Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 25, 2016

G. Huston
APNIC
P. Koch
DENIC eG
A. Durand
ICANN
W. Kumari
Google

May 24, 2016

Problem Statement for the Reservation of Top-Level Domains in the Special-Use Domain Names Registry
draft-adpkja-dnsop-special-names-problem-03

Abstract

The dominant protocol for name resolution on the Internet is the Domain Name System (DNS). However, other protocols exist that are fundamentally different from the DNS, and may or may not share the same namespace.

When an end-user triggers resolution of a name on a system that supports multiple, different protocols (or resolution mechanisms), it is desirable that the protocol used is unambiguous, and that requests intended for one protocol are not inadvertently answered using another.

RFC 6761 introduced a framework by which a particular domain name could be acknowledged as being special. Various challenges have become apparent with this application of the guidance provided in RFC 6761. This document aims to document those challenges in the form of a problem statement in order to facilitate further discussion of potential solutions.

Status of This Memo

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 25, 2016.

Copyright Notice

Table of Contents

1. Introduction: DNS, Name space or Name Spaces, Name Resolution Protocols

For a very long time, DNS and the name space have been perceived as one and the same. However, this has not always been the case; in the past, other name resolution protocols were popular. One can remember NIS, NIS+, host files, UUCP addresses... Most of those have been obsoleted by the DNS in the late 1990s. More information on the

history of names and namespaces can be found in [I-D.lewis-domain-names].

More recently, new name resolution protocols have been proposed, each addressing a particular need or a particular community. For example, the DONA handle system has been used by the publication industry. The Apple "Bonjour" set of protocols, inspired by what was available on Appletalk networks, has been developed to perform automatic name resolution on a local IP network. The TOR project is using the onion system to obfuscate communications, the GNU Name System (GNS) system is using block chains to build a decentralized name system to offer "privacy and censorship resistance". Many more have been proposed.

Those alternate name resolution protocols do not exist in a vacuum. Application developers have expressed a strong desire to build their software so it will function in any of those universes with minimal changes. Doing so means that the software has to recognize deterministically what kind of name it is dealing with and associate it with the corresponding name resolution protocol. Because of this desired lack of explicit signaling, an algorithmic solution frequently chosen by application developers consists simply to use a special tag padded at the end of a name to indicate an alternate name resolution method. Examples: if a name ends in .local, the software uses the Apple Bonjour protocol based on multicast DNS; if the name ends in .onion, it uses the TOR protocol; if the name ends in .gnu, it uses the GNS protocol, etc... One noteworthy exception to this approach is the DONA system that exists independently and has developed its own interoperability solution with the DNS.

A result of the above is that a number of applications have been developed (and massively distributed) that have encoded their favorite "tag" as a DNS TLD in a free-for-all, beginning their existence squatting on that DNS space... .local, .gnu, .onion started out like that.

2. IETF RFC6761 Special Names

The IETF used a provision from the IETF/ICANN MoU [RFC2860] section 4.3 that says that "(a) assignments of domain names for technical uses" is to be considered the purview of IETF (as in, outside of the scope of ICANN) in order to create a way to reserve such names in a list of "special names". That process is documented in [RFC6761] (which curiously does not directly refer the IETF/ICANN MoU). It was first applied for .local and more recently for .onion. When that process was put in place, it was thought it would only be used a handful of times. However, a large number of applications have since been made to the IETF. The .onion evaluation took almost a year and has started a massive (and often heated) discussion in the IETF.

This [RFC6761] process to reserve special name has a number of issues, that can be grouped in two categories:

- o Issues with [RFC6761] itself, including issues discovered during the evaluation of .onion

- o Higher level issues regarding candidate string evaluation and relationship with ICANN

3. Issues with 6761

1. It can be use to reserve any names, not just TLDs. For example, it could potentially be used to forbid a registrar to register specific names in any TLD.

2. [RFC6761] does not mention if the protocol for which it is requested to reserve a string should be published as an RFC document. Most applications have, so far, come from outside organizations, and the described protocols that have not been developed by the IETF.

3. [RFC6761] does not provide clear enough direction as to what party is responsible for carrying out the evaluation.

4. There are ambiguities and no formal criteria on how the IETF can (or even whether the IETF should) evaluate the merits of applicants to [RFC6761] reservations. Section 5 of [RFC6761] describes seven questions to be answered by an applicant for [RFC6761] status. However, running this process for the .onion application showed that those seven questions are inadequate for making the determination for whether a particular strings qualifies as requiring special/different treatment.

5. Placing a string in the [RFC6761] registry does not guarantee that DNS queries for names within a reserved domain will not be sent over the Internet. As such, the applicant for [RFC6761] status cannot be guaranteed that leakage will not occur and will need to take this into account in the protocol design. Useful reservations of top-level domains should be accompanied by documentation of realistic expectations of each of the seven audiences, and the evaluation of particular requests should consider the practical likelihood of those expectations being met and the implications if they are not.

