

Individual submission
Internet-Draft
Intended status: Standards Track
Expires: October 19, 2009

M. Kucherawy
Sendmail, Inc.
April 17, 2009

SMTP Service Extension for Indicating Message Authentication Status
draft-kucherawy-sender-auth-esmtp-02

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on October 19, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft Authentication-Results SMTP Extension

April 2009

Abstract

This memo defines an extension to the Simple Mail Transfer protocol (SMTP) service whereby a server can indicate its ability to accept and apply information regarding the efforts of upstream SMTP servers to establish authenticity of the message via various authentication methods.

Table of Contents

1.	Introduction	3
1.1.	Purpose	3
1.2.	Definitions	4
2.	Framework for the Authentication Results Extension	6
3.	The Authentication-Results Service Extension	7
3.1.	Client Implementation	7
3.2.	Server Implementation	7
3.3.	MAIL Command Extension	8
3.4.	Local Policy Enforcement	8
4.	Conformance and Usage Requirements	9
5.	IANA Considerations	10
6.	Security Considerations	11
6.1.	Trusting SMTP Clients	11
6.2.	Misleading Results	11
6.3.	Reverse IP Query Denial-Of-Service Attacks	11
6.4.	Mitigation of Backscatter	11
6.5.	Internal MTA Lists	12
6.6.	Attacks Against Authentication Methods	12
6.7.	Intentionally Malformed Extension Parameters	12
6.8.	Compromised Internal Hosts	12
7.	References	13
7.1.	Normative References	13
7.2.	Informative References	13
Appendix A.	Acknowledgements	15
Appendix B.	Examples	16
B.1.	Single authentication result	16
Appendix C.	Public Discussion	17
	Author's Address	18

1. Introduction

Electronic mail, though ubiquitous and highly useful, is also prone to increasing abuse by parties that choose to exploit its lenient design for nefarious purposes such as "spam" and "phishing." Abuse of this leniency has become so widespread as to become an economic problem. Several nascent methods of mitigating this problem such as [\[DKIM\]](#) appear to make strides in this direction but are themselves not sufficient. In many cases the results of attempts to authenticate messages must be relayed to the user for final disposition.

This memo defines a new SMTP extension which is used to relay message authentication results from upstream (e.g. "border") mail servers to internal mail servers which ultimately do message delivery. This information can then be used by delivery agents or even the users themselves when determining whether or not the content of such messages is trustworthy.

The extension is defined using the methods specified in [\[SMTP\]](#) to enable a server to announce that it is willing to accept this information from upstream mail servers. Clients observing this announcement can then elect to send that information with the message when the latter is relayed.

The message header defined in [\[AUTH-RESULTS\]](#) serves a similar purpose and is simple to implement but has some moderate security implications, so a more secure channel is required. In particular, the header block of a message is generally unauthenticated and is also typically relayed intact, meaning it is an obvious vector for data forgery. Thus, trusting part of a message header to be secure is a difficult problem. This method establishes a much better trust boundary and removes that obvious attack vector.

[UPDATE PRIOR TO FINAL VERSION] At the time of publication of this draft, [\[AUTH\]](#), [\[DKIM\]](#), [\[DOMAINKEYS\]](#), [\[SENDERID\]](#) and [\[SPF\]](#) are the

published e-mail authentication methods in common use. As various methods emerge, it is necessary to prepare for their appearance and encourage convergence in the area of interfacing these filters to electroic mail servers.

1.1. Purpose

The SMTP extension defined in this memo is expected to serve several purposes:

1. Convey to MUAs from filters and Mail Transfer Agents (MTAs) the results of various message authentication checks being applied;

Kucherawy

Expires October 19, 2009

[Page 3]

Internet-Draft

Authentication-Results SMTP Extension

April 2009

2. Provide a common location for the presentation of this data;
3. Create an extensible framework for specifying results from new authentication methods as such emerge;
4. Convey the results of message authentication tests to later filtering agents within the same "trust domain", as such agents might apply more or less stringent checks based on message authentication results;
5. Do all of this in a way not prone to forgery or misinterpretation.

1.2. Definitions

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 [RFC2119](#).

An "MTA" is a Mail Transfer Agent, or any agent which uses [[SMTP](#)] or its extensions to format and transport a message.

