DMARC
Internet-Draft
Intended status: Informational
Expires: December 23, 2016

F. Martin, Ed.
LinkedIn
E. Lear, Ed.
Cisco Systems GmbH
T. Draegen, Ed.
dmarcian, inc.
E. Zwicky, Ed.
Yahoo
K. Andersen, Ed.
LinkedIn

June 21, 2016

Interoperability Issues Between DMARC and Indirect Email Flows

draft-ietf-dmarc-interoperability-17

Abstract

DMARC (Domain-based Message Authentication, Reporting, and Conformance) introduces a mechanism for expressing domain-level policies and preferences for email message validation, disposition, and reporting. The use of restrictive policies through the DMARC framework can cause interoperability issues when messages do not flow directly from the author's administrative domain to the final recipients. Collectively these email flows are referred to as indirect email flows. This document describes interoperability issues between DMARC and indirect email flows. Possible methods for addressing interoperability issues are presented.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 23, 2016.

Copyright Notice

Table of Contents

1. Introduction

DMARC [RFC7489] introduces a mechanism for expressing domain-level policies and preferences for message validation, disposition, and reporting. The DMARC mechanism, especially when employed with restrictive policies, encounters several different types of interoperability issues due to third-party message sourcing, message transformation, or rerouting.

At the time of the writing of this document, the DMARC base specification is published as Informational RFC 7489 [RFC7489] and has seen significant deployment within the email community.

Cases in which email does not flow directly from the author's administrative domain to the recipient's domain(s) are collectively referred to in this document as indirect email flows. Due to existing and increasing adoption of DMARC, the impact of DMARC-based email rejection policies on indirect email flows can be significant for a select subset of general email traffic.

Several known causes of interoperability issues are presented, followed by a description of components within the Internet Mail Architecture [RFC5598] where interoperability issues can arise.

Finally, known and possible methods for addressing interoperability issues are presented. There are often multiple ways to address any given interoperability issue. While this document strives to be comprehensive in its review, it should not be treated as complete. Note that some practices which are in use at the time of this document may or may not be "best practices", especially as future standards evolve.

1.1. Document Conventions

The notation used in this document for structured fields is taken from [RFC5598] section 1.3.

The term "notification message" [RFC5321] section 4.5.5 is used to refer to a message with a null RFC5321.MailFrom.

The terms "Organizational Domain" and "Authenticated Identifiers" are specified in DMARC [RFC7489] section 3.

2. Causes of Interoperability Issues

Interoperability issues between DMARC and indirect email flows arise when conformance to the DMARC specification leads a receiving implementation to apply DMARC-based policy restrictions to messages that are both compliant with the architecture as specified in [RFC5598] and viewed as legitimate by the intended recipient.

Note that domains which assert a "p=none" policy and email which passes standard DMARC validation do not have any interoperability issues.

Email messages that do not conform to IETF email specifications but are considered legitimate by the intended recipients are not discussed in this document.

The rest of this section describes several conceptual causes of interoperability issues.

2.1. Identifier Alignment

Note to operators and administrators: The identifiers which are used by SPF are technical components of the transport process for SMTP. They may or may not, as described below, bear a meaningful relationship to the content or source of the message itself. This "relationship by proximity" can be a point of confusion for non-technical end users, either recipients or senders.

DMARC relies on DKIM [RFC6376] and SPF [RFC7208] to perform message source validation. The DMARC [RFC7489] specification refers to source domains that are validated by DKIM or SPF as "Authenticated Identifiers". To be used by DMARC an "Authenticated Identifier" must also be related to the domain found in the message's RFC5322.From header field [RFC5322]. This relationship between an Authenticated Identifier's domain and the domain of the RFC5322.From is referred to as "Identifier Alignment".

DMARC allows for Identifier Alignment to be determined in two different modes: strict and relaxed. Strict mode requires an exact match between the domain of any of the Authenticated Identifiers and the message's RFC5322.From header field [RFC5322]. Relaxed mode allows for Identifier Alignment if Authenticated Identifiers and the message's RFC5322.From header field [RFC5322] share the same Organizational Domain. In general, DMARC interoperability issues are the same for both strict and relaxed alignment, but strict alignment constrains the possible solutions because of the more rigorous matching requirement. Some of mitigations described in this document only work with the relaxed mode of Identifier Alignment.

2.1.1. DKIM Identifier(s)

DKIM provides a cryptographic means for one or more domain identifier to be associated with a particular message. As a standalone technology DKIM identifiers are not required to be related to the source of the message's content. However, for a DKIM identifier to align in DMARC, the signing domain of a valid signature must be part of the same Organizational Domain as the domain in the RFC5322.From header field [RFC5322].

