Internet Engineering Task Force (IETF)
Request for Comments: 6591
Category: Standards Track
ISSN: 2070-1721

H. Fontana

April 2012

Authentication Failure Reporting Using the Abuse Reporting Format

Abstract

This memo registers an extension report type for the Abuse Reporting Format (ARF), affecting multiple registries, for use in generating receipt-time reports about messages that fail one or more email message authentication checks.

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/rfc6591.

Copyright Notice

Table of Contents

1. Introduction

The Abuse Reporting Format [ARF] defines a message format for sending reports of abuse in the messaging infrastructure, with an eye towards automating both the generation and consumption of those reports. There is now also a desire to extend the ARF to include the reporting of messages that fail to authenticate using known message authentication methods, such as DomainKeys Identified Mail [DKIM] and Sender Policy Framework [SPF], as these are sometimes evidence of abuse that can be detected and reported through automated means. The same mechanism can be used to convey forensic information about the specific reason the authentication method failed. Thus, this memo presents such extensions to ARF that allow for detailed reporting of message authentication method failures.

2. Definitions

2.1. Key Words

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].

2.2. Email Architecture

This memo uses some terms whose definitions and descriptions can be found in [EMAIL-ARCH].

2.3. Base64

Base64 is defined in Section 4 of [BASE64].

The values that are base64 encodings MAY contain folding whitespace (FWS) for formatting purposes as per the usual header field wrapping defined in [MAIL]. During decoding, any characters not in the base64 alphabet are ignored so that such line wrapping does not harm the value. The ABNF token "FWS" is defined in [DKIM]. No other extensions to the valid base64 character set are permitted.

2.4. Technologies

There are technologies in email security that provide authentication services and some that do authorization. These are often conflated. A discussion that is useful for establishing context can be found in Section 1.5.2 of [AUTH-RESULTS].

3. ARF Extension for Authentication Failure Reporting

The current report format defined in [ARF] lacks some specific features required to do effective email authentication failure reporting. This section defines extensions to ARF to accommodate this requirement.

A single report describes a single email authentication failure. Multiple reports MAY be used to report multiple failures for a single message.

3.1. New ARF Feedback Type

A new feedback type, "auth-failure", is defined in this document as an extension, per Section 7.3 of [ARF].

A message that uses this feedback type has the following modified header field requirements for the second (machine-parseable) [MIME] part of the report:

Authentication-Results: Syntax as specified in [AUTH-RESULTS]. Furthermore, [ARF] specifies this field is OPTIONAL and appears at most once; for this extension, this field MUST be present, but it MUST reflect only a single authentication method's result.

Original-Envelope-Id: Syntax as specified in [ARF]. Furthermore, [ARF] specifies this field is OPTIONAL and appears at most once; for this extension, this field's inclusion is RECOMMENDED, where that value is available, to aid in diagnosing the authentication failure.

Original-Mail-From: Syntax as specified in [ARF]. Furthermore, [ARF] specifies this field is OPTIONAL and appears at most once; for this extension, this field's inclusion is RECOMMENDED, where that value is available, to aid in diagnosing the authentication failure.

Source-IP: Syntax as specified in [ARF]. Furthermore, [ARF] specifies this field is OPTIONAL and appears at most once; for this extension, this field's inclusion is RECOMMENDED, where that value is available, to aid in diagnosing the authentication failure.

Reported-Domain: Syntax as specified in [ARF]. Furthermore, [ARF] specifies this field is OPTIONAL and appears at most once; for this extension, this field MUST be present if such a value is available.

Delivery-Result: As specified in Section 3.2.2. This field is OPTIONAL, but it MUST NOT appear more than once. If present, it SHOULD indicate the outcome of the message in some meaningful way, but it MAY be set to "other" for local policy reasons.

The third MIME part of the message is either of type "message/rfc822" (as defined in [MIME-TYPES]) or of type "text/rfc822-headers" (as defined in [REPORT]) and contains a copy of the entire header block from the original message. This part MUST be included (contrary to [REPORT], which makes it optional).

