MARF Working Group   H. Fontana
Internet-Draft   December 2, 2011
Intended status: Standards Track
Expires: June 4, 2012

        Authentication Failure Reporting using the Abuse Report Format
                  draft-ietf-marf-authfailure-report-05

Abstract

   This memo registers an extension report type to ARF for use in
   reporting messages that fail one or more authentication checks
   performed on receipt of a message, with the option to include
   forensic information describing the specifics of the failure.

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 4, 2012.

Table of Contents

1. Introduction

   [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 format to include reporting of messages that
   fail to authenticate using known authentication methods, 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 the Abuse
   Reporting Format to allow for detailed reporting of message
   authentication failures.

2. Definitions

2.1. 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].

2.2. Base 64

base64 is defined in [MIME].

The values that are base64 encodings may contain 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].

3. Extension ARF Fields for Authentication Failure Reporting

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

3.1. New ARF Feedback Type

   A new feedback type of "auth-failure" is defined as an extension to
   Section 8.2 of [ARF]. See Section 3.3 for details.

   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: MUST appear exactly once. It MUST be
      formatted according to [AUTH-RESULTS], and MUST reflect only a
      single authentication failure. To report multiple failures for a
      single message, multiple reports MUST be generated. This
      indicates to the receiver the failure that generated the report.

   Original-Envelope-Id: As specified in [ARF]. This field SHOULD be
      included exactly once if available to the entity generating the
      report.

   Original-Mail-From: As specified in [ARF]. This field SHOULD be
      included exactly once for SPF, or for other methods that evaluate
      authentication during the SMTP phase.

   Source-IP: As specified in [ARF]. This field SHOULD be included
      exactly once for SPF, or for other methods that evaluate
      authentication during the SMTP phase.

   Reported-Domain: As specified in [ARF]. This field MUST appear at
      least once.

   Delivery-Result: As specified in Section 3.2.1. This field is
      OPTIONAL, but MUST NOT appear more than once. If present, it
      SHOULD indicate the outcome of the message in some meaningful way,
      but might be redacted 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 "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]).

   For privacy reasons, report generators might need to redact portions

of a reported message such as the end user whose complaint action
resulted in the report. See [I-D.IETF-MARF-REDACTION] for a
discussion of this.

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 type of authentication failure 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 ADMD generating the report and MUST NOT appear more than once.
      Possible values are:

      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 authentication failure. 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 bytes 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 Section 5 and Section 7.6 for further discussion.)

3.2.5. Required For ADSP Reports

   DKIM-ADSP-DNS: Includes the ADSP record discovered and applied by the
   entity generating this report.

3.2.6. Required For SPF Reports

   SPF-DNS MUST appear once for every SPF record used to obtain the SPF
   result.

3.3. Authentication Failure Types

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

   adsp: The message did not conform to the sender's published [ADSP]
      signing practises. 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 sending domain's SPF record produced a
   "fail", "softfail", "temperror" or "permerror" result.

Supplementary data MAY be included in the form of [MAIL]-compliant
comments. 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] token [CFWS] CRLF
           ; "token" must be a registered authentication failure type
           ; as specified elsewhere in this memo
           ; "token" is imported from [MIME]
           ; "CFWS" is imported from [MAIL]

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

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

        dkim-sig-domain = "DKIM-Domain:" [CFWS] dkim-domain [CFWS] CRLF
                        ; "dkim-domain" is imported from [DKIM]

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

        dkim-selector = "DKIM-Selector:" [CFWS] token [CFWS] CRLF

        dkim-adsp-dns = "DKIM-ADSP-DNS:" [CFWS]
                        quoted-string [CFWS] CRLF
           ; "quoted-string" is imported from [MAIL]

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

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

        spf-dns = "SPF-DNS:" : { "txt" / "spf" } [FWS] ":" [FWS]
                  domain [FWS] ":" [FWS] quoted-string

5. IANA Considerations

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

5.1. Updates to ARF Feedback Types

   The following feedback type is added to the Feedback Report Feedback
   Type Registry:

      Feedback Type: auth-failure
      Description: sender authentication failure report
      Registration: (this document)

5.2. Updates to ARF Header Field Names

   The following headers are added to the Feedback Report Header Names
   Registry:

      Field Name: Auth-Failure
      Description: Type of authentication failure
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: Delivery-Result
      Description: Final disposition of the subject message
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-ADSP-DNS
      Description: Retrieved DKIM ADSP record
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-Canonicalized-Body
      Description: Canonicalized body, per DKIM
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-Canonicalized-Header
      Description: Canonicalized header, per DKIM
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-Domain
      Description: DKIM signing domain from "d=" tag
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-Identity
      Description: Identity from DKIM signature
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-Selector
      Description: Selector from DKIM signature
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: DKIM-Selector-DNS
      Description: Retrieved DKIM key record
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

      Field Name: SPF-DNS
      Description: Retrieved SPF record
      Multiple Appearances: No
      Related "Feedback-Type": auth-failure

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 may 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
   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 authentication 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 may
   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 e-mail is sent that
   causes sender authentication failures for whatever reason.

