dnsop
Internet-Draft
Intended status: Informational
Expires: January 17, 2019

W. Kumari
Google
A. Sullivan
Oracle

July 16, 2018

The ALT Special Use Top Level Domain
draft-ietf-dnsop-alt-tld-10

Abstract

This document reserves a string (ALT) to be used as a TLD label in non-DNS contexts. It also provides advice and guidance to developers developing alternative namespaces.

[Ed note: Text inside square brackets ([]) is additional background information, answers to frequently asked questions, general musings, etc. They will be removed before publication. This document is being collaborated on in Github at: https://github.com/wkumari/draft-wkumari-dnsop-alt-tld. The most recent version of the document, open issues, etc should all be available here. The authors (gratefully) accept pull requests.]

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any 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 January 17, 2019.

Table of Contents

1. Introduction

Many protocols and systems need to name entities. Names that look like DNS names (a series of labels separated with dots) have become common, even in systems that are not part of the global DNS administered by IANA. This document reserves the label "ALT" (short for "Alternative") as a Special Use Domain ([RFC6761]). This label is intended to be used as the final (rightmost) label to signify that the name is not rooted in the DNS, and that it should not be resolved using the DNS protocol.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Terminology

This document assumes familiarity with DNS terms and concepts. Please see [RFC1034] for background and concepts, and [RFC7719] for terminology. Readers are also expected to be familiar with the discussions in [I-D.ietf-dnsop-sutld-ps]

- DNS name: Domain names that are intended to be used with DNS resolution, either in the global DNS or in some other context
- DNS context: The namespace anchored at the globally-unique DNS root. This is the namespace or context that "normal" DNS uses.
- non-DNS context: Any other (alternative) namespace.
- pseudo-TLD: A label that appears in a fully-qualified domain name in the position of a TLD, but which is not registered in the global DNS. This term is not intended to be pejorative.
- TLD: The last visible label in either a fully-qualified domain name or a name that is qualified relative to the root. See the discussion in Section 2.

2. Background

The success of the DNS makes it a natural starting point for systems that need to name entities in a non-DNS context.

In many cases, these systems build a DNS-style tree parallel to, but separate from, the global DNS. They often use a pseudo-TLD to cause resolution in the alternative namespace, using browser plugins, shims in the name resolution process, or simply applications that perform special handling of this particular alternative namespace. An example of such a system is the Tor network's [Dingledine2004] use of the ".onion" Special-Use Top-Level Domain Name (see [RFC7686]).

In many cases, the creators of these alternative namespaces have chosen a convenient or descriptive string and started using it. These strings are not registered anywhere nor are they part of the DNS. However, to users and to some applications, they appear to be TLDs; and issues may arise if they are looked up in the DNS. This document suggests that name resolution libraries (stub resolvers) recognize names ending in ".alt" as special, and not attempt to look them up using the DNS protocol in order to limit the effects of queries accidentally leaking into the DNS.

The techniques in this document are primarily intended to address the "Experimental Squatting Problem", the "Land Rush Problem" and "Name

Collisions" issues discussed in [I-D.ietf-dnsop-sutld-ps] (which contains much additional background, etc).

3. The ALT namespace

This document reserves the ALT label, using the [RFC6761] process, for use as an unmanaged pseudo-TLD namespace. The ALT label MAY be used in any domain name as a pseudo-TLD to signify that this is an alternative (non-DNS) namespace, and should not be looked up in a DNS context.

Alternative namespaces should differentiate themselves from other alternative namespaces by choosing a name and using it in the label position just before the pseudo-TLD (ALT). For example, a group wishing to create a namespace for Friends Of Olaf might choose the string "foo" and use any set of labels under foo.alt.

As names beneath ALT are in an alternative namespace, they have no significance in the regular DNS context and so should not be looked up in the DNS context.

Groups wishing to create new alternative namespaces may create their alternative namespace under a label that names their namespace under the ALT label. They should attempt to choose a label that they expect to be unique and, ideally, descriptive. There is no IANA registry for names under the ALT TLD - it is an unmanaged namespace, and developers are responsible for dealing with any collisions that may occur under .alt. Informal lists of namespaces under .alt may be created to assist the developer community.

Currently deployed projects and protocols that are using pseudo-TLDs may choose to move under the ALT TLD, but this is not a requirement. Rather, the ALT TLD is being reserved so that current and future projects of a similar nature have a designated place to create alternative resolution namespaces that will not conflict with the regular DNS context.

3.1. Choice of the ALT Name

A number of names other than "ALT" were considered and discarded. While these are not DNS names, in order for this technique to be effective the names need to continue to follow both the DNS format and conventions (a prime consideration for alternative name formats is that they can be entered in places that normally take DNS context names); this rules out using suffixes that do not follow the usual letter, digit, and hyphen label convention.

