Individual submission
Internet-Draft
Intended status: Standards Track
Expires: April 22, 2010

Y. Shafranovich
ShafTek Enterprises
J. Levine
Domain Assurance Council
M. Kucherawy
Cloudmark

October 19, 2009

An Extensible Format for Email Feedback Reports
draft-shafranovich-feedback-report-08

Status of this Memo

Copyright Notice

Abstract

This document defines an extensible format and MIME type that may be used by network operators to report feedback about received email to other parties. This format is intended as a machine-readable replacement for various existing report formats currently used in Internet email.

Table of Contents

1. Introduction

As the spam problem continues to expand and potential solutions evolve, network operators are increasingly exchanging abuse reports among themselves and other parties. However, different operators have defined their own formats, and thus the receivers of these reports are forced to write custom software to interpret each. In addition, many operators use various other report formats to provide non-abuse-related feedback about processed email. This memo seeks to define a standard extensible format by creating the "message/feedback-report" [MIME] type for these reports.

This format and content type are intended to be used within the scope of the framework of the "multipart/report" content type defined in [REPORT]. While there has been previous work in this area (e.g. [STRADS-BCP] and [ASRG-ABUSE]), none of them have yet been successful. It is hoped that this document will have a better fate.

This format is intended primarily as an Abuse Reporting Format (ARF) for reporting email abuse but also includes support for direct feedback via end user mail clients, reports of some types of virus activity, and some similar issues. It also has the capacity to support message authentication failure reporting, in particular [DKIM].

This document only defines the format and [MIME] content type to be used for these reports. Determination of where these reports should be sent, how trust among report generators and report recipients is established, and reports related to more than one message are outside the scope of this document. It is assumed that best practices will evolve over time, and will be codified in future documents.

1.1. Purpose

The reports defined in this document are intended for several purposes:

- To inform ISPs about email abuse originating from or related to their networks;
- To inform email service providers or other primarily outbound senders that there may be issues regarding their mail; these issues include (but are not limited to) reports that the mail may be considered to be "spam" by a recipient of the message;
- To inform email service provides about opt-out requests;

- To advise providers that certify or otherwise make assertions about mail of recipient disagreement with the assertions.

Please note that while the parent "multipart/report" content type defined in [REPORT] is used for all kinds of administrative messages, this format is intended specifically for communications among providers regarding email abuse and related issues, and SHOULD NOT be used for other reports.

1.2. Requirements

The following requirements are necessary for feedback reports (the actual specification is defined later in this document):

- They must be both human and machine readable;
- A copy of the original email message (both body and header) or the message header must be enclosed in order to allow the receiver to handle the report properly;
- The machine readable section must provide ability for the report generators to share meta-data with receivers;
- The format must be extensible.

1.3. Definitions

This section defines various terms used throughout this document.

1.3.1. General

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].

1.3.2. E-mail Specific

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

2. Format of Email Feedback Reports

To satisfy the requirements, an email feedback report is defined as a [MIME] message with a top-level MIME content type of "multipart/report" (as defined in [REPORT]). The following apply:

a. The "report-type" parameter of the "multipart/report" type is set to "feedback-report";

b. The first MIME part of the message contains a human readable description of the report and MUST be included.

c. The second MIME part of the message is a machine-readable section with the content type of "message/feedback-report" (defined later in this memo) and MUST be included. This section is intended to convey meta-data about the report in question that may not be readily available from the included email message itself.

d. The third MIME part of the message is either of type "message/rfc822" (as defined in [MIME-TYPES] and contains the original message in its entirety, OR is of type "text/rfc822-headers" (as defined in [REPORT] and contains a copy of the entire header block from the orignal message. This part MUST be included (contrary to [REPORT]). While some operators may choose to modify or redact this portion for privacy or legal reasons, it is RECOMMENDED that the entire original email message be included without any modification as such modifications can impede forensic work by the recipient of this report.

e. Except as discussed below, each feedback report MUST be related to only a single email message. Summary and aggregate formats are outside of the scope of this specification.

f. The Subject header field of the feedback report SHOULD be the same as the included email message about which the report is being generated and MAY include only the standard forwarding prefix used by MUAs such as "FW:". (Many smaller operators using MUAs for abuse handling rely on the subject lines for processing.)

