SSAC Activities Update

Rod Rasmussen, SSAC Chair | ICANN65 | June 2019

Agenda

1. SSAC Overview
2. SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges
3. DNS-over-HTTPS and DNS-over-TLS
4. Name Collision Analysis Project (NCAP)
5. Registration Data Services Query Reporting
6. SSAC Review

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

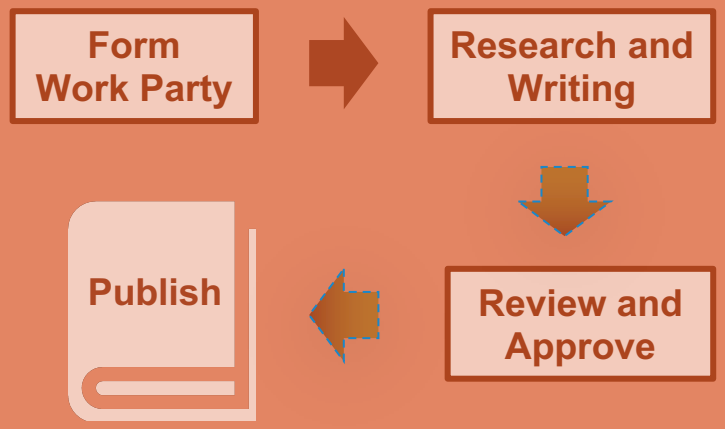
105 Publications since 2002

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

[SAC105] The DNS and the Internet of Things: Opportunities, Risks, and Challenges (3 June 2019)

[SSAC2019-04] SSAC Review Feasibility Assessment and Initial Implementation Plan (27 May 2019)

[SSAC2019-03] SSAC Input to Issues For Consideration Regarding Establishment of a Standing Panel for the Independent Review Process (IRP) (13 May 2019)

[SSAC2019-02] Registration Data Services Query Reporting (3 May 2019)

ICANN | SSAC
Security and Stability Advisory Committee

Outreach

https://ssac.icann.org/

SSAC Intro: https://www.youtube.com/watch?v=eOVgtCY59e4

SSAC Chair Rod Rasmussen on IDN Homographic Attacks: https://www.youtube.com/watch?v=g3keTroHN2w

Current Work

- Name Collision Analysis Project (NCAP)
- SSAC Organizational Review
- DNS-over-HTTPS (DoH) & DNS-over-TLS (DoT)
- EPDP on Temp Spec for gTLD Registration Data
- Root Server System
- Improving SSAC Working Processes
- Emerging Security Topics (Ongoing)
- DNSSEC Workshops (Ongoing)
- Membership Committee (Ongoing)

