dmarc
Internet-Draft
Intended status: Experimental
Expires: December 9, 2015

D. Otis
Trend Micro

June 7, 2015

DMARC Escape
draft-otis-dmarc-escape-03

Abstract

DMARC assumes the From header field has the combined role of Author and Sender or that it shares the same domain as that of the Sender. Message delivery becomes unreliable and the Author role may be supplanted as services adapt to DMARC's incompatible policies affecting otherwise valid and well formed messages. This document recommends two methods to allow DMARC to be compatible with RFC5322.

Requirements Language

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 [RFC2119].

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 9, 2015.

Copyright Notice

Table of Contents

1. Introduction

Services that depend on email notification experience customer attrition when notifications become phishing targets. DMARC [RFC7489] leveraged either SPF or DKIM records to request message Reject or Quarantine handling when From header field domains do not align with either of these records. From header fields also having the role of Sender occurs with transactional notifications. However when the From header field does not play the role of Sender and does not share the same domain as the Sender header field, a different alignment strategy is needed to ensure delivery. Section 10.5 of [RFC7489] offers feeble advice by stating although mediator transformations may conform with standards, Reject or Quarantine handling may not be avoidable.

Large Email Service Providers (ESPs) are able to manage their service in a manner not tolerated with smaller providers. Many large ESPs ignore abuse reports indicating compromised or abused user accounts or even message security being exploited. They are in a class best described as Too Big to Fail. DMARC permits these ESPs to export managerial roles onto receivers who must then cope with disrupted services. Both SPF and DKIM favor these ESPs by being referenced from domains not actually managing the sending of messages. These authorization mechanisms leave others to suffer the repercussions caused by unbeknownst access.

Email reputation often use identities imposing little assessment overhead, such as source IP addresses. Most providers rate limit users, but DKIM's replay-ability leaves DKIM identifiers vulnerable to rate-limiting abuse. Mailing-lists are able to dynamically confirm source identities with confirmation links, but since DKIM signatures easily bypass rate limiting this does not bode well for Too Big to Fail domains. Currently, mailing-lists either refuse or mung email address domains that assert a restrictive DMARC policy. Establishing restrictive confirmations "as-if" DMARC had been applied may not see rapid adoption because DMARC lacks provisions to assert a policy suitable for third-party message sourcing on behalf of the general public, message transformation, or message rerouting. Efforts at handling messages based only on the Author role rather than the Sender when present is at the heart of the problem.

Only the Sender role can establish a trustworthy message source and ensure domain alignment with SPF or DKIM records, not the Author. If DMARC had a provision for Sender header field alignment, its confirmation would also better enable effective exclusion of known bad or inclusion of known good domains by MTAs or MUAs. Controlling abuse while causing limited collateral blocking requires identifying actual sources. Permitting alignment with the Sender header field

would not benefit those seeking to protect only email notifications from being phished where an assumption of From header alignment permits ignoring the Sender header field.

Unfortunately this simplification can not accommodate normal email exchange in many cases. Such simplification ignores the identity of the Sender, relationships with the From header field identity, and even whether the identity of the Sender is in a likely displayed header field. Rather than obfuscating authorizations with the use of DKIM linked DKIM signature fragments to authorized a subsequent domain.

Allowing and displaying Sender alignment in MUAs is readily available for normal public user email offered on a free basis or bundled with broadband services. Such provisions would allow DMARC to be more compliant with [RFC5322] and less likely to disrupt messages undergoing mediator transformations or originating from different verified domains. Such a provision would also better ensure the identity of Author remains intelligible and carried in predictable locations.

SPF authorizes outbound IP addresses used by domains to send mail. Until DMARC, SPF largely only squelched Delivery Status Notifications (DSNs) emitted from spoofed sources and DKIM never required domain alignment with From header fields. Now DMARC attempts to exclude messages where either DKIM or SPF records do not align with the From header field domains. DMARC lacks any fallback strategy when DMARC domains allow users to interact with mediators unable to retain compliance with DMARC. DMARC refuses to adopt assertions to indicate a policy that allows alignment with Sender header fields on the basis few recipients see these header fields and insist this will lead to increased phishing.