In addition, DKIM allows for the possibility of multiple valid signatures. These multiple signatures may be from the same or different domains, there are no restrictions within the DKIM specification. The DMARC mechanism will process Authenticated Identifiers that are based on DKIM signatures until an aligned Authenticated Identifier is found (if any). However, operational experience has shown that some implementations have difficulty processing multiple signatures. Implementations that cannot process multiple DKIM signatures may incorrectly flag messages as "not passing" (DMARC alignment) and erroneously apply DMARC-based policy to otherwise conforming messages.

2.1.2. SPF Identifier(s)

The SPF specification [RFC7208] defines two Authenticated Identifiers for each message. These identifiers derive from:

a. the RFC5321.MailFrom [RFC5321] domain, and
b. the RFC5321.HELO/.EHLO SMTP domain.

In the SPF specification, the RFC7208.MAILFROM [RFC7208] value is defined to be based on RFC5321.MailFrom unless that value is absent (as in the case of notification messages) in which case, the second (RFC5321.HELO/.EHLO) identifier value is used. This "fallback" definition has occasionally been misunderstood by operators of MTA systems since notification messages are often an "automatic" feature of MTA software. Some MTA software does not provide the ability to apply a DKIM signature to such notification messages.

See Appendix A for an example treatment of this scenario.

For the purposes of DMARC validation/alignment, the hybrid RFC7208.MAILFROM [RFC7208] identifier's domain is used if and only if it is aligned with the RFC5322.From [RFC5322] domain. The alignment of the validated domain is determined based on the DMARC record's "strict" or "relaxed" designation as described above for the DKIM identifiers and in [RFC7489].

2.1.3. Multiple RFC5322.From Addresses

[RFC5322] permits only one From header field, but it may contain multiple mailboxes. Since this is an extremely rare usage, DMARC specifies that the handling of this situation is implementation dependent.

Because the presence of multiple domains can be used by an attacker (an attacker could add their domain to the RFC5322.From field, provide arbitrary new content, and sign the message) the DMARC specification recommends that the strictest policy be applied to such messages (section 6.6.1 [RFC7489]).

2.2. Message Forwarding

Section 3 describes forwarding behavior as it relates to the components of the Internet Mail Architecture.

All forwarding operations involve the retransmission of email. As discussed above, in order for SPF to yield an Authenticated Identifier that is pertinent to DMARC, the domain of the RFC7208.MAILFROM must be in alignment with the RFC5322.From header field. Forwarding introduces specific issues to the availability of SPF-based Authenticated Identifiers:

- If the RFC5321.MailFrom is present and the forwarder maintains the original RFC5321.MailFrom, SPF validation will fail unless the forwarder is an authorized part of the originator's email sending infrastructure. If the forwarder replaces the RFC5321.MailFrom with its own domain, SPF might pass but Identifier Alignment with the RFC5322.From header field will fail.
- If the RFC5321.MailFrom is empty (as in the case of Delivery Status Notifications), the RFC5321.HELO/.EHLO domain of the forwarder will likely be in a different organizational domain than the original RFC5322.From header field's domain. SPF

may pass but Identifier Alignment with the RFC5322.From header field will fail.

In both cases, SPF cannot yield relevant Authenticated Identifiers, and DKIM must be relied upon to produce results that are relevant to DMARC.

2.3. Message Modification

Modification of email content invalidates most DKIM signatures, and many message forwarding systems modify email content. Mailing list processors are a common example of such systems, but other forwarding systems also make modifications.

Although DKIM provides a length flag so that content can be appended without invalidating the signature, in practice, particularly with MIME-encoded [RFC2045] messages, a mailing list processor will do more than simply append content (see Section 5.3 of [RFC5598] for details). Furthermore, the length flag is seldom used due to security issues (see Section 8.2 of [RFC6376] for additional security considerations), therefore, this method is only here mentioned for completeness.

DKIM describes two canonicalizations for use when preparing header and body for DKIM processing: simple and relaxed. The latter is designed to accommodate trivial modifications to whitespace and folding which, at least in the header case, generally have no semantic significance. However, the relaxed canonicalization is more computationally intensive and may not have been preferred in the early deployment of DKIM, leaving some deployments using the less forgiving "simple" canonicalization. While the prevalence is unknown, there are some DKIM verifiers which have problems evaluating relaxed canonicalization correctly.

3. Internet Mail Architecture, DMARC, and Indirect Email Flows

This section describes components within the Internet Mail Architecture [RFC5598] where interoperability issues between DMARC and indirect email flows can be found.

