Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: July 13, 2016

J. Fenton

January 10, 2016

SMTP Require TLS Option
draft-fenton-smtp-require-tls-00

Abstract

The SMTP STARTTLS option, used in negotiating transport-level encryption of SMTP connections, is not as useful from a security standpoint as it might be because of its opportunistic nature; message delivery is prioritized over security. This document describes a complementary option, REQUIRETLS, which causes message delivery to fail if a TLS connection with the required security characteristics cannot be negotiated with the next hop MTA or if that MTA does not also support REQUIRETLS. Message originators may therefore expect transport security for messages sent with this option.

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 July 13, 2016.

Copyright Notice

Table of Contents

1. Introduction

The SMTP [RFC5321] STARTTLS service extension [RFC3207] provides a means by which an SMTP server and client can negotiate a Transport Layer Security (TLS) protected session for the transmission of email messages. In this application, TLS is used only upon mutual agreement (successful negotiation) between the client and server; if this is not possible, the message is sent unencrypted. Furthermore, even if a TLS protected session is negotiated, it is uncommon for the client to abort the SMTP session if certificate validation fails.

The opportunistic nature of SMTP TLS enables several "on the wire" attacks on SMTP security between MTAs. These include passive eavesdropping on connections for which TLS was not negotiated, interference in the SMTP protocol to prevent TLS from being negotiated (usually followed by subsequent eavesdropping), and insertion of a man-in-the-middle attacker taking advantage of the lack of server authentication by the client. Attacks are more described in more detail in the Security Considerations section of

this document.

The REQUIRETLS SMTP service extension allows the SMTP client to specify that all messages sent during a particular session MUST be sent over a TLS protected session with specified security

characteristics. It also requires that the SMTP server advertise that it also supports REQUIRETLS, in effect promising that it will honor the requirement to negotiate STARTTLS and REQUIRETLS for all onward transmissions of any of the messages contained in this session.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. The REQUIRETLS Service Extension

1. The textual name of the extension is "Require TLS".

2. The EHLO keyword value associated with this extension is "REQUIRETLS".

3. One additional SMTP verb, also named REQUIRETLS, is defined by this extension.

4. Two new SMTP status codes are defined by this extension to convey error conditions resulting from failure of the client to negotiate a TLS connection with the required security and as a result of an attempt to send to a server not also supporting the REQUIRETLS extension.

An optional parameter to the REQUIRETLS SMTP verb, if present, specifies the method(s) for server authentication that the server MUST use for any onward transmission of the following messages. The parameter takes the form of either a single value or comma-separated list, separated from the verb by a single "=" (equals-sign) character. If present, the parameter MUST take one or more of the following values:

- CHAIN - The certificate presented by the SMTP server MUST verify successfully in a trust chain leading to a certificate trusted by the SMTP client. The choice of trusted (root) certificates by the client is at their own discretion. The client MAY choose to use the certificate set maintained by the CA/B forum [citation needed] for this purpose.

- DANE - The certificate presented by the SMTP server MUST verify succesfully using DANE as specified in RFC 7672 [RFC7672].

If the parameter is not present, the default behavior is that the certificate presented by the SMTP server MAY be authenticated, but is not required to be.

3. REQUIRETLS Semantics

3.1. REQUIRETLS Receipt Requirements

Upon receipt of a REQUIRETLS verb from a client, an SMTP server MUST tag all subsequent messages received during that session as requiring TLS transmission with the specified authentication method(s). The manner in which this tagging takes place is implementation-dependent.

3.2. REQUIRETLS Sender Requirements

When sending a message tagged with a TLS requirement, the sending (client) MTA MUST:

- Open an SMTP session with the peer SMTP server using the EHLO verb. If the server does not advertise the REQUIRETLS capability, the client MUST bounce the message with a TBD error code as described in section xxx.

- Negotiate a TLS-protected SMTP session with its peer SMTP server and authenticate the server's certificate with the specified authentication method. If it is unable to do so, the client MUST bounce the message with a TBD error code as described in section xxx.

- Issue the REQUIRETLS verb with the required authentication method(s), if any.

- Transmit the associated message(s).

- If multiple messages are to be transmitted with different authentication requirements, the REQUIRETLS command can be repeated to change the authentication method for subsequent messages. However, the TLS connection being used MUST satisfy the new as well as the former authentication method(s).

