SAC090
SSAC Advisory on the Stability of the Domain Namespace

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)

22 December 2016

Preface

This is an advisory to the ICANN Board, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) on the stability of the domain namespace.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). 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. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Table of Contents

1 Introduction

The Domain Name System (DNS) was developed[1] as an extension of a network architecture that originally relied on a manually maintained list of host name to Internet Protocol (IP) address mappings. The ability to use hierarchically structured domain names rather than IP addresses to identify endpoints in this network simplified its management and administration, and contributed significantly to the successful scaling of an early research project into today's ubiquitous global Internet.

Many people are unaware that the concept of hierarchical domain names did not originate with the DNS. Domain Names probably made their first formal appearance in Request for Comment (RFC) 799,[2] "Internet Name Domains," and were an important part of the discussions that ultimately led to the specification of the Simple Mail Transfer Protocol (SMTP):

> *Two or three decades into the history of Domain Names, a popular notion has taken hold that Domains Names were defined and specified in STD 13, the definition of the Domain Name System (DNS). The definitions within RFC 1034 and RFC 1035 have become the apparently-authoritative source for discussions on what is a Domain Name. The truth is, RFC 1034 and RFC 1035 do not define Domain Names; those documents define only how Domain Names are used and processed in the DNS.*[3]

Because the DNS model for identifying network endpoints and managing essential information about them has been so successful in helping to establish the global public Internet at the scale and diversity we see today, domain names and the DNS resolution protocol have been adopted and adapted for use in other environments, such as private networks. These different uses of the domain namespace threaten one of its most important properties: the unambiguous relationship between a domain name and its object, which ensures that resolution of a domain name always produces the expected result.

In principle, domain namespace ambiguity, and its harmful consequences for name resolution stability could be avoided either by globally enforcing the singular association of each namespace element with one and only one meaning regardless of context, or by establishing and maintaining perfect isolation among different name resolution contexts (enforcing singular association independently within each). This concept of identifier

---

[1] See RFC1034 at https://www.ietf.org/rfc/rfc1034.txt and RFC1035 at https://www.ietf.org/rfc/rfc1035.txt.

[2] See RFC799 at: https://tools.ietf.org/html/rfc799.

[3] From the Internet Draft "Domain Names" at: https://datatracker.ietf.org/doc/draft-lewis-domain-names, which includes a comprehensive summary of the history of domain names.

isolation is a familiar feature of most programming languages, which distinguish variables declared with global or a more localized scope.[4]

However, because the domain namespace is so closely associated with the DNS, the global DNS is widely assumed to be the default resolution context for anything that looks like a domain name. Even if it were possible to put principles for disambiguation into practice by reference to context or scope, unambiguous resolution would fail due to the default practice of "when in doubt, send it to the DNS for resolution."

In practice, ambiguous resolution of names (often referred to as "name collisions") occurs because of an uncoordinated hybrid of approaches. Domain names are allocated and used within the public DNS as if they were globally scoped, but other uses of lexically identical domain names can occur, thereby leading to ambiguity when the intended isolation of the different uses cannot be maintained. This ambiguity creates the security and stability risks summarized in SAC062,[5] and presents a particularly difficult challenge to software and system developers who cannot reliably determine how to interpret a string that appears to be a syntactically valid domain name.

This advisory is concerned only with the risks to security and stability that arise from ambiguity in the use of the domain namespace. Because no one owns (or can own) the domain namespace, and programmers and network managers cannot be prevented from creating their own names and naming scopes, these risks arise regardless of how policy debates about authority or oversight are resolved. Therefore, the observations and recommendations in this advisory are directed at mitigating clearly identified risks and developing policies that provide practical guidance to software and system developers, rather than debating whether or not private network operators should use the domain namespace, or who (if anyone) should have the authority to declare and enforce exclusive uses for specific individual domain name labels or categories of labels.

---

[4] In Java, for example, a package defines the scope of names for the classes contained within the package; syntactically identical names can appear in different packages without colliding semantically because they are always resolved within their respective scopes. See: http://docs.oracle.com/javase/specs/jls/se8/html/jls-6.html#jls-6.3.

[5] See SAC062, "SSAC Advisory Concerning the Mitigation of Name Collision Risk" at: https://www.icann.org/en/system/files/files/sac-062-en.pdf.

2 The Domain Namespace

The domain namespace[6] is the set of all possible domain names that can be assembled from a tree-structured hierarchy of individual labels. Although it is closely associated with the public DNS, both the domain namespace and the DNS protocol have been used in other environments that are intended to be separate from, but for a variety of reasons related to, the Internet's DNS. This would not be a problem if each use of a domain name could be rigidly confined to the scope within which it is properly defined. As other SSAC Advisories[7] have described in detail, this rigid separation of scope cannot be maintained in practice. Context and other cues do not always allow either Internet or non-Internet systems to unambiguously determine the meaning (and therefore the proper handling) of a domain name. Ambiguity threatens the stability of the domain namespace when processing agents cannot reliably determine "what to do" when presented with a domain name.

