DNS-Based Authentication of Named Entities (DANE)
Internet-Draft
Intended status: Standards Track
Expires: August 29, 2013

T. Finch
University of Cambridge

February 25, 2013

Secure SMTP using DNS-Based Authentication of Named Entities (DANE) TLSA records.

draft-ietf-dane-smtp-01

Abstract

SMTP has a STARTTLS extension, but (especially in the case of inter-domain mail transfer) it only provides very limited security because it does not specify how to authenticate the server's certificate. This memo specifies how TLSA records in the DNS can be used for proper SMTP server authentication.

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 August 29, 2013.

Table of Contents

1. Introduction

The specification for SMTP over TLS [RFC3207] does not describe how to authenticate a server: which identity relating to the connection ought to be authenticated by the server's certificate. In practice, most certificates presented by publicly-referenced SMTP servers either cannot be validated with respect to a well-known certification authority, or do not verify any identity expected by the client.

As a result, inter-domain SMTP clients cannot require working server authentication if they want to successfully send mail using TLS. Therefore TLS currently provides only a limited amount of additional security for inter-domain SMTP. Its encryption protects against on-path passive eavesdropping; but it does not protect against an active attack, since the client has no way to detect when an attacker is spoofing the server.

This memo describes how to fix this using DNSSEC [RFC4033] and TLSA records [RFC6698] set up as described in [I-D.ietf-dane-srv]. To summarize, we use DNSSEC to secure the association between a mail domain and its SMTP server host names (i.e. the MX recods), and between the host names and their certificates (using TLSA records). Connections to servers are authenticated by their TLS certificates. The existance of TLSA records also signals to the client that it can expect the server to offer TLS with a valid certificate.

The security situation is better for intra-domain SMTP, because in this case the client and server can be configured with prior knowledge of how to authenticate each other. This specification can also be used for authenticating servers in intra-domain SMTP.

This memo does not cover message submission [RFC4409] [RFC5068] [RFC6186], nor does it cover LMTP [RFC2033], since they use the DNS in a different way than MTA-to-MTA SMTP.

The protocol described in this memo adds new security checks that can cause email delivery to be delayed when a security failure is detected. We specify that clients treat such problems as a "temporary failure", causing the message to be queued for a later delivery attempt, in the hope that the attack (or configuration error) will have been dealt with.

2. Terminology

ADMD: An ADministrative Management Domain, as described in the Internet Mail Architecture [RFC5598].

Inter-domain SMTP: SMTP between different ADMDs across the public Internet, where a client MTA sends mail to a publicly-referenced SMTP server MTA.

Intra-domain SMTP: SMTP between MTAs within an ADMD.

Mail domain: The part of an email address after the "@"; also the query name for a (possibly implicit) MX record.

MX resolution: The algorithm for resolving a mail domain into a set of SMTP server hosts, described in [RFC5321] section 5.

Publicly-referenced SMTP server: An SMTP server which runs on port 25 of an Internet host located using MX resolution. (This term is from [RFC3207].)

SMTP server host name: The target of a (possibly implicit) MX record.

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

3. Inter-domain SMTP with TLSA

This is a combination of the usual MX resolution algorithm described in [RFC5321] section 5, and the rules for using DANE TLSA records with SRV and MX records [I-D.ietf-dane-srv]. The former determines the server ordering and selection rules (which differ slightly from the rules for SRV records, for instance, in the case of backup MX relaying). The latter determines the rules for handling TLSA records.

Note the difference between the (effective) absence of TLSA records, and the presence of unusable TLSA records. If a server has no TLSA records, or their DNSSEC validation status is "indeterminate" or "insecure", the client can attempt to deliver to this server insecurely (which might be over unauthenticated TLS, as described in the introduction). If a server has TLSA records whose DNSSEC validation status is "secure", whether they are usable or not, the client MUST use TLS to connect to the server and validate the certificate according to [I-D.ietf-dane-srv] section 3.