Topics of Interest/Possible New Work

- 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

SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges

Cristian Hesselman

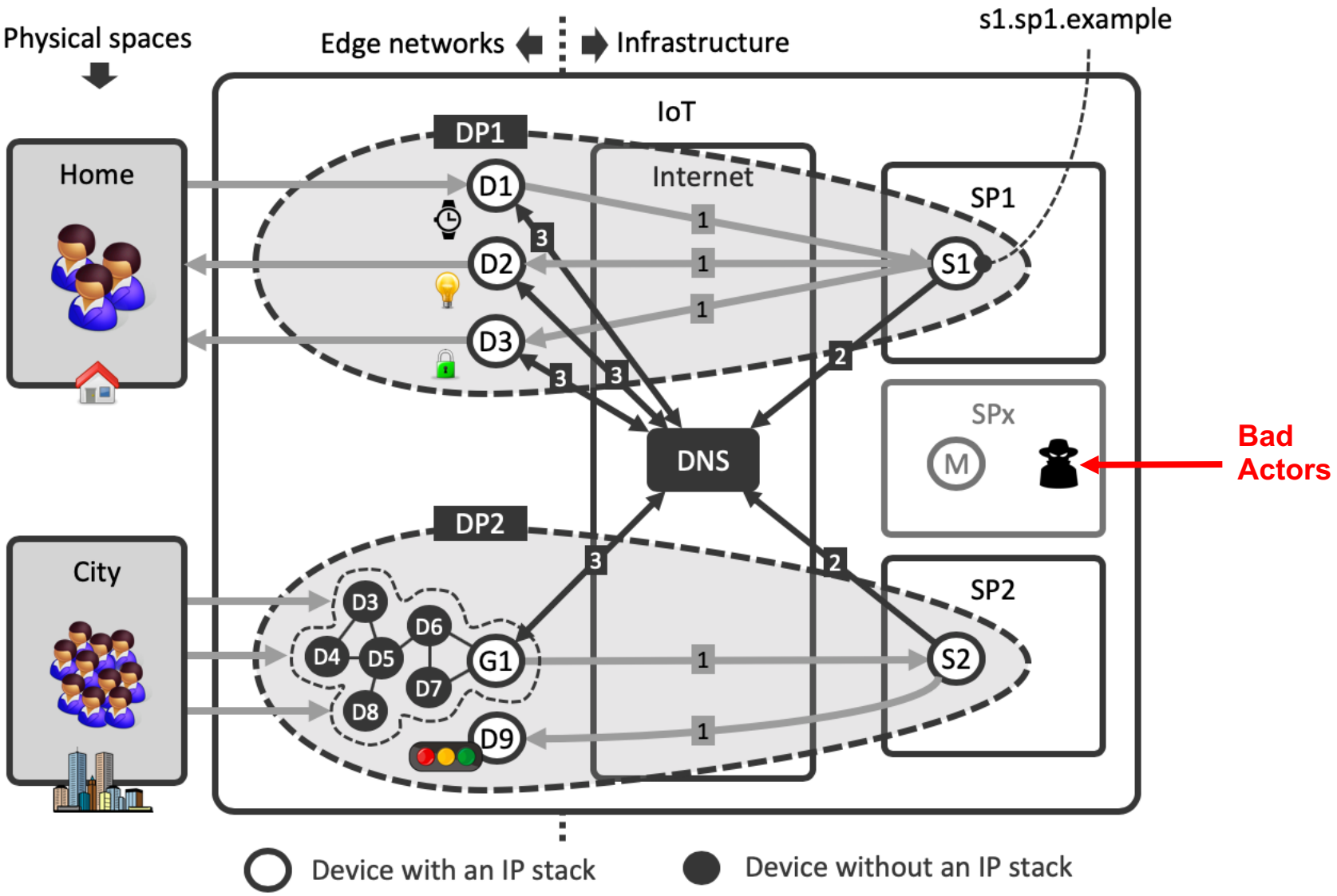
SAC105: The DNS and the Internet of Things

- SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges, published June 3rd, 2019
- A different kind of SSAC report:
  - **No recommendations** to the ICANN Board
  - A tutorial-style discussion intended to trigger and **facilitate dialogue** in the broader ICANN community
  - More **forward looking** than operational in nature
  - Partly within SSAC and ICANN's remit, but also goes beyond it
- Many aspects of our discussion are not new, except as they consider new challenges from IoT

The Internet of Things (IoT)

- Internet application that extends “network connectivity and computing capability to objects, devices, sensors, and items **not ordinarily considered to be computers**” (ISOC, 2015)
- Examples: smart homes, smart cities, self-organizing dynamic networks of drones and robots
- Differences with “traditional” applications
  - IoT continually senses, interprets, and acts upon physical world
  - Often without user awareness or involvement (passive interaction)
  - Pervasive 20-30 billion devices operating “in the background” of people’s daily lives
  - Widely heterogeneous devices (hardware, operating systems, network connection)
  - Longer lifetimes (perhaps decades) and unattended operation

Role of the DNS for the IoT



IoT and the DNS

- Remote services (cloud services) assist devices in performing their task (e.g., combining and analysing data from multiple sensors)
- Measurement studies show that IoT devices use the DNS to locate remote services (e.g., sleep trackers, light switches)
- **Opportunity:** DNS helps fulfilling IoT's more stringent security, stability, and transparency requirements stemming from seamless interaction with physical world
- **Risk:** IoT stresses the DNS, accidentally (e.g., large number of devices coming online simultaneously after a power outage) or on purpose (IoT-powered DDoS attack)
- **Challenge:** DNS and IoT industries can seize opportunities and address risks

DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT)

Suzanne Woolf & Barry Leiba

DoH / DoT Overview

- DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) are two new protocols for transporting DNS data
- Both protocols support encrypting DNS data in transport

  Traditional DNS queries and responses are unencrypted
- DNS data integrity is unrelated to DoH and DoT

  The need for DNSSEC has not changed
- Standardization on how DoH and DoT resolvers are configured in applications and operating systems is still ongoing

  DoH and DoT implementations are still developing and current deployments are limited

Why DoH / DoT ?