For privacy reasons, report generators might need to redact portions of a reported message, such as an identifier or address associated with the end user whose complaint action resulted in the report. A discussion of relevant issues and a suggested method for doing so can be found in [RFC6590].

3.2. New ARF Header Field Names

The following new ARF field names are defined as extensions to Section 3.1 of [ARF].

3.2.1. Required for All Reports

Auth-Failure: Indicates the failure from an email authentication method that is being reported. The list of valid values is enumerated in Section 3.3.

3.2.2. Optional for All Reports

Delivery-Result: The final message disposition that was enacted by the ADministrative Management Domain (ADMD) generating the report. It MUST NOT appear more than once. Possible values are as follows:

delivered: The message was delivered (not specific as to where).

spam: The message was delivered to the recipient’s spam folder (or equivalent).

policy: The message was not delivered to the intended inbox due to a failure from an email authentication method. The specific action taken is not specified.

reject: The message was rejected.

other: The message had a final disposition not covered by one of the above values.

3.2.3. Required for DKIM Reports

DKIM-Domain: The domain that signed the message, taken from the "d=" tag of the signature.

DKIM-Identity: The identity of the signature that failed verification, taken from the "i=" tag of the signature.

DKIM-Selector: The selector of the signature that failed verification, taken from the "s=" tag of the signature.

3.2.4. Optional for DKIM Reports

DKIM-Canonicalized-Header: A base64 encoding of the canonicalized header of the message as generated by the verifier.

DKIM-Canonicalized-Body: A base64 encoding of the canonicalized body of the message as generated by the verifier. The encoded content MUST be limited to those octets that contribute to the DKIM body hash (i.e., the value of the "l=" tag; see Section 3.7 of [DKIM]).

If DKIM-Canonicalized-Header and DKIM-Canonicalized-Body encode redacted data, they MUST NOT be included. Otherwise, they SHOULD be included. The data presented there have to be exactly the canonicalized header and body as defined by [DKIM] and computed at the verifier. This is because these fields are intended to aid in identifying message alterations that invalidate DKIM signatures in transit. Including redacted data in them renders the data unusable. (See also Sections 3.1 and 6.6 for further discussion.)

3.2.5. Required for ADSP Reports

DKIM-ADSP-DNS: Includes the Author Domain Signing Practices (ADSP) policy used to obtain the verifier’s ADSP result. This MUST be formatted per Section 4.2.1 of [ADSP].

3.2.6. Required for SPF Reports

SPF-DNS: This field MUST appear once for every SPF record [SPF] used to obtain the SPF result. It MUST include the DNS RRTYPE used, the DNS domain from which the record was retrieved, and the content of that record. The syntax is defined in Section 4.

3.3. Authentication Failure Types

The list of defined email authentication failure types used in the "Auth-Failure:" header field (defined above), is as follows:

adsp: The message did not conform to the author domain’s published [ADSP] signing practices. The DKIM-ADSP-DNS field MUST be included in the report.

bodyhash: The body hash in the signature and the body hash computed by the verifier did not match. The DKIM-Canonicalized-Body field SHOULD be included in the report (see Section 3.2.4).

revoked: The DKIM key referenced by the signature on the message has been revoked. The DKIM-Domain and DKIM-Selector fields MUST be included in the report.

signature: The DKIM signature on the message did not successfully verify against the header hash and public key. The DKIM-Domain and DKIM-Selector fields MUST be included in the report, and the DKIM-Canonicalized-Header field SHOULD be included in the report (see Section 3.2.4).

spf: The evaluation of the author domain’s SPF record produced a "none", "fail", "softfail", "temperror", or "permerror" result. ("none" is not strictly a failure per [SPF], but a service that demands successful SPF evaluations of clients could treat it like a failure.)

Supplementary data MAY be included in the form of comments compliant with [MAIL]. For example, "Auth-Failure: adsp" could be augmented by a comment to indicate that the failed message was rejected because it was not signed when it should have been. See Appendix B for an example.

