DNSOP
Internet-Draft
Updates: 4035 (if approved)
Intended status: Informational
Expires: September 11, 2019

P. Wouters
Red Hat
W. Hardaker
USC/ISI

March 10, 2019

The DELEGATION_ONLY DNSKEY flag
draft-pwouters-powerbind-02

Abstract

This document introduces a new DNSKEY flag called DELEGATION_ONLY that indicates that the particular zone will never sign zone data aside from records at the apex of the zone or delegation records for its children. That is, every label (dot) underneath is considered a zone cut and must have its own (signed) delegation. DNSSEC Validating Resolvers can use this bit to mark any data that violates the DELEGATION_ONLY policy as BOGUS.

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 September 11, 2019.

Table of Contents

1. Introduction

The DNS Security Extensions [DNSSEC] use public key cryptography to create a 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.

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 delegation policy verification, 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 aside from records at the zone apex and child delegation records, 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 zone cuts. 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 targeted attacks would require a transparency audit setup ([RFC6962]) that would need to log all signed DNS data to prove that data signed by a parent zone's DNSKEY was out of expected policy. The very distributed nature of the DNS makes such transparency logs prohibitively expensive and nearly impossible to operate. Additionally, it would require zone owners to expose all their zone data to any public log operators, thereby introducing privacy implications and exposing all relevant DNS data to a public archive. Though this may be acceptable for some domains, such as the root, where data is already public, other delegation domains have legal implications that prohibit them from participating in such a system.

4. The DELEGATION_ONLY DNSKEY flag

This document introduces a new DNSKEY flag called DELEGATION_ONLY. When this flag is set on a DNSKEY with its Secure Entry Point (SEP) bit set - that is the DNSKEY is a Key Signing Key (KSK) - the zone owner commits to not sign any data aside from its records at the apex of the zone and delegation records for its children. This commits a parent in the DNS hierarchy to only publish signed DS records and unsigned glue records (NS and A/AAAA) for its child zones. It will no longer be able to ignore (or briefly delete, see below) a child

delegation and publish data beyond its own label 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 (temporarily) 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 DNSSEC Transparency logs.

4.1. _underscore label exception

Some protocols, such as the DANE protocol [RFC6698] use a number of labels that start with an underscore (_) prefix to publish information about the zone itself. For example, the TLSA record for example.com is published at the location _443._tcp.example.com. These records are semantically part of the zone itself and are not delegated child zones. Any chain of labels consisting of only labels each starting with an underscore (_) under the apex of the zone is not considered to violate the DELEGATION_ONLY flag limitation of being DELEGATION_ONLY, as this data is logically part of the zone itself and is never meant to be interpreted as an independent delegated child zone.

4.2. Parent Zone 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 first publishes an additional updated DS record to its parent.

In the case of the root key, it would require updating out-of-band root key meta information and/or performing 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 process 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 targeted attack by a parent, but these events are something that can be easily tracked by a transparency infrastructure similar to

what is now in use for the WebPKI using [RFC6962](bis). With client implementations of transparency, all DELEGATION_ONLY flag changes would be logged and become visible to the owner of attacked child zones, exposing a parent's malicious actions.

4.3. Marking the Root DNSKEY DELEGATION_ONLY

Once the Root DNSKEY is marked with a DELEGATION_ONLY flag and deployed resolvers are configured with the new DNSKEY, all TLDs will be assured that the Root DNSKEY can no longer be abused to override child zone data. Until the Root KSK DNSKEY sets this bit, software SHOULD imply this bit is always set, as this is the current expectation of the Root Zone.

4.4. Migrating to and from DELEGATION_ONLY

There might be multiple DNSKEYs with the SEP bit set in a zone. For the purpose of declaring 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 the DELEGATION_ONLY flag set 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 committing to a DELEGATION_ONLY zone (or the reverse). During the overlap, the zone is considered to be a delegation-only zone.

4.5. Allowed record types for labels inside DELEGATION_ONLY zones

Some labels within a DELEGATION_ONLY marked zone must be published by a parent in order to properly sign its zone and its child's referral data. Thus, any published and signed zone data deeper than the zone apex MUST only include DNS TYPEs of glue (NS, A and AAAA), DS, NSEC and NSEC3 records.

5. 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.

Zones setting the DELEGATION_ONLY flag can no longer publish non-delegation records in their zone. That means that for those RRTYPEs that take DNS targets as parameters (NS, MX, SRV, ...), the targets cannot have their own host names on the zone. Instead, a sub-zone needs to be created to place those targets in. If "example.com" has an NS record pointing to "ns0.example.com", this entry needs to be moved to a sub-zone such as ns0.nic.example.com before the zone can be switched to DELEGATION_ONLY. Otherwise, the signed record "ns0.example.com" would be interpreted as the parent's hostile takeover of the child zone "ns0.example.com". Similarly, an MX target pointing to "mail.example.com" would have to be moved to a sub-zone, such as "mail.nic.example.com". The zone "nic.example.com" MUST NOT be made DELEGATION_ONLY in that case, otherwise it would have the exact same problem.

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 depend on these incorrect glue records.

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.

6. Security Considerations

Some parent zone attacks cannot be detected when the validating resolver's cache is empty. Care should be taken by resolvers to not unnecessarily empty their cache. This is specifically important for roaming clients that re-connect frequently to different wireless or mobile data networks.

The DELEGATION_ONLY DNSKEY flag is only valid for DNSKEY's that have the SEP bit set. It MUST be ignored on DNSKEY's without the SEP bit set.

This DELEGATION_ONLY mechanism is not designed to completely foil attacks (since parent's can simply change a child's referral data), but rather to empower transparency logging mechanisms.

7. Privacy Considerations

Some of the protection offered by the DELEGATION_ONLY flag is only available when DNS resolvers report changes in the signing depth of high level (root or TLD) DNSKEYs to gain DNSSEC Transparency. This reporting can reveal that a particular node is trying to access a certain DNS name. Defensive measures to prevent exposing users should be taken when implementing DNSSEC Transparency. It is expected that DNSSEC Transparency behaviour will be written up in a separate document.

8. Human Rights Considerations

The DNS protocol's hierarchy limits zones authority to themselves and their child zones only. While this provides a finer grained trust model compared to a simple list of all-powerful trusted entities, such as those used in the WebPKI, it consolidates a lot of power in the few keys at the top of the DNS hierarchy. With the increased reliance on DNSSEC for securely identifying resources, such as DANE records, it is important to monitor and audit the keys at the top of the DNS hierarchy to prevent their abuse and coercion of child zones. This DNS protocol extension specifically aims at increasing parent zone transparency and blocks some parent zone attacks from those parents who have publicly claimed to never override their child zone data and thus increases the security and stability of DNS and DNSSEC.

Zones publishing the DELEGATION_ONLY flag to increase their public trust are still able to remove child zones from their zone, for example in cases of legal compliance or to prevent malicious activity happening in its child zones. But these parents can only do so publicly and can no longer surreptitiously take control of their own child zones. This protocol extension does not limit legal enforcement of child zones by their parent zones other than making it visible for everyone when a childzone is legally taken over for compliance or legal reasons.

9. 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.

10. Acknowledgements

The authors thank Thomas H. Ptacek for his insistence on pointing out the trust issues at the top of the DNSSEC hierarchy.

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

11. References

11.1. 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>.

11.2. 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>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[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
Red Hat

Email: pwouters@redhat.com

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

Email: ietf@hardakers.net