DNSOP
Internet-Draft
Updates: 4035 (if approved)
Intended status: Informational
Expires: December 31, 2018

P. Wouters, Ed.
Red Hat
L. Xia
Huawei
W. Hardaker
USC/ISI

June 29, 2018

The Delegation_Only DNSKEY flag
draft-pwouters-powerbind-01

Abstract

This document introduces a new DNSKEY flag called DELEGATION_ONLY that indicates that the particular zone will never sign zone data across a label. That is, every label (dot) underneath is considered a zone cut and must have its own (signed) delegation.

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 December 31, 2018.

Copyright Notice

Table of Contents

1. Introduction

The DNS Security Extensions [DNSSEC] use public key cryptography to create an hierarchical trust base with the DNSSEC root public keys at the top, followed by Top Level domain (TLD) keys one level underneath. While the root and TLD zones are asumed to be almost exclusively delegation-only zones, there is currently no method to audit these zones to ensure they behave as a delegation-only zone. This creates an attractive target for malicious use of these zones - either by their owners or through coercion. For example, the DNSSEC root key could simply sign an A record and TLSA record for "www.example.com", overriding the authority of "com" and "example.com". If such a change is done in a targetted attack, the attack would be near impossible to detect without prior knowledge of what zone contents are legitimate within a given zone. This document defines a mechanism for zone owners, at DNSKEY creation time, to indicate they will only delegate the remainder of the tree to lower-level zones, allowing easier logging and auditing of DNS responses they serve.

This document introduces a new DNSKEY flag allowing zone owners to commit that the zone will never sign any DNS data that traverses a single label and if any such signed data is encountered by validating resolvers, that this data should be interpreted as BOGUS.

2. 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 [RFC2119].

3. The Deep Link State problem

The hierarchical model of DNS and DNSSEC ([RFC4033], [RFC4034] and [RFC4035]) comes with the property that a zone at one point in the hierarchy can define, and therefor override, everything in the DNS tree from their point and below. For example, the DNSSEC root key could ignore the NS records for ".org" and "example.org" and could place a record "www.example.org" directly into its own zone, with a corresponding RRSIG signed by the root key itself. Even if resolvers would defend against this attack by not allowing RRSIG's to span across a potential zone cut, the zone operator (any level higher in the hierarchy than the target victim) could briefly remove the NS and DS records, and create a "legitimate" DNS entry for "www.example.org", hiding the normal zonecuts. The attacker can then publish DNS addresses records (e.g. A and AAAA records), as well as records used for authentication (e.g. TLSA, SMIME, OPENPGPKEY, SSHP or IPSECKEY records).

Exposing such targetted attacks requires a transparency audit setup ([RFC6962]) that needs to log all signed DNS data to prove that data signed by a parental DNSKEY was out of expected policy. The very distributed nature of DNS makes such transparency logs prohibitively expensive and nearly impossible to operate. Additionally, it would expose all zone data to any public log operators, thereby exposing all DNS data to a public archive. This data could then be used for other malicious purposes.

4. Limiting the scope of a DNSKEY RRset to just delegations

This document introduces a new DNSKEY flag called DELEGATION_ONLY. When this flag is set on a DNSKEY with SEP bit set (KSK), the zone owner commits to not sign any data that crosses a label down in the hierarchy. This commits a parent in the DNS hierarchy to only sign NS and DS records (i.e. all non-glue, delegation records) for its child zones. It will no longer be able to ignore (or briefly delete, see below) a child delegation and publish data crossing zone labels by pretending the next label is not a zone cut.

For such a parent to take over data that belongs to its child zone, it has two choices. It can (temporarilly) remove its own DNSKEY DELEGATION_ONLY flag or it can replace the NS and DS records of its child zone with its own data (destinations and key references) so it

can sign DNS data that belongs to its own child zone. However, both of these actions cannot be hidden, thus exposing such malicious behavior when combined with public transparency logs.

5. Parental Transparency

A parent zone, such as the root zone, a TLD or any public suffix list delegation point, that has published a key with the DELEGATION_ONLY flag can no longer make an exception for a single delegated zone without removing the DELEGATION_ONLY flag, switching off its published policy. This action would be highly visible, and for some domains such as the root or TLDs, require human interaction to notify the stake holders to prevent loss of trust.