3. The 'message/feedback-report' Content Type

A new [MIME] content type called "message/feedback-report" is defined. This content type provides a machine-readable section intended to let the report generator convey meta-data to the report receiver. The intent of this section is to convey information which may not be obvious or may not be easily extracted from the original email message or headers.

The body of this content type consists of multiple "fields" formatted according to the ABNF of [MAIL] header fields. This section defines the initial set of fields provided by this specification. Additional fields may be registered according to the procedure described later in this memo. Although these fields have a syntax similar to those of mail message header fields, they are semantically distinct; hence they SHOULD NOT be repeated in the header area of the message containing the report. Note that these fields represent information that the receiver is asserting about the report in question, but are not necessarily verifiable. Report receivers MUST NOT assume that these assertions are always accurate.

3.1. Required Fields

The following report header fields are REQUIRED and MUST only appear once:

- "Feedback-Type" contains the type of feedback report (as defined in the corresponding IANA registry and later in this memo). This is intended to let report parsers distinguish among different types of reports.

- "User-Agent" indicates the name and version of the software program that generated the report. The format of this field MUST follow section 14.43 of [HTTP]. This field is for documentation only; there is no registry of user agent names or versions, and report receivers SHOULD NOT expect user agent names to belong to a known set.

- "Version" indicates the version of specification that the report generator is using to generate the report. The version number in this specification is set to "0.1". [NOTE TO RFC EDITOR: This should be changed to "1" at time of publication.]

The following report header fields MUST appear exactly once in a [DKIM] failure report (defined below) and MUST NOT appear in other reports:

- "DKIM-Failure" names the type of DKIM verification failure that occurred.

3.2. Optional Fields Appearing Once

The following header fields are OPTIONAL and MUST NOT appear more than once:

- "Original-Envelope-Id" contains the envelope ID string used in the original [SMTP] transaction (see section 2.2.1 of [DSN]).

- "Original-Mail-From" contains a copy of the email address used in the MAIL FROM portion of the original SMTP transaction. The format of this field is defined in section 4.1.1.2 of [SMTP].

- "Arrival-Date" indicates the date and time at which the original message was received by recipient system's MTA. This field MUST be formatted as per section 3.3 of [MAIL].

- "Reporting-MTA" indicates the name of the MTA generating this feedback report. This field is defined in section 2.2.2 of [DSN], except that it is an optional field in this report.

- "Source-IP" contains an IPv4 or IPv6 address of the MTA from which the original message was received. Addresses MUST be formatted as per section 4.1.3 of [SMTP].

- "Incidents" contains an integer indicating the number of incidents this report represents. The absence of this field implies the report covers a single incident. This field MUST NOT be used for report types other than "dkim".

The historic field "Received-Date" SHOULD also be accepted and interpreted identically to "Arrival-Date".

The following header fields are OPTIONAL and may each appear once in a [DKIM] failure report:

- "DKIM-Canonicalized-Body" contains the canonicalized message body of a message which failed DKIM verification, base64-encoded and line-wrapped to remain inside [MAIL] limits. base64 encoding is defined in [MIME].

- DKIM-Canonicalized-Header" contains the canonicalized message header block of a message which failed DKIM verification, base64-encoded and line-wrapped to remain inside [MAIL] limits. This filed SHOULD be included for DKIM reports.

- "DKIM-Domain" contains the domain whose private key was used to sign a message, taken from the signature's "d=" tag.

- "DKIM-Identity" contains the signing agent's identity, taken from the signature's "i=" tag.

- "DKIM-Selector" contains the selector referenced by a DKIM signature, taken from the signature's "s=" tag.

3.3. Optional Fields Appearing Multiple Times

The following set of header fields are OPTIONAL and MAY appear more than once:

- "Authentication-Results" indicates the result of one or more authentication checks run by the report generator. The format of this field is is defined in [AUTH-RESULTS]. Report receivers should note that this field only indicates an assertion made by the report generator.

- "Original-Rcpt-To" includes a copy of the email address used in the RCPT TO portion of the original [SMTP] transaction. The format of this field is defined in section 4.1.1.3 of that memo. This field SHOULD be repeated for every SMTP recipient seen by the report generator.

