A DANE Record and DNSSEC Authentication Chain Extension for TLS

draft-ietf-tls-dnssec-chain-extension-01

Abstract

This draft describes a new TLS extension for transport of a DNS record set serialized with the DNSSEC signatures needed to authenticate that record set. The intent of this proposal is to allow TLS clients to perform DANE authentication of a TLS server certificate without needing to perform additional DNS record lookups. It will typically not be used for general DNSSEC validation of TLS endpoint names.

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 http://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 January 8, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Requirements Notation

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].

2. Introduction

This draft describes a new TLS [RFC5246] extension for transport of a DNS record set serialized with the DNSSEC signatures [RFC4034] needed to authenticate that record set. The intent of this proposal is to allow TLS clients to perform DANE authentication [RFC6698] of a TLS server certificate without performing additional DNS record lookups and incurring the associated latency penalty. It also provides the ability to avoid potential problems with TLS clients being unable to look up DANE records because of an interfering or broken middlebox on the path between the client and a DNS server. And lastly, it allows a TLS client to validate DANE records itself without necessarily needing access to a validating DNS resolver to which it has a secure...
connection. It will typically not be used for general DNSSEC validation of endpoint names, but is more appropriate for validation of DANE TLSA records.

This mechanism is useful for TLS applications that need to address the problems described above, typically web browsers or VoIP and XMPP applications. It may not be relevant for many other applications. For example, SMTP MTAs are usually located in data centers, may tolerate extra DNS lookup latency, are on servers where it is easier to provision a validating resolver, or are less likely to experience traffic interference from misconfigured middleboxes. Furthermore, SMTP MTAs usually employ Opportunistic Security [RFC7435], in which the presence of the DNS TLSA records is used to determine whether to enforce an authenticated TLS connection. Hence DANE authentication of SMTP MTAs [RFC7672] will typically not use this mechanism.

The extension described here allows a TLS client to request in the client hello message that the DNS authentication chain be returned in the (extended) server hello message. If the server is configured for DANE authentication, then it performs the appropriate DNS queries, builds the authentication chain, and returns it to the client. The server will usually use a previously cached authentication chain, but it will need to rebuild it periodically as described in Section 5. The client then authenticates the chain using a pre-configured trust anchor.

This specification is based on Adam Langley’s original proposal for serializing DNSSEC authentication chains and delivering them in an X.509 certificate extension [I-D.agl-dane-serializechain]. It modifies the approach by using wire format DNS records in the serialized data (assuming that the data will be prepared and consumed by a DNS-specific library), and by using a TLS extension to deliver the data.

3. DNSSEC Authentication Chain Extension

3.1. Protocol

A client MAY include an extension of type "dnssec_chain" in the (extended) ClientHello. The "extension_data" field of this extension MUST be empty.

Servers receiving a "dnssec_chain" extension in the client hello, and which are capable of being authenticated via DANE, MAY return a serialized authentication chain in the extended ServerHello message, using the format described below. If a server is unable to return an authentication chain, or does not wish to return an authentication chain, it does not include a dnssec_chain extension. As with all TLS
extensions, if the server does not support this extension it will not
return any authentication chain.

A client must not be able to force a server to perform lookups on
arbitrary domain names using this mechanism. Therefore, a server
MUST NOT construct chains for domain names other than its own.

3.2. DNSSEC Authentication Chain Data

The "extension_data" field of the "dnssec_chain" extension MUST
contain a DNSSEC Authentication Chain encoded in the following form:

    opaque AuthenticationChain<0..2^16-1>

The AuthenticationChain structure is composed of a sequence of
uncompressed wire format DNS resource record sets (RRset) and
corresponding signatures (RRsig) records. The record sets and
signatures are presented in validation order, starting at the target
DANE record, followed by the DNSKEY and DS record sets for each
intervening DNS zone up to a trust anchor chosen by the server,
typically the DNS root.

This sequence of native DNS wire format records enables easier

generation of the data structure on the server and easier

verification of the data on client by means of existing DNS library

functions. However this document describes the data structure in

sufficient detail that implementers if they desire can write their

own code to do this.

Each RRset in the chain is composed of a sequence of wire format DNS
resource records. The format of the resource record is described in
RFC 1035 [RFC1035], Section 3.2.1. The resource records SHOULD be
presented in the canonical form and ordering as described in RFC 4034
[RFC4034].

    RR(i) = owner | type | class | TTL | RDATA length | RDATA

RRs within the RRset are ordered canonically, by treating the RDATA
portion of each RR as a left-justified unsigned octet sequence in
which the absence of an octet sorts before a zero octet.