2.1 DNS Use of the Domain Namespace

After the publication in 1987 by the Internet Engineering Task Force (IETF)[8] of the RFCs that eventually became Internet Standard STD 13,[9] the domain namespace was widely considered to be an integral part of the DNS in the global public Internet. When a processing agent encountered a syntactically correct domain name, it was expected to submit it to the DNS for resolution.[10] With very few exceptions, resolution represented a straightforward tree traversal starting at the singular universally-recognized root. For the most part, global DNS use of the domain namespace today follows the same model.

2.2 Other Uses of the Domain Namespace

As the Internet expanded to become the dominant global telecommunication system, its DNS became the correspondingly dominant model for network node naming and name resolution. Its conventions and protocols, including the domain namespace, were widely adapted to other uses that were not strictly "part of the global Internet," such as the

---

[6] In formal graph-theoretic terms, the domain namespace constitutes a labelled directed rooted tree in which the syntax of the label associated with each vertex other than the unlabeled root is defined by RFCs 1035, 1123, and 2181. The term "*n*th level domain name label" refers to a member of the set of all vertices for which the path to the root contains n edges. For *n*=1 the term most often used is "top-level domain name label" or simply "top-level domain" (TLD). In this formulation, the term "domain namespace" refers to the complete graph consisting of all possible vertices and edges, not just those with which a specific use has been associated.

[7] See SAC045, SAC053, SAC057, SAC060, SAC062, SAC064, SAC066, and SAC070 at: https://www.icann.org/groups/ssac/documents.

[8] See https://www.ietf.org.

[9] See https://tools.ietf.org/html/std13.

[10] This description omits, for simplicity, a tremendous amount of detail about caches and other DNS implementation internals.

Active Directory component of Microsoft's Windows domain networks. Top-level domain names that have been commonly used in private environments, presumably as a result of vendors adopting DNS-based naming conventions and protocols, include .home, .corp, .mail, .homestation, .belkin, .lan, and .dlink. These names are frequently seen outside of their intended context in queries to the public DNS.[11] [12] [13]

For example, the string .lan is currently not delegated in the DNS root zone, but queries for .lan are seen at the root servers with considerable regularity.[14] It is difficult to know the exact causes of these queries. Some home routers will assign .lan by default to devices via Dynamic Host Configuration Protocol (DHCP). These devices will then often use .lan as their default search suffix when querying the DNS. If these queries leak outside of their respective home networks, they will often be seen at the root. Currently a query for a name under .lan sent to the root zone will return NXDOMAIN, signifying that the name does not exist. However, if .lan were to be delegated in the DNS root zone these queries would start returning resource records for the .lan TLD name servers, which could then result in security consequences for the querying device.[15]

Given the distributed and autonomous way in which Internet and Internet-related technologies are developed and evolve, it is unproductive to argue that the domain namespace should not be used for purposes other than those that directly support the global DNS, or that the people who do so are behaving badly. Reasonable (and in any case unpreventable) uses of the domain namespace extend beyond the global DNS. Also, these arguments distract attention from what matters for security and stability: the unambiguous relationship between each element of the domain namespace and how it should be interpreted whenever and wherever it appears.

2.3 Domain Namespace Stability

The security and stability consequences of domain name ambiguity have been documented by SSAC previously.[16] The direct approach to domain namespace stability—designating a central authority to control the way in which domain names are used in all contexts—is both infeasible and undesirable given the robustly non-centralized way in which the Internet ecosystem evolves. Alternatively, a multi-stakeholder approach in

---

[11] See "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report," JAS Global Advisors at: https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf.

[12] See "On Queries to the Root," Geoff Huston & George Michaelson at: http://www.potaroo.net/presentations/2014-06-24-namecollide.pdf.

[13] See SAC045, "Invalid Top Level Domain Queries at the Root Level of the Domain Name System" at: https://www.icann.org/en/committees/security/sac045.pdf.

[14] See "Name Collision in the DNS," Interisle Consulting Group at: https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf.

[15] Ibid. 13

[16] Ibid. 5

which the uses of the domain namespace are coordinated to mitigate the risks of ambiguity but not administered by a central authority might be both feasible and desirable. However, it is unreasonable to require a user to know when alternative interpretations of a domain name exist, particularly when information necessary to determine that may not be available.