4. Syntax for Added ARF Header Fields

The [ABNF] definitions for the new fields are as follows:

```
auth-failure = "Auth-Failure:" [CFWS]
               ( "adsp" / "bodyhash" / "revoked" /
                 "signature" / "spf" ) [CFWS] CRLF
             ; "CFWS" is defined in [MAIL]

delivery-result = "Delivery-Result:" [CFWS]
                  ( "delivered" / "spam" / "policy" /
                    "reject" / "other" ) [CFWS] CRLF

dkim-header = "DKIM-Canonicalized-Header:" [CFWS]
              base64string CRLF
            ; "base64string" is defined in [DKIM]

dkim-sig-domain = "DKIM-Domain:" [CFWS] domain-name [CFWS]
                  CRLF
                ; "domain-name" is defined in [DKIM]

dkim-identity = "DKIM-Identity:" [CFWS] [ local-part ] "@"
                domain-name [CFWS] CRLF
              ; "local-part" is defined in [MAIL]

dkim-selector = "DKIM-Selector:" [CFWS] selector [CFWS] CRLF
              ; "selector" is defined in [DKIM]
```

```
     dkim-adsp-dns = "DKIM-ADSP-DNS:" [CFWS]
                     quoted-string [CFWS] CRLF
                   ; "quoted-string" is defined in [MAIL]

     dkim-body = "DKIM-Canonicalized-Body:" [CFWS]
                 base64string CRLF

     dkim-selector-dns = "DKIM-Selector-DNS:" [CFWS]
                         quoted-string [CFWS] CRLF

     spf-dns = "SPF-DNS:" [CFWS] ( "txt" / "spf" ) [CFWS] ":" [CFWS]
               domain [CFWS] ":" [CFWS] quoted-string [CFWS] CRLF
```

5. IANA Considerations

As required by [IANA], this section contains registry information for the extension to [ARF].

5.1. Updates to ARF Feedback Types

The following feedback type has been added to the Feedback Report Type Values registry:

Feedback Type: auth-failure
Description: email authentication failure report
Published in: [RFC6591]
Status: current

5.2. Updates to ARF Header Field Names

The following headers are added to the Feedback Report Header Fields registry:

Field Name: Auth-Failure
Description: Type of email authentication method failure
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: Delivery-Result
Description: Final disposition of the subject message
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-ADSP-DNS
Description: Retrieved DKIM ADSP record
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-Canonicalized-Body
Description: Canonicalized body, per DKIM
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-Canonicalized-Header
Description: Canonicalized header, per DKIM
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-Domain
Description: DKIM signing domain from "d=" tag
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-Identity
Description: Identity from DKIM signature
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-Selector
Description: Selector from DKIM signature
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: DKIM-Selector-DNS
Description: Retrieved DKIM key record
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

Field Name: SPF-DNS
Description: Retrieved SPF record
Multiple Appearances: No
Related "Feedback-Type": auth-failure
Published in: [RFC6591]
Status: current

6. Security Considerations

Security issues with respect to these reports are similar to those found in [DSN].

6.1. Inherited Considerations

Implementers are advised to consider the Security Considerations sections of [DKIM], [ADSP], [SPF], and [ARF].

6.2. Forgeries

These reports can be forged as easily as ordinary Internet electronic mail. User agents and automatic mail-handling facilities (such as mail distribution list exploders) that wish to make automatic use of Delivery Status Notifications (DSNs) of any kind should take appropriate precautions to minimize the potential damage from denial-of-service attacks.

Security threats related to forged DSNs include the sending of

a. A falsified email authentication method failure notification when the message was in fact delivered to the indicated recipient;

b. Falsified signature information, such as selector, domain, etc.

Perhaps the simplest means of mitigating this threat is to assert that these reports should themselves be signed with something like DKIM. On the other hand, if there’s a problem with the DKIM infrastructure at the verifier, signing DKIM failure reports might produce reports that aren’t trusted or even accepted by their intended recipients.

6.3. Automatic Generation

Automatic generation of these reports by verifying agents can cause a denial-of-service attack when a large volume of email is sent that causes email authentication failures for whatever reason.