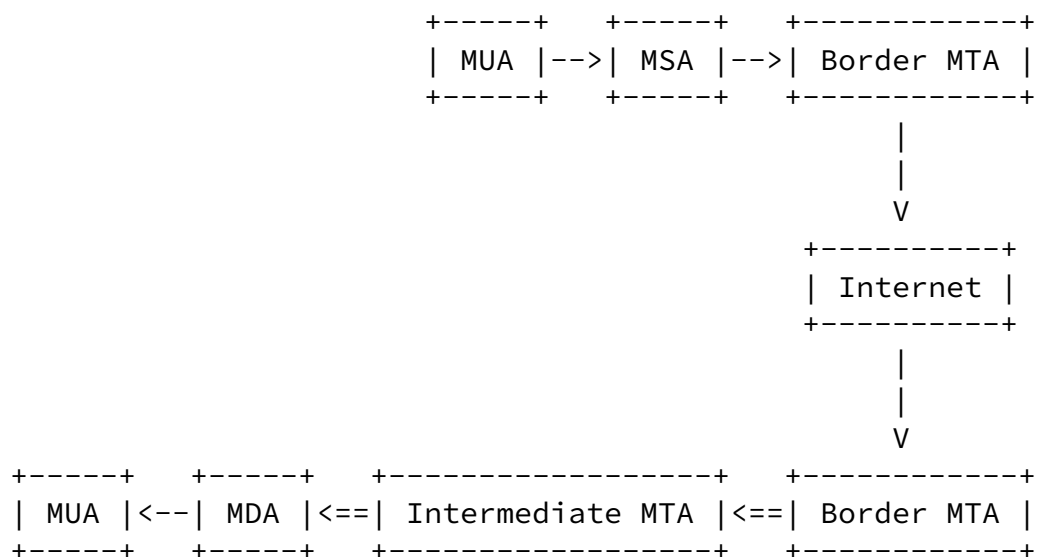
An "MDA" is a Mail Delivery Agent (also sometimes referred to as "LDA" or Local Delivery Agent), or any agent which has access to receive a message from an MTA and write it into the receiving user's "inbox".

An "MUA" is a Mail User Agent, or any software which retrieves and displays messages on behalf of a user.

A "border MTA" is an MTA which acts as a gateway between the general Internet and the users within an organizational boundary.

A "delivery MTA" (or Mail Delivery Agent or MDA) is an MTA which actually enacts delivery of a message to a user's inbox or other final delivery.

An "intermediate MTA" is an MTA which handles messages after a border MTAs and before a delivery MTA.



Generally it is assumed that the work of applying message authentication schemes takes place at a border MTA or a delivery MTA. This specification is written with that assumption in mind. However, there are some sites at which the entire mail infrastructure consists of a single host. In such cases, such terms as "border MTA" and "delivery MTA" may well apply to the same machine or even the very

same agent. It is also possible that message authentication could take place on an intermediate MTA. Although this document doesn't specifically include such cases, they are not meant to be excluded from this specification.

See [[I-D.DRAFT-CROCKER-EMAIL-ARCH](#)] for further discussion on e-mail system architecture.

In the figure shown above, the double-lines indicate the portions of the transport of a message where this protocol would be applied. Note also that the Local Mail Transfer Protocol [[LMTP](#)] could benefit from a similar extension.

[2.](#) Framework for the Authentication Results Extension

The framework for the Authentication Results Extension is as follows:

1. The name of the SMTP service extension is "Authentication-Results";
2. The SMTP buffer length is extended by 256 bytes on servers offering this service extension;
3. The EHLO keyword value associated with the extension is AUTHRES;
4. No parameter is used with the AUTHRES EHLO keyword;
5. An additional, optional parameter called AUTHRES is added to the

MAIL command;

6. No additional parameters are added to the RCPT command;
7. No additional SMTP verbs are defined by this extension; and
8. The next section specifies how support for the extension affects the behaviour of a server and client SMTP session.

[3.](#) The Authentication-Results Service Extension

When a client wishes to relay message authentication information to a downstream server, it first issues the EHLO command to the SMTP server. If the SMTP server responds with code 250 to the EHLO command and the response includes the EHLO keyword AUTHRES, then the SMTP server has indicated that it can accept message authentication information from the client.

[3.1.](#) Client Implementation

Once the client has confirmed that support exists for this extension in the server to which it has connected, it may then elect to relay its collected message authentication results as part of an extended MAIL command. The format of the extended command is defined below.

More than one such result may be relayed in a single extended MAIL command.

The authentication results relayed by this method need not have been established by the agent acting as SMTP client. A client may elect to forward, by way of this extension, authentication results relayed to it about a message by previous clients.

[3.2.](#) Server Implementation

The SMTP server, upon receiving the EHLO command from the new client, may decide to advertise its support of this extension by including the AUTHRES keyword in its reply to the EHLO command.

Although software support for the extension may be present, the server is not required to advertise such support if, for example, the client making the connection is not one from which the server wishes to trust such data.

Upon receipt of authentication results from the upstream MTA, the receiving MTA may analyze the results and, if it decides the results are not favourable, may elect to return an SMTP result code other than the typical 250 success result to the extended MAIL command in order to reject the message.