3 Findings

Finding 1: The SSAC finds that uncoordinated use of the domain namespace in overlapping environments can lead to ambiguity when those environments overlap and their names collide. This ambiguity threatens the stability of the domain namespace when processing agents cannot reliably determine "what to do" when presented with an identifier that is a syntactically valid domain name.

Finding 2: More specifically, the SSAC finds that the lack of adequate coordination among the activities of several different groups contributes to the domain namespace instability identified in Finding 1:

- ICANN, in its role as coordinator of the allocation and assignment of names in the root zone of the Domain Name System,[17] by inviting applications for new top-level domains without specifying unambiguous criteria for determining whether a given string may or may not be (or potentially become) a top-level domain name label;
- the Internet Engineering Task Force (IETF), in its role as the Standards Development Organization for the DNS protocol, by reserving some domain names for special use;[18] and
- other individuals and organizations, by using independently selected domain names in environments that cannot reliably be distinguished from the environment in which domain names are resolved by reference to the global DNS root.[19]

4 Recommendations

Recommendation 1: The SSAC recommends that the ICANN Board of Directors take appropriate steps to establish definitive and unambiguous criteria for determining whether or not a syntactically valid domain name label could be a top-level domain name in the global DNS.

---

[17] See Section 1.1(a)(i) of "Bylaws for Internet Corporation for Assigned Names and Numbers" at: https://www.icann.org/en/system/files/files/adopted-bylaws-27may16-en.pdf.

[18] See RFC 6761, "Special-Use Domain Names" at: https://datatracker.ietf.org/doc/rfc6761.

[19] This group includes common private network uses such as .corp, .home, and .mail as well as uses that arise within organizations that develop Internet technologies outside of the IETF.

Recommendation 2: The SSAC recommends that the scope of the work presented in Recommendation 1 include at least the following issues and questions:

1) In the Applicant Guidebook for the most recent round of new generic Top Level Domain (gTLD) applications,[20] ICANN cited or created several lists of strings that could not be applied-for new gTLD names, such as the "reserved names" listed in Section 2.2.1.2.1, the "ineligible strings" listed in Section 2.2.1.2.3, the two-character ISO 3166 codes proscribed by reference in Section 2.2.1.3.2 Part III, and the geographic names proscribed by reference in Section 2.2.1.4. More recently, the IETF has placed a small number of potential gTLD strings into a Special-Use Domain Names Registry.[21] As described in RFC 6761[22], a string that is placed into this registry is expected to be processed in a defined "special" way that is different from the normal process of DNS resolution.

   Should ICANN formalize in policy the status of the names on these lists? If so:

   i) How should ICANN respond to changes that other parties may make to lists that are recognized by ICANN but are outside the scope of ICANN's direct influence?

   ii) How should ICANN respond to a change in a recognized list that occurs during a round of new gTLD applications?

2) The IETF is an example of a group outside of ICANN that maintains a list of "special use" names.[23] What should ICANN's response be to groups outside of ICANN that assert standing for their list of special names?

3) Some names that are not on any formal list are regularly presented to the global DNS for resolution as TLDs. These so-called "private use" names are independently selected by individuals and organizations that intend for them to be resolved only within a defined private context. As such they are harmlessly discarded by the global DNS—until they collide with a delegated use of the same name as a new ICANN-recognized gTLD.

   Should ICANN formalize in policy the status of "private use" names? If so:

   i) How should ICANN deal with private use names such as .corp, .home, and .mail that already are known to collide on a large scale with formal applications for the same names as new ICANN-recognized gTLDs?

   ii) How should ICANN discover and respond to future collisions between private use names and proposed new ICANN-recognized gTLDs?

---

[20] See https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf.

[21] See https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml.

[22] Ibid. 18

[23] Ibid. 21

Recommendation 3: Pursuant to its finding that lack of adequate coordination among the activities of different groups contributes to domain namespace instability, the SSAC recommends that the ICANN Board of Directors establish effective means of collaboration on these issues with relevant groups outside of ICANN, including the IETF.

Recommendation 4: The SSAC recommends that ICANN complete this work before making any decision to add new TLD names to the global DNS.

5 Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

5.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this advisory.

SSAC members

Joe Abley
Jaap Akkerhuis
Don Blumenthal
Lyman Chapin
Patrik Fältström
Jim Galvin
Geoff Huston
Warren Kumari
John Levine
Danny McPherson
Ram Mohan
Russ Mundy
Rod Rasmussen
Doron Shikmoni
Suzanne Woolf

ICANN staff

Julie Hedlund
Andrew McConachie (editor)
Kathy Schnitt
Steve Sheng

5.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2016-12-15-en.

5.3 Dissents

There were no dissents.

5.4 Withdrawals

There were no withdrawals.

Appendix A: Relevant Background Documents

In this appendix, the SSAC lists some relevant background documents related to the discussions of domain namespace.

