Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2019

M. Bretelle
Facebook

March 11, 2019

DNS-over-TLS for insecure delegations
draft-bretelle-dprive-dot-for-insecure-delegations-01

Abstract

This document describes an alternative mechanism to DANE ([RFC6698]) in order to authenticate a DNS-over-TLS (DoT [RFC7858]) authoritative server by not making DNSSEC a hard requirement, making DoT server authentication available for insecure delegations.

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 September 12, 2019.

Table of Contents

1. Introduction 2
2. Terminology 2
3. Authenticating an insecure delegation 3
3.1. Public Key Infrastructure (PKIX) 3
3.2. Subject Public Key Info (SPKI) 3
3.3. Authenticating from the parent 4
3.3.1. Example 4
4. DSPKI Resource Record 4
4.1. The DSPKI Resource Record 5
4.1.1. DSPKI RDATA Wire Format 5
5. Security Considerations 6
6. IANA Considerations 6
7. Normative References 6
Acknowledgments 7
Author's Address 7

1. Introduction

This document describes an alternative mechanism to DANE ([RFC6698]) as described in [I-D.bortzmeyer-dprive-resolver-to-auth] Section 2 extending the authentication of DNS over Transport Layer Security (DoT) [RFC7858] to insecure delegations and therefore enabling the onboarding of DoT authoritative servers without the requirement for the authorities to support DNSSEC ([RFC4033], [RFC4034], and [RFC4035]). To do so, this document introduce the Delegation Subject Public Key Info (DSPKI) resource record, its purpose, usage and format.

2. Terminology

A server that supports DNS-over-TLS is called a "DoT server" to differentiate it from a "DNS Server" (one that provides DNS service over any other protocol), likewise, a client that supports this protocol is called a "DoT client"

A secure delegation ([RFC4956] Section 2) is a signed name containing a delegation (NS RRset), and a signed DS RRset, signifying a delegation to a signed zone.

An insecure delegation ([RFC4956] Section 2) is a signed name containing a delegation (NS RRset), but lacking a DS RRset,

signifying a delegation to an unsigned subzone.

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. Authenticating an insecure delegation

To authenticate a DoT server of a secure delegation, it is possible to use the TLSA resource record [RFC6698] of the nameserver as decribed in [I-D.bortzmeyer-dprive-resolver-to-auth] Section 2, while this method is valid, the absence of support of DNSSEC for such delegations precludes the onboarding and discovery of nameservers serving those zones as DoT servers.

Without the use of DNSSEC, a delegation is not able to authenticate itself as the chain of trust cannot be followed, however other mechanisms exist to have a server authenticate itself, such as Public Key Infrastructure (PKIX [RFC6125]) , SPKI, which have their own pros and cons.

3.1. Public Key Infrastructure (PKIX)

It would be possible to authenticate the name servers of the insecure delegation using PKIX, relying on an existing trust model and trust anchors.

While simple, a single trusted Certificate Authority (CA) that breaks said trust (voluntarily or involuntarily), can issue certificate for any domains, allowing an attacker to potentially impersonate both the application and the DoT server.

Another issue that rises is that the DoT servers may use an identity which belong to the same origin as application servers, which could permit personal information (such as cookies) to be leaked to the DoT servers.

3.2. Subject Public Key Info (SPKI)

The zone owner generates his own certificate and distribute the SPKI fingerprint into the DNS.

This is in essence what, amongst other things, TLSA records solve but with the requirement for DNSSEC to be enabled and functional for the queried zone. For insecure delegations, simply advertising the SPKI fingerprint would be trivial to intercept, disable, and modify.

3.3. Authenticating from the parent

While a delegation is not secured, the DNS core infrastructure already support, for the most part, DNSSEC, meaning that if the owner of an insecure delegation could set the SPKI fingerprint in a resource record (RR) at the parent, such fingerprint could be signed and validated by the DoT client. The DoT client can then establish a TLS connection to the zone name servers and authenticate the DoT server against the fingerprint acquired earlier from the parent zone.

3.3.1. Example

example.com is an insecure delegation from .com which has set the DSPKI RRset.

