DNS-Based Authentication of Named Entities (DANE)
Internet-Draft
Intended status: Standards Track
Expires: October 17, 2015

T. Finch
University of Cambridge
M. Miller
Cisco Systems, Inc.
P. Saint-Andre
&yet

April 15, 2015

Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records
draft-ietf-dane-srv-13

Abstract

The DANE specification (RFC 6698) describes how to use TLSA resource records secured by DNSSEC (RFC 4033) to associate a server's connection endpoint with its TLS certificate. However, application protocols that use SRV records (RFC 2782) to indirectly name the target server connection endpoints for a service domain cannot apply the rules from RFC 6698. Therefore this document provides guidelines that enable such protocols to locate and use TLSA records.

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 October 17, 2015.

Table of Contents

1. Introduction

The base DANE specification [RFC6698] describes how to use TLSA resource records secured by DNSSEC [RFC4033] to associate a target server's connection endpoint with its TLS certificate. Some application protocols locate connection endpoints indirectly via SRV records [RFC2782]. As a result of this indirection, the rules specified in [RFC6698] cannot be directly applied to such application protocols. (Rules for SMTP [RFC5321], which uses MX resource records instead of SRV records, are described in [I-D.ietf-dane-smtp-with-dane].)

This document describes how to use DANE TLSA records with SRV records. To summarize:

- We rely on DNSSEC to secure SRV records that map the desired service, transport protocol, and service domain to the corresponding target server connection endpoints (i.e., the target server host names and port numbers returned in the SRV records for that service type).

- Although in accordance with [RFC2782] a service domain can advertise a number of SRV records (some of which might map to connection endpoints that do not support TLS), the intent of this specification is for a client to securely discover connection endpoints that support TLS.

- The TLSA records for each connection endpoint are located using the transport protocol, port number, and host name for the target server (not the service domain).

- When DNSSEC-validated TLSA records are published for a given connection endpoint, clients always use TLS when connecting (even if the connection endpoint supports cleartext communication).

- If there is at least one usable TLSA record for a given connection endpoint, the connection endpoint's TLS certificate or public key needs to match at least one of those usable TLSA records.

- If there are no usable TLSA records for a given connection endpoint, the target server host name is used as one of the acceptable reference identifiers, as described in [RFC6125]. Other reference identifiers might arise through CNAME expansion of either the service domain or target server host name, as detailed in [I-D.ietf-dane-ops].

- If there are no usable TLSA records for any connection endpoint (and thus the client cannot securely discover a connection endpoint that supports TLS), the client's behavior is a matter for the application protocol or client implementation; this might involve a fallback to non-DANE behavior using the public key infrastructure [RFC5280].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this memo are to be interpreted as described in [RFC2119].

This draft uses the definitions for "secure", "insecure", "bogus", and "indeterminate" from Section 4.3 of [RFC4035]. This draft uses the acronyms from [RFC7218] for the values of TLSA fields where appropriate.

Additionally, this document uses the following terms:

connection endpoint: A tuple of a fully qualified DNS host name, transport protocol, and port number that a client uses to establish a connection to the target server.

service domain: The fully qualified DNS domain name that identifies an application service; corresponds to the term "source domain" from [RFC6125].

This document uses the term "target server host name" in place of the term "derived domain" from the CertID specification [RFC6125].

3. DNS Checks

3.1. SRV Query

When the client makes an SRV query, a successful result will typically be a list of one or more SRV records (or possibly a chain of CNAME / DNAME aliases leading to such a list).

NOTE: Implementers need to be aware that unsuccessful results can occur because of various DNS-related errors; guidance on avoiding downgrade attacks can be found in Section 4 of [I-D.ietf-dane-smtp-with-dane].

For this specification to apply, the entire chain of DNS RRset(s) returned MUST be "secure" according to DNSSEC validation (Section 5 of [RFC4035]). In the case where the answer is obtained via a chain of CNAME and/or DNAME aliases, the whole chain of CNAME and DNAME RRsets MUST also be secure.

If the SRV lookup fails because the RRset is "bogus" (or the lookup fails for reasons other than no records), the client MUST abort its attempt to connect to the desired service. If the lookup result is "insecure" (or no SRV records exist), this protocol does not apply and the client SHOULD fall back to its non-DNSSEC, non-DANE (and possibly non-SRV) behavior.

When the lookup returns a "secure" RRset (possibly via a chain of "secure" CNAME/DNAME records), the client now has an authentic list of target server connection endpoints with weight and priority values. It performs server ordering and selection using the weight

and priority values without regard to the presence or absence of DNSSEC or TLSA records. It also takes note of the DNSSEC validation status of the SRV response for use when checking certificate names (see Section 4). The client can then proceed to making address queries on the target server host names as described in the following section.