3.1. Message Handling System

Section 4 of [RFC5598] describes six basic components that make up the Message Handling System (MHS):

- Message
- Message User Agent (MUA)
- Message Submission Agent (MSA)
- Message Transfer Agent (MTA)
- Message Delivery Agent (MDA)
- Message Store (MS)

Of these components MSA, MTA, and MDA are discussed in relation to interoperability with DMARC.

[RFC5598] Section 5 also defines a Mediator as a hybrid of several component types. A Mediator is given special consideration in this section due to the unique issues they face when attempting to interoperate with DMARC.

3.1.1. Message Submission Agents

An MSA accepts messages submitted by a Message User Agent (MUA) and enforces the policies of the hosting ADministrative Management Domain (ADMD) and the requirements of Internet standards.

MSAs are split into two sub-components:

- Author-focused MSA functions (aMSA)
- MHS-focused MSA functions (hMSA)

MSA interoperability issues with DMARC begin when an aMSA accepts a message where the RFC5322.From header field contains a domain that is outside of the ADMD of the MSA. This situation manifests in one of several ways, such as when someone uses a mail service with their own domain but has failed to properly configure an SPF record; or when an MUA attempts to transmit mail as someone else. Examples of the latter situation include "forward-to-friend" functionality commonly found on news/article websites or "send-as" functionality present on some MUAs.

When an hMSA takes responsibility for transit of a message containing a domain in the RFC5322.From header field that is outside of the hMSA's ADMD, the hMSA faces DMARC interoperability issues if the domain publishes a DMARC policy of "quarantine" or "reject". These issues are marked by the inherent difficulty of establishing alignment with the domain present in a message's RFC5322.From header field. Examples of this issue include:

- Partially-open relays - a residential ISP that allows its customers to relay non-local domains through its infrastructure.
- Embedded devices - cable/DSL modems, firewalls, wireless access points, printers that send email using hardcoded domains.
- Devices that send mail on behalf of a user - scanners, security cameras, alarms that send mail as their owner or a device user.
- Email service providers - ESPs that service customers who are using domains that publish a DMARC "reject" policy.
- Calendaring software - an invited member of an event modifies the event causing calendaring software to emit an update that claims to come from the creator of the event.

3.1.2. Message Transfer Agents

MTAs relay a message until the message reaches a destination MDA. Some common message handling strategies break the integrity of DKIM signatures. A restrictive DMARC policy along with a broken DKIM signature causes latent interoperability problems to become overt problems.

3.1.2.1. Message Encoding

An MTA may modify the message encoding, for instance by converting 8-bit MIME sections to quoted-printable 7-bit sections. This modification is outside the scope of DKIM canonicalization and will invalidate DKIM signatures that include message content.

An MTA could also re-encode the message without changing the encoding type, receiving a MIME-encoded message and producing a semantically and semiotically-equivalent MIME body that is not identical to the original. This is characteristic of systems that use some

other message representation internally.

3.1.2.2. Header Standardization

An MTA may rewrite headers to bring them into compliance with existing RFCs. For example, some common MTAs will correct comprehensible but non-compliant date formats to compliant ones.

Header rewriting is outside the scope of DKIM canonicalization and will invalidate DKIM signatures. All downstream DMARC processing with be unable to utilize DKIM to yield Authenticated Identifiers due to header rewriting.

Providing solutions for issues relating to non RFC-compliant emails is outside the scope of this document.

3.1.2.3. Content Validation

An MTA may also implement security-motivated changes to the content of email messages, dropping or altering sections of messages, causing breakage of DKIM signatures

3.1.3. Message Delivery Agents

The MDA transfers a message from the MHS to a mailbox. Like the MSA, the MDA consists of two sub-components:

- MHS-focused MDA functions (hMDA)
- Recipient-focused MDA functions (rMDA)

Both the hMDA and the rMDA can redirect a message to an alternative address. DMARC interoperability issues related to redirecting of messages are described in Section 3.2.

SIEVE [RFC5228] functionality often lives in the rMDA sub-component and can cause DMARC interoperability issues. The SIEVE 'addheader' and 'deleteheader' filtering actions can modify messages and invalidate DKIM signatures, removing DKIM-supplied Authenticated Identifiers as inputs to the DMARC mechanism. There are also SIEVE extensions [RFC5703] that modify the body. SIEVE alterations may only become an issue when the email is reintroduced into the transport infrastructure.

3.2. Mediators

Mediators [RFC5598] forward messages through a re-posting process. Mediators share some functionality with basic MTA relaying, but have greater flexibility in both addressing and content modifications.

DMARC interoperability issues are common within the context of Mediators, which are often used precisely for their ability to modify messages.

