Network Working Group
Internet-Draft
Updates: 7001 (if approved)
Intended status: Standards Track
Expires: June 22, 2015

F. Martin, Ed.
LinkedIn

December 19, 2014

Authentication-Results Registration for TLS
draft-martin-authentication-results-tls-03

Abstract

This memo updates the registry of properties in Authentication-Results: message header fields to allow relaying of the results of an email sent using STARTTLS [RFC3207] or not.

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 June 22, 2015.

Copyright Notice

Table of Contents

1. Introduction

STARTTLS [RFC3207] defines how to send an email over an SMTP [RFC5321] encrypted session between two mail servers.

This memo thus registers an additional reporting property allowing a TLS result to be relayed as an annotation in a message header.

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].

1.2. Discussion

STARTTLS [RFC3207] defines how to send an email over an encrypted session between two mail servers, Message Transfer Agent (MTA), using the TLS [RFC5246] protocol.

Most of these exchanges are opportunistic, meaning a best effort is done to establish an encrypted message exchange regardless of the strength of the cipher or the validity of the certificates used. However, the results of this negotiation should be recorded in the message via the Authentication-Results header [RFC7001] to indicate to other message processing algorithms, including Messaging User Agents (MUA), how securely this message was transmitted from the MTA client to the MTA server.

The concept of authentication here is related to the presentation of a certificate which is verified valid by a set of trusted Certificate

Authorithies (CA), via DANE [RFC6698] or by local policy. This does not indicate that any string in the certificate is related to any string in the email.

The usage and usefulness of the Authentication-Results header is discussed in [RFC7001].

2. Definitions

This memo adds to the "Email Authentication Methods" registry, created by IANA upon publication of [RFC7001], the following:

- The method "tls"; and
- Associated with that method, the properties (reporting items) "cert.client", "cert.server", "cert.verif", "tls.v", "key.ciphersuite", "key.fingerprint", "key.length" and "key.strength".

2.1. results meaning

The "tls" method can have the following results:

none: the message was sent in clear.

pass: the message was sent encrypted and the client certificate was verified valid either using a trusted CA, via DANE [RFC6698] or via a local policy and host identity was verified.

selfsigned: the message was sent encrypted but the client certificate is self signed.

invalidhost: the message was sent encrypted and the client certificate is verified valid but the host identity is invalid.

fail: the message was sent encrypted but the client certificate is not valid. It is advised to use comments to indicate the nature of the problem like certifcate expired, not linked to a trusted CA,...

temperror: the message was sent encrypted and the server was not able to verify the client certificate at this time. This may indicate for instance that the server could not fetch the CRL.

permerror: the message was sent encrypted and the client certificate was not verified by the MTA server. MTA should always attempt to verify the client certificate.

2.2. properties

cert.client: the subject of the X.509 certificate used by the client to initiate TLS.

cert.server: the subject of the X.509 certificate used by the server to initiate TLS (optional).

cert.clientalt: the subject alternative name of the X.509 certificate used by the client to initiate TLS (optional).

cert.serveralt: the subject alternative name of the X.509 certificate used by the server to initiate TLS (optional).

cert.clientissuer: the issuer of the X.509 certificate used by the client to initiate TLS (optional).

cert.serverissuer: the issuer of the X.509 certificate used by the server to initiate TLS (optional).

cert.verif: the type of certification performed: CA, DANE [RFC6698], LOCAL (optional).

tls.v: the protocol version used to encrypt SSL2.0, SSL3.0, TLS1.0, TLS1.1,... (optional)

key.ciphersuite: the description of the TLS cipher suite used as defined in the IANA cipher suite registry.

key.fingerprint: the fingerprint of the key used (optional).

key.length: the length in bits of the key used (optional).

key.strength: as many SMTP TLS are opportunistic in nature this property is an arbitrary value set by the MTA server to indicate the strength of the encryption (optional).

While ciphers strength vary overtime, and key length in bits does not indicate a comparable strength between various cyphers, it may be difficult for all the processors of the authentication-results header to redo the analysis based on the cipher used and all to arrive to the same conclusion. It seems, therefore, best if the receiving MTA does that analysis and communicate it to the other layers. This is the purpose of the key.strength. For instance This value could be used by the MUA to indicate to the end user some quality of the encryption channel.

