Workgroup: Network Working Group
Internet-Draft:
draft-dickson-dnsop-glueless-00
Published: 16 September 2021
Intended Status: Informational
Expires: 20 March 2022
Authors: B. Dickson
GoDaddy

Operating a Glueless DNS Authority Server

Abstract

This Internet Draft proposes a Best Current Practice for protecting authority servers against MITM and poisoning attacks, using a domain naming strategy to not require glue A/AAAA records and use of DNSSEC.

This BCP assumes the use of validating resolvers, which should already be a BCP itself.

MITM and poisoning attacks should only be effective/possible against unsigned domains.

However, until all domains are signed, this guidance is relevant, in that it can limit the attack surface of unsigned domains.

This guidance should be combined with [I-D.dickson-dnsop-ds-hack]

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 20 March 2022.

Table of Contents

1. Introduction

DNS Security extensions (DNSSEC) are additions to the DNS protocol which provide data integrity and authenticity protections, but do not provide privacy.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Background

Use of DNSSEC requires upgrades to software for authorative servers, resolvers, and optionally clients, in order to benefit from these protections. It also requires that DNS operators actually sign their zones.

When a given zone is unsigned, those protections to the zone contents are not available.

Any unsigned zone is trivially able to be altered by an on-path attacker.

An off-path attacker is limited to use of cache poisoning attacks.

However, some class of cache poisoning attacks target unsigned delegation data. These records consist of the necessary NS records, and when necessary, "glue" records for IP address corresponding to these NS records.

The impact to successful cache poisoning of delegation records is that the attacker may substitute their own name servers for the legitimate name server. In other words, the attacker is able to promote itself to being effectively on-path, and trivially modify unsigned domain results.

4. Proposed Solutions

There are two delegation record types that require protection against off-path attackers, for unsigned domains.

For protecting NS records used in delegations, there is a new proposal for use of a new DS record. See [I-D.dickson-dnsop-ds-hack] for details.

The present draft addresses the "glue" records, by recommending methods to make them unnecessary. If there is no delegation glue data, an attacker cannot poison that data. The resolver cache would contain only authoritative data, which cannot be pre-empted by such poisoning attacks.

5. Recommendations

The following practice is RECOMMENDED for unsigned zones:

* Do not use in-bailiwick name server names for unsigned zones.

* Use out-of-zone names for the name servers for unsigned zones

Example:

```
Do NOT do the following (delegations requiring glue):
unsigned-zone.example NS ns1.unsigned-zone.example
unsigned-zone.example NS ns2.unsigned-zone.example
// glue
ns1.unsigned-zone.example A (IP address)
ns1.unsigned-zone.example AAAA (IP address)
ns2.unsigned-zone.example A (IP address)
ns2.unsigned-zone.example AAAA (IP address)

Instead, do the following (glueless delegations):
unsigned-zone.example NS ns1.nameserver-signed-zone.example
unsigned-zone.example NS ns2.nameserver-signed-zone.example
//
// Delegation to signed zone containing name server names
nameserver-signed-zone.example NS ns1.nameserver-signed-zone.example
nameserver-signed-zone.example NS ns2.nameserver-signed-zone.example
nameserver-signed-zone.example DS (DS record data)
// glue records for this delegation
ns1.nameserver-signed-zone.example A (IP address)
ns1.nameserver-signed-zone.example A (IP address)
ns2.nameserver-signed-zone.example AAAA (IP address)
ns2.nameserver-signed-zone.example AAAA (IP address)
```

The following practice is RECOMMENDED (for signed name server name zones, i.e. large operators' zones):

- For name server name zones (zones containing data for name servers), use dedicated name server names for the zone itself
- Consider use of another zone for the dedicated name server names, to make the name server name zone itself fully glueless
- For this additional zone, also consider using a different name server *name* for its delegation's exclusive use
- Decoupling the respective NS names, ensures changes and updates to the zone that uses glue, don't affect any other zones
- Depending on parent zone policy (e.g. TLD database policy), renaming or renumbering name servers may affect delegations using them (NS entries)
- A single zone with non-reused NS names guarantees side effects of this sort are not possible
- Additional lookups are required on the initial reference to any NS in the main glueless zone
- Subsequent (new) queries for the IP addresses of glueless name servers only require single queries