The DMARC design does not cope with some Mediator functionality such as content modifications that invalidate DKIM signatures and RFC5321.MailFrom rewriting to support SPF authentication of resent mail when the new Recipient receives the message from the Mediator rather than the initial organization.

3.2.1. Alias

An Alias is a simple re-addressing facility that provides one or more new Internet Mail addresses, rather than a single, internal one. A message continues through the transfer service for delivery to one or more alternative addresses.

Aliases can be implemented by mailbox-level forwarding (e.g., through "dot-forwarding") or SIEVE-level forwarding (through the SIEVE 'redirect' action) or other methods. When an Alias preserves message content and does not make significant header changes, DKIM signatures may remain valid. However, Aliases often extend the delivery path outside of the scope covered by the originating ADMD's SPF record(s).

Examples of Aliasing include:

- Forwarding email between free email (freemail) providers to try different interfaces while maintaining an original email address;
- Consolidating many email addresses into a single account to centralize processing;
- Services that provide "activity-based", "role-based" , "vanity" or "temporary" email addresses such as universities and professional associations. For instance professional or alumni institutions may offer their members an alias for the duration of their membership but may not want to deal with the long term storage of emails.

In most cases, the aMSA providing Alias services has no administrative relationship to the ADMD of the originator or the final recipient, so solutions to Alias-related DMARC failure should not assume such a relationship.

3.2.2. ReSenders

ReSenders "splice" a message's addressing information to connect the Author of the original message with the Recipient(s) of the new message. The new Recipient sees the message as being from the original Author, even if the Mediator adds commentary.

Without Authenticated Identifiers aligned with the Author's RFC5322.From header field domain, the new Recipient has no way to achieve a passing DMARC evaluation.

Examples of ReSenders include MUA-level forwarding by resending a message to a new recipient or by forwarding a message "inline" to a new recipient (this does not include forwarding a message "as an attachment"). An additional example comes in the form of calendaring software that allows a meeting attendee (not the meeting organizer) to modify the content of an invite generating new invitations that claim to be reissued from the meeting organizer.

3.2.3. Mailing Lists

A Mailing List receives messages as an explicit addressee and then reposts them to a list of subscribed members. The Mailing List performs a task that can be viewed as an elaboration of the ReSender actions.

Mailing Lists share the same DMARC interoperability issues as ReSenders [resenders], and very commonly modify headers or message content in ways that will cause DKIM to fail, including:

- prepending the RFC5322.Subject header field with a tag, to allow the recipient to easily identify the mailing list within a subject line listing;
- adding a footer to the email body to contain administrative instructions;
- removing some MIME-parts from the email or converting the message to text only;
- PGP-encrypting or S/MIME encrypting the body with the receiver's key;
- enforcing community standards by rewriting banned words;
- allowing moderators to add arbitrary commentary to messages (discussed in [RFC6377]).

Any such modifications would invalidate a DKIM signature.

Header and content modifications are common for many mailing lists and are often central to present mailing list functionality and usage. Furthermore, MUAs have come to rely on mailing list message modifications to present messages to end users in expected ways.

3.2.3.1. Mailing List Operational Effects

Mailing Lists may also have the following DMARC interoperability issues:

- Subscribed members may not receive email from members that post using domains that publish a DMARC "p=reject" policy.
- Mailing Lists may interpret DMARC-related email rejections as an inability to deliver email to the recipients that are checking and enforcing DMARC policy. This processing may cause subscribers that are checking and enforcing DMARC policy to be inadvertently suspended or removed from the Mailing List.

3.2.4. Gateways

A Gateway performs the basic routing and transfer work of message relaying, but it also is permitted to modify content, structure, addressing, and/or other attributes as needed to send the message into a messaging environment that operates under different standards or potentially incompatible policies.

Gateways share the same DMARC interoperability issues as ReSenders [resenders].

Gateways may also share the same DMARC interoperability issues as MTAs [mta].

Receiver systems on the non-SMTP side of a protocol gateway may be unable to evaluate DKIM and SPF. If a message passes through a second protocol gateway back into the SMTP domain, the transformations commonly break the original DKIM signature(s).

Gateway-level forwarding can introduce DMARC interoperability issues if the Gateway is configured to rewrite the message into alternate recipient domains. For example, an acquisition may lead an acquiring company to decide to decommission the acquired company's domains by rewriting messages to use the domain of the acquiring company. Since the RFC5322.To header field is usually DKIM-signed, this kind of rewriting will invalidate such DKIM signatures.

3.2.5. Boundary Filters

To enforce security boundaries, organizations can subject messages to analysis for

conformance with their safety policies. A filter might alter the content to render it safe, such as by removing or otherwise altering content deemed unacceptable.

