DNSOP
Internet-Draft
Intended status: Standards Track
Expires: April 5, 2018

G. Huston
J. Damas
APNIC

October 2, 2017

A Sentinel for Detecting Trusted Keys in DNSSEC
draft-huston-kskroll-sentinel-00.txt

Abstract

The DNS Security Extensions (DNSSEC) were developed to provide origin authentication and integrity protection for DNS data by using digital signatures. These digital signatures can be verified by building a chain of trust starting from a trust anchor and proceeding down to a particular node in the DNS. This document specifies a mechanism that will allow an end user to establish the trusted key state of the resolvers that handle the user's DNS queries. This allows users to discover the trusted key state used by their DNS resolution service.

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 April 5, 2018.

Table of Contents

1. Introduction

The DNS Security Extensions (DNSSEC) [RFC4033]", [RFC4034] and [RFC4035] were developed to provide origin authentication and integrity protection for DNS data by using digital signatures. DNSSEC uses Key Tags to efficiently match signatures to the keys from which they are generated. The Key Tag is a 16-bit value computed from the RDATA portion of a DNSKEY RR using a formula not unlike a ones-complement checksum. RRSIG RRs contain a Key Tag field whose value is equal to the Key Tag of the DNSKEY RR that validates the signature.

This document specifies how validating resolvers should respond to certain queries so that a user can deduce whether a key has been loaded into a resolver's trusted key store. This mechanism can be used to determine whether a certain Root Zone KSK is ready to be used as a trusted key within the context of a key roll.

This new mechanism is OPTIONAL to implement and use, although for reasons of supporting broad based measurement techniques, it is strongly preferred if configurations of DNSSEC-vbalidating resolvers enabled this mechanism by default, allowing for configuration directives to disable this mechanism if desired.

1.1. Terminology

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 RFC 2119.

2. Sentinel Mechanism

DNSSEC-Validating resolvers that implement this mechanism MUST be performing validation of responses in accordance with the DNSSEC response validation specification [RFC4035].

If the outcome of the DNS response validation process indicates that the response is authentic, and if the original query contains exactly one label that matches the template ".is-ta-<tag-index>.", then the following rule should be applied to the response. If the resolver has placed a Root Zone Key Signing Key with tag index value matching the value specified in the query into the local resolver's store of trusted keys, then the resolver should return a response indicatating that the response contains authenticated data according to section 5.8 of [RFC6840]. Otherwise, the resolver MUST return RCODE 2 (server failure). Note that the <tag-index> is specified in the DNS label using hex notation.

If the outcome of the DNS response validation process indicates that the response is authentic, and if the original query contains exactly one label that matches the template ".not-ta-<tag-index>.", then the following rule should be applied to the response. If the resolver has not placed a Root Zone Key Signing Key with tag index value matching the value specified in the query into the local resolver's store of trusted keys, then the resolver should return a response indicatating that the response contains authenticated data according to section 5.8 of [RFC6840]. Otherwise, the resolver MUST return RCODE 2 (server failure). Note that the <tag-index> is specified in the DNS label using hex notation.

If a query contains one instance of both of these query templates then the resolver MUST NOT alter the outcome of the DNS response validation process.

3. Sentinel Processing

[Text to be added as to how to pose queries and interpret responses]

4. Sentinel Considerations

[Text to be added about considerations relating to caching, and resolver forwarding partial deployment of the mechanism, as well as any other issues that may arise with this mechanism]

5. Security Considerations

This document describes a mechanism to allow users to determine the trust state of root zone key signing keys in the DNS resolutiojn system that they use.

The mechanism does not require resolvers to set outwise unauthenticated responses to be marked as authenticated, and does not alter the security properties of DNSSEC with respect to the interpretation of the authenticity of responses that are do marked.

The mechanism does not require any further significant processing of DNS responses, and queries of the form described in this document do not impose any additional load that could be exploited in an attack over the the normal DNSSEC validation processing load.

6. IANA Considerations

[Note to IANA, to be removed prior to publication: there are no IANA considerations stated in this version of the document.]

7. Acknowledgements

This document has borrowed extensively from RFC8145 for the introductory text, and the authors would like to acknowledge and thank the authors of that document both for some text excerpts and for the more general stimulation of thoughts about monitoring the progress of a roll of the Key Signing Key of the Root Zone of the DNS.

8. References

8.1. Normative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, <https://www.rfc-editor.org/info/rfc6840>.

8.2. Informative References

[RFC8145] Wessels, D., Kumari, W., and P. Hoffman, "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)", RFC 8145, DOI 10.17487/RFC8145, April 2017, <https://www.rfc-editor.org/info/rfc8145>.

Authors' Addresses

Geoff Huston

Email: gih@apnic.net
URI: http://www.apnic.net

Joao da Silva Damas

Email: joao@apnic.net
URI: http://www.apnic.net