Domain Name System Operations
Internet-Draft
Intended status: Informational
Expires: November 05, 2015

J. Livingood
Comcast

May 6, 2015

In Case of DNSSEC Validation Failures, Do Not Change Resolvers
draft-livingood-dnsop-dont-switch-resolvers-02

Abstract

DNS Security Extensions (DNSSEC) are being widely deployed, particularly via validating resolvers. However, domain signing tools and processes are not yet as mature and reliable as is the case for non-DNSSEC-related domain administration tools and processes. As a result, some DNSSEC validation failures may occur. When these failures do occur, end users should not change to a non-validating DNS resolver.

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 November 05, 2015.

Copyright Notice

Copyright (c) 2015 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

The Domain Name System (DNS), DNS Security Extensions (DNSSEC), and related operational practices are defined extensively [RFC1034] [RFC1035] [RFC4033] [RFC4034] [RFC4035] [RFC4398] [RFC4509] [RFC6781] [RFC5155].

DNSSEC has now entered widespread deployment. However, domain signing tools and processes are not yet as mature and reliable as is the case for non-DNSSEC-related domain administration tools and processes. As a result, some DNSSEC validation failures may occur. When these failures do occur, end users should not change to a non-validating DNS resolver.

2. Domain Validation Failures

A domain name can fail validation for two general reasons, an actual security failure such as due to an attack or compromise of some sort, or as a result of misconfiguration (mistake) on the part of an domain administrator. There is no way for end users to discern which of these issues has caused a DNSSEC-signed domain to fail validation, and end users should therefore assume that it may be due to an actual security problem.

3. Misunderstanding DNSSEC Validation Failures

End users may incorrectly interpret the failure to reach a domain due to DNSSEC-related misconfiguration as their ISP or DNS resolver operator purposely blocking access to the domain, or as a performance-related failure on the part of their ISP. In reality,

these failures may be due to a security issue of which the end user is not aware.

4. Comparison to Other DNS Misconfigurations

Authoritative DNS-related mistakes and errors typically affect the entire Internet, and all DNS recursive resolver operators equally. So for example, in an A record is incorrect, an end user would get the incorrect record in a DNS response no matter what resolver they used.

In contrast to this, DNSSEC-related mistakes, errors, or validation security failures would only affect end users of validating resolvers.

5. Switching to a Non-Validating Resolver is NOT Recommended

As noted in Section 3 some end users may not understand why a domain fails to validate on one network but not another (or with one DNS resolver but not another) Section 4. As a result, they may consider switching to an alternative, non-validating resolver themselves. But if a domain fails DNSSEC validation and is inaccessible, this could very well be due to a security-related issue. Changing to a non-validating resolver is a critical security downgrade and is not well advised.

As a recommended best practice: In order to be as safe and secure as possible, end users should not change to DNS servers that do not perform DNSSEC validation as a workaround.

Even if a website in a domain seems to look "normal" and valid, according to the DNSSEC protocol, that domain is not secure. Domains that fail DNSSEC validation may fail due to an actual security incident or compromise, and may be in control of hackers or there could be other significant security issues with the domain. Thus, switching to a non-validating resolver to restore access to a domain that fails DNSSEC validation is NOT recommended and is potentially harmful to end user security.

6. Other Considerations

6.1. Security Considerations

The use of a non-validating DNS recursive resolver has comparatively less security capabilities than a validating resolver, since one implements DNS Security Extensions and one does not.

In the case of a DNSSEC validation failure, if an end user changes to a non-validating resolver they may subject themselves to increased security risks and threats against which DNS Security Extensions may have provided protection.

6.2. Recommendations for Validating Resolver Operators

Since it is not recommended that end users change to non-validating resolvers, operators of validating resolvers may wish to consider what tools they might make available to their end users to assist in these cases. For example, there may be a DNS looking glass that enables someone to use a web page or other tool to remotely check DNS resolution on the operator's servers, as well as possibly another operator's servers. Such a web page or tool may also provide a link to independent third party sites or tools that can confirm whether or not a DNSSEC-related error is present, of which several exist today (e.g. DNSViz [1], Verisign DNSSEC Debugger [2]). Finally, the operator may also wish to consider a web page form or other tool to enable end users to report possible DNS resolution issues.

6.3. Privacy Considerations

There are no privacy considerations in this document.

6.4. IANA Considerations

There are no IANA considerations in this document.

7. Acknowledgements

- William Brown

- Peter Koch

8. References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4398] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", RFC 4398, March 2006.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

[RFC5155] Laurie, B., Sisson, G., Arends, R. and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

[RFC5914] Housley, R., Ashmore, S. and C. Wallace, "Trust Anchor Format", RFC 5914, June 2010.

[RFC6781] Kolkman, O., Mekking, W. and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, December 2012.

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]

Individual-00: First version published as an individual draft.

Individual-01: Fixed nits identified by William Brown

Individual-02: Updated prior to IETF-91

WG-00: Renamed at request of DNSOP co-chairs

WG-01: Updated doc to keep it from expiring

WG-02: Addressed some feedback from Peter Koch on RFC 2119 text, changed from BCP to Informational since this is more a recommended practice, added a section with recommendations for operators.

Appendix B. Open Issues

[RFC Editor: This section is to be removed before publication]

Author's Address

Jason Livingood
Comcast
One Comcast Center
1701 John F. Kennedy Boulevard
Philadelphia, PA 19103
US

Email: jason_livingood@cable.comcast.com
URI: http://www.comcast.com