Boundary Filters share the same DMARC interoperability issues as ReSenders.

Issues may arise with SPF and DKIM evaluation if performed after filter modifications.

Examples of Boundary Filters include:

- Malware scanning: To protect readers and its reputation, an MTA that transfers a message may remove content believed to be harmful from messages, reformulate content to canonical formats in order to make them more trustworthy or easier to scan, and/or add text in the body to indicate the message has been scanned. Any such modifications would invalidate a DKIM signature.
- Spam filtering: To protect reputation and assist other MTAs, an MTA may modify a message to indicate its decision that the message is likely to be unwanted, and/or add text in the body to indicate that such filtering has been done.
- Other text additions: An MTA may add an organizational disclaimer or advertisement, for instance.
- URL alteration: Some systems will rewrite or alter embedded URLs as a way to control the potential threat from malware.
- Secondary MX services: The secondary MX for an organization may be external to the normal mail processing for the organization, and queue and forward to the primary when it becomes available. This will not invalidate DKIM but will prevent the primary from validating SPF normally. In this case, however, it is inappropriate for a primary MX server to perform an SPF check against its own secondaries. Rather, the secondary MX should perform this function and employ some trusted mechanism to communicate the results of the SPF, DKIM, and DMARC evaluation(s) to the primary MX server.

3.3. Combinations

Indirect email flows can be combined. For example, a university student may subscribe to a mailing list (using his university email address) while this university email address is configured to forward all emails to a freemail or a post-education corporate account provider where a more permanent email address for this student exists.

Within an organization the message may pass through various MTAs [mta], each of which performs a different function (authentication, filtering, distribution, etc.)

4. Possible Mitigations of Interoperability Issues

Solutions to interoperability issues between DMARC and indirect email flows vary widely in their scope and implications. They range from improvements to underlying processing, such as proper handling of multiple DKIM signatures, to more radical changes to the messaging architecture. This section describes possible ways to address interoperability issues. Note that these particular mechanisms may not be considered "best practices" and may, in some cases, violate various conventions or expectations.

Receivers sometimes need to deliver email messages that do not conform to any standard or protocol, but are otherwise desired by end users. Mitigating the impact of DMARC on

indirect email flows is especially important to receivers that operate services where ease of use and compatibility with existing email flows is a priority.

DMARC provides a mechanism (local policy) for receivers to make decisions about identity alignment acceptability based on information outside DMARC and communicate those decisions as "overrides" to the sender. This facility can be used to ease some interoperability issues, although care is needed to ensure that this does not create loopholes for abuse.

To further complicate the usage of mitigations, mitigation may not be desired if the email in question is of a certain category of high value or high risk (security-related) transactional messages (dealing with financial transactions or medical records, for example). In these cases, mitigating the impact of DMARC due to indirect email flows may not be desirable (counterproductive or allowing for abuse).

As a final note, mail systems are diverse and widely deployed. Systems of various ages and capabilities are expected to preserve interoperability with the rest of the SMTP ecosystem. For instance, Qmail is still used, although the base code has not been updated since 1998. ezmlm, a once popular mailing list manager, is still deployed but has not been updated since 1997, although a new version, ezmlm-idx exists. Old versions of other open and closed source MTAs are still commonly in operation. When dealing with aging or unsupported systems, some solutions may be time-consuming and/or disruptive to implement.

4.1. Mitigations in Current Use

Because DMARC is already widely deployed, many operators already have mitigations in use. These mitigations vary in their effectiveness and side effects, but have the advantage that they are currently available.

4.1.1. Mitigations for Senders

4.1.1.1. Identifier Alignment

- MTAs handling multiple domains may choose to change RFC5321.MailFrom to align with RFC5322.From to improve SPF usability for DMARC.
- MTAs handling multiple domains may also choose to align RFC5321.HELO/.EHLO to RFC5322.From, particularly when sending notification messages. Dynamically adjusting the RFC5321.HELO/.EHLO based on the RFC5322.From may not be possible for some MTA software.
- MTAs may choose to DKIM-sign notification messages with an aligned domain to allow a DKIM-based DMARC pass.
- MTAs sending email on behalf of multiple domains may require Domain Owners to provide DKIM keys to use DKIM to avoid SPF validation issues, given the requirement for DMARC alignment with the RFC5322.From header field. Managing DKIM keys with a third party has security risks that should be carefully managed (see also [RFC6376] section 8). Methods involving CNAMEs and/or subdomains may alleviate some risks.
- Senders who are sending on behalf of users in other Administrative Domains may choose to use an RFC5322.From under the sender's control. The new From can be either a forwarding address in a domain controlled by the Sender, or a placeholder

address, with the original user's address in an RFC5322.Reply-to header field. However, performing this modification may cause the recipient's MUA to deviate from customary behavior.
- When implementing "forward-to-friend" functionality, one approach to avoid DMARC failures is to pass a well-formed message to the user's MUA so that it may fill in an appropriate identity and submit through its own MSA.
- Senders can use domains with distinct DMARC policies for email sent directly and email known to use indirect mail flows. However, for most well-known brands, all active domains are likely to be targeted equally by abusers.