3.2. Address Queries

For each SRV target server connnection endpoint, the client makes A and/or AAAA queries, performs DNSSEC validation on the address (A or AAAA) response, and continues as follows based on the results:

- If either the A or AAAA RRSets are "secure", the client MUST perform a TLSA query for that target server connection endpoint as described in the next section.

- If both RRsets are "insecure", the client MUST NOT perform a TLSA query for that target server connection endpoint; the TLSA query will most likely fail or produce spurious results.

- If the address record lookup fails (this a validation status of either "bogus" or "indeterminate"), the client MUST NOT connect to this connection endpoint; instead it uses the next most appropriate SRV target. This mitigates against downgrade attacks.

3.3. TLSA Queries

The client SHALL construct the TLSA query name as described in Section 3 of [RFC6698], based on the fields from the SRV record: the port number from the SRV RDATA, the transport protocol from the SRV query name, and the TLSA base domain from the SRV target server host name.

For example, the following SRV record for IMAP (see [RFC6186]):

```
_imap._tcp.example.com. 86400 IN SRV 10 0 9143 imap.example.net.
```

leads to the TLSA query shown below:

```
_9143._tcp.imap.example.net. IN TLSA ?
```

3.4. Impact on TLS Usage

The client SHALL determine if the TLSA records returned in the previous step are usable according to Section 4.1 of [RFC6698]. This affects the use of TLS as follows:

- If the TLSA response is "secure" and usable, then the client MUST use TLS when connecting to the target server. The TLSA records are used when validating the server's certificate as described in Section 4.

- If the TLSA response is "bogus" or "indeterminate" (or the lookup fails for reasons other than no records), then the client MUST NOT connect to the target server (the client can still use other SRV targets).

- If the TLSA response is "insecure" (or no TLSA records exist), then the client SHALL proceed as if the target server had no TLSA records. It MAY connect to the target server with or without TLS, subject to the policies of the application protocol or client implementation.

4. TLS Checks

When connecting to a server, the client MUST use TLS if the responses to the SRV and TLSA queries were "secure" as described above. The rules described in the next two sections apply to such secure responses; Section 4.2 where there is at least one usable TLSA record, and Section 4.1 otherwise.

4.1. SRV Records Only

If the client received zero usable TLSA certificate associations, it SHALL validate the server's TLS certificate using the normal PKIX rules [RFC5280] or protocol-specific rules (e.g., following [RFC6125]) without further input from the TLSA records. In this case, the client uses the information in the server certificate and the DNSSEC validation status of the SRV query in its authentication checks. It SHOULD use the Server Name Indication extension (TLS SNI) [RFC6066] or its functional equivalent in the relevant application protocol (e.g., in XMPP [RFC6120] this is the 'to' address of the initial stream header). The preferred name SHALL be chosen as follows, and the client SHALL verify the identity asserted by the server's certificate according to Section 6 of [RFC6125], using a list of reference identifiers constructed as follows (note again that in RFC 6125 the terms "source domain" and "derived domain" to refer to the same things as "service domain" and "target server host name" in this document). The examples below assume a service domain of "im.example.com" and a target server host name of "xmpp23.hosting.example.net".

SRV is insecure: The reference identifiers SHALL include the service domain and MUST NOT include the SRV target server host name (e.g., include "im.example.com" but not "xmpp23.hosting.example.net").

The service domain is the preferred name for TLS SNI or its equivalent.

SRV is secure: The reference identifiers SHALL include both the service domain and the SRV target server host name (e.g., include both "im.example.com" and "xmpp23.hosting.example.net"). The target server host name is the preferred name for TLS SNI or its equivalent.

In the latter case, the client will accept either identity to ensure compatibility with servers that support this specification as well as servers that do not support this specification.

4.2. TLSA Records

If the client received one or more usable TLSA certificate associations, it SHALL process them as described in Section 2.1 of [RFC6698].

If the TLS server's certificate -- or the public key of the server's certificate -- matches a usable TLSA record with Certificate Usage "DANE-EE", the client MUST ignore validation checks from [RFC5280] and reference identifier checks from [RFC6125]. The information in such a TLSA record supersedes the non-key information in the certificate.

5. Guidance for Protocol Authors

This document describes how to use DANE with application protocols in which target servers are discovered via SRV records. Although this document attempts to provide generic guidance applying to all such protocols, additional documents for particular application protocols could cover related topics, such as:

- Fallback logic in the event that a client is unable to connect securely to a target server by following the procedures defined in this document.

- How clients ought to behave if they do not support SRV lookups, or if clients that support SRV lookups encounter service domains that do not offer SRV records.