- "Removal-Recipient" indicates the email address to be removed from the mailing list (MUST NOT be used with report types other than "opt-out"). The format of this field is defined in section 3.4.1 of [MAIL].

- "Reported-Domain" includes a domain name that the report generator believes to be relevant to the report, e.g. the domain whose apparent actions provoked the generation of the report. Domain format is defined in section 2.3.1 of [DNS].

- "Reported-URI" indicates a URI that the report generator believes to be relevant to the report, e.g. a URI to which the report recipient can go for further details. URI format is defined in [URI].

3.4. Formal Definition

The formal definition of the contents of a "message/feedback-report" media type using [ABNF] is as follows:

```
feedback-report = *( feedback-type / user-agent / version )
                  [ dkim-failure ]
```

```
                    opt-fields-once
                    dkim-fields-once
                    *( opt-fields-many )

   feedback-type = "Feedback-Type:" [CFWS] token [CFWS] CRLF
       ; the "token" must be a registered feedback type as
       ; described elsewhere in this document

   user-agent = "User-Agent:" [CFWS] product [CFWS] CRLF

   version = "Version:" [CFWS] token [CFWS] CRLF
       ; as described above

   dkim-failure = "DKIM-Failure:" [CFWS] token [CFWS] CRLF
       ; the "token" must be a registered DKIM failure type
       ; as described elsewhere in this document

   opt-fields-once = [ arrival-date ]
                     [ dkim-failure ]
                     [ incidents ]
                     [ original-envelope-id ]
                     [ original-mail-from ]
                     [ reporting-mta ]
                     [ source-ip ]

   arrival-date = "Arrival-Date:" [CFWS] date-time [CFWS] CRLF

   incidents = "Incidents:" [CFWS] 1*DIGIT [CFWS] CRLF

   original-envelope-id = "Original-Envelope-Id:" [CFWS]
                          envelope-id [CFWS] CRLF

   original-mail-from = "Original-Mail-From:" [CFWS]
                        reverse-path [CFWS] CRLF

   reporting-mta = "Reporting-MTA:" [CFWS] mta-name [CFWS] CRLF

   source-ip = "Source-IP:" [CFWS]
               ( IPv4-address-literal /
                 IPv6-address-literal ) [CFWS] CRLF

   dkim-fields-once = [ dkim-canon-body ]
                      [ dkim-canon-header ]
                      [ dkim-domain ]
                      [ dkim-identity ]
                      [ dkim-selector ]

   dkim-canon-body = "DKIM-Canonicalized-Body:" [CFWS]
```

```
                    base64string [CFWS] CRLF

   dkim-canon-header = "DKIM-Canonicalized-Header:" [CFWS]
                       base64string [CFWS] CRLF

   dkim-domain = "DKIM-Domain:" [CFWS] domain-name [CFWS] CRLF

   dkim-identity = "DKIM-Domain:" [CFWS] [ local-part ] "@"
                   domain-name [CFWS] CRLF

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

   opt-fields-many = [ authres-header ]
                     [ original-rcpt-to ]
                     [ removal-recipient ]
                     [ reported-domain ]
                     [ reported-uri ]

   original-rcpt-to = "Original-Rcpt-To:" [CFWS]
                      forward-path [CFWS] CRLF

   removal-recipient = "Removal-Recipient:" [CFWS]
                       mailbox [CFWS] CRLF

   reported-domain = "Reported-Domain:" [CFWS]
                     domain-name [CFWS] CRLF

   reported-uri = "Reported-Domain:" [CFWS] URI [CFWS] CRLF
```

A set of fields satisfying this ABNF may appear in the transmitted message in any order.

"CRLF" is imported from [ABNF].

"token" is imported from [MIME].

"product" is imported from [HTTP].

"mailbox", "CFWS" and "date-time" are imported from [MAIL].

"envelope-id" and "mta-name" are imported from [DSN].

"reverse-path", "forward-path", "local-part", "IPv4-address-literal" and "IPv6-address-literal" are imported from [SMTP].

"base64string", "domain-name" and "selector" are imported from [DKIM]. Furthermore, a "base64string" SHOULD be line-wrapped as described in section 6.8 of [MIME].