A DoT client looking for records under example.com will learn from .com that example.com is delegated to

```
example.com IN 172800 NS ns1.example.com
example.com IN 172800 NS ns2.example.com
# sha256
example.com IN DSPKI (
    1 4e44f900cdeb8c769f4df97e23f8fc81
      4ac4bf45a3d9dc265a2ed925171f0b71 )
# sha512
example.com IN DSPKI (
    2 ab40ed300fd220d8c72a600069f9ceb1
      f9fd7c003117e4ef34b228da1c9d76a0
      500be99e82a0c01e7f80930a46ad28b8
```

```
      ed3d5ed2df34d822b5f56c99f45889ef
)
ns1.example.com IN 172800 AAAA 2001:db8:abcd:12:1:2:3:4
ns2.example.com IN 172800 AAAA 2001:db8:abcd:ab:1:2:3:4
```

with the accompanying signature.

The DSPKI RRset signals that the nameservers are able to support DNS-over-TLS. The DoT client can then establish a TLS connection to the DoT server and authenticate them by ensuring that the SPKI matches the one learned from the parent zone.

4. DSPKI Resource Record

There may be 0 or more DSPKI served by the parent of the delegation. 0 means that DSPKI is not supported, therefore the DoT client could try other alternatives. 1 or multiple public keys can be distributed to let the DoT client validate multiple public keys, which can be useful while doing certificate rotation or when willing to provide

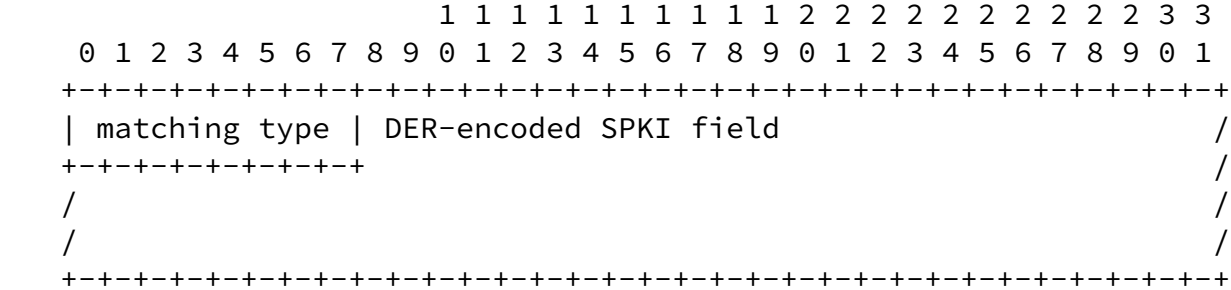
different secret keys to different providers that may serve the delegated zone.

4.1. The DSPKI Resource Record

The DSPKI resource record (RR) is used to associate a DoT server public key (SPKI) with the zone it is serving.

4.1.1. DSPKI RDATA Wire Format

The RDATA of the DSPKI RR consists of a one-octet matching type field, and the DER-encoded binary structure of the SubjectPublicKeyInfo field as defined in [RFC5280].



4.1.1.1. The Matching Type Field

A one-octet value, called "matching type", specifies how the SPKI is presented. The types defined in this document are:

- 0 - Exact match on SPKI
- 1 - SHA-256 hash of SPKI
- 2 - SHA-512 hash of SPKI

Where the SPKI can be extracted as follow:

```
openssl x509 -in cert.pem -pubkey -noout | openssl pkey -pubin -outform der
```

and the SHA-256 as:

```
openssl x509 -in cert.pem -pubkey -noout | openssl pkey -pubin -outform der | \
    openssl dgst -sha256 -binary
```

FIXME: consider

- alternate URI to support DoT (host, port, spki), DoH (host, port, URL template), DNS-over-QUIC... would rather be an ALTNS type of record

- CDSPKI a la CDS, CDNSKEY

5. Security Considerations

TODO Security

6. IANA Considerations

TODO: This document requires IANA actions (new RR type).

7. Normative References

[I-D.bortzmeyer-dprive-resolver-to-auth]
Bortzmeyer, S., "Encryption and authentication of the DNS resolver-to-authoritative communication", draft-

bortzmeyer-dprive-resolver-to-auth-01 (work in progress), March 2018.

[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>.

[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>.

[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>.

[RFC4956] Arends, R., Kosters, M., and D. Blacka, "DNS Security (DNSSEC) Opt-In", RFC 4956, DOI 10.17487/RFC4956, July 2007, <https://www.rfc-editor.org/info/rfc4956>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[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>.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250, June 2014, <https://www.rfc-editor.org/info/rfc7250>.

[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>.

[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>.

Acknowledgments

TODO acknowledge.

Author's Address

Emmanuel Bretelle
Facebook

Email: chantra@fb.com