Responsibility for Authoritative DNS and DNSSEC Mistakes
draft-livingood-dnsop-auth-dnssec-mistakes-05

Abstract

DNS Security Extensions (DNSSEC) validation by recursive DNS resolvers has been deployed at scale. 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. This sometimes results in DNSSEC-validation failures, for which operators of validating resolvers are often blamed. This is similar to other, non-DNSSEC-related authoritative DNS errors, for which individual recursive DNS operators are sometimes incorrectly blamed. This document makes clear that responsibility for any and all authoritative DNS failures rests squarely with authoritative domain name operators, who are the only party that can properly maintain their domain names and rectify associated authoritative DNS errors.

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 February 14, 2020.

Copyright Notice

Copyright (c) 2019 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
1. Introduction

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

DNS Security Extensions (DNSSEC) validation by recursive DNS resolvers has been deployed at scale. 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. This sometimes results in DNSSEC-validation failures, for which operators of validating resolvers are often blamed. This is similar to other, non-DNSSEC-related authoritative DNS errors, for which individual recursive DNS operators are sometimes incorrectly blamed. This documents makes clear that responsibility for any and all authoritative DNS failures rests squarely with authoritative domain name operators, who are the only party that can properly maintain their domain names and rectify associated authoritative DNS errors.

Operators of DNS recursive resolvers, including Internet Service Providers (ISPs) and cloud-based DNS resolvers, occasionally observe
domains incorrectly managing DNSSEC-related resource records. This mismanagement triggers DNSSEC validation failures, and then causes large numbers of end users to be unable to reach a domain. Similarly, errors in non-DNSSEC-related authoritative DNS resource records result in failures, from NXDOMAIN responses to valid responses containing outdated or unreachable hosts.

Many end users, as well as reporters, policymakers, regulators, and others often interpret this as a failure of particular recursive DNS resolvers. Rather than seeing this as a failure on the part of the domain they wanted to reach, they may themselves and/or recommend to others that they switch to a non-validating resolver (which reduces their security), switch to a different DNS resolver (which can reduce non-DNS application layer performance), or contact their ISP or DNS resolver operator to complain.

This document makes clear, however, that responsibility for these types of authoritative DNS failures rests squarely with authoritative domain name operators, as noted in Section 3.

2. Domain Validation Failures

A domain name can fail validation for two general reasons, a legitimate security failure such as due to an attack or compromise of some sort, or as a result of misconfiguration or other error or omission on the part of a domain administrator. As domains transition to DNSSEC the most likely reason for a validation failure during and shortly after the transition is likely due to misconfiguration. Thus, domain administrators should be sure to read [RFC6781] in full. They should also pay special attention to Section 4.2, pertaining to key rollovers, which appears to be the cause of many validation failures.

In one example [DNSSEC-Validation-Failure-Analysis], a specific domain name failed to validate. An investigation revealed that the domain’s administrators performed a Key Signing Key (KSK) rollover by (1) generating a new key and (2) signing the domain with the new key. However, they did not use a double-signing procedure for the KSK and a pre-publish procedure for the ZSK. Double-signing refers to signing a zone with two KSKs and then updating the parent zone with the new DS record so that both keys are valid at the same time. This meant that the domain name was signed with the new KSK, but it was not double-signed with the old KSK. So, the new key was used for signing the zone but the old key was not. As a result, the domain could not be trusted and returned an error when trying to reach the domain. Thus, the domain was in a situation where the DNSSEC chain of trust was broken because the Delegation Signer (DS) record pointed to the old KSK, which was no longer used for signing the zone. (A DS
record provides a link in the chain of trust for DNSSEC from the parent zone to the child zone - in this case between TLD and domain name.)

In a non-DNSSEC-related example, a domain administrator may add a new host with an A and AAAA resource record pointing the name to the IP addresses of new servers with a Time To Live (TTL) of two days. But they may turn down the old servers with a similar two day TTL before that TTL has expired. As a result, some number of users are likely to continue to attempt to connect to the old IP addresses that are no longer reachable. While a best practice is to reduce the TTL to a matter of seconds or minutes before such a shift, many domains continue to forget the impact that the TTL can have, or make countless other errors in their domain name, server, and network administration that negatively impacts domain name-based reachability.