"URI" is imported from [URI].

"authres-header" is imported from [AUTH-RESULTS].

4. Extensibility

Like many other formats and protocols, this format may need to be extended over time to fit the ever changing landscape of the Internet. Therefore, extensibility is provided via two IANA registries: one for feedback types and a second for report header fields. The feedback type registry is to be used in conjunction with the "Feedback-Type" field above. The header name registry is intended for registration of new meta-data fields to be used in the machine readable portion (part 2) of this format. Please note that version numbers do not change with new field registrations unless a new specification of this format is published. Also note that all new field registrations may only be registered as OPTIONAL fields. Any new required fields REQUIRE a new version of this specification to be published.

In order to encourage extensibility and interoperability of this format, implementors MUST ignore any fields they do not support.

5. IANA Considerations

IANA is requested to register a new [MIME] type and create three new registries, as described below.

5.1. MIME Type Registration of 'message/feedback-report'

This section provides the media type registration application from [MIME-REG] for processing by IANA:

To: ietf-types@iana.org

Subject: Registration of media type message/feedback-report

Type name: message

Subtype name: feedback-report

Required parameters: none

Optional parameters: none

Encoding considerations: "7bit" encoding is sufficient and MUST be used to maintain readability when viewed by non-MIME mail readers.

Security considerations: See the Security Considerations section of [this document].

Interoperability considerations: Implementors MUST ignore any fields they do not support.

Published specification: [this document]

Applications which use this media type: Abuse helpdesk software for ISPs, mail service bureaus, mail certifiers, and similar organizations

Additional information: none

Person and email address to contact for further information:

Yakov Shafranovich <ietf@shaftek.org>

Murray S. Kucherawy <msk@sendmail.com>

Intended usage: COMMON

Author:

Yakov Shafranovich

John Levine

Murray S. Kucherawy

Change controller: IESG

5.2. Feedback Report Header Fields

IANA is requested to create the "Feedback Report Header Fields" registry. This registry will contain header fields for use in feedback reports, defined by this memo.

New registrations to this registry MUST have approval by a Designated Expert in accordance with the Expert Review guidelines as described in [IANA-CONSIDERATIONS]. The expert should be appointed by the Area Director for the Applications Area. Any new field registered is considered OPTIONAL by this specification unless a new version of this memo is published.

New registrations MUST contain the following information:

1. Name of the field being registered

2. Short description of the field

3. Whether the field can appear more than once

4. To which feedback type(s) this field applies (or "any")

5. The document in which the specification of the field is published

The initial registry should contain these values:

Field Name: Arrival-Date
Description: date/time the original message was received
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]

Field Name: Authentication-Results
Description: results of authentication check(s)
Multiple Appearances: Yes
Related "Feedback-Type": any
Published in: [this document]

Field Name: DKIM-Canonicalized-Body
Description: Canonicalized body, per DKIM, base64-encoded
Multiple Appearances: No
Related "Feedback-Type": dkim
Published in: [this document]

Field Name: DKIM-Canonicalized-Header
Description: Canonicalized header blcok, per DKIM, base64-encoded
Multiple Appearances: No
Related "Feedback-Type": dkim
Published in: [this document]

Field Name: DKIM-Domain
Description: selector from DKIM signature ("d=" signature tag
value)
Multiple Appearances: No
Related "Feedback-Type": dkim
Published in: [this document]

Field Name: DKIM-Failure
Description: registered DKIM failure type
Multiple Appearances: No
Related "Feedback-Type": dkim
Published in: [this document]

Field Name: DKIM-Identity
Description: DKIM signing identity ("i=" signature tag value)
Multiple Appearances: No
Related "Feedback-Type": dkim
Published in: [this document]

Field Name: DKIM-Selector
Description: selector from DKIM signature ("s=" signature tag
value)
Multiple Appearances: No
Related "Feedback-Type": dkim

Published in: [this document]

Field Name: Feedback-Type
Description: registered feedback report type
Multiple Appearances: No
Related "Feedback-Type": N/A
Published in: [this document]

Field Name: Original-Mail-From
Description: email address used in the MAIL FROM portion of the
original SMTP transaction
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]

