Network Working Group
Internet-Draft
Intended status: Experimental
Expires: March 26, 2021

S. Kitterman
fTLD Registry Services

September 22, 2020

DMARC (Domain-based Message Authentication, Reporting, and Conformance) Extension For PSDs (Public Suffix Domains)

draft-ietf-dmarc-psd-09

Abstract

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling. The design of DMARC presumes that domain names represent either nodes in the tree below which registrations occur, or nodes where registrations have occurred; it does not permit a domain name to have both of these properties simultaneously. Since its deployment in 2015, use of DMARC has shown a clear need for the ability to express policy for these domains as well.

Domains at which registrations can occur are referred to as Public Suffix Domains (PSDs). This document describes an extension to DMARC to enable DMARC functionality for PSDs.

This document also seeks to address implementations that consider a domain on a public Suffix list to be ineligible for DMARC enforcement.

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 https://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 26, 2021.

Table of Contents

1. Introduction

DMARC [RFC7489] provides a mechanism for publishing organizational policy information to email receivers. DMARC allows policy to be specified for both individual domains and for organizational domains and their sub-domains within a single organization. DMARC leverages public suffix lists to determine which domains are organizational domains. It presumes that public suffix list listed domains are not organizational domains and not subject to DMARC processing; domains are either organizational domains, sub-domains of organizational domains, or listed on a public suffix list. For domains listed in a public suffix list, i.e. TLDs and domains that exist between TLDs and organization level domains, policy can only be published for the exact domain. No method is available for these domains to express policy or receive feedback reporting for sub-domains. This missing method allows for the abuse of non-existent organizational-level domains and prevents identification of domain abuse in email.

As an example, imagine a country code TLD (ccTLD) which has public subdomains for government and commercial use (.gov.example and .com.example). Suppose there exists a registered domain "tax.gov.example" that is responsible for taxation in this imagined country. However, by exploiting the typically unauthenticated nature of email, there are regular malicious campaigns to impersonate this organization that use similar-looking ("cousin") domains such as "t4x.gov.example". These domains are not registered. Within the ".gov.example" public suffix, use of DMARC has been mandated, so "gov.example" publishes the following DMARC DNS record:

```
_dmarc.gov.example. IN TXT ( "v=DMARC1; p=reject; "
                             "rua=mailto:dmc@dmarc.svc.gov.example" )
```

This DMARC record provides policy and a reporting destination for mail sent from @gov.example. However, due to DMARC's current method of discovering and applying policy at the organizational domain level, the non-existent organizational domain of @t4x.gov.example does not and cannot fall under a DMARC policy.

Defensively registering all variants of "tax" is obviously not a scalable strategy. The intent of this specification, therefore, is to enhance the DMARC algorithm by enabling an agent receiving such a message to be able to determine that a relevant policy is present at "gov.example", which is precluded by the current DMARC algorithm.

This document provides a simple extension to DMARC [RFC7489] to allow operators of Public Suffix Domains (PSDs) to:

- Express policy at the level of the PSD that covers all organizational domains that do not explicitly publish DMARC records
- Extends the DMARC policy query functionality to detect and process such a policy
- Describes receiver feedback for such policies
- Provides controls to mitigate potential privacy considerations associated with this extension

This document also provides a new DMARC [RFC7489] tag to indicate requested handling policy for non-existent subdommains. This is provided specifically to support phased deployment of PSD DMARC, but is expected to be useful more generally. Undesired rejection risks for mail purporting to be from domains that do not exist are substantially lower than for those that do, so the operational risk of requesting harsh policy treatment (e.g. reject) is lower.

As an additional benefit, the PSD DMARC extension clarifies existing requirements. Based on the requirements of DMARC [RFC7489], DMARC should function above the organizational level for exact domain matches (i.e. if a DMARC record were published for 'example', then mail from example@example should be subject to DMARC processing). Testing had revealed that this is not consistently applied in different implementations.