Removing the DELEGATION_ONLY flag from a DNSKEY requires that the zone signals a new DS record to its parent, as changing any DNSKEY flag requires changes to the DS record data for that corresponds to it.

In the case of the root key, it would require updating out-of-band root key meta information and/or perform an [RFC5011] style rollover for the same key with updated DNSKEY flags. Due to the timings of such a rollover, it would take at least 30 days for the first validating resolvers to even pick this policy change. It would also be a highly visible event.

Replacing the NS and DS records of a child zone can still be done in a targetted attack mode, but these events are something that can be easilly tracked by a transparency infrastructure similar to what is now in use for the WebPKI using [RFC6962](bis). With client implementations of transparency, all records would be logged and become visible to the owner of attacked child zones, exposing a parent’s malicious actions.

6. Marking the root key DELEGATION_ONLY

Once the root key is marked with a DELEGATION_ONLY flag, and deployed resolvers are configured with the new key, all TLDs will be ensured that the root key can no longer be abused to create "deep link" data. Until the root key sets this bit, software MAY imply this bit is always set, as this is the current expectation of the root zone.

7. Marking TLD keys DELEGATION_ONLY

Even before the root key has been marked with DELEGATION_ONLY, TLDs can already signal their own willingness to commit being DELEGATION_ONLY zones. Any changes of that state in a TLD DNSKEY will require those TLDs to submit a new DS record to the root.

8. Migrating to and from DELEGATION_ONLY

There might be multiple DNSKEYs with the SEP bit set in a zone. For the purpose of delcaring a zone as DELEGATION_ONLY, only those DNSKEY's that have a corresponding DS record at the parent MUST be considered. If multiple DS records appear at the parent, some of which point to DNSKEY's with and some of which point to DNSKEY's without the DELEGATION_ONLY flag set, the zone MUST be considered DELEGATION_ONLY. This situation will occur when a zone is rolling its DNSKEY key at the same time as it is commiting to a DELEGATION_ONLY zone (or the reverse).

9. Similarities to the Public Suffix List

The DELEGATION_ONLY flag has a strong overlap in functionality with the Public Suffix List; both signal a formal split of authority between parent and child. The DELEGATION_ONLY flag allows zones to formally state their intention.

10. Operational Considerations

Setting or unsetting the DELEGATION_ONLY flag must be handled like any other Key Signing Key rollover procedure, with the appropriate wait times to give resolvers the chance to update their caches.

Some TLDs offer a service where small domains can be hosted in-zone at the TLD zone itself. In that case, the TLD MUST NOT set the DELEGATION_ONLY flag. Another solution for such TLDs is to create delegations for these child zones with the same or different DNSKEY as used in the parent zone itself.

If a zone is publishing glue records for a number of zones, and the zone that contains the authoritative records for this glue is deleted, a resigning of the zone will make this orphaned glue authoritative within the zone. However, with the DELEGATION_ONLY bit set, this (signed) DNSSEC data will be considered BOGUS as it violations the commitment to only delegate. This may impact domains that depended on this unsigned glue.

For example, if "example.com" and "example.net" use NS records pointing to "ns.example.net", then if "example.net" is deleted from the ".net" zone, and the previously unsigned glue of "ns.example.net" is now signed by the ".net" zone, the "example.com" zone will lose its NS records and fail to resolve.

The bind DNS software has an option called "delegation_only zones" which is an option that means something completely different. It

refers to ignoring wildcard records in specified zones that are deemed delegation-only zones.

11. Security Considerations

There are no negative security impacts of using the DELEGATION_ONLY bit?

12. IANA Considerations

This document defines a new DNSKEY flag, the DELEGATION_ONLY flag, whose value [TBD] has been allocated by IANA from the DNSKEY FLAGS registry.

13. Acknowledgements

The author wishes to thank Thomas H. Ptacek for his insistence on this matter.

Thanks to the following IETF participants: Viktor Dukhovni, Shumon Huque, Geoff Huston, Rick Lamb and Sam Weiler.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <https://www.rfc-editor.org/info/rfc5011>.

14.2. Informative 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>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/info/rfc6962>.

Authors' Addresses

Paul Wouters (editor)
Red Hat

Email: pwouters@redhat.com

Liang Xia
Huawei

Email: frank.xialiang@huawei.com

Wes Hardaker
USC/ISI
P.O. Box 382
Davis, CA 95617
US

Email: ietf@hardakers.net