The authentication results ultimately received by an MDA may elect to store that information for ultimate consumption by the end user, either graphically or by way of filtering. This can be accomplished using the message header field defined in [[AUTH-RESULTS](#)] or by means of a new and as-yet-unspecified [[IMAP](#)] annotation via [[ANNOTATE](#)].

[3.3.](#) MAIL Command Extension

The MAIL command is extended by this specification to allow the relaying of authentication results. As there are several message authentication schemes in common and growing use, the extension must permit multiple results to be relayed for a given message.

The extension adds an AUTHRES parameter to the MAIL command. The formal definition, using [\[ABNF\]](#):

```
authres = 1*( "AUTHRES" "=" version ":"  
              authserv-id ":"  
              methodspec ":"  
              propspec )  
          ; relays a single unit of authentication results  
          ; information
```

The "version", "authserv-id", "methodspect" and "propspect" are defined in Section 2.2 of [\[AUTH-RESULTS\]](#). The "version" refers to the version of this memo in use, not the version of [\[AUTH-RESULTS\]](#) referenced.

[3.4.](#) Local Policy Enforcement

If a site's local policy is to consider a non-recoverable failure result (e.g. "fail" for DKIM, "hardfail" for SPF) for any particular authentication method as justification to reject the message completely, the border MTA SHOULD issue an [\[SMTP\]](#) rejection response to the message rather than using this extension with the failure result and allowing it to proceed toward delivery. This is more desirable than allowing the message to reach an internal host's MTA or spam filter, thus possibly generating a local rejection such as a [\[DSN\]](#) to a forged originator.

The same MAY also be done for local policy decisions overriding the results of the authentication methods (e.g. the "policy" result codes described in Section 2.4 of [\[AUTH-RESULTS\]](#)).

Such rejections at the SMTP protocol level are not possible if local policy is enforced at the MUA and not the MTA. Unfortunately, this may be a common scenario.

[4.](#) Conformance and Usage Requirements

An agent acting as an SMTP server conforms to this specification if it offers the AUTHRES extension to upstream MTAs from which it would trust such data. Servers that advertise AUTHRES in their EHLOs MUST expect the additional envelope information described in this draft.

A client wishing to use this extension MUST first see AUTHRES as part of the EHLO response from a server.

5. IANA Considerations

Per [[IANA-CONSIDERATIONS](#)], IANA is requested to register this new SMTP extension as described in [Section 2](#).

[6.](#) Security Considerations

The following security considerations apply when applying or processing the Authentication-Results SMTP service extension:

[6.1.](#) Trusting SMTP Clients

As described in [Section 3.2](#), an MTA server implementing this extension need not offer the AUTHRES service to an SMTP client if it's sure it won't care what that client has to say about the authenticity of the message. This establishes a "trust boundary" within which SMTP clients are offered the extension; clients outside that boundary are not offered the extension.

A client that tries to use the extension when it was not offered may be deemed a security risk.

Although an obvious location of this boundary would be a published MX for the recipient's domain, this is not always the case. Thus, implementors are advised to default to a "trust no-one" posture and have the trust boundary established explicitly by the user.

[6.2.](#) Misleading Results

Until some form of service for querying the reputation of a sending agent is widely deployed, the existence of the AUTHRES extension indicating a "pass" does not render the message trustworthy. It is possible for an arriving piece of spam or other undesirable mail to pass checks by several of the methods enumerated above (e.g. a piece of spam signed using [\[DKIM\]](#) by the originator of the spam, which might be a spammer or a compromised system).

[6.3.](#) Reverse IP Query Denial-Of-Service Attacks

Section 5.5 of [[SPF](#)] describes a DNS-based denial-of-service attack for verifiers that attempt to DNS-based identity verification of arriving client connections. A verifier wishing to do this check and report this information SHOULD take care not to go to unbounded lengths to resolve "A" and "PTR" queries. MUAs or other filters making use of an "iprev" result specified by this memo SHOULD be aware of the algorithm used by the verifier reporting the result and thus be aware of its limitations.

[6.4.](#) Mitigation of Backscatter

Failing to follow the instructions of [Section 3.4](#) can result in a denial-of-service attack caused by the generation of [[DSN](#)] messages (or equivalent) to addresses which did not send the messages being

Kucherawy

Expires October 19, 2009

[Page 11]

Internet-Draft

Authentication-Results SMTP Extension

April 2009

rejected.

[6.5.](#) Internal MTA Lists

[Section 3.2](#) mentions that the participating server need not offer this extension to untrusted clients. A compliant installation will have to include at each MTA a list of other MTAs known to be compliant and trustworthy. Failing to keep this list current as internal infrastructure changes may expose a domain to attack.