The RRsig record is in DNS wire format as described in RFC 4034
[RFC4034], Section 3.1. The signature portion of the RDATA, as
described in the same section, is the following:
signature = sign(RRSIG_RDATA | RR(1) | RR(2)... )

where, RRSIG_RDATA is the wire format of the RRSIG RDATA fields with
the Signer’s Name field in canonical form and the signature field
excluded.

The first RRset in the chain MUST contain the DANE records being
presented. The subsequent RRsets MUST be a sequence of DNSKEY and DS
RRsets, starting with a DNSKEY RRset. Each RRset MUST authenticate
the preceding RRset:

- A DNSKEY RRset must include the DNSKEY RR containing the public
  key used to verify the previous RRset.
- For a DS RRset, the set of key hashes MUST overlap with the
  preceding set of DNSKEY records.

In addition, a DNSKEY RRset followed by a DS RRset MUST be self-
signed, in the sense that its RRSIG MUST verify under one of the keys
in the DNSKEY RRSET.

The final DNSKEY RRset in the authentication chain, containing the
trust anchor may be omitted. If omitted, the client MUST verify that
the key tag and owner name in the final RRSIG record correspond to a
trust anchor. There may however be reason to include the trust
anchor RRset and signature if clients are expected to use RFC5011
compliant key rollover functions inband via the chain data. In that
case, they will need to periodically inspect flags (revocation and
secure entry point flags) on the trust anchor DNSKEY RRset.

For example, for an HTTPS server at www.example.com, where there are
zone cuts at "com." and "example.com.", the AuthenticationChain
structure would comprise the following RRsets and signatures (the
data field of the records are omitted here for brevity):

```
_443._tcp.www.example.com. TLSA
RRSIG(_443._tcp.www.example.com. TLSA)
example.com. DNSKEY
RRSIG(example.com. DNSKEY)
example.com. DS
RRSIG(example.com. DS)
com. DNSKEY
RRSIG(com. DNSKEY)
com. DS
RRSIG(com. DS)
. DNSKEY
RRSIG(. DNSKEY)
```
Names that are aliased via CNAME and/or DNAME records may involve multiple branches of the DNS tree. In this case the authentication chain structure will be composed of a sequence of these multiple intersecting branches. DNAME chains should omit unsigned CNAME records that may have been synthesized in the response from a DNS resolver. Wildcard DANE records will need to include the wildcard name, and negative proof (i.e. NSEC or NSEC3 records) that no closer name exists MUST be included.

A CNAME example:

```
_443._tcp.www.example.com. IN CNAME ca.example.net.
ca.example.net. IN TLSA 2 0 1 ...
```

Here the authentication chain structure is composed of two consecutive chains, one for `_443._tcp.www.example.com/CNAME` and one for `ca.example.net/TLSA`. The second chain can omit the record sets at the end that overlap with the first.

TLS DNSSEC chain components:

```
_443._tcp.www.example.com. CNAME
RRSIG(_443._tcp.www.example.com. CNAME)
example.com. DNSKEY
RRSIG(example.com. DNSKEY)
exmple.com. DS
RRSIG(example.com. DS)
com. DNSKEY
RRSIG(com. DNSKEY)
com. DS
RRSIG(com. DS)
. DNSKEY
RRSIG(. DNSKEY)

ca.example.net. TLSA
RRSIG(ca.example.net. TLSA)
example.net. DNSKEY
RRSIG(example.net. DNSKEY)
exmple.net. DS
RRSIG(example.net. DS)
net. DNSKEY
RRSIG(net. DNSKEY)
net. DS
RRSIG(net. DS)
```
Note as well that if a user has a specific TLSA record for port 443, and a different wildcard covering other ports, attackers MUST NOT be able to substitute the wildcard TLSA RRset for the more specific one for port 443. DNSSEC wildcards must not be confused with the X.509 wildcards.

4. Construction of Serialized Authentication Chains

This section describes a possible procedure for the server to use to build the serialized DNSSEC chain.

When the goal is to perform DANE authentication [RFC6698] of the server’s X.509 certificate, the DNS record set to be serialized is a TLSA record set corresponding to the server’s domain name.

The domain name of the server MUST be that included in the TLS Server Name Indication extension [RFC6066] when present. If the Server Name Indication extension is not present, or if the server does not recognize the provided name and wishes to proceed with the handshake rather than to abort the connection, the server uses the domain name associated with the server IP address to which the connection has been established.

The TLSA record to be queried is constructed by prepending the _port and _transport labels to the domain name as described in [RFC6698], where "port" is the port number associated with the TLS server. The transport is "tcp" for TLS servers, and "udp" for DTLS servers. The port number label is the left-most label, followed by the transport, followed by the base domain name.

