DNSOP
Internet-Draft
Intended status: Standards Track
Expires: April 11, 2018

G. Huston
J. Damas
APNIC
W. Kumari
Google

October 8, 2017

A Sentinel for Detecting Trusted Keys in DNSSEC
draft-huston-kskroll-sentinel-01.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 determine the trusted key state of the resolvers that handle the user's DNS queries.

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 11, 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 can respond to certain queries in a manner that allows a querier to deduce whether a particular key has been loaded into that resolver's trusted key store. In particular, this response 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 by this resolver.

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-validating 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].

This mechanism makes use of 2 special labels, ".is-ta-<tag-index>." (Intended to be used in a query where the response can answer the question: Is this the key tag a trust anchor which the validating DNS resolver is currently trusting?) and ".not-ta-<tag-index>." (Intended to be used in a query where the response can answer the question: Is this the key tag of a key that is NOT in the resolver's current trust store?). The use of the positive question and its inverse also allows for the detection of resolvers which do not implement this mechanism.

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 indicating 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 indicating 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.

This mechanism is to be applied only by resolvers that perform DNSSEC validation, and applies only to responses to an A or AAAA query (Query Type value 1 or 28) where the resolver has authenticated the response according to the DNSSEC validation process and where the query name contains either of the labels described in this section. In this case, the resolver is to perform an additional test following the conventional validation function as described in this section. The result of this test directs whether the resolver is to change an authentic response to a response that indicates validation failure.

3. Sentinel Processing

This proposed test that uses the DNS resolver mechanism described in this document is based on three DNS names that have three distinct DNS resolution behaviours. The test is intended to allow a user to determine the state of their DNS resolution system, and, in particular, whether or not they are using validating DNS resolvers that have picked up an incoming trust anchor in a key roll.

The name format can be defined in a number of ways, and no name form is intrinsically better than any other in terms of the test itself. The critical aspect of the DNS names used in any such test is that they contain the specified label for either the positive and negative test.

The sentinel process is envisaged to use a test with three names:

a. a name containing the label ".is-ta-<tag-index>.". This is a validly signed name so that responses about names in this zone can be authenticated by a validating resolver.

b. a name containing the label ".not-ta-<tag-index>.". This is also a validly-signed name.

c. a third name that is signed with a DNSSEC signature that cannot be validated.

The responses received from queries to resolve each of these names would allow us to infer a trust key state of the resolution environment.

o Vnew: A DNSSEC-Validating resolver that includes this mechanism that has loaded the nominated key into its trusted key stash will

respond with an A record response for "is-ta", SERVFAIL for "not-ta" and SERVFAIL for the invalid name.

- o Vold: A DNSSEC-Validating resolver that includes this mechanism that has not loaded the nominated key into its trusted key stash will respond with an SERVFAIL record for "is-ta", an A record response for "not-ta" and SERVFAIL for the invalid name.

- o Vleg: A DNSSEC-Validating resolver that does not include this mechanism will respond with an A record response for "is-ta", an A record response for "not-ta" and SERVFAIL for the invalid name.

- o nonV: A non-DNSSEC-Validating resolver will respond with an A record response for "is-ta", an A record response for "not-ta" and an A record response for the invalid name.

Given the clear delineation amongst these three cases, if a client directs these three queries to a simple resolver, the variation in response to the three queries should allow the client to determine the category of the resolver, and if it supports this mechanism, whether or not it has loaded a particular key into its local trusted key stash.

Type\Query	is_ta	not_ta	invalid
Vnew	A	SERVFAIL	SERVFAIL
Vold	SERVFAIL	A	SERVFAIL
Vleg	A	A	SERVFAIL
nonV	A	A	A

A Vnew response pattern says that the nominated key is trusted by the resolver and has been loaded into its local trusted key stash. A Vleg response pattern says that the nominated key is not yet trusted by the resolver in its own right. A Vleg response is indeterminate, and a nonV response indicates that the client does not have a validating resolver.

4. Sentinel Test Result Considerations

The description in the previous section describes a simple situation where the test queries were being passed to a single recursive resolver that directly queried authoritative name servers, including the root servers.

There is also the common case where the end client is configured to use multiple resolvers. In these cases the SERVFAIL responses from one resolver will prompt the end client to repeat the query against one of the other configured resolvers.

If any of the client's resolvers are non-validating resolvers, the tests will result in the client reporting that it has a non-validating DNS environment (nonV), which is effectively the case.

If all of the client resolvers are DNSSEC-validating resolvers, but some do not support this trusted key mechanism, then the result will be indeterminate with respect to trusted key status (Vleg). Simlarly, if all the client's resolvers support this mechanism, but some have loaded the key into the trusted key stash and some have not, then the result is indeterminate (Vleg).

There is also the common case of a recursive resolver using a forwarder.

If the resolver is non-validating, and it has a single forwarder clause, then the resolver will presumably mirror the capabilities of the forwarder target resolver. If this non-validating resolver it has multiple forwarders, then the above considerations will apply.

If the validating resolver has a forwarding configuration, and uses the CD flag on all forwarded queries, then this resolver is acting in a manner that is identical to a standalone resolver. The same consideration applies if any one one of the forwarder targets is a non-validating resolver. Similarly, if all the forwarder targets do not apply this trusted key mechanism, the same considerations apply.

A more complex case is where the following conditions all hold:

- both the validating resolver and the forwarder target resolver support this trusted key sentinel mechanism, and

- the local resolver's queries do not carry the CD bit, and

- the trusted key state differs between the forwarding resolver and the forwarder target resolver

then either the outcome is indeterminate validating (Vleg), or a case of mixed signals (SERVFAIL in all three responses), which is similarly an indeterminate response with respect to the trusted key state.

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 resolution system that they use.

The mechanism does not require resolvers to set otherwise 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 so 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 Silva Damas

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

Warren Kumari

Email: warren@kumari.net