Example:

```
Entries in the example TLD
//
// Same unsigned zone uses the same name servers
// However, the name server is in its own glueless zone
unsigned-zone.example NS ns1.nameserver-signed-zone.example
unsigned-zone.example NS ns2.nameserver-signed-zone.example
//
nameserver-signed-zone.example NS ns1.separate-zone.example
nameserver-signed-zone.example NS ns2.separate-zone.example
nameserver-signed-zone.example DS (DS record data)
//
separate-zone.example NS special-ns1.separate-zone.example
separate-zone.example NS special-ns2.separate-zone.example
separate-zone.example DS (DS record data)
// glue for special-ns1 and -2
// special-ns1 and -2 are used only for/by separate-zone
special-ns1.separate-zone.example A (IP address)
special-ns1.separate-zone.example AAAA (IP address)
special-ns2.separate-zone.example A (IP address)
special-ns2.separate-zone.example AAAA (IP address)

Zone file for nameserver-signed-zone:
nameserver-signed-zone.example SOA (soa record data)
// glueless NS are used
nameserver-signed-zone.example NS ns1.separate-zone.example
nameserver-signed-zone.example NS ns2.separate-zone.example
// actual glueless address records for "real" name server names
ns1.nameserver-signed-zone.example A (IP address)
ns1.nameserver-signed-zone.example AAAA (IP address)
ns2.nameserver-signed-zone.example A (IP address)
ns2.nameserver-signed-zone.example AAAA (IP address)
// etc etc etc

Zone file for separate-zone:
separate-zone.example SOA (soa record data)
// This is the only non-glueless NS in use
// NB: matches glue in parent
separate-zone.example NS special-ns1.separate-zone.example
separate-zone.example NS special-ns2.separate-zone.example
special-ns1.separate-zone.example A (IP address)
special-ns1.separate-zone.example AAAA (IP address)
special-ns2.separate-zone.example A (IP address)
special-ns2.separate-zone.example AAAA (IP address)
// actual address records for "real" name server name
// (only used by nameserver-signed-zone)
ns1.separate-zone.example A (IP address)
ns1.separate-zone.example AAAA (IP address)
ns2.separate-zone.example A (IP address)
ns2.separate-zone.example AAAA (IP address)
```

6. Security Considerations

This guidance is not a substitute for use of DNSSEC for DNS domains.

This guidance is useful in preventing off-path attackers from poisoning DNS cache entries necessary for delegations.

However, an on-path attacker is still able to manipulate DNS responses sent over UDP or unencrypted TCP.

Use of an encrypted transport is one potential method of preventing MITM attacks (i.e. DNS over TLS from resolver to authoritative server, aka ADoT), but this is still less secure than use of DNSSEC.

7. IANA Considerations

This document has no IANA actions.

8. Normative References

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9. Informative References

[I-D.dickson-dnsop-ds-hack] Dickson, B., "DS Algorithms for Securing NS and Glue", Work in Progress, Internet-Draft, draft-dickson-dnsop-ds-hack-00, 11 August 2021, <https://datatracker.ietf.org/doc/html/draft-dickson-dnsop-ds-hack-00>.

[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>.

Appendix A. Acknowledgments

Thanks to everyone who helped create the tools that let everyone use Markdown to create Internet Drafts, and the RFC Editor for xml2rfc.

Thanks to Dan York for his Tutorial on using Markdown (specifically mmark) for writing IETF drafts.

Thanks to YOUR NAME HERE for contributions, reviews, etc.

Author's Address

Brian Dickson

GoDaddy

Email: brian.peter.dickson@gmail.com