4.1.1.2. Message Modification

- Senders can maximize survivability of DKIM signatures by limiting the header fields they sign and using relaxed canonicalization. Using the DKIM length tag to allow appended signatures is discouraged due to the security risk created by allowing arbitrary content to be appended to legitimate email.
- Senders can also maximize survivability by starting with RFC-compliant headers and common body formats.
- In order to minimize transport-based conversions, Senders can convert messages to a lowest denominator MIME content-transfer encoding such as quoted-printable or base64 before signing ([RFC6376] Section 5.3).

4.1.2. Mitigations for Receivers

4.1.2.1. Identifier Alignment

- Receivers should update DKIM handling libraries to ensure that they process all valid DKIM signatures and check each signature for alignment.

4.1.2.2. Policy Override

- Receivers can amalgamate data from their user base to create lists of forwarders and use such lists to inform DMARC local policy overrides. This process may be easier for large receivers where data and resources to create such lists are more readily available than at smaller sites where the recipient footprint and other resources may be scarce.

4.1.3. Mitigations for ReSenders

4.1.3.1. Changes to the RFC5322.From

Many ReSender issues can be avoided by using an RFC5322.From header field under the ReSender's control, instead of the initial RFC5322.From. This will correct identifier alignment issues and allow arbitrary message modification as long as the ReSender signs the message with an aligned domain signature. When ReSenders change the RFC5322.From, it is desirable to preserve the information about the original initiator of the message.

A first option is to use the Original-From [RFC5703] (or X-Original-From) header field for

this purpose in various contexts (X- header field names are discouraged by [RFC6648]). However, handling of Original-From (or X-Original-From) is not defined anywhere. It is not currently used consistently or displayed to the user, and in any situation where it is used, it is a new unauthenticated identifier available for exploitation unless included within the scope of the new DKIM signature(s).

Another option for ReSenders is to rewrite the RFC5322.From header field address to a locally controlled address which will be forwarded back to the original sender (subject to its own ReSender forwarding mitigations!).

4.1.3.2. Avoiding Message Modification

- Forwarders can choose to add email header fields instead of modifying existing headers or bodies, for instance to indicate a message may be spam.
- Forwarders can minimize the circumstances in which they choose to fix messages, preferring to preserve non-compliant headers to creating DKIM failures.
- Forwarders can choose to reject messages with suspect or harmful content instead of modifying them.

4.1.3.3. Mailing Lists

[RFC6377] provides some guidance on using DKIM with Mailing lists. The following mitigation techniques can be used to ease interoperability issues with DMARC and Mailing lists:

- Configuring the Mailing List Manager (MLM) to alter the RFC5322.From header field to use the domain of the MLM is a mitigation policy that is now present in several different Mailing List software distributions. Since most list subscribers prefer to know the identity of the author of the original message, typically this information may be provided in the display name part of the RFC5322.From header field. This display name needs to be carefully crafted so as to not collide with the original display name of the author, nor contain something that looks like an email address or domain name. These modifications may to some extent defeat the purpose of DMARC itself. It may make it difficult to ensure that users of all email clients can easily reply to the author, the list, or all using the email client features provided for that purpose. Use of RFC5322.Reply-To header field can alleviate this problem depending on whether the mailing list is configured to reply-to-list, reply-to-author or reply-to-fixed-address, however it is important to note that this header field can take multiple email addresses. When altering the RFC5322.From there are three possibilities:
    1. change it to put the mailing list email address,
    2. change it to a locally-defined address which will be forwarded back to the original sender, or
    3. "break" the address by modifying the domain to a non-existent domain (such as by adding a suffix like ".invalid".)

  The latter modification may create issues because it is an invalid domain name, and some MTAs may pay particular attention to the validity of email addresses in RFC5322.From and the reputation of the domains present there.