A short label was deemed desirable for a number of reasons, including:

- this is a switch to other resolution contexts, some which may have long labels (for example derived from public keys).
- some queries will undoubtedly leak into the DNS. As many of these alternate resolution systems are specifically designed for privacy, limiting how far they leak is desirable.
- as there are not protocol police, the label needs to be attractive to implementors of alternate resolution contexts so that they are willing to use this.

4. IANA Considerations

The IANA is requested to add the ALT string to the "Special-Use Domain Name" registry ([RFC6761], and reference this document.

4.1. Domain Name Reservation Considerations

This section is to satisfy the requirement in Section 5 of RFC6761.

The string ".alt." (and names ending with the string .alt) are special in the following ways:

1. Users are expected to know that strings that end in .alt behave differently to normal DNS names. Users are expected to have applications running on their machines that intercept strings of the form <namespace>.alt and perform special handing of them, or that applications themselves will recognize the strings as special, and perform special handling. If the user tries to resolve a name of the form <namespace>.alt without the <namespace> plugin installed (or in the wrong application), the request will leak into the DNS, receive a negative response, and the resolution will fail.

2. Writers of application software that implement a non-DNS namespace are expected to intercept names of the form <namespace>.alt and perform application specific handing with them. Other applications are not required to perform any special handing (but may choose to provide helpful informational messages if able).

3. Writers of name resolution APIs and libraries which operate in the DNS context should not attempt to look these names up in the DNS. If developers of other namespaces implement their namespace

through a "shim" or library, they will need to intercept and perform their own handling.

4. Caching DNS servers SHOULD NOT recognize these names as special and should not perform any special handling with them.

5. Authoritative DNS servers SHOULD NOT recognize these names as special and should not perform any special handling with them.

6. DNS server operators SHOULD be aware that queries for names ending in .alt are not DNS names, and were leaked into the DNS context (for example, by a missing browser plugin). This information may be useful for support or debugging purposes.

7. DNS Registries/Registrars MUST NOT grant requests to register ".alt" names in the normal way to any person or entity. These ".alt" names are defined by protocol specification to be nonexistent, and they fall outside the set of names available for allocation by registries/registrars.

Earlier versions of this document requested that .ALT be added to the "Locally Served Zones" registry, and that a DNSSEC insecure delegation (a delegation with no DS record) be created at the root. Significant discussion on the DNSOP list (and an interim meeting) generated the consensus that these names are specifically not DNS names, and that them leaking into the DNS is an error. This means that the current (non-delegated) response of NXDOMAIN is correct as there is no DNS domain .alt, and so the document was updated to remove these requests.

5. Privacy Considerations

This document reserves ALT to be used to indicate that a name is not a DNS name, and so should not attempt to be resolved using the DNS. Unfortunately, these queries will undoubtedly leak into the DNS - for example, a user may receive an email containing a hostname which should be resolved using a specific resolution context (implemented by a specific application or resolution mechanism). If the user does not have that particular application installed (and their stub resolver library has not been updated to ignore queries for names ending in .alt), it is likely that this will instead be resolved using the DNS. This DNS query will likely be sent to the configured iterative resolver. If this resolver does not have a cache entry for this name (or, if the resolver implements [I-D.ietf-dnsop-nsec-aggressiveuse], a entry for .alt) this query will likely be sent to the DNS root servers. This exposes the (leaked) query name to the operator of the resolver, the operator of the queried DNS root server, and anyone watching queries along the

path. This is a general problem with alternative name spaces and not confined to names ending in .alt.

6. Security Considerations

One of the motivations for the creation of the .alt pseudo-TLD is that unmanaged labels in the managed root name space are subject to unexpected takeover. This could occur if the manager of the root name space decides to delegate the unmanaged label.

The unmanaged and "registration not required" nature of labels beneath .alt provides the opportunity for an attacker to re-use the chosen label and thereby possibly compromise applications dependent on the special host name.

7. Acknowledgements

We would like to thank Joe Abley, Mark Andrews, Marc Blanchet, John Bond, Stephane Bortzmeyer, David Cake, David Conrad, Steve Crocker, Brian Dickson, Ralph Droms, Robert Edmonds, Patrik Faltstrom, Olafur Gudmundsson, Bob Harold, Paul Hoffman, Joel Jaeggli, Ted Lemon, Edward Lewis, John Levine, George Michaelson, Ed Pascoe, Jim Reid, Arturo Servin, Paul Vixie, Suzanne Woolf for feedback.

Christian Grothoff was also very helpful.

