Internet Engineering Task Force (IETF)
Request for Comments: 6008
Category: Standards Track
ISSN: 2070-1721

M. Kucherawy
Cloudmark, Inc.

September 2010

Authentication-Results Registration for Differentiating among Cryptographic Results

Abstract

This memo updates the registry of properties in Authentication-Results: message header fields to allow a multiple-result report to distinguish among one or more cryptographic signatures on a message, thus associating specific results with the signatures they represent.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6008.

Copyright Notice

Table of Contents

1. Introduction

[AUTHRES] defined a new header field for electronic mail messages that presents the results of a message authentication effort in a machine-readable format. Absent from that specification was the means by which the results of two cryptographic signatures, such as those provided by [DKIM], can both have results reported in an unambiguous manner.

Fortunately, [AUTHRES] created IANA registries of reporting properties, enabling an easy remedy for this problem. This memo thus registers an additional reporting property allowing a result to be associated with a specific digital signature.

2. Keywords

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 [KEYWORDS].

3. Discussion

A message can contain multiple signatures of a common sender authentication mechanism, such as [DKIM]. For example, a DomainKeys Identified Mail (DKIM) signer could apply signatures using two or more different message canonicalization algorithms to determine the resistance of each to being broken in transit.

By applying supported "ptype.property" combinations (cf. the ABNF in [AUTHRES]), a result can be associated with a given signature provided the signatures are all unique within one of the registered values (e.g., all of them had unique "header.d" or "header.i" values). This is not guaranteed, however; a single signing agent might have practical reasons for affixing multiple signatures with the same "d=" values while varying other signature parameters. This means one could get a "dkim=pass" and "dkim=fail" result simultaneously on verification, which is clearly ambiguous.

It is thus necessary either to create or to identify a signature attribute guaranteed to be unique, such that it is possible to unambiguously associate a result with the signature to which it refers.

Collisions during general use of SHA1 and SHA256 are uncommon (see [HASH-ATTACKS]), and RSA key signing mechanisms are resilient to producing common substrings. Thus, the actual digital signature for a cryptographic signing of the message is an ideal property for such a unique identification. It is not, however, necessary to include the entire digital signature in an [AUTHRES] header field just to identify which result goes with which signature; since the signatures will almost always be substantially different, it is anticipated that only the first several bytes of a signature will be needed for disambiguating results.

4. Definition

This memo adds the "header.b" reporting item to the IANA "Email Authentication Methods" registry created upon publication of [AUTHRES]. The value associated with this item in the header field MUST be at least the first eight characters of the digital signature (the "b=" tag from a DKIM-Signature) for which a result is being relayed, and MUST be long enough to be unique among the results being reported. Where the total length of the digital signature is fewer than eight characters, the entire signature MUST be included. Matching of the value of this item against the signature itself MUST be case-sensitive.

If an evaluating agent observes that, despite the use of this disambiguating tag, unequal authentication results are offered about the same signature from the same trusted authserv-id, that agent SHOULD ignore all such results.

5. IANA Considerations

Per [IANA-CONSID], the following item is added to the "Email Authentication Methods" registry:

Method	Defined	ptype	property	value
dkim	RFC4871	header	b	full or partial value of signature "b" tag

6. Security Considerations

[AUTHRES] discussed general security considerations regarding the use of this header field. The following new security considerations apply when adding or processing this new ptype/property combination:

6.1. Improvement

Rather than introducing a new security issue, this can be seen to fix a security weakness of the original specification: Useful information can now be obtained from results that could previously have been ambiguous and thus obscured or, worse, misinterpreted.

6.2. Result Forgeries

An attacker could copy a valid signature and add it to a message in transit, modifying some portion of it. This could cause two results to be provided for the same "header.b" value even if the entire "b=" string is used in an attempt to differentiate the results. This attack could cause an ambiguous result to be relayed and possibly neutralize any benefit given to a "pass" result that would have otherwise occurred, possibly impacting the delivery of valid messages.

It is worth noting, however, that a false negative ("fail") can be generated in this way, but it is extremely difficult to create a false positive ("pass") through such an attack. Thus, a cautious implementation could discard the false negative in that instance.

6.3. New Schemes with Small Signatures

Should a new signing scheme be introduced with a signature whose length is less than eight characters, Section 4 specifies that the entire signature must be used. The obvious concern in such a case would be that the signature scheme is itself prone to collisions, making the value reported by this field not useful. In such cases, the risk is created by the likelihood of collisions and not by this mechanism; furthermore, Section 4 recommends the results be ignored if that were to occur, preventing the application of an ambiguous result.

7. References

7.1. Normative References

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

[DKIM] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

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

7.2. Informative References

[HASH-ATTACKS] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

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

Appendix A. Authentication-Results Example

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

A.1. Multiple DKIM Signatures with One Failure

A message that had two DKIM signatures applied by the same domain, one of which failed:

```
Authentication-Results: mail-router.example.net;
      dkim=pass (good signature) header.d=newyork.example.com
            header.b=oINEO8hg;
      dkim=fail (bad signature) header.d=newyork.example.com
            header.b=EToRSuvU
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 ESMTP 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:Message-Id:Subject;
      bh=sEu28nfs9fuZGD/pSr7ANysbY3jtdaQ3Xv9xPQtS0m7=;
      b=oINEO8hgn/gnunsg ... 9n9ODSNFSDij3=
DKIM-Signature: v=1; a=rsa-sha256; s=rashani;
      d=newyork.example.com;
      t=1188964191; c=simple/simple;
      h=From:Date:To:Message-Id:Subject;
      bh=sEu28nfs9fuZGD/pSr7ANysbY3jtdaQ3Xv9xPQtS0m7=;
      b=EToRSuvUfQVP3Bkz ... rTB0t0gYnBVCM=
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
```

Example 1: Header field reporting results from multiple signatures added at initial signing

Here we see an example of a message that was signed twice by the author’s ADministrative Management Domain (ADMD). One signature used "relaxed" header canonicalization, and the other used "simple" header canonicalization; both used "simple" body canonicalization.

Presumably due to a change in one of the five header fields covered by the two signatures, the former signature passed, while the latter signature failed to verify. In particular, the "relaxed" header canonicalization of [DKIM] is resilient to changes in whitespace in the header, while "simple" is not, and the latter is the one that failed in this example.

The item registered by this memo allows an evaluation module to determine which DKIM result goes with which signature. Without the "header.b" portion of the result, it is unclear which one passed and which one failed.

Appendix B. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: Dave Crocker, Tony Hansen, Eliot Lear, S. Moonesamy, and Alessandro Vesely.

Author's Address

Murray S. Kucherawy
Cloudmark, Inc.
128 King St., 2nd Floor
San Francisco, CA 94107
US

Phone: +1 415 946 3800
EMail: msk@cloudmark.com