RFC 920 "Domain Requirements", J. Postel, J. Reynolds, October 1984.

https://tools.ietf.org/rfc/rfc920

An early description of the Domain Name System and its intended use.

RFC 1034 "Domain Names – Concepts and Facilities", P. Mockapetris, November 1987.

https://tools.ietf.org/rfc/rfc1034

The original canonical specification of the DNS.

RFC 2826 "IAB Technical Comment on the Unique DNS Root", IAB, May 2000.

https://tools.ietf.org/rfc/rfc2826

The Internet Architecture Board's comment on one namespace and its utility for the Internet.

RFC 2860 "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority", B. Carpenter, F. Baker, M. Roberts, June 2000.

https://tools.ietf.org/rfc/rfc2860

The agreement between the IETF and ICANN over names and addresses.

RFC 3869 "IAB Concerns and Recommendations Regarding Internet Research and Evolution", R. Atkinson S. Floyd, August 2004

https://tools.ietf.org/rfc/rfc3869

Section 3.2 considers research topics in the general area of names research

RFC 4795 "Link-Local Multicast Name Resolution (LLMNR)", B. Aboba et al, January 2007.

https://tools.ietf.org/rfc/rfc4795

A non-DNS locally scoped name resolution protocol specification.

RFC 6761 "Special Use Domain Names", S. Cheshire, M. Krochmal, February 2013.

https://tools.ietf.org/rfc/rfc6761

Describes what it means to say that a Domain Name (DNS name) is reserved for special use, when reserving such a name is appropriate, and the procedure for doing so. It establishes an IANA registry for such domain names, and seeds it with entries for some of the already established special domain names.

RFC 6762 “Multicast DNS”, S. Cheshire, M. Krochmal, February 2013.

https://tools.ietf.org/rfc/rfc6762

The specification of the Multicast DNS resolution protocol and the reservation of .local in the Special Use Names Registry.

RFC 7686 “The ".onion" Special-Use Domain Name”, J. Appelbaum, A. Muffet, October 2015.

https://tools.ietf.org/rfc/rfc7686

The justification for listing .onion in the Special Use Names registry.

RFC 7788 "Home Networking Control Protocol", M. Stenberg, S. Barth, P. Pfister,

April 2016.

https://tools.ietf.org/html/rfc7788

Describes the Home Networking Control Protocol (HNCP), an extensible configuration protocol, and a set of requirements for home network devices.

DNSOP Special Use Domain Names of P2P Systems, IETF 93, July 2015

https://www.ietf.org/proceedings/93/slides/slides-93-dnsop-5.pdf

A list of other names that have been proposed as candidates for listing in the Special Use Names Registry.

DNSOP “The ALT Special Use Top Level Domain”, W. Kumari, A. Sullivan, work in progress, October 2016

https://tools.ietf.org/html/draft-ietf-dnsop-alt-tld-06

A working draft adopted in the DNS Operations Working Group of the IETF that considers the use of .alt as a common top level domain for Special Use contexts.

DNSOP “Problem Statement for the Reservation of Top-Level Domains in the Special-Use Domain Names Registry”, G. Huston, P. Koch, A. Durand, W. Kumari, work in progess, September 2016

https://tools.ietf.org/html/draft-adpkja-dnsop-special-names-problem-06

An individual authorship internet-draft proposed as a problem statement for special use names in the IETF.

DNSOP "Special-Use Names Problem Statement", T. Lemon, R. Droms, W. Kumari, work in progress, October 2016

https://tools.ietf.org/html/draft-ietf-dnsop-sutld-ps-00

A working draft adopted in the DNS Operations Working Group of the IETF as a problem statement for special use names in the IETF.

Homenet "Redacting .home from HNCP", T. Lemon, work in progress, November 2016

https://tools.ietf.org/html/draft-ietf-homenet-redact-01

A working draft adopted in the Homenet Working Group of the IETF that updates the Home Networking Control Protocol (RFC 7788), eliminating the recommendation for a default top-level name for local name resolution.

Homenet "Special Use Top Level Domain '.homenet'", P. Pfister, T. Lemon, work in progress, November 2016

https://tools.ietf.org/html/draft-ietf-homenet-dot-00

A working draft adopted in the Homenet Working Group of the IETF that specifies the behavior that is expected from the Domain Name System with regard to DNS queries for names ending with '.homenet.', and designates this top-level domain as a special-use domain name.

NSRG "What's In A Name: Thoughts from the NSRG", abandoned work, September 2003

https://tools.ietf.org/html/draft-irtf-nsrg-report-10

A report from the Namespace Research Group of the IRTF. It appears that the report failed to achieve consensus within the group, and was never published as an RFC.