Field Name: Original-Rcpt-To
Description: email address used in the RCPT TO portion of the
original SMTP transaction
Multiple Appearances: Yes
Related "Feedback-Type": any
Published in: [this document]

Field Name: Received-Date
Description: date/time the original message was received
(historic; deprecated)
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]

Field Name: Removal-Recipient
Description: email address to be removed from the mailing list
Multiple Appearances: Yes
Related "Feedback-Type": opt-out
Published in: [this document]

Field Name: Reported-Domain
Description: relevant domain name
Multiple Appearances: Yes
Related "Feedback-Type": any
Published in: [this document]

```
Field Name: Reported-URI
Description: relevant URI
Multiple Appearances: Yes
Related "Feedback-Type": any
Published in: [this document]


Field Name: Reporting-MTA
Description: MTA generating this report
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]


Field Name: Source-IP
Description: IPv4 or IPv6 address from which the original message
             was received
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]


Field Name: User-Agent
Description: name and version of the program generating the
             report
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]


Field Name: Version
Description: version of specification used
Multiple Appearances: No
Related "Feedback-Type": any
Published in: [this document]
```

5.3. Feedback Report Type Values

IANA is requested to create the "Feedback Report Type Values" registry. This registry will contain feedback types for use in feedback reports, defined by this memo.

New registrations to this registry MUST have approval by a Designated Expert in accordance with the Expert Review guidelines as described in [IANA-CONSIDERATIONS]. The expert should be appointed by the Area Director for the Applications Area. Any new field registered is considered OPTIONAL by this specification unless a new version of this memo is published.

New registrations MUST contain the following information:

1. Name of the feedback type being registered

2. Short description of the feedback type

3. The document in which the specification of the field is published

The initial registry should contain these values:

Feedback Type Name: abuse
Description: spam or some kind of email abuse
Published in: [this document]

Feedback Type Name: dkim
Description: a DKIM signature verification or policy violation error
Published in: [this document]

Feedback Type Name: fraud
Description: indicates some kind of fraud or phishing activity
Published in: [this document]

Feedback Type Name: miscategorized
Description: indicates that the content categorization applied in connection with a certification or reputation system was incorrect
Published in: [this document]

Feedback Type Name: not-spam
Description: indicates that a message that was tagged or categorized as spam (such as by an ISP) is not spam
Published in: [this document]

Feedback Type Name: opt-out
Description: a request to opt out from mailings from this provider
Published in: [this document]

Feedback Type Name: other
Description: any other feedback that does not fit into other registered types

Published in: [this document]

Feedback Type Name: virus
Description: report of a virus found in the originating message
Published in: [this document]

5.4. Feedback Report DKIM Failure Values

IANA is requested to create the "Feedback Report Header Fields" registry. This registry will contain header fields for use in feedback reports, defined by this memo.

New registrations to this registry MUST have approval by a Designated Expert in accordance with the Expert Review guidelines as described in [IANA-CONSIDERATIONS]. The expert should be appointed by the Area Director for the Applications Area. Any new field registered is considered OPTIONAL by this specification unless a new version of this memo is published.

New registrations MUST contain the following information:

1. Name of the DKIM failure type being registered

2. Short description of the failure type

3. The document in which the specification of the field is published

The initial registry should contain these values:

DKIM Failure Type: bodyhash
Description: The body hash in the signature and the body hash computed by the verifier did not match.
Published in: [this document]

DKIM Failure Type: granularity
Description: The key referenced by the signature on the message was not authorized for use by the sending user.
Published in: [this document]

DKIM Failure Type: other
Description: The signature verification process failed for a reason not enumerated by some other registered DKIM failure type.
Published in: [this document]

DKIM Failure Type: policy
Description: The DKIM Author Domain Signing Practises (ADSP)
evaluation failed.
Published in: [this document]

DKIM Failure Type: revoked
Description: The key referenced by the signature on the message
has been revoked.
Published in: [this document]

DKIM Failure Type: signature
Description: The signature on the message did not successfully
verify against the header hash and public key.
Published in: [this document]

DKIM Failure Type: syntax
Description: The key referenced by the signature on the message,
or the signature itself, contained a syntax error.
Published in: [this document]

6. Security Considerations

The following security considerations apply when generating or processing a feedback report:

6.1. Inherited from RFC3462

All of the Security Considerations from [REPORT] are inherited here.