- Traditional DNS transport is unencrypted

  Can cause users to leak confidential information (surveillance)

  DNS responses can be tampered with (censorship)

- DoH and DoT provide channel **confidentiality** while DNSSEC provides response **integrity** when validation is performed

- Technologies such as QNAME Minimization may also be effective at preserving user privacy

DoH / DoT Conclusions

- Some potential deployments of DoH and DoT may impact traditional policy control points in DNS resolution
- Standardization on how DoH and DoT resolvers are configured in applications and operating systems is still ongoing
- For registry and registrar operators there is **currently** little impact from DoH and DoT
- It is **too early** to say what the impact of DoH and DoT on users will be
- The need for DNSSEC and QNAME Minimization has not changed

Name Collision Analysis Project

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 2019:** Board approves study 1 project plan
- **24 April 2019:** NCAP Discussion Group (NCAP WP plus community) formed and meeting weekly, currently 20 participants, 22 observers
- **30 May 2019:** Discussion Group finalized the Statement of Work for Study One and sent to OCTO.
- **July 2019:** Next Steps: OCTO start an open RFP process to engage a contractor
- **July 2019:** Discussion Group preparing a second deliverable: definition of name collisions, to be ready for public comment after ICANN65.

Registration Data Services Query Reporting

Rod Rasmussen

Registration Data Services Query Reporting

- 3 May 2019 SSAC sent SSAC2019-02 to ICANN regarding anomalies it sees in Registration Data Services (a.k.a. WHOIS) Query reporting
- SSAC's analysis on gTLD registry reporting of WHOIS queries count shows that:
  - Some registries counting monitoring queries while others do not
  - Some operators are reporting that many of their TLDs receive the exact same number of queries in a given month
  - For some operators, the number of WHOIS queries per TLD have an abnormal distribution.

Registration Data Services Query Reporting

SSAC Recommendations

1. ICANN Org issue guidance to all registry operators, clarifying expectations for reporting port 43 queries and RDAP queries. The guidance should make clear the purposes and goals of the data collection and the contractual obligations.
2. SSAC believes that a purpose of gathering the data is to document queries made by the users (consumers) of the registration data service. Registry operators should exclude the queries they make to their own systems.
3. It is vital that ICANN collect valid, accurate data regarding RDAP queries. The WHOIS query data is unreliable, but the move to RDAP offers an opportunity to get things right.

Registration Data Services Query Reporting

- 30 May 2019, ICANN responded to SSAC2019-02:
  - ICANN shared the SSAC letter with the gTLD Registry Stakeholders Group
  - ICANN proposes to facilitate a discussion between SSAC and RySG at ICANN 65 in Marrakech.

SSAC Review

Julie Hammer

Response to IE Recommendations - Agree

The SSAC agrees with 19 of the 30 IE recommendations

- 1-6, 8-11, 15-16, 18-20, 27-30

Response to IE Recommendations – Agree in Principle

The SSAC agrees in principle with 5 of the 30 IE Recommendations but proposes an alternate solution

- 7 - Quick look documents
- 12 - Internships
- 24 - Recruit legal/policy experts
- 25 - Recruit for geography and gender
- 26 - Annual review of liaisons

Response to IE Recommendations – Disagree

The SSAC disagrees with 6 of the 30 IE Recommendations

- 13 - Data storage
- 14 - SSAC Liaisons to SO/ACs
- 17 - Email update before ICANN meetings
- 21 - Recruiting plan, list of potential future members
- 22 - Funding to attend 2-3 security conferences
- 23 - Maintain list of academic institutions

Thank you