3.3. REQUIRETLS Submission

An MUA or other agent making the initial introduction of a message to SMTP has authority to decide whether to require TLS, and if so, using what authentication method(s). It does so by issuing the REQUIRETLS verb in the SMTP session associated with message submission. This MAY be done based on a user interface selection, on a header field included in the message, or based on policy. The manner in which the

decision to require TLS is made is implementation-dependent and is beyond the scope of this specification.

3.4. Delivery of REQUIRETLS messages

Messages are usually delivered to end users using protocols other than SMTP such as IMAP [RFC3501], POP [RFC1939], or web mail systems. Mail delivery agents supporting REQUIRETLS SHOULD require that message delivery take place over authenticated, encrypted channels.

4. Error handling

Error ("bounce") messages contain important metadata, and therefore MUST be protected in the same manner as the original message. All error handling, whether resulting from a REQUIRETLS error or some other, MUST employ REQUIRETLS at the same authentication method(s) as the message that caused the error to occur.

It should be noted that the path from the origination of an error bounce message back to the MAIL FROM address may not share the same REQUIRETLS support as the forward path. Therefore, users of REQUIRETLS are advised to make sure that they are capable of

receiving mail using REQUIRETLS at the same authentication method(s) as messages they send. Otherwise, such error bounces will be lost.

5. IANA Considerations

If published as an RFC, this draft requests the addition of the keyword REQUIRETLS to the SMTP Service Extensions registry MAILPARAMS [MailParams]

If published as an RFC, this draft also requests the creation of a registry, REQUIRETLS Security Requirements, to be initially populated with the CHAIN and DANE keywords.

This section is to be removed during conversion into an RFC by the RFC Editor.

6. Security Considerations

The purpose of REQUIRETLS is to improve communications security for email by giving the originator of a message an expectation that it will be transmitted in an encrypted form "over the wire". When used, REQUIRETLS changes the traditional behavior of email transmission, which favors delivery over the ability to send email messages using transport-layer security, to one in which messages are not transmitted unless the required security is available.

REQUIRETLS is negotiated over SMTP by the MTAs along the message transmission path. Accordingly, a bad-actor MTA could misrepresent its support of REQUIRETLS and/or actively strip REQUIRETLS tags from messages it handles. However, since the originator of a message trusts the MTA that it submits the message to forward the message according to its instructions, and the recipient trusts MTAs that it lists in its MX records. MTAs that can be trusted with the cleartext of messages (since encryption is at the transport layer) are assumed to also be trustworthy to honor their REQUIRETLS obligations as well.

One exception to this trust can occur if an attacker is able to spoof the MX record(s) for the receiving domain to an earlier hop MTA. The attacker could then successfully negotiate TLS with the earlier MTA, since it should be able to obtain a certificate for the hostname it spoofed. This is actually a more generic attack on SMTP TLS that is

also effective against REQUIRETLS since the attacker could forward the message onward without REQUIRETLS. For these reasons, domains receiving email SHOULD deploy DNSSEC [RFC4033].

It should be reemphasized that since SMTP TLS is a transport-layer security protocol, messages sent using REQUIRETLS are not encrypted end-to-end and are visible to MTAs that are part of the message delivery path. Messages containing sensitive information that MTAs should not have access to MUST be sent using end-to-end content encryption such as OpenPGP [RFC4880] or S/MIME [RFC5751].

7. References

7.1. Normative References

[MailParams] Internet Assigned Numbers Authority (IANA), "IANA Mail Parameters", 2007, <http://www.iana.org/assignments/mail-parameters>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <http://www.rfc-editor.org/info/rfc3207>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

7.2. Informative References

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, DOI 10.17487/RFC1939, May 1996, <http://www.rfc-editor.org/info/rfc1939>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003,

<http://www.rfc-editor.org/info/rfc3501>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <http://www.rfc-editor.org/info/rfc4880>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <http://www.rfc-editor.org/info/rfc5751>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <http://www.rfc-editor.org/info/rfc7672>.

Author's Address

Jim Fenton
704 Benvenue Avenue
Los Altos, California 94024
USA

Email: fenton@bluepopcorn.net