Individual submission
Internet-Draft
Updates: 7001 (if approved)
Intended status: Standards Track
Expires: December 19, 2014

M. Kucherawy
June 17, 2014

A Property Types Registry for the Authentication-Results Header Field
draft-kucherawy-authres-ptypes-registry-00

Abstract

[RFC7001] describes a header field called Authentication-Results for use with electronic mail messages to indicate the results of message authentication efforts. Any receiver-side software, such as mail filters or Mail User Agents (MUAs), can use this header field to relay that information in a convenient and meaningful way to users, or make sorting and filtering decisions.

One portion of the definition in that document limits the types of authentication properties about a message to a small, fixed set. This document updates the specification to allow new property types to be declared and used.

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 19, 2014.

Table of Contents

1. Introduction

[RFC7001] describes a header field called Authentication-Results for electronic mail messages that presents the results of a message authentication effort in a machine-readable format. The intent of the header field is to create a place to collect such data when message authentication mechanisms are in use so that a Mail User Agent (MUA) and downstream filters can make filtering decisions and/or provide a recommendation to the user as to the validity of the message's origin and possibly the safety and integrity of its content.

The specification in that document enumerated a small set of types of properties that can be reported using this mechanism. There has emerged a desire to report types of properties about a message through this mechanism. Accordingly, this document updates the specification to allow for additional property types ("ptypes") beyond the original set, and creates a registry where new ones can be listed and their defining documents referenced.

2. Updated 'ptype' Definition

Advanced Backus Naur Form (ABNF) is defined in [RFC5234].

The ABNF in Section 2.2 of [RFC7001] is updated as follows:

```
ptype = Keyword
      ; indicates whether the property being evaluated was
      ; a parameter to an [SMTP] command, was a value taken
      ; from a message header field, was some property of
      ; the message body, or was some other property evaluated by
      ; the receiving MTA
```

The ABNF token "Keyword" is defined in Section 4.1.2 of [RFC5321].

Legal values of "ptype" are as defined in this document, or in the IANA "Email Authentication Property Types" registry (see Section 3). The initial values are as follows, matching those defined in [RFC7001]:

body: Indicates information that was extracted from the body of the message. This might be an arbitrary string of bytes, a hash of a string of bytes, a Uniform Resource Identifier, or some other content of interest.

header: Indicates information that was extracted from the header of the message. This might be the value of a header field or some portion of a header field.

policy: As defined in Section 2.3 of [RFC7001].

smtp: Indicates information that was extracted from an SMTP command that was used to relay the message.

A consumer of this header field encountering a "ptype" it does not understand simply ignores the result it is reporting.

3. IANA Considerations

IANA is requested to create the Email Authentication Property Types registry. Entries in this registry are subject to the Expert Review rules as described in [RFC5226]. Each entry in the registry requires the following values:

- The "ptype" token to be registered, which must fit within the ABNF described in Section 2.
- A brief description of what sort of information this "ptype" is meant to cover.
- A reference to the defining document, if any.

The initial entries in this table are enumerated in Section 2. This document should be listed as their defining document values.

For new entries, the Designated Expert simply needs to assure that the description provided for the new entry adequately describes the intended use. An example would be helpful to include, although entries in the Email Authentication Methods registry or the Email Authentication Result Names registry might also serve as examples of intended use.

4. Security Considerations

A consumer of this header field might be confused by a result bearing a "ptype" it does not understand. The advice is simply to ignore such a result since its semantics are unknown to such a consumer. It is unknown how legacy code, which expects one of a fixed set of "ptype" tokens, will handle new tokens as they begin to appear. This could conceivably result in undesirable deliveries for consumers that have been implemented to "fail open".

5. Normative References

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

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

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

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

Appendix A. Acknowledgements

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

Author's Address

Murray S. Kucherawy
270 Upland Drive
San Francisco, CA 94127
US

EMail: superuser@gmail.com