There are two types of Public Suffix Operators (PSOs) for which this extension would be useful and appropriate:

- Branded PSDs (e.g., ".google"): These domains are effectively Organizational Domains as discussed in DMARC [RFC7489]. They control all subdomains of the tree. These are effectively private domains, but listed in the Public Suffix List. They are treated as Public for DMARC purposes. They require the same protections as DMARC Organizational Domains, but are currently unable to benefit from DMARC.
- Multi-organization PSDs that require DMARC usage (e.g., ".bank"): Because existing Organizational Domains using this PSD have their own DMARC policy, the applicability of this extension is for non-existent domains. The extension allows the brand protection benefits of DMARC to extend to the entire PSD, including cousin domains of registered organizations.

Due to the design of DMARC [RFC7489] and the nature of the Internet email architecture [RFC5598], there are interoperability issues associated with DMARC [RFC7489] deployment. These are discussed in Interoperability Issues between DMARC and Indirect Email Flows [RFC7960]. These issues are not typically applicable to PSDs, since they (e.g., the ".gov.example" used above) do not typically send mail.

2. Terminology and Definitions

This section defines terms used in the rest of the document.

2.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Public Suffix Domain (PSD)

The global Internet Domain Name System (DNS) is documented in numerous Requests for Comment (RFC). It defines a tree of names starting with root, ".", immediately below which are Top Level Domain names such as ".com" and ".us". The domain name structure consists of a tree of names, each of which is made of a sequence of words ("labels") separated by period characters. The root of the tree is simply called ".". The Internet community at large, through processes and policies external to this work, selects points in this tree at which to register domain names "owned" by independent organizations. Real-world examples are ".com", ".org", ".us", and ".gov.uk". Names at which such registrations occur are called Public Suffix Domains (PSDs), and a registration consists of a label selected by the registrant to which a desirable PSD is appended. For example, "ietf.org" is a registered domain name, and ".org" is its PSD.

2.3. Organizational Domain

The term Organizational Domains is defined in DMARC [RFC7489] Section 3.2.

2.4. Longest PSD

The longest PSD is the Organizational Domain with one label removed.

2.5. Public Suffix Operator (PSO)

A Public Suffix Operator is an organization which manages operations within a PSD, particularly the DNS records published for names at and under that domain name.

2.6. PSO Controlled Domain Names

PSO Controlled Domain Names are names in the DNS that are managed by a PSO and are not available for use as Organizational Domains. PSO Controlled Domain Names may have one (e.g., ".com") or more (e.g., ".co.uk") name components, depending on PSD policy.

2.7. Non-existent Domains

For DMARC purposes, a non-existent domain is a domain for which there is an NXDOMAIN or NODATA response for A, AAAA, and MX records. This is a broader definition than that in NXDOMAIN [RFC8020].

3. PSD DMARC Updates to DMARC Requirements

This document updates DMARC [RFC7489] as follows:

3.1. General Updates

References to "Domain Owners" also apply to PSOs.

3.2. Changes in Section 6.3 "General Record Format"

A new tag is added after "fo":

np: Requested Mail Receiver policy for non-existent subdomains (plain-text; OPTIONAL). Indicates the policy to be enacted by the Receiver at the request of the Domain Owner. It applies only to non-existent subdomains of the domain queried and not to either existing subdomains or the domain itself. Its syntax is identical to that of the "p" tag defined below. If the 'np' tag is absent, the policy specified by the "sp" tag (if the 'sp' tag is present) or the policy specified by the "p" tag, if the 'sp' tag is not present, MUST be applied for non-existent subdomains. Note that "np" will be ignored for DMARC records published on subdomains of Organizational Domains and PSDs due to the effect of the DMARC policy discovery mechanism described in DMARC [RFC7489] Section 6.6.3.

The following tag definitions from DMARC [RFC7489] are updated:

p: The sentence 'Policy applies to the domain queried and to subdomains, unless subdomain policy is explicitly described using the "sp" tag' is updated to read 'Policy applies to the domain queried and to subdomains, unless subdomain policy is explicitly described using the "sp" or "np" tags.'

sp: The sentence 'If absent, the policy specified by the "p" tag MUST be applied for subdomains' is updated to read 'If both the 'sp' tag is absent and the 'np' tag is either absent or not applicable, the policy specified by the "p" tag MUST be applied for subdomains.