6. The [RFC6761] registry lists the reserved names but does not include direct guidance, neither in free text form nor in machine readable instructions, for any of the seven audiences, relying instead upon a reference for each entry in the Registry to the

document that requested its insertion. Such documents might well be opaque to many readers; [RFC6762] is a seventy-page protocol specification, for example, which is arguably not the most effective way to set expectations of non-technical end-users

4. Candidate string evaluation and relationship with ICANN

1. IETF does not have process to evaluate the proposed strings candidate to [RFC6761] status for things like trademark, IPR, name collision, etc.. Instead, the IETF relies on document reviews, working group and IETF-wide last call, and ultimately a decision is made by the IESG. That decision can be appealed, first to the IAB and second to the ISOC board of trusties.

2. The IETF "review" process is not foolproof. [RFC7788] describing the "home networking control protocol" was recently published. That document includes text instructing devices to use names terminating by default with the .home suffix. [RFC7788] did not reference [RFC6761] anywhere and had no IANA sections about this reservation. It was published without anyone noticing this during the entire review process. The issue was caught after the publication, and an errata was published.

3. There exists now at least 2 streams to take strings out of the global namespace: IETF RFC6761 "special names" and ICANN "gTLD program" (see [NEW-GTLD]). It is important to observed that the IETF RFC6761 reservations could happen in a ad-hoc fashion at any time, while ICANN delegations typically happen in batches, and the latest gTLD round is closed. Note: the ICANN gTLD application process is described in the applicant guide book [GUIDEBOOK].

4. The major risk is having a conflict when both the IETF and ICANN want to use the same or similar strings. There exist no defined cooperation between ICANN and IETF to avoid this problem.

5. There might be limited concerns if IETF were to reserve a string outside of an ICANN gTLD round. The next ICANN gTLD applicant book would simply refer to the existing list at publication time. However, there is a possibility of conflict if an IETF reservation were to happen during an ICANN gTLD round. A hypothetical case study could be somebody trying a denial of service attack early in the ICANN application process by asking the IETF to reserved a string sought after by a competitor.

5. Security Considerations

This document aims to provide a problem statement that will inform future work. While security and privacy are fundamental considerations, this document expects that future work will include such analysis, and hence no attempt is made to do so here. See among other places [SAC-057]

Reserving names has been presented as a way to prevent leakage into the DNS. However, instructing resolvers to not forward the queries (and/or by instructing authoritative servers not to respond) is not a guarantee that such leakage will be prevented. The security (or privacy) of an application MUST NOT rely on names not being exposed to the Internet DNS resolution system.

6. IANA Considerations

This document has no IANA actions.

7. Acknowledgements

Thanks to Paul Hoffman for a large amount of editing.

8. References

8.1. Normative References

[IANA-SPECIAL-USE]
IANA, "Special-Use Domain Names", 2016, <https://www.iana.org/assignments/special-use-domain-names>.

[RFC2860] Carpenter, B., Baker, F., and M. Roberts, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority", RFC 2860, DOI 10.17487/RFC2860, June 2000, <http://www.rfc-editor.org/info/rfc2860>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <http://www.rfc-editor.org/info/rfc6761>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <http://www.rfc-editor.org/info/rfc6762>.

[RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", RFC 7788, DOI 10.17487/RFC7788, April 2016, <http://www.rfc-editor.org/info/rfc7788>.

8.2. Informative References

[GUIDEBOOK]
ICANN, "gTLD Application Guidebook", June 2012, <https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf>.

[HUSTON] Huston, G., "What's in a Name?", December 2015, <http://www.circleid.com/posts/20151222_whats_in_a_name/>.

[I-D.lewis-domain-names]
Lewis, E., "Domain Names", draft-lewis-domain-names-02 (work in progress), January 2016.

[NEW-GTLD]
ICANN, "New Generic Top-Level Domains", 2016, <https://newgtlds.icann.org/>.

[SAC-057] ICANN Security and Stability Advisory Committee, "SSAC Advisory on Internal Name Certificates", March 2013, <https://www.icann.org/en/system/files/files/sac-057-en.pdf>.

Appendix A. Editorial Notes

This section (and sub-sections) to be removed prior to publication.

A.1. Venue

An appropriate forum for discussion of this draft is for now the DNSOP WG.

A.2. Change History

A.2.1. draft-adpkja-special-names-problem-00

Initial draft circulated for comment.

Appendix B. Change history

[RFC Editor: Please remove this section before publication]

-01 to -02:

- o A very large number of readability / grammar / reference fixes from Paul Hoffman.

-00 to -01:

- o Significant readability changes.

-00:

- o Initial draft circulated for comment.

Authors' Addresses

Geoff Huston
APNIC

Email: gih@apnic.net

Peter Koch
DENIC eG
Kaiserstrasse 75-77
Frankfurt 60329
Germany

Email: pk@denic.de

Alain Durand
ICANN

Email: alain.durand@icann.org

Warren Kumari
Google

Email: warren@kumari.net