[6.6.](#) Attacks Against Authentication Methods

If an attack becomes known against an authentication method, clearly then the agent verifying that method can be fooled into thinking an inauthentic message is authentic, and thus the value of the AUTHRES extension can be misleading. It follows that any attack against the authentication methods supported by this document (and later amendments to it) is also a security consideration here.

[6.7.](#) Intentionally Malformed Extension Parameters

It is possible for an attacker to add AUTHRES parameter which is extraordinarily large or otherwise malformed in an attempt to discover or exploit weaknesses in parsing code. Implementors must thoroughly verify all such data received from MTAs and be robust

against intentionally as well as unintentionally malformed data.

[6.8.](#) Compromised Internal Hosts

An internal MUA or MTA which has been compromised could generate mail with forged data, eventually generating an AUTHRES parameter which endorses it. Although it is clearly a larger concern to have compromised internal machines than it is to prove the value of this extension, this risk can be mitigated by arranging that internal MTAs not relay this data if it claims to have been added by a trusted border MTA (as described above) yet the [\[SMTP\]](#) connection is not coming from an internal machine known to be running an authorized MTA. However, in such a configuration, legitimate MTAs will have to add this data when legitimate internal-only messages are generated.

[7.](#) References

[7.1.](#) Normative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 5234](#), January 2008.

[AUTH-RESULTS]

Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", [RFC 5451](#), April 2009.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", [RFC 2821](#), April 2001.

[7.2.](#) Informative References

[ANNOTATE]

Daboo, C. and R. Gellens, "IMAP ANNOTATE Extension",

[RFC 5257](#), June 2008.

- [AUTH] Siemborski, R. and A. Melnikov, "SMTP Service Extension for Authentication", [RFC 4954](#), July 2007.
- [DKIM] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4871](#), May 2007.
- [DOMAINKEYS] Delany, M., "Domain-based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)", [RFC 4870](#), May 2007.
- [DSN] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", [RFC 3464](#), January 2003.
- [I-D.DRAFT-CROCKER-EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", I-D [draft-crocker-email-arch](#), May 2007.
- [IANA-CONSIDERATIONS] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 5226](#), October 1998.
- [IMAP] Crispin, M., "Internet Message Access Protocol - Version 4rev1", [RFC 3501](#), March 2003.

Kucherawy

Expires October 19, 2009

[Page 13]

Internet-Draft

Authentication-Results SMTP Extension

April 2009

- [LMTP] Meyers, J., "Local Mail Transport Protocol", [RFC 2033](#), October 1996.
- [SENDERID] Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", [RFC 4406](#), April 2006.
- [SPF] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", [RFC 4408](#), April 2006.

[Appendix A](#). Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: (add names here)

[Appendix B](#). Examples

This section presents some examples of the use of this protocol extension to relay message authentication results. In these examples, "C" indicates data sent by the SMTP client and "S" indicates data sent by the SMTP server, and other annotations are enclosed in square brackets.

[B.1](#). Single authentication result

Relaying a single authentication result:

```
[connection established]
S: 220 inbox.example.com SMTP server ready
C: EHLO border.example.com
S: 250-inbox.example.com Hello root@foobar.example.net
S: 250-ENHANCEDSTATUSCODES
S: 250-SIZE
S: 250-DSN
S: 250-AUTHRES
S: 250 HELP
C: MAIL FROM:<me@example.net> AUTHRES=dkim=pass:header.i=@example.net
S: 250 Sender OK
C: RCPT TO:<postmaster@example.com>
S: 250 Recipient OK
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: [message body]
C: .
S: 250 l9NE6WYF026506 Message received
C: QUIT
S: 221 Bye!
[connection closed]
```

Example 1: Relaying a single authentication result

In this example we see a border SMTP server relaying a message to an internal SMTP server which will do local delivery for example.com's users. The SMTP extension is advertised by the server (it trusts this source as one likely to relay valid authentication data) and used by the client. In this instance, the server validated the message's authenticity using [\[DKIM\]](#) and determined that the verification test passed. Also relayed is information about what agent was responsible for affixing the signature.

Internet-Draft Authentication-Results SMTP Extension

April 2009

[Appendix C](#). Public Discussion

[REMOVE BEFORE PUBLICATION]

Public discussion of this proposed specification is handled via the mail-vet-discuss@mipassoc.org mailing list. The list is open. Access to subscription forms and to list archives can be found at <http://mipassoc.org/mailman/listinfo/mail-vet-discuss>.

Internet-Draft Authentication-Results SMTP Extension

April 2009

Author's Address

Murray S. Kucherawy
Sendmail, Inc.
6475 Christie Ave., Suite 350
Emeryville, CA 94608
US

Phone: +1 510 594 5400
Email: msk+ietf@sendmail.com

Kucherawy

Expires October 19, 2009

[Page 18]