3.3. Changes in Section 6.5 "Domain Owner Actions"

In addition to the DMARC domain owner actions, PSOs that require use of DMARC and participate in PSD DMARC ought to make that information available to receivers. This document is an experimental mechanism for doing so. See the [this document] experiment description (Appendix A).

3.4. Changes in Section 6.6.1 "Extract Author Domain"

Experience with DMARC has shown that some implementations short-circuit messages, bypassing DMARC policy application, when the domain name extracted by the receiver (from the RFC5322.From) is on the public suffix list used by the receiver. This negates the capability being created by this specification. Therefore, the following paragraph is appended to Section 6.6.1 of DMARC [RFC7489]:

Note that domain names that appear on a public suffix list are not exempt from DMARC policy application and reporting.

3.5. Changes in Section 6.6.3 "Policy Discovery"

A new step between step 3 and 4 is added:

3A. If the set is now empty and the longest PSD (Section 2.4) of the Organizational Domain is one that the receiver has determined is acceptable for PSD DMARC (discussed in the [this document] experiment description (Appendix A)), the Mail Receiver MUST query the DNS for a DMARC TXT record at the DNS domain matching the [this document] longest PSD (Section 2.4) in place of the RFC5322.From domain in the message (if different). A possibly empty set of records is returned.

As an example, for a message with the Organizational Domain of "example.compute.cloudcompany.com.example", the query for PSD DMARC would use "compute.cloudcompany.com.example" as the [this document]

longest PSD (Section 2.4). The receiver would check to see if that PSD is listed in the DMARC PSD Registry, and if so, perform the policy lookup at "_dmarc.compute.cloudcompany.com.example".

Note: Because the PSD policy query comes after the Organizational Domain policy query, PSD policy is not used for Organizational domains that have published a DMARC policy. Specifically, this is not a mechanism to provide feedback addresses (RUA/RUF) when an Organizational Domain has declined to do so.

3.6. Changes in Section 7 "DMARC Feedback"

Operational note for PSD DMARC: For PSOs, feedback for non-existent domains is desirable and useful, just as it is for org-level DMARC operators. See Section 4 of [this document] for discussion of Privacy Considerations for PSD DMARC.

4. Privacy Considerations

These privacy considerations are developed based on the requirements of [RFC6973]. Additionally, the Privacy Considerations of [RFC7489] apply to the mechanisms described by this document.

4.1. Feedback leakage

Providing feedback reporting to PSOs can, in some cases, cause information to leak out of an organization to the PSO. This leakage could potentially be utilized as part of a program of pervasive surveillance (See [RFC7624]). There are roughly three cases to consider:

- Single Organization PSDs (e.g., ".google"), RUA and RUF reports based on PSD DMARC have the potential to contain information about emails related to entities managed by the organization. Since both the PSO and the Organizational Domain owners are common, there is no additional privacy risk for either normal or non-existent Domain reporting due to PSD DMARC.

- Multi-organization PSDs that require DMARC usage (e.g., ".bank"): PSD DMARC based reports will only be generated for domains that do not publish a DMARC policy at the organizational or host level. For domains that do publish the required DMARC policy records, the feedback reporting addresses (RUA and RUF) of the organization (or hosts) will be used. The only direct feedback leakage risk for these PSDs are for Organizational Domains that are out of compliance with PSD policy. Data on non-existent cousin domains would be sent to the PSO.

- Multi-organization PSDs (e.g., ".com") that do not mandate DMARC usage: Privacy risks for Organizational Domains that have not deployed DMARC within such PSDs are significant. For non-DMARC Organizational Domains, all DMARC feedback will be directed to the PSO. PSD DMARC is opt-out (by publishing a DMARC record at the Organizational Domain level) vice opt-in, which would be the more desirable characteristic. This means that any non-DMARC organizational domain would have its feedback reports redirected to the PSO. The content of such reports, particularly for existing domains, is privacy sensitive.