- Whether the application protocol has a functional equivalent for TLS SNI that is preferred within that protocol.

- Use of SRV records with additional discovery technologies, such as the use of both SRV records and NAPTR records [RFC3403] for transport selection in the Session Initiation Protocol (SIP).

For example, [I-D.ietf-xmpp-dna] covers such topics for the Extensible Messaging and Presence Protocol (XMPP).

6. Guidance for Server Operators

To conform to this specification, the published SRV records and subsequent address (A and AAAA) records MUST be secured with DNSSEC. There SHOULD also be at least one TLSA record published that authenticates the server's certificate.

When using TLSA records with Certificate Usage "DANE-EE", it is not necessary for the deployed certificate to contain an identifier for either the source domain or target server host name. However, operators need to be aware that servers relying solely on validation using Certificate Usage "DANE-EE" TLSA records might prevent clients that do not support this specification from successfully connecting with TLS.

For TLSA records with Certificate Usage types other than "DANE-EE", the certificate(s) MUST contain an identifier that matches:

- the service domain name (the "source domain" in [RFC6125] terms, which is the SRV query domain); and/or

- the target server host name (the "derived domain" in [RFC6125] terms, which is the SRV target host name).

Servers that support multiple service domains (i.e., so-called "multi-tenanted environments") can implement the Transport Layer Security Server Name Indication (TLS SNI) [RFC6066] or its functional equivalent to determine which certificate to offer. Clients that do not support this specification will indicate a preference for the service domain name, while clients that support this specification will indicate the target server host name. However, the server determines what certificate to present in the TLS handshake; e.g., the presented certificate might only authenticate the target server host name.

7. Guidance for Application Developers

Developers of application clients that depend on DANE-SRV often would like to prepare as quickly as possible for making a connection to the intended service, thus reducing the wait time for end users. To make this optimization possible, a DNS library might perform the SRV queries, address queries, and TLSA queries in parallel. (Because a TLSA record can be ignored if it turns out that the address record on which it depends is not secure, performing the TLSA queries in

parallel with the SRV queries and address queries is not harmful from a security perspective and can yield some operational benefits.)

8. Internationalization Considerations

If any of the DNS queries are for an internationalized domain name, then they need to use the A-label form [RFC5890].

9. IANA Considerations

No IANA action is required.

10. Security Considerations

10.1. Mixed Security Status

We do not specify that all of the target server connection endpoints for a service domain need to be consistent in whether they have or do not have TLSA records. This is so that partial or incremental deployment does not break the service. Different levels of deployment are likely if a service domain has a third-party fallback server, for example.

The SRV sorting rules are unchanged; in particular they have not been altered in order to prioritize secure connection endpoints over insecure connection endpoints. If a site wants to be secure it needs to deploy this protocol completely; a partial deployment is not secure and we make no special effort to support it.

10.2. Certificate Subject Name Matching

Section 4 of the TLSA specification [RFC6698] leaves the details of checking names in certificates to higher level application protocols, though it suggests the use of [RFC6125].

Name checks are not necessary if the matching TLSA record is of Certificate Usage "DANE-EE". Because such a record identifies the specific certificate (or public key of the certificate), additional checks are superfluous and potentially conflicting.

Otherwise, while DNSSEC provides a secure binding between the server name and the TLSA record, and the TLSA record provides a binding to a certificate, this latter step can be indirect via a chain of certificates. For example, a Certificate Usage "PKIX-TA" TLSA record only authenticates the CA that issued the certificate, and third parties can obtain certificates from the same CA. Therefore, clients need to check whether the server's certificate matches one of the expected reference identifiers to ensure that the certificate was

issued by the CA to the server the client expects (naturally, this is in addition to standard certificate-related checks as specified in [RFC5280], including but not limited to certificate syntax, certificate extensions such as name constraints and extended key usage, and handling of certification paths).

11. References

11.1. Normative References

[I-D.ietf-dane-ops]
Dukhovni, V. and W. Hardaker, "Updates to and Operational Guidance for the DANE Protocol", draft-ietf-dane-ops-07 (work in progress), October 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[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, May 2008.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August 2010.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[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, March 2011.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

[RFC7218] Gudmundsson, O., "Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)", RFC 7218, April 2014.

11.2. Informative References

[I-D.ietf-dane-smtp-with-dane]
Dukhovni, V. and W. Hardaker, "SMTP security via opportunistic DANE TLS", draft-ietf-dane-smtp-with-dane-15 (work in progress), March 2015.

[I-D.ietf-xmpp-dna]
Saint-Andre, P., Miller, M., and P. Hancke, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", draft-ietf-xmpp-dna-10 (work in progress), March 2015.

[RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, March 2011.

