DNS-Based Authentication of Named Entities (DANE)   T. Finch
Internet-Draft   University of Cambridge
Intended status: Standards Track   M. Miller
Expires: August 17, 2014   Cisco Systems, Inc.
                                                          P. Saint-Andre
                                                                    &yet
                                                       February 13, 2014

Using DNS-Based Authentication of Named Entities (DANE) TLSA records with SRV and MX records.
draft-ietf-dane-srv-05

Abstract

The DANE specification (RFC 6698) describes how to use TLSA resource records in the DNS to associate a server's host name with its TLS certificate. The association is secured with DNSSEC. Some application protocols use SRV records (RFC 2782) to indirectly name the server hosts for a service domain (SMTP uses MX records for the same purpose). This specification gives generic instructions for how these application protocols locate and use TLSA records when technologies such as SRV records are used. Separate documents give the details that are specific to particular application protocols.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The base DANE specification [RFC6698] describes how to use TLSA resource records in the DNS to associate a server's host name with its TLS certificate. The association is secured using DNSSEC. That document "only relates to securely associating certificates for TLS and DTLS with host names" (see the last paragraph of section 1.2 of [RFC6698]).

Some application protocols do not use host names directly; instead, they use a service domain and the relevant host names are located indirectly via SRV records [RFC2782], or MX records in the case of

SMTP [RFC5321] (Note: in the "CertID" specification [RFC6125], the source domain and host name are referred to as the "source domain" and the "derived domain"). Because of this intermediate resolution step, the normal DANE rules specified in [RFC6698] do not directly apply to protocols that use SRV or MX records.

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

- o We rely on DNSSEC to secure the association between the service domain and the target server host names (i.e., the host names that are discovered by the SRV or MX query).

- o The TLSA records are located using the port, protocol, and target host name fields (not the service domain).

- o Clients always use TLS when connecting to servers with TLSA records.

- o Assuming that the association is secure, the server's certificate is expected to authenticate the target server host name, rather than the service domain.

Separate documents give the details that are specific to particular application protocols, such as SMTP [I-D.ietf-dane-smtp-with-dane] and XMPP [I-D.ietf-xmpp-dna].

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 [RFC4035]. This draft uses the acronyms from [I-D.ietf-dane-registry-acronyms] for the values of TLSA fields where appropriate.

3. Relation between SRV and MX records

For the purpose of this specification (to avoid cluttering the description with special cases) we treat each MX record ([RFC5321] section 5) as being equivalent to an SRV record [RFC2782] with corresponding fields copied from the MX record and the remaining fields having fixed values as follows:

Table 1: SRV Fields and MX Equivalents

DNS SRV Field	Equivalent MX Value
Service	smtp
Proto	tcp
Name	MX owner name (mail domain)
TTL	MX TTL
Class	MX Class
Priority	MX Priority
Weight	0
Port	25
Target	MX Target

Thus we can treat the following MX record as if it were the SRV record shown below:

```
example.com.            86400 IN MX  10      mx.example.net.

_smtp._tcp.example.com. 86400 IN SRV 10 0 25 mx.example.net.
```

Other details that are specific to SMTP are described in [I-D.ietf-dane-smtp-with-dane].

4. DNS Checks for TLSA and SRV Records

4.1. SRV Query

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

For this specification to apply, all of these DNS RRsets MUST be "secure" according to DNSSEC validation ([RFC4033] section 5). In the case of aliases, the whole chain of CNAME and DNAME RRsets MUST be secure as well. This corresponds to the AD bit being set in the response(s); see [RFC4035] section 3.2.3.

If they are not all secure, this protocol has not been correctly deployed. The client SHOULD fall back to its non-DNSSEC non-DANE behavior (this corresponds to the AD bit being unset).

If any of the responses are "bogus" or "indeterminate" according to DNSSEC validation, the client MUST abort (This usually corresponds to a "server failure" response).

In the successful case, the client now has an authentic list of server host names 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 takes note of the DNSSEC validation status of the SRV response for use when checking certificate names (see Section 5).

4.2. TLSA Queries

If the SRV response was insecure, the client MUST NOT perform any TLSA queries. If the SRV response is "secure" according to DNSSEC validation, the client performs a TLSA query for each SRV target as described in this section.

For each SRV target host name, the client performs DNSSEC validation on the address (A, AAAA) response and continues based on the results:

- o if the response is "insecure", the client MUST NOT perform a TLSA query for that target; the TLSA query will most likely fail.

- o If the response is "bogus" or "indeterminate", the client MUST NOT connect to this host name; instead it uses the next most appropriate SRV target.

