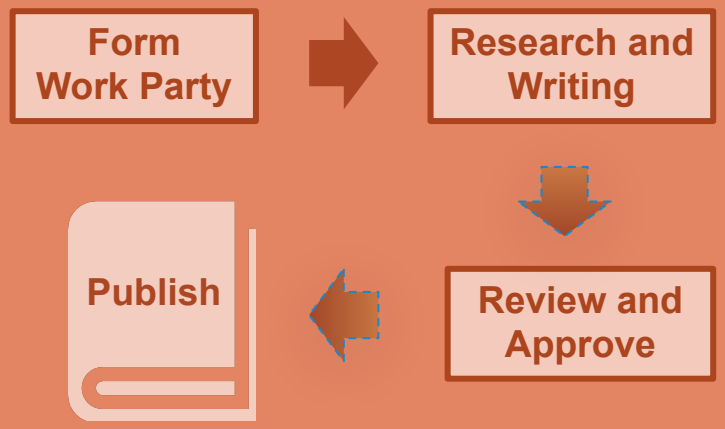
104 Publications since 2002

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)

Recent Publications

[SAC104]: SSAC Comment on Initial Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process (21 December 2018)

[SAC103]: SSAC Response to the new gTLD Subsequent Procedures PDP WG Initial Report (3 October 2018)

[SAC101v2]: SSAC Advisory Regarding Access to Domain Name Registration Data (12 December 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

- Name Collision Analysis Project
- SSAC Organizational Review
- The DNS in the IoT: Opportunities, Risks, and Challenges
- Improving SSAC Working Processes
- Emerging Security Topics (Ongoing)
- DNSSEC Workshops (Ongoing)
- Membership Committee (Ongoing)
- SSAC and ccNSO Joint Working Group on EPSRP (concluded)

Topics of Interest/Possible New Work

- DNS Privacy, DNS over HTTP, DNS over TLS
- Pros and Cons of Hyper Local Root / RFC 7706
- DNSSEC DS key Management and other Registrar/Registry Control Issues
- Best Practices for Handling Take-down Procedures
- Studying Abuse in new gTLDs
- Domain Name Hijacking Attacks

SAC101v2: Advisory Regarding Access to Domain Name Registration Data

Greg Aaron

SAC101: Advisory Regarding Access to Domain Name Registration Data

- Reflect evolving circumstances in relation to ICANN's Temporary Specification for gTLD Registration Data and the ongoing EPDP in this area

- Clarify the recommendations given in the original SAC101 document, based on feedback on its wording, to better enable the ICANN Board to take action and improve implementability.

- The substance of the advice given in SAC101 has not changed.

SSAC Input to Temporary Specification of gTLD Registration Data EPDP

Ben Butler / Benedict Addis

SSAC Input to EPDP

- SAC104: SSAC Comment on Initial Report of the Temporary Specification for gTLD Registration Data EPDP
  - Overarching comments: timing and future GNSO policy-making process, the need for legal advice, level of consensus, data flows and responsibilities of parties, reduction of contactability and manageability, risks and costs
  - Specific comments on seven recommendations.

SSAC Input to EPDP Report

General support with clarifying comments.

- Detailed SSAC recommendations and supporting information are contained in SAC101v2 and SAC104.

- Purpose 2 (and Rec 2) “Phase 2”
  - Access discussions is key and needs to proceed immediately. SSAC recommends clear charter and appropriate timeline for Phase 2.

- Rec 4 “Accuracy”
  - Reports of invalid Reg Data is a vital piece that is missing under the temp spec. Accredited RDS users need to be able to make reports of inaccurate data.

- Rec 5 “Data Elements”
  - Tech contact should be optional for the Registrant to provide, but must be supported by Rr and Ry if provided.

Dissenting opinions

- Rec 16 “Geographic Basis”
  - Lack of distinction results in significant over-redaction of data, and allows “venue shopping” and a race to the bottom.
  - Needs to be included in the Phase 2 discussions

- Rec 17 “Legal v Natural”
  - Support Phase 2 discussions, but...
  - The balancing test needs to include possible harm to the overall DNS / domain ecosystem in addition to costs and risks to controllers and privacy rights of data subjects.

Securing Your Domain against Registration Hijacking

Tim April

Recent Domain Registration Hijacking

1. Attackers had the ability to modify registration records at the registry, typically by compromising login credentials
2. Attackers changed DNS delegations (NS) pointing the zones to the attackers' DNS servers. A and MX records also modified.
3. Once zones were redirected, attackers impersonated services hosted by the victims (eg: e-mail, websites)
4. Attackers could Man-In-The-Middle (MITM) user traffic

Conclusions

- This is not the last time we will see these kinds of attacks
- Deploy security in-depth, there is no holy grail
  - Secure the credentials used to access your registrar
  - Use MFA where possible
  - Secure email addresses used for password reset
  - Deploy DNSSEC signing and validation
- Use Registry Locks
- Monitor your domains

Relevant SSAC Publications

- SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse
- SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts
- SAC049: SSAC Report on DNS Zone Risk Assessment and Management
- SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

Name Collision Analysis Project

Jay Daley and Jim Galvin

Name Collision Analysis Project Update

- ICANN Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board
  - 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 other technical experts