6.2. Interpretation

This specification describes a report format. This memo makes no normative assertions of any kind about actions to be taken by recipients of these reports. Actions taken by recipients are done entirely at their own discretion.

There will be some desire to perform some actions in an automated fashion in order to enact timely responses to common feedback reports. Caution must be taken, however, as there is no substantial security around the content of these reports. An attacker could craft a report meant to generate undesirable actions on the part of a report recipient.

It is recommended that ARF reports be vetted using common message authentication schemes such as [DKIM], [SPF] or [SENDERID] to confirm that they represent a valid message from the purported sender of the report prior to the undertaking of any kind of automated action in response to receipt of the report.

6.3. Envelope Sender Selection

When generating an ARF message, it is necessary to construct the message so as to avoid amplification or backscatter attacks, deliberate or otherwise. Thus, per Section 2 of [DSN], the envelope sender address of the ARF message should be chosen to ensure that no delivery status reports will be issued in response to the ARF message itself, and must be chosen so that these reports will not generate mail loops. Whenever an SMTP transaction is used to send an ARF message, the MAIL FROM command must use a NULL return address, i.e. "MAIL FROM:<>".

6.4. 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 this header field 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.

6.5. Intentionally Malformed Reports

It is possible for an attacker to generate an ARF message field which is extraordinarily large or otherwise malformed in an attempt to discover or exploit weaknesses in recipient parsing code. Implementors must thoroughly verify all such messages and be robust against intentionally as well as unintentionally malformed messages.

7. References

7.1. Normative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 5234, January 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-REG] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", RFC 4288, December 2005.

[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.

7.2. Informative References

[ASRG-ABUSE] Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF), "Abuse Reporting Standards Subgroup oof the ASRG", May 2005.

[AUTH-RESULTS] 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.

[DNS] Mockapetris, P., "Domain Names -- Implementation and Specification", RFC 1035, November 1987.

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

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[I-D.DRAFT-CROCKER-EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", draft-crocker-email-arch (work in progress), May 2007.

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

[SENDERID] Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", RFC 4406, April 2006.

[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.

[STRADS-BCP] Crissman, G., "Proposed Spam Reporting BCP Document", May 2005.

[URI] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, January 2005.

Appendix A. Acknowledgements

The authors would like to thank many of the members of the email community who provided helpful comments and suggestions for this document including many of the participants in ASRG, IETF and MAAWG activities, and all of the members of the abuse-feedback-report public mailing list.

Appendix B. Sample Feedback Reports

This section presents some examples of the use of this message format to report feedback about an arriving message.

B.1. Simple Report for Email Abuse without Optional Headers

Simple report:

```
From: <abusedesk@example.com>
Date: Thu, 8 Mar 2005 17:40:36 EDT
Subject: FW: Earn money
To: <abuse@example.net>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
     boundary="part1_13d.2e68ed54_boundary"

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

This is an email abuse report for an email message received from IP
192.0.2.1 on Thu, 8 Mar 2005 14:00:00 EDT. For more information
about this format please see http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: abuse
User-Agent: SomeGenerator/1.0
Version: 0.1

--part1_13d.2e68ed54_boundary
Content-Type: message/rfc822
Content-Disposition: inline

From: <somespammer@example.net>
Received: from mailserver.example.net
     (mailserver.example.net [192.0.2.1])
     by example.com with ESMTP id M63d4137594e46;
     Thu, 08 Mar 2005 14:00:00 -0400
To: <Undisclosed Recipients>
Subject: Earn money
MIME-Version: 1.0
Content-type: text/plain
Message-ID: 8787KJKJ3K4J3K4J3K4J3.mail@example.net
Date: Thu, 02 Sep 2004 12:31:03 -0500

Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
--part1_13d.2e68ed54_boundary--
```

Example 1: Required fields only

Illustration of a feedback report generated according to this

specification. Only the required fields are used.