Limiting the rate of generation of these messages might be appropriate but threatens to inhibit the distribution of important and possibly time-sensitive information.

In general ARF feedback loop terms, it is suggested that report generators only create these (or any) ARF reports after an out-of-band arrangement has been made between two parties. This mechanism then becomes a way to adjust parameters of an authorized abuse report feedback loop that is configured and activated by private agreement rather than starting to send them automatically based solely on discovered data in the DNS.

6.4. Envelope Sender Selection

In the case of transmitted reports in the form of a new message, it is necessary to consider the construction and transmission of the message so as to avoid amplification attacks, deliberate or otherwise. See Section 5 of [ARF] for further information.

6.5. Reporting Multiple Incidents

If it is known that a particular host generates abuse reports upon certain incidents, an attacker could forge a high volume of messages that will trigger such a report. The recipient of the report could then be inundated with reports. This could easily be extended to a distributed denial-of-service attack by finding a number of report-generating servers.

The incident count referenced in [ARF] provides a limited form of mitigation. The host generating reports may elect to send reports only periodically, with each report representing a number of identical or near-identical incidents. One might even do something inverse-exponentially, sending reports for each of the first ten incidents, then every tenth incident up to 100, then every 100th incident up to 1000, etc., until some period of relative quiet after which the limitation resets.

The use of this technique for "near-identical" incidents in particular causes a degradation in reporting quality, however. If, for example, a large number of pieces of spam arrive from one attacker, a reporting agent might decide only to send a report about a fraction of those messages. While this averts a flood of reports to a system administrator, the precise details of each incident are similarly not sent.

6.6. Redaction of Data in DKIM Reports

This memo requires that the canonicalized header and body be returned without being subject to redaction when a DKIM failure is being reported. This is necessary to ensure that the returned canonicalized forms are useful for debugging, as they must be compared to the equivalent form at the signer. If a message is altered in transit, and the returned data are also redacted, the redacted portion and the altered portion may overlap, rendering the comparison results meaningless. However, unredacted data can leak information the reporting entity considers to be private. It is for this reason the return of the canonicalized forms is not required.

7. References

7.1. Normative References

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

[ADSP] Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", RFC 5617, August 2009.

[ARF] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, August 2010.

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

[BASE64] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[DKIM] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", RFC 6376, September 2011.

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

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

[MAIL] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[MIME-TYPES] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

[REPORT] Kucherawy, M., Ed., "The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages", STD 73, RFC 6522, January 2012.

[RFC6590] Falk, J., Ed., and M. Kucherawy, Ed., "Redaction of Potentially Sensitive Data from Mail Abuse Reports", RFC 6590, April 2012.

[SPF] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

7.2. Informative References

[DSN] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, January 2003.

[EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: Frank Ellermann, J.D. Falk, Scott Kitterman, John Levine, Mike Markley, Kelly Wanser, Murray Kucherawy, and Alessandro Vesely.

Appendix B. Example

This section contains an example of the use of the extension defined by this memo.

