Network Working Group M. Bretelle
Internet-Draft Facebook
Intended status: Standards Track September 27, 2018
Expires: March 31, 2019

DNS-over-TLS for insecure delegations
draft-bretelle-dprive-dot-for-insecure-delegations-00

Abstract

This document describes an alternate 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

Copyright Notice

Table of Contents

1. Introduction

This document describes an alternate mechanism to [RFC6698] as described in [I-D.bortzmeyer-dprive-resolver-to-auth] Section 2 extending the authentication of 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 SPKI (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 Infranstructure (PKIX)

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

While simple, a single trusted 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. Simple Public-Key Infrastructure (SPKI)

SPKI on the other hand does not have the same issues than PKIX, the certificates can be generated by the authority itself, adding a separation of privileges between the PKIX infrastructure and the DNS one.

The problem is now on how to advertise/distribute the delegation's public key.

This is in essence what TLSA records solve, but with the use of DNSSEC enabled and functional for the queried zone. For insecure delegations, simply advertising the public key would be subject to interception and mangling.

3.3. Authenticating from the parent

While a delegation is not secured, the DNS core infrastructure already support DNSSEC, meaning that if the owner of an insecure delegation could set the public key to authenticate the DoT servers against, such key could be authenticated using DNSSEC at the parent level, which would then permit trusting the DoT servers providing their certificate validates against the (then validated) public key provided by the parent.

From this stage, the "formerly" insecure delegation can be authenticated, and therefore considered secure, allowing delegating to other zones which can be authenticated by either DNSSEC or TLS.

In order to provide its public key to the DoT clients, an insecure would set the DSPKI RRset at the parent with the content of its extracted SPKI, which the parent then sign.

A DoT client which is about to talk with a DoT server can obtain and validate the DSPKI RRset from the parent and authenticate the DoT server, without needing the DoT server to serve a secure delegation.

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 172800 NS ns1.example.com
example.com 172800 NS ns2.example.com
example.com 86400 DSPKI h0KPxSKAPTEGXnvOPPA/5HUJZjHl4Hu9eg/eYMTPJcc=
ns1.example.com 172800 AAAA 2001:db8:abcd:12:1:2:3:4
ns2.example.com 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 and the DoT client can authenticate them using the provided public key,

If subzone.example.com is a delegation from example.com, example.com can provide the DSPKI RRSet of the delegation. While example.com is not a secured delegation, because it has been authenticated using TLS, it is also able to be part of the chain of trust and provide either a DS or DSPKI RRset for subzone.example.com

4. DSPKI Resource Record

There may be 0 or more DSPKI served by the parent of the delegation. 0 would mean 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. DSPKI RDATA Format

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
/                  PUBKEY                       /
/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Where PUBKEY: A base64 encoded string of the sha256sum of the public key, as generated by: ~~~~ openssl x509 -in cert.pem -pubkey -noout | openssl pkey -pubin -outform der | \ openssl dgst -sha256 -binary | openssl enc -base64 ~~~~

FIXME: consider * format that can evolve over time, e.g 1 byte specifying hashing algorithm. * no need for base64, raw bytes are fine. * 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>.

[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