B.2. Opt-Out Report without Message Body

A sample opt-out report

```
From: <abusedesk@example.com>
Date: Thu, 8 Mar 2005 17:40:36 EDT
Subject: FW: Earn money
To: <abuse@example.net>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
     boundary="part1_13d.2e68ed54_boundary"

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

This is an opt-out report for an email message received from IP
192.0.2.1 on Thu, 8 Mar 2005 14:00:00 EDT. For more information
about this format please see http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: opt-out
User-Agent: SomeGenerator/1.0
Version: 0.1
Removal-Recipient: user@example.com

--part1_13d.2e68ed54_boundary
Content-Type: text/rfc822-header

From: <somespammer@example.net>
Received: from mailserver.example.net
     (mailserver.example.net [192.0.2.1])
     by example.com with ESMTP id M63d4137594e46;
     Thu, 08 Mar 2005 14:00:00 -0400
To: <Undisclosed Recipients>
Subject: Earn money
MIME-Version: 1.0
Content-type: text/plain
Message-ID: 8787KJKJ3K4J3K4J3K4J3.mail@example.net
Date: Thu, 02 Sep 2004 12:31:03 -0500
--part1_13d.2e68ed54_boundary--
```

Example 2: An opt-out feedback report, which indicates the address of a user who wishes to opt out of a mailing list

The report is generated as a result of a user indicating to its ISP that it does not wish to receive further messages of this kind. The report returned only the header block from the original message. The report's recipient receives the address of the requesting user and can use the header block and its own records to determine from which distribution list the requesting user should be removed.

B.3. Full Report for Email Abuse with All Headers

A full email abuse report:

```
From: <abusedesk@example.com>
Date: Thu, 8 Mar 2005 17:40:36 EDT
Subject: FW: Earn money
To: <abuse@example.net>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
     boundary="part1_13d.2e68ed54_boundary"

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

This is an email abuse report for an email message received from IP
192.0.2.1 on Thu, 8 Mar 2005 14:00:00 EDT. For more information
about this format please see http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: abuse
User-Agent: SomeGenerator/1.0
Version: 0.1
Original-Mail-From: <somespammer@example.net>
Original-Rcpt-To: <user@example.com>
Received-Date: Thu, 8 Mar 2005 14:00:00 EDT
Source-IP: 192.0.2.1
Authentication-Results: mail.example.com
               smtp.mail=somespammer@example.com;
               spf=fail
Reported-Domain: example.net
Reported-Uri: http://example.net/earn_money.html
Reported-Uri: mailto:user@example.com
Removal-Recipient: user@example.com

--part1_13d.2e68ed54_boundary
Content-Type: message/rfc822
Content-Disposition: inline
```

```
From: <somespammer@example.net>
Received: from mailserver.example.net (mailserver.example.net
     [192.0.2.1]) by example.com with ESMTP id M63d4137594e46;
     Thu, 08 Mar 2005 14:00:00 -0400
To: <Undisclosed Recipients>
Subject: Earn money
MIME-Version: 1.0
Content-type: text/plain
Message-ID: 8787KJKJ3K4J3K4J3K4J3.mail@example.net
Date: Thu, 02 Sep 2004 12:31:03 -0500

Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
--part1_13d.2e68ed54_boundary--
```

Example 3: Generic abuse report with maximum returned information

A contrived example in which the report generator has returned all possible information about an abuse incident.

B.4. Sample DKIM Failure Report

[TBD]

Appendix C. Public Discussion, History and Support

[REMOVE BEFORE PUBLICATION]

Public discussion of this proposed specification is handled via the abuse-feedback-report@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/abuse-feedback-report. Active participation has included such sectors as messaging software vendors, messaging service providers, messaging consultants, anti-spam vendors, large Internet service providers, etc.

Copies of this and earlier versions including multiple formats can be found at <http://www.shaftek.org/publications/drafts/abuse-report/>. A public website regarding this draft and related efforts is located at <http://mipassoc.org/arf/>.

(impetus for the work should be discussed here)

(MAAWG activity should be discussed here)

Several companies have already adopted use of this proposal, including large-scale e-mail hosting providers and Internet service providers. For a list of these, see the PROTO document supporting this draft.