In reaction to incompatible limitations imposed by a few domains handling public email, some advocate use of [I-D.levine-dkim-conditional]. This proposes a new DKIM signature in the hope ESPs disrupting standards compliant messages with restrictive DMARC policy will instead use this mechanism to delegate their signing to third-party domains listed within the signature's header field. This new DKIM signature may require some selected header fields be retained unaltered while allowing the entire message body to change. A strategy that creates interesting situations when the header fields selected by this new DKIM signature does not coincide with those signed by the third-party DKIM signature designated to forward altered messages.

DKIM is unable to ensure where a signed message fragment originates and is unable to constrain overall message volume or an associated

number of recipients. While permitting third-parties to sign a different domain's From header field, the retained header fields represent those that DMARC advocates claim will not prevent phishing. Especially retention of never seen Message-IDs or Date header fields where any asserted expiry must still allow reasonable intervals for delivery, especially for moderated lists. Any replay window will allow subscribed malefactors a means to side step normal rate limits when acceptance is based on DKIM signatures while ignoring other source identifiers that forms the general simplified basis for DMARC.

Selection of message destinations to receive a new DKIM delegation signature represents similar vetting as required of [I-D.otis-tpa-label]. TPA-Label has an advantage of being able to mitigate actual detected sources of abuse. An effort to deploy TPA-Label can be greatly reduced for customers of large ESPs by having DMARC records reference a consolidated and centrally managed TPA-Label zone. Establishing restrictive source identifier confirmations "as-if" DMARC will be a struggle to adopt due to the lack of benefit alignment.

ESPs unwilling to accept DMARC alignment with Sender header fields as a fallback scheme seem equally unlikely to include a new DKIM signature dynamically delegating a proxy signer for their domain. Especially since a mailing-list is unlikely to reject messages a DMARC domain may consider egregious or that use weak confirmation techniques. A scheme that allows any such message to be replicated without limit within whatever expiry time adopted. Even the mailing-list may not see all header fields a malefactor might employ in their campaign.

Some also advocate use of [I-D.kucherawy-dkim-transform] to introduce several encapsulation schemes where unverifiable versions are conveyed together with a portion verified by a DKIM signature. In effect, this offers recipients confusing information in a form most are likely to find unpleasant, while increasing message overhead and weakening desired protections where malware might be partially encoded and then reconstructed by users. Most mobile devices offering the least flexibility already support highly visible S/MIME methods.

Users naturally expect an ability to use email services gainfully employed for decades. Instead, due to some ESPs making misleading alignment assertions, users may encounter these service's messages either being rejected or quarantined. These users may ironically find the identity of the Author difficult to ascertain when services are forced to abandon the role of the From header field as a practical means to ensure delivery. In addition, DMARC's use of DKIM or SPF means malefactors only need an ability to exploit either

scheme. An unfortunate progression making email less reliable and identifying the Author less certain.

As DMARC becomes more broadly deployed, how will improved SMTP security via opportunistic DANE TLS [I-D.ietf-dane-smtp-with-dane] be introduced? SMTP with DANE should soon offer a secure global host identity scheme. DNSSEC/DANE overcomes security weaknesses found in both routing and message exchange. While some claim DNSSEC/DANE is not practical they also misrepresent weaker methods based on IP address authorization or signed message fragments as representing domain authentication. IP address based authorization or potentially malformed message fragments can not safely verify the binding of a domain with that of a message. DMARC even offers malefactors feedback that can enhance the exploitation effectiveness or leak relationship information that can be used to facilitate deceptions. Misleading use of the term "authentication" which conflicts with [RFC3552] and [RFC4949] occurs with [RFC7001] and [RFC7489].

2. Policy Suitable for Non-transactional Public Email

DMARC Section 6.7 of [RFC7489] recommends Mail Receivers make a best effort not to increase the likelihood of accepting abusive mail when not complying with a Domain Owner's "reject" request. Reject request being applied against normal public email exchange is not compatible with [RFC5322] which proves highly disruptive.

Such efforts could be declared as checking the DMARC policy of the Sender header field domain or considering multiple From identities and treating the list as <First> on behalf of <Second(s)> as-if the First identity represents the identity of the Sender header field. A "p:" Requested Mail Receiver policy may include "public" where alignment requirements may include the domain of the first listed From identity or that of the Sender header field where a check failure results in a Quarantine status. The "public" provision also allows a simple override mechanism for domains offering inappropriate "reject" for otherwise disruptive domains determined to be handling public email where From header field alignment can not be assured. Such an override is preferable to diverted placement of valid and legitimate messages being rejected or placed into quarantine folders.

