Network Working Group
Internet-Draft
Intended status: Experimental
Expires: January 16, 2014

W. Kumari
Google

July 15, 2013

A questionable method for mitigating namespace collisions
draft-wkumari-dnsop-defense-collision-mitigate-01

Abstract

This document outlines a method to mitigate the effect of collisions in the DNS namespace by providing a means for end users to disambiguate the conflict.

I am publishing this to maybe establish prior art, but not to have anyone implement it.

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 http://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 16, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction / Background 2
2. Mitigation 2
3. Implementation / Disclaimers 3
4. IANA Considerations 4
5. Security Considerations 4
6. Acknowledgements 4
7. References 4
Appendix A. Changes / Author Notes. 4
Author's Address 4

1. Introduction / Background

Collisions in the DNS occur in multiple ways; one common case is that an organization has used an sub-domain (foo) of their primary domain (example.com) for corporate infrastructure, and then the string "foo" is delegated as a TLD. When a employee of the organization enters 'www.foo', are they trying to reach a machine in the internal namespace (www.foo.example.com) or the hostname 'www' in the 'foo' TLD?

This document describes a means of disambiguating these, and similar cases.

Implementation of these methods are not recommended; they are documented here for defensive purposes / to ensure that if one organization decides to implement it, others can as well.

2. Mitigation

The mitigation described in this document involves presenting the multiple options to the user, and allowing them to indicate which of the names is the one they were trying to reach, and then connecting to that.

This could be accomplished in a number of ways, including:

Intercepting the resolution requests from the application in a "shim" type library

Replacing the resolver library entirely

Integrating this type of mitigation into applications (some web browsers already do something similar to this)

Running a resolver locally on the workstation / host that return the address of a proxy.

The mitigation would lookup the name in multiple namespaces, and if a conflict is detected, it would then provide a means for the user to indicate which one of the colliding names they wish to connect to, and return the disambiguated answer to the application. An additional feature could be for the described mitigation to cache the user's choice, and / or provide a means to set priorities.

There are a number of issues with this solution, including but not limited to:

- There may not be a human available to disambiguate the answer (unattended machines, mail servers, etc.).
- The human / user may have no idea which is the correct choice.
- The additional latency introduced may cause the originating application to time out.
- The user experience will almost definitely be horrid.

For these reasons, implementation of this technique is NOT RECOMMENDED.

3. Implementation / Disclaimers

This document does not reference an implementation as it is unclear if the idea is worth implementing - this document exists primarily so that searches for prior-art will find this, and to prevent nefarious deeds. The idea itself may be / probably is horrendous, but if anyone wants to give it a whirl, everyone should be able to give it a whirl.

This is a very slight mitigation.

It should not be viewed as a solution to the "namespace collision" issue.

4. IANA Considerations

This document contains no IANA considerations.

5. Security Considerations

Yes, there probably are some. Don't do this then.

6. Acknowledgements

The authors wish to thank some folk, including Tarquin Ole-Biscuitbarrel.

7. References

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication.]

From -00 to -01.

o Nothing changed in the template!

Author's Address

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

Email: warren@kumari.net