B.1. Example Use of ARF Extension Headers

An ARF-formatted report using the proposed ARF extension fields:

```
Message-ID: <433689.81121.example@mta.mail.receiver.example>
From: "SomeISP Antispam Feedback" <feedback@mail.receiver.example>
To: arf-failure@sender.example
Subject: FW: You have a new bill from your bank
Date: Sat, 8 Oct 2011 15:15:59 -0500 (CDT)
MIME-Version: 1.0
Content-Type: multipart/report;
  boundary="------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg";
  report-type=feedback-report
Content-Transfer-Encoding: 7bit

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
Content-Type: text/plain; charset="us-ascii"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit

This is an authentication failure report for an email message
received from a.sender.example on 8 Oct 2011 20:15:58 +0000 (GMT).
For more information about this format, please see [RFC6591].

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit

Feedback-Type: auth-failure
User-Agent: Someisp!Mail-Feedback/1.0
Version: 1
Original-Mail-From: anexample.reply@a.sender.example
Original-Envelope-Id: o3F52gxO029144
Authentication-Results: mta1011.mail.tp2.receiver.example;
 dkim=fail (bodyhash) header.d=sender.example
Auth-Failure: bodyhash
```

```
   DKIM-Canonicalized-Body: VGhpcyBpcyBhIG1lc3NhZ2UgYm9keSB0
     aGF0IGdvdCBtb2RpZmllZCBpbiB0cmFuc2l0LgoKQXQgdGhlIHNhbWU
     gdGltZSB0aGF0IHRoZSBib2R5aGFzaCBmYWlscyB0byB2ZXJpZnksIH
     RoZQptZXNzYWdlIGNvbnRlbnQgaXMgY2xlYXJseSBhYnVzaXZlIG9yI
     HBoaXNoeSwgYXMgdGhlClN1YmplY3QgYWxyZWFkeSBoaW50cy4gIElu
     ZGVlZCwgdGhpcyBib2R5IGFsc28gY29udGFpbnMKdGhlIGZvbGxvd2l
     uZyB0ZXh0OgoKICAgUGxlYXNlIGVudGVyIHlvdXIgZnVsbCBiYW5rIG
     NyZWRlbnRpYWxzIGF0CiAgIGh0dHA6Ly93d3cuc2VuZGVyLmV4YW1wb
     GUvCgpXZSBhcmUgaW1wbHlpbmcgdGhhdCwgYWx0aG91Z2ggbXVsdGlw
     bGUgZmFpbHVyZXMKcmVxdWlyZSBtdWx0aXBsZSByZXBvcnRzLCBhIHN
     pbmdsZSBmYWlsdXJlIGNhbiBiZQpyZXBvcnRlZCBhbG9uZyB3aXRoIH
     BoaXNoaW5nIGluIGEgc2luZ2xlIHJlcG9ydC4K
   DKIM-Domain: sender.example
   DKIM-Identity: @sender.example
   DKIM-Selector: testkey
   Arrival-Date: 8 Oct 2011 20:15:58 +0000 (GMT)
   Source-IP: 192.0.2.1
   Reported-Domain: a.sender.example
   Reported-URI: http://www.sender.example/

   --------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
   Content-Type: text/rfc822-headers
   Content-Transfer-Encoding: 7bit

   Authentication-Results: mta1011.mail.tp2.receiver.example;
    dkim=fail (bodyhash) header.d=sender.example;
    spf=pass smtp.mailfrom=anexample.reply@a.sender.example
   Received: from smtp-out.sender.example
    by mta1011.mail.tp2.receiver.example
    with SMTP id oB85W8xV000169;
    Sat, 08 Oct 2011 13:15:58 -0700 (PDT)
   DKIM-Signature: v=1; c=relaxed/simple; a=rsa-sha256;
    s=testkey; d=sender.example; h=From:To:Subject:Date;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
    4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
    KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
    4bmp/YzhwvcubU4=
   Received: from mail.sender.example
    by smtp-out.sender.example
    with SMTP id o3F52gxO029144;
    Sat, 08 Oct 2011 13:15:31 -0700 (PDT)
   Received: from internal-client-001.sender.example
    by mail.sender.example
    with SMTP id o3F3BwdY028431;
    Sat, 08 Oct 2011 13:15:24 -0700 (PDT)
   Date: Sat, 8 Oct 2011 16:15:24 -0400 (EDT)
   Reply-To: anexample.reply@a.sender.example
   From: anexample@a.sender.example
   To: someuser@receiver.example
   Subject: You have a new bill from your bank
   Message-ID: <87913910.1318094604546@out.sender.example>

   --------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg--
```

Example 1: Example ARF Report Using These Extensions

This example ARF message is making the following assertion:

- o DKIM verification of the signature added within "sender.example" failed.

- o The cause of the verification failure was a mismatch between the body contents observed at the verifier and the body hash contained in the signature.

Author's Address

Hilda L. Fontana
3579 E. Foothill Blvd., Suite 282
Pasadena, CA 91107
US

Phone: +1 626 676 8852
EMail: hilda@hfontana.com