3. IANA Considerations

Per [IANA], the following items have been added to the "Email Authentication Methods" registry:

Method	Defined	ptype	property	value
tls	RFC 3207	cert	client	subject of client certificate section 4.1.2.6 of RFC 5280
tls	RFC 3207	cert	server	subject of server certificate section 4.1.2.6 of RFC 5280
tls	RFC 3207	cert	clientalt	alternate subject of client certificate section 4.2.1.6 of RFC 5280
tls	RFC 3207	cert	serveralt	alternate subject of server certificate section 4.2.1.6 of RFC 5280
tls	RFC 3207	cert	clientissuer	issuer of client certificate section 4.1.2.4 of RFC 5280
tls	RFC 3207	cert	serverissuer	issuer of server certificate section 4.1.2.4 of RFC 5280
tls	RFC 3207	cert	verif	CA DANE LOCAL

tls	RFC 3207	tls	v	protocol version description from RFC 5246	
tls	RFC 3207	key	ciphersuite	IANA cipher suite registry description from RFC 5246	
tls	RFC 3207	key	fingerprint	key fingerprint from RFC 5246	
tls	RFC 3207	key	length	in bits	
tls	RFC 3207	key	strength	low medium high	

Also, the following items have been added to the "Email Authentication Result Names" registry:

Code	Existing/New	Defined In	Method	Meaning
none	existing	RFC 7001	tls (added)	this memo
pass	existing	RFC 7001	tls (added)	this memo
selfsigned	existing	RFC 7001	tls (added)	this memo
invalidhost	existing	RFC 7001	tls (added)	this memo
fail	existing	RFC 7001	tls (added)	this memo
temperror	existing	RFC 7001	tls (added)	this memo
permerror	existing	RFC 7001	tls (added)	this memo

4. Security Considerations

This memo creates a mechanism for relaying STARTTLS [RFC3207] results using the structure already defined by [RFC7001]. The Security Considerations sections of those documents should be consulted.

By this mechanism, some identifiers of the client certificates gets to live pass the receiving MTA. This is a change in the sender expectation on where the client certificate is used

5. References

5.1. 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.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[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.

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

[RFC7001] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7001, September 2013.

5.2. Informative References

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Appendix A. Authentication-Results Examples

This section presents an example of the use of this new header field to indicate TLS results.

A.1. TLS Results

A message that went over a successful TLS session:

```
Authentication-Results: mail-router.example.net;
  dkim=pass (good signature) header.d=newyork.example.com
    header.b=oINEO8hg;
  tls=pass (verified, expires 20140505)
    cert.verif=CA
    cert.client="CN=smtp.example.com,O=ACME,L=ToonTown,
      ST=CA,C=US"
    cert.clientalt="DNS:smtp.example.com, DNS:newyork.example.com"
    cert.clientissuer="C=US, O=AcmeCert Inc, CN=AcmeCert CA"
    key.ciphersuite=TLS_RSA_WITH_RC4_128_SHA
    tls.v=TLS1.0
    key.fingerprint="68:B3:29:DA:98:93:E3:40:99:C7:D8:
      AD:5C:B9:C9:40"
    key.length=128
    key.strength=MEDIUM;
Received: from newyork.example.com
  (newyork.example.com [192.0.2.250])
  by mail-router.example.net (8.11.6/8.11.6)
  for <recipient@example.net>
  with ESMTPS id i7PK0sH7021929;
  Fri, Feb 15 2002 17:19:22 -0800
DKIM-Signature: v=1; a=rsa-sha256; s=rashani;
  d=newyork.example.com;
  t=1188964191; c=relaxed/simple;
  h=From:Date:To:VBR-Info:Message-Id:Subject;
  bh=sEu28nfs9fuZGD/pSr7ANysbY3jtdaQ3Xv9xPQtS0m7=;
   b=oINEO8hgn/gnunsg ... 9n9ODSNFSDij3=
From: sender@newyork.example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: meetings@example.net
Message-Id: <12345.abc@newyork.example.com>
Subject: here's a sample
```

Author's Address

Franck Martin (editor)
LinkedIn
Mountain View, CA
US

Email: fmartin@linkedin.com