It seems a best effort should include quarantine handling when:

1) sender can not be confirmed

2) identity of sender not likely apparent

The identity of the sender should be confirm by recognized methods and be contained in the first identity in the From header field or the only identity in the Sender header field. Authentication-Results header fields [RFC7001] will not make identities apparent to recipients.

This represents improved protections over the typical handling of messages from domains making inaccurate assertions of their message alignments. An override entails replacing "reject" with "public" for a few often large domains to avoid disruptions.

This mode of operation does not demand the cooperation of the larger domains. Often these domains already are making exceptions for their internal services.

3. Domain Authorization Issues

A domain referenced by SPF [RFC7208] or a domain confirmed in a DKIM [RFC6376] signature has not posed a problem since seldom was acceptance based on From header field Domain Alignment with a domain used by these two methods. However, when acceptance is based on From header field alignment in the case of DMARC [RFC7489] which may use either SPF or DKIM related domains, this may disrupt many Third-Party Services where the expected reaction to this problem has the effect of deprecating the use of the From header field retaining the role of Author. The disruption becomes egregious when messages from the domain's own users are rejected based on an erroneous level of the domain's asserted alignment practices. At the strictest alignment level, erroneous assertions not only disrupt messages from their users, it also affects subscriptions or services for other users of affected third-party services.

SPF normally provides a form of authorization by listing IP addresses of authorized outbound servers. In many cases, these servers represent a shared resource used by perhaps thousands of domains. SPF is unable to verify an IP address represents the actions of a claimed domain which does not meet the definition of "$ authentication" in [RFC4949].

DKIM intended to establish increased levels of trust based upon verified DKIM signatures controlling acceptance and what a user sees within the From header field. But DKIM failed to include in its header stack processing a scheme to actively guard against pre-pended header fields. This would ensure acceptance is not based on verified DKIM signatures that fail to prevent header field spoofing. Even now, this weakness allows malefactors to exploit DKIM signature acceptance established by large ESPs to spoof ANY other domain, even

when prohibited within the Signer's network.

DKIM signatures are verified by a process that MUST examine the entire header field stack and yet needs some prior unreported and unknown message structure verification. Inclusion of this undefined process has proven problematic in preventing header spoofing. It took several years for one of the largest service providers to notice this oversight long after arguments were made about this risk. Ignoring essential header field stack validation that MUST occur represents an oversight in the DKIM deployment specifications that at one time had been partially addressed by the earlier DMARC specifications. It seems even this validation was removed by what might be described as a misguided insistence such processing is to remain the responsibility of the transport.

Section 3.3 of [RFC5321] clearly indicates messages SHOULD NOT be rejected based on perceived defects in [RFC5322] message structure. Section 7.1 of [RFC5321] also warns against preventing spoofing within the SMTP transport and suggests much safer PGP or S/MIME, both of which benefit by deployment of DANE. DMARC was developed to curtail phishing attempts leading to user attrition with high volume transactional services. Unfortunately, DMARC is being (ab)used to lessen phishing attempts related to general user accounts where there seems little interest at finding a solution for the problems this creates.

4. Escaping DMARC Disruptions

Conditionally permit Sender header field alignment: For domains handling normal user email, a special DMARC policy assertion "public" requests policy suitable for public email users which recognizes alignment with Sender header fields when present or the first identity in the From header field when Sender is not present. This makes an assumption users employ Mail User Agents that display the identity contained in the Sender header field when used as a basis for acceptance.

Define a replacement Author header: A new "IM-From" header field re-establishes the Author role for RFC5322.From domains affected by DMARC. This header permits re-locating the Author role to a new header to establish the integrity of third-party services. Establishing a new header prevents confusion caused by unknown alternatives, such as Reply-To, or Original-From, or indirectly through the use of Original Authentication Results header (OAR). Munging Reply-To or From header fields removes information essential for establishing side discussions rather than having all

conversations on the list. Not all conversations are suitable for the entire forum.

Third-Party Authorization: A different domain is specifically excluded from actions caused by non-alignment when authorized by the DMARC domain using [I-D.otis-tpa-label]. DMARC could make an assertion of "sam=tpa; and tpa=third-party-authority.example.com;" when the DMARC domain offers the Specific Advisory Methods "sam=" tag indicating the third-party advisory methods supported. The "tpa=" tag can also indicate the domain location where third-party-authorization hashes have been consolidated with an assumed prefix of "_smtp._tpa.<tpa-domain>".

A few large domains have had a high percentage of user accounts compromised. These events gave malefactors access to prior private exchanges and contact lists. Even after accounts were reclaimed, malefactors continue sending convincing spoofed messages from other sources. To mitigate harm, some domains have asserted DMARC Alignment policies similar to those used by domains that only emit transactional messaging where a prior DMARC recommendation of restricted use was normally heeded. In addition, some domains also recommended "reject" rather than "quarantine" as a misalignment response. In conjunction with misleading DMARC alignment assertions, rejection becomes a highly disruptive choice.

Currently, the least disruptive adjustment made by receivers faced with Third-Party services used by a RFC5322.From domain is to override their policy of "reject" with "quarantine" to allow delivery of the message causing users to search through their "quarantine" folder for otherwise lost messages. Alternatively, the From header field may replace the Author role with that of the Sender by asserting a policy of "public" intended to assert the strongest protection suitable for a domain supporting email being used by the general public which allows alignment to occur with Sender header fields and multiple identities within the From header field. Some have suggested the From header field contents be retained in the Reply-To header. This document offers an alternative to the use of X-Original-From header field and that it be given the name IM-From header field that has additional semantics not available with the normal From header field. Use of IM-From header field claims the role of Author that has been lost due to DMARC.

It is unfair to place a large burden on receivers and expect them to remain cooperative. Prior to making alignment assertions likely to disrupt services handling legitimate messages, it is possible for

RFC5322.From domains to make assertions which allow compliance with normal email handling. When RFC5322.From domains proactively guard against disrupting legitimate messages, receivers are more likely to cooperate with their recommendations. When the asserted policies prove disruptive over time, DMARC should offer receivers reasonable overrides.

5. Handing DMARC Disruptions

Deterrents based upon reputation and/or path based scoring strategies that utilize a variety of originating header fields has proved ineffective. These header fields often remain invisible to recipients, and contain domains exploited for periods measured in hours to avoid any Whack-A-Mole like response. Even long term reputations have issues due to an intermix of messages from compromised accounts. Content filtering is unable to keep up with the polymorphic abuse. Few recipients will inspect the stack of message header fields, or be able to draw useful conclusions from a profusion of unfriendly information. As a result, many recipients deal with abuse by sorting messages into groups based on assumed sources found in a few originating header fields.

DMARC represents an open registry that offers domain specific guidance for DKIM/SPF alignment sending practices to determine whether messages should be delivered, quarantined, or refused. However, appropriate actions become unclear whenever Third-Party Services are involved. Although DMARC warns of a potential for disruption, the specific handling requested by DMARC is very limited. DMARC expects receivers to devise their own special handling to mitigate disruptions that DMARC assertions might cause for legitimate messaging. This is unfortunate, since the necessary feedback is given to the DMARC asserting domain and not to the cooperating receivers.

When a Third Party domain does not employ DKIM or SPF or does not include Authentication-Results header fields [RFC7001] or perhaps [I-D.kucherawy-original-authres] (OAR) or its "X-" version could allow authorizations to be exploited. For Third Party domains not applying DMARC but capture the OAR, past compliance with DMARC based on the OAR can be made a requirement for authorization.

While conceivably Domain Alignment might just rely on the content of the Original-Authentication-Results header, whether to trust this, or any other message content can not be based on the mere acceptance of the message alone. Whether false content even effects message acceptance would be difficult to determine. Only the DMARC asserting domain is able to make this type of determination based on their

knowledge of outbound messages and corrections needed based on DMARC feedback.

```
im-from = "IM-From:" (mailbox-list / address-list) CRLF

address = mailbox / group

group = display-name ":" [group-list] ";" [CFWS]

mailbox = name-addr / addr-spec

addr-spec = local-part "@" domain ["/" resourcepart]

name-addr = [display-name] angle-addr

angle-addr = [CFWS] "<" addr-spec ">" [CFWS]

group = display-name ":" [group-list] ";" [CFWS]

display-name = phrase

mailbox-list = (mailbox *("," mailbox))

address-list = (address *("," address))

group-list = mailbox-list / CFWS

mailbox-list = (mailbox *("," mailbox))
```

Use of the IM-From header group display name can be used to replace the use of list tags embedded in the Subject header field. Since this header is ignored by DMARC, it can also retain the identity of the Author. This field also permits the use of the resourcepart extension to support XMPP endpoints as defined in [RFC6122] and which is to be ignored otherwise.

5.1. Privacy Considerations

DMARC policy assertions are transitory so exclusion of users within a DMARC domain is never assured. Unless all valid Third-Party Domains have been authorized or allowed a suitable From header field alternative, personally identifiable information will be exchanged within the DMARC feedback. This feedback can unintentionally expose private exchanges made on behalf of the RFC5322.From domain's users. To the greatest extent possible, this feedback information should not be shared with other domains not offering the information. This feedback can even identify mailing-list subscribers that never sent any message to the list, or invoices made on behalf of an

accountant's client.

5.2. Security Considerations

This draft extends Domain Alignment validation practices that depend on DKIM [RFC6376] or SPF [RFC7208]. Most related security matters are discussed in those specifications. Additional considerations are also included in [RFC6377]. Some receivers mistakenly bypass validation of the [RFC5322] header fields because a signature from a Trusted Domain had been confirmed as perhaps suggested in [RFC5863]. Validation of the header stack MUST NOT be omitted unless the message is not accepted for other reasons.

Services that depend only upon path authorizations might permit the RFC5322.From domain to be spoofed and obtain acceptance. During such events, the RFC5322.From domain might need to retract its authorization from the service. For this reason, path related validation based on IP addresses should only be used as a carefully monitored interim solution.

6. Acknowledgements

Terry Zink, J. Gomez, Hector Santos, John Levine, Stephen Turnbull

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", RFC 3552, July 2003.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

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

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC6122] Saint-Andre, P., ""Extensible Messaging and Presence Protocol (XMPP): Address Format"", RFC 6122, March 2011.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

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

[RFC7001] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7001, September 2013.

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

7.2. Informative References

[I-D.ietf-dane-smtp-with-dane]
Dukhovni, V. and W. Hardaker, "SMTP security via opportunistic DANE TLS", draft-ietf-dane-smtp-with-dane-19 (work in progress), May 2015.

[I-D.kucherawy-dkim-transform]
Kucherawy, M., "Recognized Transformations of Messages Bearing DomainKeys Identified Mail (DKIM) Signatures", draft-kucherawy-dkim-transform-00 (work in progress), April 2015.

[I-D.kucherawy-original-authres]
Chew, M. and M. Kucherawy, "Original-Authentication-Results Header Field", draft-kucherawy-original-authres-00 (work in progress), February 2012.

[I-D.levine-dkim-conditional]
Levine, J., "Mandatory Tags for DKIM Signatures", draft-levine-dkim-conditional-01 (work in progress), April 2015.

[I-D.otis-tpa-label]
Otis, D., "Third-Party Authorization Label",

draft-otis-tpa-label-07 (work in progress), April 2015.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC4686] Fenton, J., "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)", RFC 4686, September 2006.

[RFC4954] Siemborski, R. and A. Melnikov, "SMTP Service Extension for Authentication", RFC 4954, July 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5863] Hansen, T., Siegel, E., Hallam-Baker, P., and D. Crocker, "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations", RFC 5863, May 2010.

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

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

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

Appendix A. MUA conventions for displaying header fields

```
####
# Header field in OS X Apple Mail(tm).
####
Mail, Preferences, Viewing, Show message headers: custom,
  type the desired headers.

####
#  Header field display in Mozilla Thunderbird(tm).
```

```
   ####
   Mail, Preferences, Advanced, General tab, click Config Editor, Enter
   mail.compose.other.header and double click
   mail.compose.other.header entry and type the desired headers
   in the string dialog.

   ####
   # Sender header field in Microsoft Outlook(tm)
   ####
   Sender and From header field identities are combined as:
   From <Sender> on behalf of <From>

   ###
   # A large percentage of Web email can be annotated by
   # JavaScript as demonstrated by Iconix.com.
   ###
```

Author's Address

Douglas Otis
Trend Micro
10101 N. De Anza Blvd
Cupertino, CA 95014
USA

Phone: +1.408.257-1500
Email: doug_otis@trendmicro.com