4. Intra-domain SMTP with TLSA

Mail transmission within an ADMD can be based on MX records (such as when delivering incoming mail to its destination host) or on statically configured host names (such as when routing outgoing mail via a border relay).

When routing internal mail using MX records, Section 3 applies the same as for inter-domain SMTP.

When routing mail using host names, the MX lookup step is skipped and TODO need a better explanation.

5. Security considerations

This memo provides only conditional security. It allows a server to publish in the DNS the details of how it can be authenticated. Clients that implement this protocol can use it to provide a strong guarantee that they are sending mail to the correct place. If either of these is missing, mail delivery will be insecure.

In addition to the following, many security considerations are covered in [I-D.ietf-dane-srv].

5.1. Temporary failures and denial of service

Many provisioning failures in SMTP cause "permanent" failures, that is the immediate and final rejection of the message. This includes missing DNS records, an SMTP server that is not configured to accept mail for the recipient domain, and so forth.

In this protocol, provisioning an incorrect TLS certificate triggers a temporary error. This is because we want to minimise the damage that occurs when an on-path attacker intercepts the TCP connection between an SMTP client and server. An attacker can cause delays, but is not able to trigger immediate delivery failures.

5.2. Deliberate omissions

This memo does not specify any changes to SMTP client authentication. Inter-domain SMTP client authentication remains extremely weak. Intra-domain SMTP can be configured as strong as necessary (using SMTP AUTH or TLS client certificates, for instance) but that is out of scope for this memo.

6. Internationalization Considerations

If any of the DNS queries are for an internationalized domain name, then they need to use the A-label form [RFC5890]. TODO: this section needs checking WRT IMA.

7. IANA Considerations

No IANA action is required.

8. Acknowledgements

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

9. References

9.1. Normative References

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

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

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

[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.

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

[I-D.ietf-dane-srv] Finch, T., "Using DNS-Based Authentication of Named

Entities (DANE) TLSA records with SRV and MX records.", draft-ietf-dane-srv (work in progress), March 2013.

9.2. Informative References

[RFC2033] Myers, J., "Local Mail Transfer Protocol", RFC 2033, October 1996.

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

[RFC5068] Hutzler, C., Crocker, D., Resnick, P., Allman, E., and T. Finch, "Email Submission Operations: Access and Accountability Requirements", BCP 134, RFC 5068, November 2007.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

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

Appendix A. 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.           AAAA   2001:db8:212:8::e:1

; 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. Change log

B.1. Changes in version -01

Strip the document down so it is now based on [I-D.ietf-dane-srv].

Drop the Transmitted: header idea.

B.2. Changes in version -00

Change doc name from draft-fanf-dane-smtp to draft-ietf-dane-smtp.

Update DANE citation to published RFC.

Be clearer about the PKIX certificate validation vs. certificate subject name matching.

Minor clarifications suggested by Phill Hallam-Baker and James Cloos.

B.3. Changes in version fanf-04

Add some questions for reviewers

Add a note about stub resolvers and the AD bit.

Internationalization considerations.

B.4. Changes in version fanf-03

Clarify how to use SNI with this protocol.

Clarify lack of changes to MX sorting rules.

Mention DNAME as well as CNAME.

An example.

B.5. Changes in version fanf-02

Clarify the wording that describes how a client determines that this protocol is in effect.

Divide the security considerations into sub-sections, and add a subsection on denial of service.

Clarify intro, mentioning TLSA owner name format.

Extend the scope to cover MTA-to-MTA mail within an ADMD as well as

between ADMDs.

B.6. Changes in version fanf-01

More about why not to authenticate mail domains in the rationale.

Change DNS-ID requirement from MUST to SHOULD to follow RFC 6125.

Acknowledgments section.

Transmitted: header trace field. Not sure if this is a good idea; feedback wanted.

"dane" MTA-name-type for use in DSNs. Even less sure if this is a good idea.

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/