dnsop
Internet-Draft
Intended status: Informational
Expires: 27 August 2025

L. Pan

23 February 2025

Compact DNSSEC
draft-pan-dnsop-compact-dnssec-00

Abstract

This document describes about a compact DNSSEC scheme for resource-limited second-level domain (SLD), which is focused on NS RR.

Table of Contents

1. Background

DNSSEC has low adoption rate on SLD [SadDNSSEC].

The operation burden of fullzone DNSSEC deployment is heavy.

DNS random subdomain attacks and amplification attacks are commonly used distributed denial-of-service (DDoS) attacks. The DDoS amplification power of the authoritative server of SLD will be larger after deploying DNSSEC [AmpDNSSEC].

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 [RFC2119].

Basic terms used in this specification are defined in the documents [RFC1034], [RFC1035], [RFC8499].

* Authoritative Server: Described in [RFC8499].

* Recursive Resolver: Described in [RFC8499].

3. Compact DNSSEC Scheme

To encourge the DNSSEC deployment on resource-limited SLD, it is resonable to give it a compact DNSSEC deployment scheme.

3.1. The Resource-limited SLD Publishes Compact DNSSEC Records

Resource-limited SLD should publish these DNSSEC records:

* the delegation signer (DS) record on TLD.

* the DNSKEY records.

* the RRSIGs for NS/A/AAAA/CNAME/TLSA records associated with NS.

Resource-limited SLD doesn’t publish other DNSSEC records on other subdomains.

Resource-limited SLD doesn’t deploy NSEC/NSEC3.

For example:

```
example.com. 345600 IN NS ns1.example.com.
example.com. 345600 IN NS ns2.example.com.
ns1.example.com. 345600 IN A 11.22.33.44
ns1.example.com. 345600 IN AAAA ::11.22.33.44
ns2.example.com. 345600 IN A 55.66.77.88
ns2.example.com. 345600 IN AAAA ::55.66.77.88
_853._tcp.ns1.example.com. 3600 IN TLSA ( 3 1 1
  63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
_853._udp.ns1.example.com. 3600 IN TLSA ( 3 1 1
  63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
_853._tcp.ns2.example.com. 3600 IN TLSA ( 3 1 1
  63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
_853._udp.ns2.example.com. 3600 IN TLSA ( 3 1 1
  63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
```

Therefore, the zone file size of the compact DNSSEC scheme is approximate with plain-text DNS, with few RRSIGs.

4. The Authoritative Server of Resource-limited SLD Deploys Secure Service

[RFC7858] and [RFC9250] defined the encrypted DoT/DoQ service for client-to-recursive.

[RFC9539] discussed the extended deployment of encrypted recursive-to-authoritative DNS.

The authoritative server of resource-limited SLD deploys the DoQ/DoT service with self-signed PKI cerificate with TLS connection.

* The NS records of the resource-limited SLD should be written into the subjectAltName extension field of the self-signed PKI certificate.

* The public key information of the self-signed PKI cerificate is published on associated TLSA records of the NS.

* The associated TLSA records are DNSSEC-signed.

An alternative secure channel solution is [DNSCurve], embeded the raw public key into the NS records.

5. The Recursive Resolver Validates The Compact DNSSEC Records

The recursive resolver validates the DNSSEC trust chain (Root -> TLD -> SLD), and gains the trustworthy A/AAAA records of the NS records of the SLD.

The trustworthy A/AAAA records are the IP addresses of the authoritative server of the resource-limited SLD.

6. Setup Secure Channel for Recursive-to-Authoritative

The Recursive Resolver setup secure DoQ/DoT channel with the authoritative server of the resource-limited SLD:

* The recursive resolver connects to the trustworthy IP addresses of the authoritative server of the resource-limited SLD.

* The recursive resolver receives the self-signed certificate from the authoritative server, and extract the public key from the self-signed PKI certificate.

* The recursive resolver validates the TLSA RRSIGs of the NS records of the SLD with the DNSSEC trust chain.

* The recursive resolver validates the digest of extracted public key match the TLSA record.

* The recursive resolver setup secure DoQ/DoT channel with the authoritative server of the resource-limited SLD successfully.

* The recursive resolver make DNS query with the authoritative server of the resource-limited SLD on the secure DoQ/DoT channel.

7. Security Considerations

The compact DNSSEC scheme does not cover the entire zone and does not deploy NSEC/NSEC3.

8. References

8.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[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>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[RFC9539] Gillmor, D. K., Ed., Salazar, J., Ed., and P. Hoffman, Ed., "Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS", RFC 9539, DOI 10.17487/RFC9539, February 2024, <https://www.rfc-editor.org/info/rfc9539>.

8.2. Informative References

[AmpDNSSEC] Nexusguard, "DNSSEC fuels new wave of dns amplification.", n.d., <https://www.nexusguard.com/blog/dnssec-fuels-new-wave-of-dns-amplification>.

[DNSCurve] J., B. D., "DNSCurve", n.d., <https://dnscurve.org/>.

[SadDNSSEC] J., E. A. and M., "The Sad Story of DNSSEC", n.d., <https://alexkelliott.github.io/dnssec/TheSadStoryOfDNSSEC.pdf>.

Author's Address

Lanlan Pan
Guangdong
China
Email: abbypan@gmail.com