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

L. Pan

23 February 2025

Authenticated subdomain whitelist (ASDWL) for second-level domain (SLD)
draft-pan-dnsop-authenticated-subdomain-whitelist-00

Abstract

This document describes about an authenticated subdomain whitelist (ASDWL) scheme to mitigate the random subdomain attacks on second-level domain (SLD).

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 27 August 2025.

Table of Contents

1. Background

The DNS random subdomain attack, also referred to as DNS water torture attack or pseudo-random subdomain attack, represents a form of DDoS attack specifically targeting DNS services. The attacker orchestrates huge amounts of bots to send queries to recursive resolvers. These queries are random subdomains under the victim domains, which are not currently cached in recursive resolvers. Consequently, the recursive resolvers must forward these queries to the authoritative servers responsible for the victim domains. This process places a significant burden on both the recursive resolvers and the authoritative servers, potentially leading to service degradation or outright failure.

We describe an authenticated subdomain whitelist (ASDWL) scheme to mitigate DNS random subdomain attacks on second-level domains.

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. Prepare Private Key and Certificate for ASDWL

The administor of SLD should generate a private key priv_wl used to sign the ASDWL, and issue an end-entity X.509 certificate Cert_wl for the corresponding public key pub_wl used to verify the ASDWL signature.

4. Structure of ASDWL

ASDWL followes the flattened JWS JSON serialization syntax, contains 3 parts: payload, header, and signature.

* payload: Contains the whitelist subdomains information configured by the domain administrator of SLD.
  - dom: Contains the name of SLD.
  - date: Contains the publish date of the ASDWL.
  - subdoms: Contains the subdomain whitelist of SLD. In this example, it means 'abc.example.com'.
  - wildcard subdoms: Contains the wildcard subdomain zone whitelist of SLD. In this example, it means '*.xxx.example.com' .
* header: Contains the parameters for the ASDWL signature, followed the definition of JSON web signature and encryption header parameters in [RFC7515].
  - alg: Contains the signature algorithm. In this example, ES256 means the ECDSA digital signature on Elliptic Curve NIST P-256 with SHA-256 message digest, followed the definition in [RFC7515].
  - x5c: Contains the X.509 certificate Cert_wl corresponding to the key priv_wl used to sign the ASDWL payload.
* signature: Contains the signature of the payload, which is signed by priv_wl, and verified by Cert_wl.

```
{
    'payload': {
        'dom': 'example.com',
        'date': '2023-12-25',
        'subdoms': [
            'abc'
        ],
        'wildcard subdoms': [
            'xxx'
        ]
    },
    'header': {
        'alg' : 'ES256',
        'x5c' : ....,
    },
    'signature': ...
}
```

5. Publish ASDWL

The administor of SLD should define a well-known subdomain '_asdwl.example.com' for the SLD 'example.com' to publish its ASDWL url address (marked as Url_wl).

And configure a DANE TLSA RR and a TXT RR for it.

* TLSA RR: The TLSA RR indicates the digest of the public key of the ASDWL certificate Cert_wl.

* TXT RR: The TXT RR indicates the ASDWL url address Url_wl of ASDWL. In this example, the url is 'https://_asdwl.example.com/asdwl.json'.

```
_443._tcp._asdwl.example.com. 3600 IN TLSA ( 3 1 1
  d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971 )

_asdwl.example.com. 3600 IN TXT
  'url=https://_asdwl.example.com/asdwl.json'
```

6. Get ASDWL

When the authoritative server of SLD detects the random subdomain attack, it can attach the TLSA and TXT records of the well-known subdomain '_asdwl.example.com' to the DNS answer section. And then the recursive resolver can get ASDWL of the SLD 'example.com' with the following steps:

* Recursive resolver extracts Url_wl from the TXT RR, and downloads ASDWL.

* Recursive resolver extracts Cert_wl from the x5c parameter of ASDWL.

* Recursive resolver extracts the public key from Cert_wl.

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

7. Recursive Resolver Mitigates Random Subdomain Attacks with ASDWL

Recursive resolver could mitigate random subdomain attacks with ASDWL:

* Recursive resolver loads ASDWL payload of SLD ‘example.com’ into the DDoS whitelist module.

* Recursive resolver makes the mitigation on random subdomain attacks:

  - Recursive resolver allows all the legitimate queries of the whitelist subdomains (subdoms) from clients, and sends the queries to the authoritative server.

  - Recursive resolver allows all the legitimate queries of the whitelist wildcard subdomains (wildcard subdoms) from clients, only sends one query to ASsld for each wildcard subdomain zone, and store one response for all queries in each wildcard subdomain zone.

  - Recursive resolver makes rate limiting responses on other subdomains queries when it could afford. Recursive resolver drops the queries of other subdomains when the traffic is overwhelmed.

8. Authoritative Server Mitigates Random Subdomain Attacks with ASDWL

Authoritative server could mitigate random subdomain attacks with ASDWL:

* Authoritative server detects that recursive resolver has sent many random subdomain queries, identifies it may be potential victim recursive resolver.

* Authoritative server makes the mitigation on random subdomain attacks:

- Authoritative server allows all the legitimate queries of the whitelist subdomains (subdoms) from recursive resolver.

- Authoritative server allows all the legitimate queries of the whitelist wildcard subdomains (wildcard subdoms) from recursive resolver.

- Authoritative server makes rate limiting responses on other subdomains queries from RS when it could afford. Authoritative server drops the queries of other subdomains from recursive resolver when the traffic is overwhelmed.

9. Security Considerations

Through ASDWL, the authoritative server of SLD can give an explict subdomain list which recursive resolver should make best effort to serve. The recursive resolver to gain the subdomain whitelist directly from the authoritative server of SLD from the Url_wl of ASDWL.

It is compatible with DNSSEC, heuristic rule defense systems, and machine learning random subdomain defense systems [HeavyHitter] [DetectWaterTorture].

If DNSSEC [RFC9364] has been deployed on the SLD ’example.com’, then the recursive resolver could make DNSSEC validation on the RRSIGs of TLSA/TXT RRs.

10. References

10.1. 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>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[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>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

10.2. Informative References

[DetectWaterTorture] Kishimoto, Y. T. T. Y. R. K. M. K. and H., "Detection of the dns water torture attack by analyzing features of the subdomain name", n.d., <Journal of Information Processing, vol. 24, no. 5, pp. 793801, 2016.>.

[HeavyHitter] Shagam, S. L. F. Y. A. A. B.-B. E. C. and M., "Mitigating dns random subdomain ddos attacks by distinct heavy hitters sketches", n.d., <in Proceedings of the fifth ACM/ IEEE workshop on hot topics in web systems and technologies, 2017, pp. 16.>.

Author’s Address

Lanlan Pan
Guangdong
China
Email: abbypan@gmail.com