3. Responsibility for Failures

An authoritative domain owner is solely and completely responsible for managing their domain name(s) and associated DNS resource records. This includes complete responsibility for the correctness of those resource records, the proper functioning and reachability of their authoritative DNS servers, and the correctness of DNS records linking their domain to a top-level domain (TLD) or other higher level domain. The domain owner is also responsible for selection of the authoritative domain administrator, operator, or service provider. Thus, even in cases where some error may be introduced by a third party, whether that is due to an authoritative server software vendor, software tools vendor, domain name registrar, Content Delivery Network (CDN), or other organization, these are all parties that the domain owner has selected and is responsible for managing successfully.

There are some cases where the domain administrator is different than the domain owner. In those cases, a domain owner has delegated operational responsibility to the domain administrator (and that domain administrator may further delegate some sub-domains and/or records to another party, such as a CDN). So no matter whether a domain owner is also the domain administrator or not, the domain owner and domain administrator are nevertheless operationally responsible for the proper configuration and operation of the domain name.

In the case of a domain name failing DNSSEC validation, even when this is due to a misconfiguration of the domain, that is the sole responsibility of the domain owner.
Any assistance or mitigation responses undertaken by other parties to mitigate the misconfiguration of a domain name by a domain owner and/or administrator, especially operators of DNS recursive resolvers, are optional and at the pleasure of those parties. This can the use of a Negative Trust Anchor [RFC7646] and/or clearing the cache in particular DNS resolvers.

4. Comparison to Other DNS Misconfigurations

As noted in Section 3 domain administrators are ultimately responsible for managing and ensuring their DNS records are configured correctly. ISPs or other DNS recursive resolver operators cannot and should not correct misconfigured A, CNAME, MX, or other resource records of domains for which they are not authoritative. Expecting non-authoritative entities to protect domain owners and administrators from any misconfiguration of resource records is therefore unrealistic and unreasonable, does not scale well, and is strongly contrary to the delegated design of the DNS and could lead to extensive operational instability and/or variation.

5. Other Considerations

5.1. Security Considerations

Authoritative domain name owners and/or administrators, in the case of DNSSEC-related mistakes that cause validation failures to occur, should focus on correcting the immediate authoritative DNS issue and then improving their processes and tools in the future.

During the period of time that their domain cannot be resolved due to a DNSSEC-related mistake, they SHOULD NOT encourage end users to switch to non-validating resolvers [I-D. draft-livingood-dnsop-dont-switch-resolvers].

5.2. Privacy Considerations

In the case of a DNSSEC validation failure, if an end user changes to a non-validating resolver they can subject themselves to increased security risks and threats against which DNSSEC may have provided protection. This can include threats to their privacy, such as by unwittingly visiting a phishing site and sharing sensitive data or other private information with a malicious party or some party other than that which was originally intended.

As a result, in order to protect their privacy, users SHOULD NOT switch to a non-validating resolver when a DNSSEC validation failure occurs [I-D. draft-livingood-dnsop-dont-switch-resolvers].
5.3. IANA Considerations

There are no IANA considerations in this document.

6. Acknowledgements

- William Brown

7. References

7.1. Normative References


7.2. Informative References

[DNSSEC-Validation-Failure-Analysis]  

[I-D.livingood-dnsop-dont-switch-resolvers]  
Livingood, J., "In Case of DNSSEC Validation Failures, Do Not Change Resolvers", draft-livingood-dnsop-dont-switch-resolvers-03 (work in progress), November 2015.

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: Removed RFC 2119 reference in XML

WG-03 to 04: Refreshed draft and broadened to all auth issues, not just DNSSEC.

WG-05: Refreshed to buy time for me to write a combined document
Appendix B. Open Issues

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

Fix I-D xref

Author’s Address

Jason Livingood
Comcast

Email: jason_livingood@comcast.com