The components of the authentication chain are built by starting at the target record set and its corresponding RRSIG. Then traversing the DNS tree upwards towards the trust anchor zone (normally the DNS root), for each zone cut, the DNSKEY and DS RRsets and their signatures are added. If DNS responses messages contain any domain names utilizing name compression [RFC1035], then they must be uncompressed.

In the future, proposed DNS protocol enhancements, such as the EDNS Chain Query extension [I-D.ietf-dnsop-edns-client-subnet] may offer easy ways to obtain all of the chain data in one transaction with an upstream DNSSEC aware recursive server.

5. Caching and Regeneration of the Authentication Chain

DNS records have Time To Live (TTL) parameters, and DNSSEC signatures have validity periods (specifically signature expiration times). After the TLS server constructs the serialized authentication chain,
it SHOULD cache and reuse it in multiple TLS connection handshakes. However, it MUST refresh and rebuild the chain as TTLs and signature validity periods dictate. A server implementation could carefully track these parameters and query component records in the chain correspondingly. Alternatively, it could be configured to rebuild the entire chain at some predefined periodic interval that does not exceed the DNS TTLs or signature validity periods of the component records in the chain.

6. Verification

A TLS client making use of this specification, and which receives a DNSSEC authentication chain extension from a server, SHOULD use this information to perform DANE authentication of the server certificate. In order to do this, it uses the mechanism specified by the DNSSEC protocol [RFC4035]. This mechanism is sometimes implemented in a DNSSEC validation engine or library.

If the authentication chain is correctly verified, the client then performs DANE authentication of the server according to the DANE TLS protocol [RFC6698], and the additional protocol requirements outlined in [RFC7671].

7. Trust Anchor Maintenance

The trust anchor may change periodically, e.g. when the operator of the trust anchor zone performs a DNSSEC key rollover. Managed key rollovers typically use a process that can be tracked by verifiers allowing them to automatically update their trust anchors, as described in [RFC5011]. TLS clients using this specification are also expected to use such a mechanism to keep their trust anchors updated. Some operating systems may have a system-wide service to maintain and keep the root trust anchor up to date. In such cases, the TLS client application could simply reference that as its trust anchor, periodically checking whether it has changed.

8. Mandating use of this extension

A TLS server certificate MAY mandate the use of this extension by means of the X.509 TLS Feature Extension described in [RFC7633]. This X.509 certificate extension, when populated with the dnssec_chain TLS extension identifier, indicates to the client that the server must deliver the authentication chain when asked to do so. (The X.509 TLS Feature Extension is the same mechanism used to deliver other mandatory signals, such as OCSP "must staple" assertions.)
9. Security Considerations

The security considerations of the normatively referenced RFCs (1035, 4034, 4035, 5246, 6066, 6698, 7633, 7671) all pertain to this extension. Since the server is delivering a chain of DNS records and signatures to the client, it MUST rebuild the chain in accordance with TTL and signature expiration of the chain components as described in Section 5. TLS clients need roughly accurate time in order to properly authenticate these signatures. This could be achieved by running a time synchronization protocol like NTP [RFC5905] or SNTP [RFC5905], which are already widely used today. TLS clients MUST support a mechanism to track and rollover the trust anchor key, or be able to avail themselves of a service that does this, as described in Section 7.

10. IANA Considerations

This extension requires the registration of a new value in the TLS ExtensionsType registry. The value requested from IANA is 53. If the draft is adopted by the WG, the authors expect to make an early allocation request as specified in [RFC7120].

11. Acknowledgments

Many thanks to Adam Langley for laying the groundwork for this extension. The original idea is his but our acknowledgment in no way implies his endorsement. This document also benefited from discussions with and review from the following people: Viktor Dukhovni, Daniel Kahn Gillmor, Jeff Hodges, Allison Mankin, Patrick McManus, Rick van Rein, Gowri Visweswaran, Duane Wessels, Nico Williams, and Paul Wouters.

12. References

12.1. Normative References


12.2. Informative References


Appendix A. Updates from -00

- Edits based on comments from Rick van Rein
- Warning about not overloading X.509 wildcards on DNSSEC wildcards (from V. Dukhovny)
- Added MUST include negative proof on wildcards (from V. Dukhovny)
- Removed "TODO" on allowing the server to deliver only one signature per RRset
- Added additional minor edits suggested by Viktor Dukhovny

Appendix B. Test vector

[data go here]

Authors’ Addresses

Melinda Shore
No Mountain Software
EMail: melinda.shore@nomountain.net

Richard Barnes
Mozilla
EMail: rlb@ipv.sx

Shumon Huque
Verisign Labs
EMail: shuque@verisign.com

Willem Toorop
NLNet Labs
EMail: willem@nlnetlabs.nl