Network Working Group
Internet-Draft
Intended status: Informational
Expires: 26 March 2022

B. Dickson
GoDaddy

22 September 2021

Operating a Glueless DNS Authority Server
draft-dickson-dnsop-glueless-02

Abstract

This Internet Draft proposes a method 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 technique assumes the use of validating resolvers.

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

Copyright Notice

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 and secure the corresponding delegations at the parent.

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

Any such insecure domain 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 addresses 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

This work does not propose any protocol changes. It provides guidance on strategies and techniques for name server naming.

There are two kinds of delegation records 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 mostly unnecessary. If there is no delegation glue data, an attacker cannot poison that data. The resolver cache would contain only authoritative address records associated with NS names. Authoritative data cannot be pre-empted by such poisoning attacks, since those are only able to replace less trusted glue records.

Additional recommendations are made to reduce the chances for errors caused by DNS operators when changing delegation records, by avoiding re-use of name server names which require glue address records.

5. Terminology:

The following terms are used to disambiguate domains and server names:

* Registered domain - end-user (registrant) domain

  - In the parent zone, the registered domain is the left-hand side of the NS record

- Registered domain name server - the name of the name server serving the registered domain

  - In the parent zone, the registered domain name server is the right-hand side of the NS record

6. Recommendations

The following practice is RECOMMENDED for unsigned domains:

- Do not use in-bailiwick registered domain name servers for unsigned domains.

- Instead, use out-of-zone names for the registered domain name servers of unsigned domains.

Example:

Do NOT do the following (delegations requiring glue):

```
$ORIGIN example.
// Records in example TLD, with relative names
unsigned-domain NS ns1.unsigned-domain
unsigned-domain NS ns2.unsigned-domain
// glue
// "strictly necessary glue"
// always required for successful resolution
ns1.unsigned-domain A (IP address)
ns1.unsigned-domain AAAA (IP address)
ns2.unsigned-domain A (IP address)
ns2.unsigned-domain AAAA (IP address)
```

Instead, do the following (glueless delegations):

```
$ORIGIN example.
// Records in example TLD, with relative names
// This is the minimum "glueless" set-up
// NS target name is not a "registered" host
// NS target is not used for glue for any domains
unsigned-domain NS ns1.nameserver-signed-domain
unsigned-domain NS ns2.nameserver-signed-domain
//
// Delegation to signed domain containing name server names
// (This domain serves the address records of name servers
//  such as the glueless example above)
nameserver-signed-domain NS ns1.nameserver-signed-domain
nameserver-signed-domain NS ns2.nameserver-signed-domain
nameserver-signed-domain DS (DS record data)
// However, this domain needs to be resolvable, and needs glue
// glue records for this delegation
ns1.nameserver-signed-domain A (IP address)
ns1.nameserver-signed-domain A (IP address)
ns2.nameserver-signed-domain AAAA (IP address)
ns2.nameserver-signed-domain AAAA (IP address)
```

The following practice is RECOMMENDED:

* For any name server domain (domain containing addresses and related data for name servers used by registered domains), use distinct dedicated name servers for the domain itself

  - I.e. avoid sharing name servers between the name server domain and any registered domains

* Consider making the name server domain itself fully glueless, with an out-of-zone name server (using a tertiary domain)

* For this tertiary domain, also consider using separating the in-bailiwick name servers, from the names used for serving the name server domain

  - Limiting the in-bailiwick NS names ensures that changes and updates to the tertiary domain don’t affect any other domains

  - Depending on parent zone policy (e.g. TLD database policy), renaming or renumbering name servers may affect delegations using them (NS entries)

  - A single domain with non-reused NS names guarantees side effects of this sort are not possible

* Overhead of tertiary domain and not re-using (or sharing) name server names in the tertiary domain:

  - Additional lookups are required on the initial reference to get the addresses of name servers for the main glueless domain

  - Subsequent (new) queries for the IP addresses of glueless name servers only require single queries

Example:

Entries in the example TLD

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

Zone file for signed-nameserver-domain.example:

```
   $ORIGIN signed-nameserver-domain.example.
   @ SOA (soa record data)
   // glueless NS are used
   @ NS ns1.tertiary-domain
   @ NS ns2.tertiary-domain
   // actual glueless address records for "real" name server names
   ns1 A (IP address)
   ns1 AAAA (IP address)
   ns2 A (IP address)
   ns2 AAAA (IP address)
   // etc etc etc

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

7. Security Considerations

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.

This guidance is not a substitute for use of DNSSEC for DNS domains. The only mechanism that can protect against on-path attackers is cryptographic protection DNSSEC signing of domains is both necessary and sufficient to provide data integrity protection.

Use of an encrypted transport is may be effective at preventing MITM attacks (i.e. DNS over TLS from resolver to authoritative server, aka ADoT), but does not provide provable data integrity.

Encrypted transport may be used in combination with DNSSEC signed zones and glueless name server domains.

Encrypted transport does not incrementally improve the data integrity or protection against MITM. DNSSEC is sufficient alone for this purpose. However, encrypted transport does add privacy protection against passive observers.

8. IANA Considerations

This document has no IANA actions.

9. 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>.

10. 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