DNS-Based Authentication of Named Entities (DANE)
Internet-Draft
Updates: 6186 (if approved)
Intended status: Standards Track
Expires: December 29, 2012

T. Finch
University of Cambridge

June 27, 2012

DNSSEC and TLSA records for IMAP, POP3, and message submission
draft-fanf-dane-mua-00

Abstract

This specification describes the effect that DNSSEC has on SRV-based autoconfiguration and TLS certificate verification in the mail user agent protocols IMAP, POP3, and message submission. It also describes how to use TLSA DNS records to provide stronger authentication of server TLS certificates.

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 December 29, 2012.

Table of Contents

1. Introduction

The mail user agent protocols IMAP [RFC3501], POP3 [RFC1939], and message submission [RFC4409] support upgrade from cleartext to TLS [RFC5246]. The STARTTLS command is part of the core IMAP specification [RFC3501]. Message submission is a profile of SMTP [RFC5321] for which there is a STARTTLS extension [RFC3207]. In POP3 the equivalent command is STLS [RFC2595]. IMAP and POP3 are also often deployed using TLS-on-connect on alternate TCP ports.

[RFC6186] specifies how an MUA can use SRV records to automatically locate mail server host names given the user's mail domain. Section 2 of this specification updates [RFC6186] to clarify how MUAs handle mail server SRV records and TLS negotiation in the presence and absence of DNSSEC.

Section 3 of this specification describes how to use TLSA DNS records [I-D.ietf-dane-protocol] to provide stronger authentication of server TLS certificates. We also use the existance of a TLSA record to signal to the MUA that it can expect the server to offer TLS.

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

2. DNSSEC, TLS, and mail server SRV records

When negotiating TLS, the MUA MUST use the Server Name Indication extension (TLS SNI) [RFC6066] with its preferred name as defined below. This is a stricter requirement than [RFC6186].

When a security-aware MUA looks up [RFC6186] SRV records, it SHALL take note of the DNSSEC status [RFC4033] of each record. It constructs the list of reference identifiers for verifying each server's TLS certificate [RFC6125] and chooses the preferred name for TLS SNI as follows:

bogus: The MUA MUST abort. (If this occurs during auto-configuration, it might fall back to a manual setup procedure.)

insecure or indeterminate: The reference identifiers SHALL include the source domain (i.e. the user's mail domain) and MUST NOT include the derived domain (i.e. the SRV target host name). The source domain is the preferred name for TLS SNI.

secure: The reference identifiers SHALL include both the source domain (i.e. the user's mail domain) and the derived domain (i.e. the SRV target host name). The derived domain is the preferred name for TLS SNI.

3. Mail server TLSA records

MUAs SHALL look up the TLSA record(s) for a mail server using its host name and port number, as described in section 3 of [I-D.ietf-dane-protocol]. The MUA MUST only do this if the host name and port number have been obtained securely, from the "target" and "port" fields of a SRV record that is secure as described in the previous section, or from user configuration.

If a TLSA record is usable as described in section 4.1 of [I-D.ietf-dane-protocol], then the server MUST support TLS. It MUST present a certificate that matches the TLSA record and that authenticates the server host name.

When an MUA is configuring itself as described in section 4 of [RFC6186], it SHOULD use the presence of a TLSA record to indicate that use of TLS is obligatory when connecting to the corresponding server.

4. Guidance for mail service providers

A mail server that is the target of an [RFC6186] SRV record MUST have a TLS certificate that authenticates the SRV owner domain (i.e. the user's mail domain). This is necessary for clients that cannot perform DNSSEC validation. This certificate MUST be the default that is presented if the client does not use the TLS Server Name Indication extension (TLS SNI) [RFC6066].

In order to support this specification, the mail server MUST also have a certificate that authenticates the SRV target domain (the mail server hostname). This can be done using a multi-name certificate or by using the client's TLS SNI to select the appropriate certificate. The mail server's TLSA record MUST correspond to this certificate.

Note: old pre-[RFC6186] clients expect a mail server's TLS certificate to authenticate its host name; they are also unlikely to support SNI. This means that servers for old clients need a different default certificate from [RFC6186] servers. If the server does not have a certificate that authenticates all relevant names, it is necessary to segregate old and new clients. This can be done by using different target hosts or non-standard ports in the SRV

targets. (The latter avoids the need for yet more certificates.)

5. Guidance for mail server software authors

In order to support this specification, mail server software MUST implement the TLS Server Name Indication extension [RFC6066] for selecting the appropriate certificate.

6. Security considerations

The MUA autoconfiguration specification [RFC6186] does not have a complete mechanism for signalling whether a server supports TLS. IMAP and POP3 have alternate TLS-on-connect ports, but not message submission. This gap is filled by using the presence of TLSA records to indicate that a client can expect a server to support TLS. This prevents a downgrade attack.

The guidance in Section 2 is mostly a straightforward consequence of the requirements set out in [RFC6125] and [RFC6186].

7. Internationalization Considerations

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

8. IANA Considerations

No IANA action is needed.

9. References

9.1. Normative References

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

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

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, June 1999.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over

Transport Layer Security", RFC 3207, February 2002.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

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

[RFC4409] Gellens, R. and J. Klensin, "Message Submission for Mail", RFC 4409, April 2006.

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

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 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.

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

[I-D.ietf-dane-protocol]
Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", draft-ietf-dane-protocol-23 (work in progress), May 2012.

9.2. Informative References

[I-D.fanf-dane-smtp]
Finch, T., "Secure SMTP with TLS, DNSSEC and TLSA records.", draft-fanf-dane-smtp-03 (work in progress), June 2012.

[I-D.miller-xmpp-dnssec-prooftype]

Miller, M. and P. Saint-Andre, "Using DNSSEC and DANE as a Prooftype for XMPP Delegation", draft-miller-xmpp-dnssec-prooftype-01 (work in progress), June 2012.

Appendix A. Rationale - where to put TLSA records

The long-term goal of this specification is to settle on TLS certificates that verify the server host name rather than the mail domain, since this is more convenient for servers hosting multiple domains and scales up more easily to larger numbers of 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 name rather than the mail domain.
- 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 mail domains.
- The same TLSA records work with and without [RFC6186] SRV records.
- Consistency with [I-D.fanf-dane-smtp] and [I-D.miller-xmpp-dnssec-prooftype].

There is no option to put TLSA records under the mail domain in order to keep the specification simple and to make it easier to deploy correctly.

The disadvantage is that the expected certificate differs between pure [RFC6186] clients and clients that are implemented to this spec. This means that Server Name Indication support is necessary for backwards compatibility.

Author's Address

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/