- Configuring the MLM to "wrap" the message in a MIME message/rfc822 part and to

send as the Mailing List email address. Many email clients (as of the publication of this document), especially mobile clients, have difficulty reading such messages and this is not expected to change soon.
- Configuring the MLM to not modify the message so that the DKIM signature remains valid. Some Mailing Lists are set up this way and require few additional changes to ensure the DKIM signature is preserved. Moving lists that currently modify mail to a policy like this may be too much of a change for the members of such lists.
- Rejecting posts or membership requests from domains with a DMARC policy other than "p=none". However members or potential members of such Mailing Lists may complain of unfair exclusion.
- To alleviate unsubscribes to the Mailing List due to the messages bouncing because of DMARC, the MLM needs to not act on notification messages due to Message Authentication issues. [RFC3463] specifies Enhanced Mail System Status Codes which help differentiate between various failure conditions. Correctly interpreting Extended SMTP error messages is useful in this case. In particular, extended status codes for SPF and DKIM causes are defined in [RFC7372] and DMARC-related failure indications are discussed in DMARC [RFC7489] section 10.3.

All these techniques may provide some specific challenges to MUAs and different operational usages for end users (like rewriting filters to sort emails in folders). There will be some time before all implications are understood and accommodated.

4.2. Proposed and In-Progress Mitigations

The following mitigations are based on Internet Drafts (I-Ds) which are still in process. They are described here to offer exploratory path for solutions. These solutions should not be used in a production environment. Because of the transient nature of I-Ds, specific citations are not included because a number of them will inevitably become obsolete and those which gain consensus in the community will become RFCs and should be discovered as such.

- Third-party authorization schemes provide ways to extend identifier alignment under control of the domain owner.
- Ways to canonicalize messages that transit mailing lists so that their alterations can be isolated from the original signed content.
- Mechanisms to record message transformations applied at each hop so they can be reversed and the original signed content recovered.
- "Conditional" DKIM signatures, whereby the author domain indicates its signature is only good if accompanied by a signature from an expected downstream relay.
- Mechanisms to extend Authentication-Results [RFC7601] to multiple hops, creating a provable chain of custody as well as a view of message authentication results at each handling step.

4.2.1. Getting More Radical: Requiring New Communication Paths Between MUAs

In practice a number of operators are using strict alignment mode in DMARC in order to avoid receiving new and innovative forms of unwanted and unauthentic email through systems purporting to be mailing list handlers. The receiving ADMD has no knowledge of

which lists the user has subscribed to and which they have not. One avenue of exploration would be for the user to authorize mailing lists as proxies for authentication, at which point the receiving ADMD would be vesting some trust in the mailing list service. The creators of DKIM foresaw precisely this possibility at the time by not tightly binding any semantics to the RFC5322.From header field. Some experimental work has taken place in this area, as mentioned above. Additional work might examine a new communication path to the user to authorize some form of transitive trust.

5. IANA Considerations

This document contains no actions for IANA. [RFC Editor: Please delete this section prior to publication.]

6. Security Considerations

This document is an analysis of DMARC's impact on indirect email flows. It describes the possibility of accidental denial-of-service that can be created by rejections of messages by DMARC-aware Mail Receivers.

Section 4.1.1.1 discusses the importance of appropriate DKIM key management vis-a-vis third-party email senders.

Section 4.1.3.3 warns that rewriting the RFC5322.From header field to create an artificial domain name should not be done with any domain.

7. Acknowledgments

Miles Fidelman, John Levine, David Crocker, Stephen J. Turnbull, Rolf E. Sonneveld, Tim Draegen, and Franck Martin contributed to the IETF DMARC Working Group's wiki page listing all known interoperability issues with DMARC and indirect email flows.

Tim Draegen created the first draft of this document from these contributions and by hamfistedly mapping contributions into the language of [RFC5598].

8. References

8.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996.

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, DOI 10.17487/RFC3463, January 2003.

[RFC5228] Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language", RFC 5228, DOI 10.17487/RFC5228, January 2008.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008.

[RFC5322] Resnick, P., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009.

[RFC5703] Hansen, T. and C. Daboo, "Sieve Email Filtering: MIME Part Tests, Iteration, Extraction, Replacement, and Enclosure", RFC 5703, DOI 10.17487/RFC5703, October 2009.

[RFC6376] Crocker, D., Hansen, T. and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011.

[RFC6377] Kucherawy, M., "DomainKeys Identified Mail (DKIM) and Mailing Lists", BCP 167, RFC 6377, DOI 10.17487/RFC6377, September 2011.

[RFC6648] Saint-Andre, P., Crocker, D. and M. Nottingham, "Deprecating the "X-" Prefix and Similar Constructs in Application Protocols", BCP 178, RFC 6648, DOI 10.17487/RFC6648, June 2012.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014.

[RFC7372] Kucherawy, M., "Email Authentication Status Codes", RFC 7372, DOI 10.17487/RFC7372, September 2014.

8.2. Informative References

[RFC7489] Kucherawy, M. and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015.

[RFC7601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7601, DOI 10.17487/RFC7601, August 2015.