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

For example, the following SRV record leads to the TLSA query shown below:

```
_imap._tcp.example.com. 86400 IN SRV 10 0 143 imap.example.net.
```

```
_143._tcp.imap.example.net. IN TLSA ?
```

The client SHALL determine if the TLSA record(s) are usable according to section 4.1 of [RFC6698]. This affects SRV handling as follows:

If the TLSA response is "secure", the client MUST use TLS when connecting to the server. The TLSA records are used when validating the server's certificate as described under Section 5.

If the TLSA response is "insecure", the client SHALL proceed as if this server has no TLSA records. It MAY connect to the server with or without TLS.

If the TLSA response is "bogus" or "indeterminate", then the client MUST NOT connect to this server (the client can still use other SRV targets).

5. TLS Checks for TLSA and SRV Records

When connecting to a server, the client MUST use TLS if the responses to the SRV and TLSA queries were "secure" as described above. 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. If the client received one or more usable TLSA certificate associations, it SHALL process them as described in [RFC6698] section 2.1.

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 consider the server to be authenticated. Because the information in such a TLSA record supersedes the non-key information in the certificate, all other [RFC5280] and [RFC6125] authentication checks (e.g., reference identifier, key usage, expiration, issuance, etc.) MUST be ignored or omitted.

Otherwise, the client uses the information in the server certificate and 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 [RFC6125] section 6, using a list of reference identifiers constructed as follows (note again that in RFC 6125 the terms "source domain" and "derived domain" refer to the same things as "service domain" and "target host name" in this document).

SRV is insecure: The reference identifiers SHALL include the service domain and MUST NOT include the SRV target host name. 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 host name. The target host name is the preferred name for TLS SNI or its equivalent.

In the latter case, the client will accept either identity so that it is compatible with servers that do and do not support this specification.

6. Guidance for Application Protocols

Separate documents describe how to apply this specification to particular application protocols. Such documents ought to cover the following points:

- Fallback logic in the event of bogus replies and the like.

- The use of TLS SNI or its functional equivalent.

- Appropriate mappings for non-SRV technologies such as MX.

- Compatibility with clients that do not support SRV lookups.

7. Guidance for Server Operators

To conform to this specification, the published SRV records and subsequent address (A, 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", the deployed certificate does not need to contain any of the possible reference identifiers discussed below. Indeed, none of the certificate's information is necessary for such certificates. However, servers that rely 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 a reference identifier that matches:

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

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

Servers that support multiple service domains (i.e., multi-tenant) can implement Server Name Indicator (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 server host name. However, the server determines what certificate to present in the TLS handshake; e.g., the presented certificate might only authenticate the server host name.

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 clients checking all of a service domain's server host names are 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 and MX sorting rules are unchanged; in particular they have not been altered in order to prioritize secure servers over insecure servers. 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. A Service Domain Trusts its Servers

By signing their zone with DNSSEC, service domain operators implicitly instruct their clients to check their server TLSA records. This implies another point in the trust relationship between service domain holders and their server operators. Most of the setup requirements for this protocol fall on the server operator: installing a TLS certificate with the correct name (where necessary), and publishing a TLSA record for that certificate. If these are not correct then connections from TLSA-aware clients might fail.

10.3. 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 the certificate was issued by the CA to the server the client expects.

11. Acknowledgements

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

12. References

12.1. Normative References

[I-D.ietf-dane-registry-acronyms]
Gudmundsson, O., "Adding acronyms to simplify DANE conversations", draft-ietf-dane-registry-acronyms-03 (work in progress), January 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.

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

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

12.2. 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-05 (work in progress), February 2014.

[I-D.ietf-xmpp-dna] Saint-Andre, P. and M. Miller, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", draft-ietf-xmpp-dna-05 (work in progress), February 2014.

Appendix A. Mail Example

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

```
; mail domain
example.com.               MX      1 mx.example.net.
example.com.               RRSIG   MX ...

; SMTP server host name
mx.example.net.            A      192.0.2.1
mx.example.net.            RRSIG  A ...

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

; TLSA resource record
_25._tcp.mx.example.net.  TLSA   ...
_25._tcp.mx.example.net.  RRSIG  TLSA ...
```

Mail for addresses at example.com is delivered by SMTP to mx.example.net. Connections to mx.example.net port 25 that use STARTTLS will get a server certificate that authenticates the name mx.example.net.

Appendix B. XMPP Example

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

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

; XMPP 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 C. Rationale

The long-term goal of this specification is to settle on TLS certificates that verify the 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 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 host name 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.

- 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.

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 server host name.

The disadvantage is that clients which do not do 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.

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: ietf@stpeter.im