Appendix D. Document History

Changes from draft-shafranovich-feedback-report-01-pre1 to draft-shafranovich-feedback-report-01:

- Added an "Outstanding Issues" section.
- Minor spelling mistakes and clarifications.
- Added links to previous work and more examples.
- Added three new types: "fraud" for phishing, "opt-out-list" for a single list opt out, and "other" as a catch-all.

Changes from draft-shafranovich-feedback-report-00 to draft-shafranovich-feedback-report-01-pre1:

- Changed the introduction section to clarify specific points that are out of scope for this document.
- Added pointers to a public mailing list for discussion and public web page.
- Clarified the intent section and added some extra points to it.
- Made it clear that the requirements section is not the one defining the standard.
- Clarified the main format section to make all three parts mandatory.
- Changed section 4f regarding subject lines to mandate that subject lines should be left intact. Removed the convention for subject lines that was defined in the previous version.
- Added text to the the machine readable section clarifying its intent. Also added RFC2119 references, reorganized fields, indicated whether specific header fields can appear more than once and provided references as to how they should be formatted.
- Removed "Original-Message-ID", "Authenticated-Domain" and "Authenticated-Domain-Method" from the draft including related IANA registries. Added "Version", "User-Agent", Original-Mail-From", "Original-Rcpt-To", "Reported-URI", "Reported-Domain" and "Authentication-Results".
- Example has been updated to reflect new fields.

- Added a new section on extensibility and changed the IANA section to reflect that.

Changes from draft-shafranovich-abuse-report-00 to draft-shafranovich-feedback-report-00:

- Name of the format and report changed to 'feedback-report'
- Minor spelling corrections
- Added authentication headers and registry
- Added feedback-type header and registry

Changes from draft-shafranovich-feedback-report-00 to draft-shafranovich-feedback-report-01:

- None significant (just a freshening)

Changes from draft-shafranovich-feedback-report-01 to draft-shafranovich-feedback-report-02:

- Much editorial cleanup
- Added John Levine and Paul Hoffman as co-authors
- Made the line lengths in Appendix A appropriate for RFCs
- Switched to symbolic names for references
- Reduced duplication of reference calls
- Removed text that specified the type of RFC and approval type that is expected
- Removed the requirement for an RFC to update the IANA registries; both are now designated expert approval only
- Added two new categories to the initial values for the "Feedback-Type" registry: "miscategorized" and "not-spam"

Changes from draft-shafranovich-feedback-report-02 to draft-shafranovich-feedback-report-03:

- Added a bit to the Security Considerations section
- Updated obsolete references

- Resolved all items in the outstanding issues list and therefore removed it

Changes from draft-shafranovich-feedback-report-03 to draft-shafranovich-feedback-report-04:

- Added Murray Kucherawy as co-author
- Added support for DKIM reporting
- Cleaned up XML a lot

Changes from draft-shafranovich-feedback-report-04 to draft-shafranovich-feedback-report-05:

- Add "Incidents" header
- RFC3464 replaces RFC1894
- RFC5226 replaces RFC2434

Changes from draft-shafranovich-feedback-report-05 to draft-shafranovich-feedback-report-06:

- Remove Paul Hoffman as co-author, per his request
- Add ABNF section
- Move MIME registration stuff from the earlier sections to the IANA Considerations section
- Some other minor re-organization
- Add more stuff to Security Considerations
- Add more project history
- Overhaul the XML
- Add and update several references; use symbolic references instead of numbered ones
- Use RFC3330 "TEST-NET" addresses in examples
- Fix some typos

Changes from draft-shafranovich-feedback-report-06 to draft-shafranovich-feedback-report-07:

- I-D.DRAFT-KUCHERAWY-SENDER-AUTH-HEADER published as RFC5451

Changes from draft-shafranovich-feedback-report-07 to draft-shafranovich-feedback-report-08:

- None.

Still to be done:

- Add a DKIM example
- Add explicit extension field and type support

Authors' Addresses

Yakov Shafranovich
ShafTek Enterprises
4014 Labyrinth Rd.
Baltimore, MD 21215

Email: ietf@shaftek.org
URI: http://www.shaftek.org

John Levine
Domain Assurance Council
PO Box 727
Trumansburg, NY 14886

Phone: +1 831 480 2300
Email: john.levine@domain-assurance.org
URI: http://www.domain-assurance.org

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

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