Appendix A. Appendix A - Example SPF Bounce

This example illustrates a notification message "bounce".

A.1. Initial Message

Here is the message as it exits the Origin MTA (segv.d1.example):

```
Return-Path: <jqd@d1.example>
Received: from [10.10.10.131] (w-x-y-z.dsl.static.isp.com [w.x.y.z])
    (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
    s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
     Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijrvQw
     bv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4Gd3TRJl
     gotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: no-recipient@dmarc.org
Subject: Example 1
```

```
Hey gang,
This is a test message.
--J.
```

A.2. Notification message

When dmarc.org rejects the message without a DKIM signature, it specifies the RFC5321.HELO/.EHLO domain as dmarc.org.local which has no SPF record. dmarc.org has a reject policy in place for such non-passing cases. Since there is no DKIM signature on the notification message, the failed SPF lookup results in a dmarc=fail and d1.example could be expected to discard the notification message itself:

```
Return-Path: <>
Received: from dmarc.org.local (mail.dmarc.org. [192.0.2.1])
   by mx.d1.example with ESMTPS id Lkm25302jJR5
   for <jqd@d1.example>
   (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
   Thu, 14 Jan 2015 15:00:24 -0800 (PST)
Authentication-Results: mx.d1.example;
   spf=none (d1.example: dmarc.org.local does not designate
   permitted sender hosts) smtp.mail=;
   dmarc=fail (p=REJECT dis=NONE) header.from=dmarc.org
MIME-Version: 1.0
Received: from segv.d1.example (segv.d1.example [198.51.100.1])
 by 192.0.2.2 with SMTP id u67mr102828634qge33; Thu,
 14 Jan 2015 15:00:24 -0800 (PST)
From: Mail Delivery Subsystem <mailer-daemon@dmarc.org>
To: jqd@d1.example
Subject: Delivery Status Notification (Failure)
Message-ID: <001a11c16e6a9ead220528df294a@dmarc.org>
Date: Thu, 14 Jan 2016 23:00:24 +0000
Content-Type: text/plain; charset=UTF-8

This is an automatically generated Delivery Status Notification

Delivery to the following recipient failed permanently:

     no-recipient@dmarc.org

Technical details of permanent failure:
Your message was rejected by the server for the recipient domain
  dmarc.org by mail.dmarc.org [192.0.2.1].

The error that the other server returned was:
550 5.1.1 <no-recipient@dmarc.org>... User unknown

----- Original message -----
Return-Path: <jqd@d1.example>
Received: from [203.252.0.131] (131-0-252-203-dsl.static.example.com
    [203.252.0.131]) (authenticated bits=0)
    by segv.d1.example with ESMTP id t0FN4a8O084569;
    Thu, 14 Jan 2015 15:00:01 -0800 (PST)
    (envelope-from jqd@d1.example)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=d1.example;
    s=20130426; t=1421363082;
    bh=EoJqaaRvhrngQxmQ3VnRIIMRBgecuKf1pdkxtfGyWaU=;
    h=Message-ID:Date:From:MIME-Version:To:CC:Subject:Content-Type:
     Content-Transfer-Encoding;
    b=HxsvPubDE+R96v9dM9Y7V3dJUXvajd6rvF5ec5BPe/vpVBRJnD4I2weEIyYijrvQw
```

```
     bv9uUA1t94kMN0Q+haFo6hiQPnkuDxku5+oxyZWOqtNH7CTMgcBWWTp4QD4Gd3TRJl
     gotsX4RkbNcUhlfnoQ0p+CywWjieI8aR6eof6WDQ=
Message-ID: <54B84785.1060301@d1.example>
Date: Thu, 14 Jan 2015 15:00:01 -0800
From: John Q Doe <jqd@d1.example>
To: no-recipient@dmarc.org
Subject: Example 1

Hey gang,
This is a test message.
--J.
```

Authors' Addresses

Franck Martin (editor)
LinkedIn
Mountain View, CA
USA
EMail: fmartin@linkedin.com

Eliot Lear (editor)
Cisco Systems GmbH
Richtistrasse 7
Wallisellen, ZH CH-8304
Switzerland
Phone: +41 44 878 9200
EMail: lear@cisco.com

Tim Draegen (editor)
dmarcian, inc.
PO Box 1007
Brevard, NC 28712
USA
EMail: tim@dmarcian.com

Elizabeth Zwicky (editor)
Yahoo
Sunnyvale, CA
USA
EMail: zwicky@yahoo-inc.com

Kurt Andersen (editor)
LinkedIn
2029 Stierlin Court
Mt. View, CA 94043
USA
EMail: kandersen@linkedin.com