8. References

8.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6303] Andrews, M., "Locally Served DNS Zones", BCP 163, RFC 6303, DOI 10.17487/RFC6303, July 2011, <https://www.rfc-editor.org/info/rfc6303>.

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

[RFC7686] Appelbaum, J. and A. Muffett, "The ".onion" Special-Use Domain Name", RFC 7686, DOI 10.17487/RFC7686, October 2015, <https://www.rfc-editor.org/info/rfc7686>.

[RFC7719] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 7719, DOI 10.17487/RFC7719, December 2015, <https://www.rfc-editor.org/info/rfc7719>.

8.2. Informative References

[Dingledine2004]
Dingledine, R., Mathewson, N., and P. Syverson, "Tor: The Second-Generation Onion Router", , 8 2004, <<https://svn.torproject.org/svn/projects/design-paper/tor-design.html>>.

[I-D.ietf-dnsop-nsec-aggressiveuse]
Fujiwara, K., Kato, A., and W. Kumari, "Aggressive use of DNSSEC-validated Cache", draft-ietf-dnsop-nsec-aggressiveuse-10 (work in progress), May 2017.

[I-D.ietf-dnsop-sutld-ps]
Lemon, T., Droms, R., and W. Kumari, "Special-Use Domain Names Problem Statement", draft-ietf-dnsop-sutld-ps-08 (work in progress), August 2017.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

From -07 to -08:

- Made it clear that this is only for non-DNS.
- As per Interim consensus, removed the "add this to local zones" text.
- Added a Privacy Considerations section
- Grammar fix -- "alternative" is more correct than "alternate", replaced.

From -06 to -07:

- Rolled up the GItHub releases in to a full release.

From -07.2 to -07.3 (GitHub point release):

Removed 'sandbox' at Stephane's suggestion - https://www.ietf.org/mail-archive/web/dnsop/current/msg18495.html

Suggested (in 4.1 bullet 3) that DNS libraries ignore these -- Bob Harold - https://mailarchive.ietf.org/arch/msg/dnsop/a_ruPf8osSzi_hCzCqOxYLXhYoA

Added some pointers to the SUTLD document.

From -07.1 to -07.2 (Github point release):

- Reverted the <TBD> string (at request of chairs).
- Added an editors note explaining the above.
- Removed some more background, editorializing, etc.

From -06 to -07.1 (https://github.com/wkumari/draft-wkumari-dnsop-alt-tld/tree/7988fcf06100f7a17f21e6993b781690b5774472):

- Replaced ALT with <TBD> at the suggestions of George.

From -05 to -06:

- Removed a large amount of background - we now have the (adopted) tldr document for that.
- Made it clear that pseudo-TLD is not intended to be pejorative.
- Tried to make it cleat that this is something people can choose to use - or not.

From -04 to -05:

- Version bump - we are waiting in the queue for progress on SUN, bumping this to keep it alive.

From -03 to -04:

- 3 changes - the day, the month and the year (a bump to keep alive).

From -02 to -03:

- Incorporate suggestions from Stephane and Paul Hoffman.

From -01 to -02:

- Merged a bunch of changes from Paul Hoffman. Thanks for sending a git pull.

From -00 to 01:

- Removed the "delegated to new style AS112 servers" text -this was legacy from the omnicient AS112 days. (Joe Abley)

- Removed the "Advice to implemntors" section. This used to recommend that people used a subdomain of a domain in the DNS. It was pointed out that this breaks things badly if the domain expires.

- Added text about why we don't want to adminster a registry for ALT.

From Individual-06 to DNSOP-00

- Nothing changed, simply renamed draft-wkumari-dnsop-alt-tld to draft-ietf-dnsop-alt-tld

From -05 to -06

- Incorporated comments from a number of people, including a number of suggestion heard at the IETF meeting in Dallas, and the DNSOP Interim meeting in May, 2015.

- Removed the "Let's have an (optional) IANA registry for people to (opportinistically) register their string, if they want that option" stuff. It was, um, optional....

From -04 to -05

- Went through and made sure that I'd captured the feedback received.

- Comments from Ed Lewis.

- Filled in the "Domain Name Reservation Considerations" section of RFC6761.

- Removed examples from .Onion.

From -03 to -04

- Incorporated some comments from Paul Hoffman

From -02 to -03

- After discussions with chairs, made this much more generic (not purely non-DNS), and some cleanup.

From -01 to -02

- Removed some fluffy wording, tightened up the language some.

From -00 to -01.

- Fixed the abstract.

- Recommended that folk root their non-DNS namespace under a DNS namespace that they control (Joe Abley)

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Andrew Sullivan
Oracle
150 Dow Street
Manchester, NH 03101
US

Email: asullivan@dyn.com