   Limiting the rate of generation of these messages may 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 innundated 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 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
   may 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

   [ADSP]   Allman, E., Delany, M., Fenton, J., and J. Levine, "DKIM
                Sender Signing Practises", 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.

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

   [I-D.IETF-MARF-REDACTION]
                Falk, JD., "Redaction of Potentially Sensitive Data from
                Mail Abuse Reports", I-D draft-ietf-marf-redaction,
                March 2011.

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

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

   [MAIL]   Resnick, P., "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]   Vaudreuil, G., "The Multipart/Report Content Type for the
                Reporting of Mail System Administrative Messages",
                RFC 3462, January 2003.

   [SMTP]   Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,

                October 2008.

   [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.

Appendix A. Acknowledgements

   The authors wish to acknowledge the following for their review and
   constructive criticism of this proposal: Frank Ellerman, 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:

   Received: from mail.example.com (mail.example.com [192.0.2.1])
    by mx.example.net (8.14.4/8.14.4) with ESMTP id c6cs67945pbm;
    Sat, 8 Oct 2011 13:16:24 +0000 (GMT)
   Return-Path: feedback@arf.mail.example.net
   Authentication-Results: mx.example.net; spf=pass (example.net: domain
     of feedback@arf.mail.example.net designates 192.0.2.1 as permitted
     sender) smtp.mail=feedback@arf.mail.example.net
   Message-ID: <433689.81121.example@mta.mail.example.net>
   From: "Someisp Mail Antispam Feedback" <feedback@mail.example.net>
   To: arf-failure@example.com
   Subject: FW: You have a new bill from your bank
   Date: 8 Oct 2011 13:16:24 +0000 (GMT)
   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 anexample.example.com on 8 Oct 2011 13:16:24
   +0000(GMT). For more information about this format please see
   http://datatracker.ietf.org/doc/draft-ietf-marf-authfailure-report

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

   Feedback-Type: auth-failure
   User-Agent: Someisp!-Mail-Feedback/1.0
   Version: 0.1
   Original-Mail-From: anexample@anexample.example.com
   Authentication-Results: mta1011.mail.tp2.example.net

```
 from=anexample.example.com; dkim=fail (bodyhash)
Auth-Failure: bodyhash
DKIM-Canonicalized-Body:VGhpcyBpcyBhIG1lc3NhZ2UgYm9ke
 SB0aGF0IGdvdCBtb2RpZmllZCBpbiB0cmFuc2l0Lgo=
Arrival-Date: 8 Oct 2011 13:16:24 +0000(GMT)
Source-IP: 192.0.2.1
Reported-Domain: anexample.example.com
Policy-Action: none
Reported-URI:http://www.example.com/

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
Content-Type: text/rfc822-headers
Content-Transfer-Encoding: 7bit
Authentication-Results: mta1011.mail.tp2.example.net
 from=anexample.example.com; dkim=fail (bodyhash); spf=pass
DKIM-Signature: v=1; c=relaxed/simple; a=rsa-sha256;
 s=testkey; d=example.net; h=From:To:Subject:Date;
 bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
 b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
 4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
 KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
 4bmp/YzhwvcubU4=
Received: from smtp-out.example.net by mail.example.com
 with SMTP id o3F52gxO029144;
 Sat, 08 Oct 2011 13:15:31 -0700 (PDT)
Received: from internal-client-001.example.com
 by mail.example.com
 with SMTP id o3F3BwdY028431;
 Sat, 08 Oct 2011 13:12:09 -0700 (PDT)
Date: Sat, 8 Oct 2011 13:16:24 -0400 (EDT)
Reply-To: anexample.reply@anexample.example.com
From: anexample@anexample.example.com
Subject: You have a new bill
Message-ID: <87913910.1318094604546>
--------------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 "example.com"
   failed

o The cause for 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