Name Collision Analysis Project Update

- **Study one: Gap Analysis**
  - Properly define name collision
  - Review and analyze past studies and work on name collision and perform a gap analysis
- **Study two: Root cause and impact analysis**
  - Name collisions - what happens for each use case under each leakage scenario and for each delegation form
  - Name collision impacts - what the system making the query, that is affected by a name collision, may or may not do as a result of a name collision
  - Impact sizing - Estimate the scale and severity of each name collision impact.
- **Study three: Analysis of Mitigation options**
  - Identification and assessment of mitigation options
  - Production of recommendations regarding delegation

Name Collision Analysis Project Update

- March 2018: Project plan goes to public comment
  - Detailed comments made and responded to
- October 2018: Revised project plan produced, but then major change in plan
  - SSAC notes how different this is from other work
  - Requests OCTO manage NCAP as a project
  - SSAC will still produce final report on OCTO work
  - Board Technical Committee (BTC) agrees
- December 2018: OCTO begin to assess work
- March 2019: BTC to consider OCTO project plan

NCAP - Proposed Project Management Structure

Roles	Entities
Project Customer	ICANN Board
Project Steering Group	BTC Leadership, SSAC Leadership, NCAP Co-Chairs, OCTO
Project Director / Owner	OCTO
Project Technical Architect	SSAC

IoT WP

Cristian Hesselman

DRAFT Report overview

- "The DNS in the IoT: opportunities, risks, and challenges"

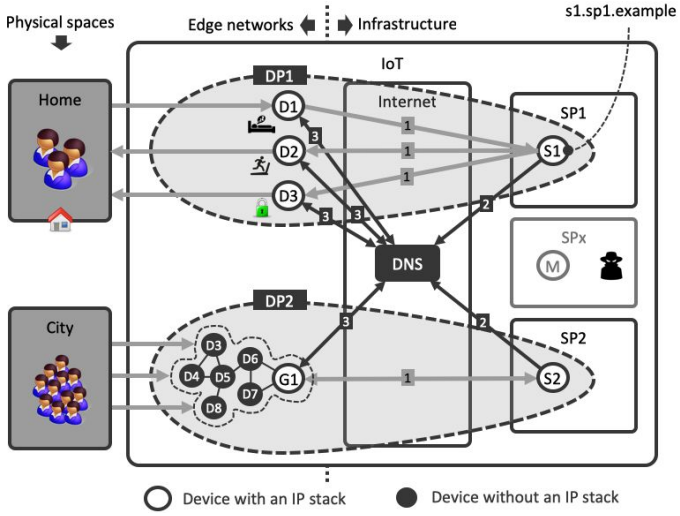
- IoT is a new kind of Internet application
  - Interacts with people's physical world (sense, actuate)
  - Often without user awareness or involvement
  - Much more heterogeneous operating environment
  - Devices use the DNS to locate services they need

- Goals
  - Explore opportunities and risks
  - "Debuzzword" term IoT

- Challenges for the DNS industry
  - Rather than recommendations for ICANN community
  - Type is report rather than advisory

Analysis

- Model of the DNS in the IoT
  - Data transfer
  - DNS interactions



- Opportunities
  - DoH and DoT on IoT devices
  - DNSSEC validation on IoT devices
  - More secure registration services
  - DNS query data to increase IoT transparency

- Risks
  - DNS unfriendly programming at IoT scale
  - Size and complexity of IoT botnets
  - Increased DDoS amplification through open resolvers

Actions

- Challenges
  - Developing a DNS security library for IoT devices
  - Training IoT and DNS professionals
  - Deploying a system to share information on IoT botnets
  - More flexible mitigation of IoT-powered DDoS attacks
  - Develop a system to measure the evolution of the IoT

- Next steps
  - SSAC internal review
  - Publish report
  - Community feedback and report update

Questions to the Community

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

Thank you

SAC101v2: Advisory Regarding Access to Domain Name Registration Data

BACK UP SLIDES

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, including security and stability.
- Access to the data for legitimate users is more constrained and more restricted than ever. 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: 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.
- Rate-limiting impedes security professionals and law enforcement from getting the data, which is vital to their work.
- Unfortunately, rate limiting is applied to everyone, indiscriminately.

SAC101: Advisory Regarding Access to Domain Name Registration Data

- SSAC: law enforcement and security practitioners have a legitimate need to access. Such access must comply with legal requirements.
- The GDPR says that security, fraud prevention, and reporting to legal authorities are legitimate uses of personal data, and allows for balanced use.
- ICANN's Temp Spec allows RDDS (WHOIS) operators complete freedom to choose when to redact domain contact data from publication, whether or not the subject is protected by GDPR or by any other privacy law. The result has been blanket redactions, hiding more data than is legally called for.
- 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.
- *Such an "accredited access" program will be discussed in the ePDP phase 2, to begin shortly.*

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 oversee the creation and execution of a plan that accomplishes the following...with timely deadlines. The creation and execution of this plan should be a top priority...
   a. ICANN policy-making should result in a domain registration data policy, including statements of purposes for 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 remaining thin gTLD registries should be required 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.

SAC101: Recommendations 2, 3

2. The ICANN Board should direct the ICANN Organization to work with the ICANN Community to: **A) develop policy with clearly defined uniform purposes for RDDS rate-limiting and corresponding service level agreement requirements and B) clarify current expectations for the use of rate limiting under existing policy and agreements.**

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.**

   #3 will be discussed in the ePDP phase 2, to begin shortly.

SAC101: Recommendations 4, 5

4. The initiation of charges for RDS access, or any significant future changes in fees for RDDS access, must include a formal assessment of user impacts and the security and stability impacts, and be conducted as part of 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.

Please see SAC101v2 for the rationales and background for these recommendations.

https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf