DMARC verification without record definitions
draft-akagiri-dmarc-virtual-verification-01.txt

Abstract

While DMARC is a powerful architecture to protect email users from malicious email activities, its deployment is still a work in progress. To encourage further adoption of DMARC, in this draft we propose an incremental deployment procedure.

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 March 24, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
1. Introduction

Currently, there are several email sender validation technologies such as SPF and DKIM, which are independent from each other. There is also need for email verification frameworks to handle the email authentication results provided by those validation technologies in a unified manner. DMARC is one of the technologies that provides such a capability.

Although DMARC is an effective technology to protect email users from malicious activities such as phishing or malware, at this moment its deployment is a work in progress. A survey[ReturnPath] indicates that by the end of 2015, less than 30% of top global companies have published DMARC records. To validate incoming emails properly on the receiving MTA side, it is desirable that more domains publish DMARC records.

At the same time, the adoption of SPF and DKIM is widespread, and, especially for email receivers, it is valuable to utilize the validation results of those technologies. From the view point of email receivers, the main goals of adopting an email verification framework are:
1. To identify malicious emails and apply policies

2. To verify non-malicious emails as authorized

This draft focuses on the second goal.

In this draft, we propose a default verification for domains that do not declare DMARC resource records. This default verification is called "virtual verification(s)" in this draft. With virtual verifications, receivers are able to validate emails from domains not publishing DMARC records. This approach allows receiving MTAs to validate email senders by utilizing virtual DNS resource records populated with default values, and notify email users of the authenticity of email senders in a manner compatible with DMARC.

2. Terminology and Definitions

- virtual DMARC record: DMARC record virtually created to verify domains that do not publish DMARC records
- regular verification: DMARC RFC7489 verification
- virtual verification: verification leveraging virtual DMARC records to verify emails which would potentially be "dmarc=pass"

3. Overview

3.1. Problem Statement

As described in Section 1, currently the adoption rate of DMARC remains low on the email sender side. This means that operators of receiver MTAs have little incentive to introduce DMARC verifiers into their MTAs. DMARC needs implementation on both sender and receiver sides, i.e. email senders have to publish DMARC TXT records on their DNS servers, while email receivers have to enable DMARC verification on their MTAs. Thus, the deployment of DMARC is a chicken-and-egg problem between email senders and receivers.

There are situations where emails from domains that do not have DMARC records can be treated as "dmarc=pass". In [RFC7489], the conditions for adding "dmarc=none" to Authentication-Results are:

1. No DMARC records are defined for email sender domains.

2. DMARC records are defined with "p=none" and DMARC verification did not pass.
Out of the conditions above, on the first condition there should be plenty of emails which would potentially be marked as "dmarc=pass". Those emails are from domains that have valid SPF records or DKIM signatures and validated as authorized with SPF or DKIM, while RFC5322. From fields of the emails are aligned with SPF or DKIM identifiers.

<table>
<thead>
<tr>
<th></th>
<th>SPF or DKIM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Align</td>
</tr>
<tr>
<td>----------+--------+---------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>DMARC</td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td>+---+--------+---------+</td>
</tr>
<tr>
<td></td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>+----------------------------------</td>
</tr>
</tbody>
</table>

Figure 1: DMARC Authentication-Results

Figure 1 illustrates the relationship between verification conditions and Authentication-Results. There are three conditions where the Authentication-Results is marked as None via DMARC regular verification. The first one is the condition where there is a DMARC record with p tag set to 'none' on a sender domain and the domain is not aligned with the email RFC5322. From field (None(1) in Figure 1).

The other two conditions are where the sender domains do not declare DMARC records on their DNS servers. In the first case, None is set when DKIM or SPF passes and the identifier aligns but no DMARC records are defined on the sender domain (None(2)). In the second case, even if the valid DMARC domain is declared for the sender domain, regular DMARC verification will fail (None(3)). Regular DMARC verification treats None(2) and None(3) in Figure 1 as the same "None", but the authenticity of received emails is different in each case.

According to an analysis performed by Re:gumi with a Japanese ISP([RegumiDmarcAnalysys]), the proportion of domains which can be verified as legitimate by DMARC rises to 41.9% after including the domains which potentially can be treated as legitimate (None(2)).

In this draft, we propose to explicitly mark emails which are potentially "dmarc=pass", but are not marked as such via regular DMARC verification (None(2)), as "dmarc=pass". This approach is current practice in some email receiver MTAs.
3.2. DMARC verification without DMARC records.

Figure 2 is the state diagram of the DMARC virtual verification.

```
+----------+        +-----------+
| SPF Pass |        | DKIM Pass |
+----------+        +----------+
      v      v
+------------------------------------------+
| DMARC Record exists?                   |
+------------------------------------------+
      v      v No
+----------+        +----------+
|           |        |           |
| regular  |       | virtual  |
| +--------+       | +--------+       |
|           |       |           |
| results  |       | other than|
|           |       | pass +/-<++|
|           |       | none |
+----------+       +--------+
```

Figure 2: State Diagram

Email receivers SHOULD verify email senders using virtual DMARC records when receivers cannot find DMARC records published by the email senders. The regular DMARC verifier just sets Authentication-Results to "none" when the receiving MTA cannot find DMARC policy records for the sender domain. In contrast, when verifications of SPF or DKIM have passed, the virtual verification validates senders against virtual DMARC records populated with _default_ values. The _default_ values of virtual DMARC records are detailed in Section 4.

Virtual DMARC verification processes received emails in the same manner as the regular DMARC verifier does using those default values. The Authentication-Result field is set to "dmarc=pass" for email that passes virtual DMARC verification and to "dmarc=none" for email that does not.

Inserting "dmarc=pass" into Authentication-Results may cause controversy. From the point of view of email operators, it is desirable to differentiate between emails that pass virtual DMARC verifications and those that pass regular DMARC verification. However, for end users without enough expertise, simply utilizing "dmarc=pass" makes it easier to leverage the field.
4. The Virtual DMARC Record

When a email sender does not publish their DMARC record, the virtual DMARC verification validates the sender against a virtual DMARC record populated with pre-determined values. This record is referred to as "virtual DMARC record" in this draft.

The values in the virtual DMARC record are listed below (Table 1).

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Virtual DMARC Record Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>DMARC1</td>
</tr>
<tr>
<td>p</td>
<td>none</td>
</tr>
<tr>
<td>adkim</td>
<td>s(strict)</td>
</tr>
<tr>
<td>aspf</td>
<td>s(strict)</td>
</tr>
</tbody>
</table>

Table 1: Values for Virtual DMARC records

These values are determined so that reasonable verifications can be performed when the sender has not published their own DMARC records.

- **version(v): DMARC1**
  
  * To allow the DMARC verifier to process virtual DMARC records properly, the version tag must be set as 'DMARC1'.

- **policy(p): none**
  
  * Received emails must be delivered to email destinations unless the email sender has published a DMARC record and has set the policy in the record to "quarantine" or "reject" explicitly. Therefore, the policy(p) must be set to "none".

- **adkim, aspf: s(strict)**
  
  * The default alignment modes for DKIM and SPF are "s(strict)". An example would be when a hosting provider ("example.com") enables DKIM and publishes a DKIM resource record for a customer ("aaa.example.com"). In this case, if the DKIM alignment mode (adkim) in the virtual record is "r(relaxed)", another customer of the hosting provider ("bbb.example.com") can pretend to be the owner of "aaa.example.com". To prevent this, the alignment modes (adkim and aspf) must be "s(strict)"
in the virtual DMARC record, as opposed to the default value for the regular DMARC record.

5. Use cases

Figuring out whether an email is potentially "dmarc=pass" or not allows email system operators to evaluate the authenticity of the email sender domain. DMARC evaluates the RFC5322. From, while SPF evaluates the RFC5321. Mailfrom and DKIM verifies the signature of email senders. By combining this information, DMARC verification helps to establish domain authenticity which can be used as domain reputation or whitelisting of email senders.

Microsoft Office365 employs the same technique as one mentioned in this draft ([BestGuessPass]). They append "dmarc=bestguesspass" to the Authentication-Results to indicate the authenticity of received emails to receiving MUAs.

6. Security consideration

TBD

7. Privacy consideration

TBD

8. Discussion

- Currently, the virtual DMARC verification sets the Authentication-Result to "pass" when the virtual verification passes. Is it better to set the result value to "bestguesspass", as Microsoft does, or to another value different from "pass" in order to indicate that the "pass" is based on virtual verification?

- Values "ruf" and "rua" for virtual records need to be decided. There would be differing opinions regarding DMARC reports. One is the opinion that reports without explicitly published DMARC records are harmful, while another one is that without reports, virtual DMARC verification can not be called DMARC. Currently, we are siding with the first opinion in this draft.

- Name of the verification

9. Acknowledgements

The authors would like to thank engineers at the Japanese ISPs So-net, NIFTY, Biglobe and CNCI especially Mr. Koichi Abe, Mr. Daisuke
Kodama and Mr. Nickolay Boyadjiev, for their technical advice and data analysis.

10. Change Log

10.1. 01 revision

- Removed Roadmap section
- Added focus of this document to Introduction and Problem Statement
- Added Use cases section

11. References

11.1. Normative References


11.2. Informative References

[BestGuessPass]

[RegumiDmarcAnalysys]

[ReturnPath]

Authors’ Addresses

Genki Yasutaka
Rakuten, Inc.
Email: genki.yasutaka@rakuten.com

Takehito Akagiri
Regumi, Inc.
Email: akagiri@regumi.net

Masaki Kase
NIFTY Corporation
Email: kase.masaki@nifty.co.jp

Kouji Okada
Lepidum Co. Ltd.
Email: okd@lepidum.co.jp

Kaoru Maeda
Lepidum Co. Ltd.
Email: maeda@lepidum.co.jp