Appendix A. Examples

In the following, most of the DNS resource data is elided for simplicity.

A.1. IMAP

```
; mail domain
_imap._tcp.example.com.   SRV 10 0 9143 imap.example.net.
example.com.              RRSIG   SRV ...

; target server host name
imap.example.net.         A      192.0.2.1
imap.example.net.         RRSIG  A ...

imap.example.net.         AAAA   2001:db8:212:8::e:1
imap.example.net.         RRSIG  ...

; TLSA resource record
_9143._tcp.imap.example.net.  TLSA   ...
_9143._tcp.imap.example.net.  RRSIG  TLSA ...
```

Mail messages received for addresses at example.com are retrieved via IMAP at imap.example.net. Connections to imap.example.net port 9143 that use STARTTLS will get a server certificate that authenticates the name imap.example.net.

A.2. XMPP

```
; XMPP domain
_xmpp-client._tcp.example.com. SRV     1 0 5222 im.example.net.
_xmpp-client._tcp.example.com. RRSIG   SRV ...

; target server host name
im.example.net.           A      192.0.2.3
im.example.net.           RRSIG  A ...

im.example.net.           AAAA   2001:db8:212:8::e:4
im.example.net.           RRSIG  AAAA ...

; TLSA resource record
_5222._tcp.im.example.net.  TLSA   ...
_5222._tcp.im.example.net.  RRSIG  TLSA ...
```

XMPP sessions for addresses at example.com are established at im.example.net. Connections to im.example.net port 5222 that use STARTTLS will get a server certificate that authenticates the name im.example.net.

Appendix B. Rationale

The long-term goal of this specification is to settle on TLS certificates that verify the target server host name rather than the service domain, since this is more convenient for servers hosting multiple domains (so-called "multi-tenanted environments") and scales up more easily to larger numbers of service domains.

There are a number of other reasons for doing it this way:

- The certificate is part of the server configuration, so it makes sense to associate it with the server host name rather than the service domain.

- In the absence of TLS SNI, if the certificate identifies the target server host name then it does not need to list all the possible service domains.

- When the server certificate is replaced it is much easier if there is one part of the DNS that needs updating to match, instead of an unbounded number of hosted service domains.

- The same TLSA records work with this specification, and with direct connections to the connection endpoint in the style of [RFC6698].

- Some application protocols, such as SMTP, allow a client to perform transactions with multiple service domains in the same connection. It is not in general feasible for the client to specify the service domain using TLS SNI when the connection is established, and the server might not be able to present a certificate that authenticates all possible service domains. See [I-D.ietf-dane-smtp-with-dane] for details.

- It is common for SMTP servers to act in multiple roles, for example as outgoing relays or as incoming MX servers, depending on the client identity. It is simpler if the server can present the same certificate regardless of the role in which it is to act. Sometimes the server does not know its role until the client has authenticated, which usually occurs after TLS has been established. See [I-D.ietf-dane-smtp-with-dane] for details.

This specification does not provide an option to put TLSA records under the service domain because that would add complexity without providing any benefit, and security protocols are best kept simple. As described above, there are real-world cases where authenticating the service domain cannot be made to work, so there would be complicated criteria for when service domain TLSA records might be

used and when they cannot. This is all avoided by putting the TLSA records under the target server host name.

The disadvantage is that clients which do not complete DNSSEC validation must, according to [RFC6125] rules, check the server certificate against the service domain, since they have no other way to authenticate the server. This means that SNI support or its functional equivalent is necessary for backward compatibility.

Appendix C. Acknowledgements

Thanks to Mark Andrews for arguing that authenticating the target server host name is the right thing, and that we ought to rely on DNSSEC to secure the SRV lookup. Thanks to Stephane Bortzmeyer, James Cloos, Viktor Dukhovni, Ned Freed, Olafur Gudmundsson, Paul Hoffman, Phil Pennock, Hector Santos, Jonas Schneider, and Alessandro Vesely for helpful suggestions.

Carl Wallace provided an insightful review on behalf of the Security Directorate.

The authors gratefully acknowledge the assistance of Olafur Gudmundsson and Warren Kumari as the working group chairs and Stephen Farrell as the sponsoring Area Director.

Peter Saint-Andre wishes to acknowledge Cisco Systems, Inc., for employing him during his work on earlier versions of this document.

Authors' Addresses

Tony Finch
University of Cambridge Computing Service
New Museums Site
Pembroke Street
Cambridge CB2 3QH
ENGLAND

Phone: +44 797 040 1426
Email: dot@dotat.at
URI: http://dotat.at/

Matthew Miller
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Email: mamille2@cisco.com

Peter Saint-Andre
&yet

Email: peter@andyet.com
URI: https://andyet.com/