PSOs will receive feedback on non-existent domains, which may be similar to existing Organizational Domains. Feedback related to such cousin domains have a small risk of carrying information related to an actual Organizational Domain. To minimize this potential concern, PSD DMARC feedback MUST be limited to Aggregate Reports. Feedback Reports carry more detailed information and present a greater risk.

Due to the inherent Privacy and Security risks associated with PSD DMARC for Organizational Domains in multi-organization PSDs that do not particpate in DMARC, any Feedback Reporting related to multi-organizational PSDs MUST be limited to non-existent domains except in cases where the reporter knows that PSO requires use of DMARC.

5. Security Considerations

This document does not change the Security Considerations of [RFC7489] and [RFC7960].

The risks of the issues identified in [RFC7489], Section 12.3, DNS Security, are amplified by PSD DMARC. In particular, DNS cache poisoning (or Name Chaining), see [RFC3833] for details, consequences are increased because a successful attack would potentially have a much wider scope.

The risks of the issues identified in [RFC7489], Section 12.5, External Reporting Addresses, are amplified by PSD DMARC. By design, PSD DMARC causes unrequested reporting of feedback to entities external to the Organizational Domain. This is discussed in more detail in Section 4.

6. IANA Considerations

This section describes actions requested to be completed by IANA.

6.1. Subdomain Policy Tag

IANA is requested to add a new tag to DMARC Tag Registry in the Domain-based Message Authentication, Reporting, and Conformance (DMARC) Parameters Registry.

The entry is as follows:

Tag Name	Reference	Status	Description
np	this document	current	Requested handling policy for non-existent subdomains

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[psddmarc.org] multiple, "PSD DMARC Web Site", April 2019, <https://psddmarc.org/>.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, DOI 10.17487/RFC3833, August 2004, <https://www.rfc-editor.org/info/rfc3833>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <https://www.rfc-editor.org/info/rfc5598>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/info/rfc7624>.

[RFC7960] Martin, F., Ed., Lear, E., Ed., Draegen. Ed., T., Zwicky, E., Ed., and K. Andersen, Ed., "Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows", RFC 7960, DOI 10.17487/RFC7960, September 2016, <https://www.rfc-editor.org/info/rfc7960>.

[RFC8020] Bortzmeyer, S. and S. Huque, "NXDOMAIN: There Really Is Nothing Underneath", RFC 8020, DOI 10.17487/RFC8020, November 2016, <https://www.rfc-editor.org/info/rfc8020>.

Appendix A. PSD DMARC Privacy Concern Mitigation Experiment

The experiment being performed has three different questions which are looking to be addressed in this document.

- Section 3.2 modifies policy discovery to add an additional DNS lookup. To determine if this lookup is useful, PSDs will add additional DMARC records in place, and will analyze the DMARC reports. Success will be determined if a consensus of PSDs that publish DMARC records are able to collect useful data.

- Section 3.2 adds the "np" tag for non-existent subdomains (DNS NXDOMAIN). PSOs wishing to test this will add this flag to their DMARC record, and will analyze DMARC reports for deployment. Success will be determined if organizations find explicitly blocking non-existent subdomains domains desirable and provide added value.

- Section 4.1 discusses three cases where providing feedback could cause information to leak out of an organization. This experiment

will analyze the feedback reports generated for each case to determine if there is information leakage.

Appendix B. DMARC PSD Registry Examples

To facilitate experimentation around data leakage mitigation, samples of the DNS based and IANA like registries are available at [psddmarc.org].

B.1. DMARC PSD DNS Query Service

A sample stand-alone DNS query service is available at [psddmarc.org]. It was developed based on the contents suggested for an IANA registry in an earlier revision of this draft. Usage of the service is described on the web site.

B.2. DMARC Public Suffix Domain (PSD) Registry

[psddmarc.org] provides an IANA like DMARC Public Suffix Domain (PSD) Registry as a stand-alone DNS query service. It follows the contents and structure described below. There is a Comma Separated Value (CSV) version of the listed PSD domains which is suitable for use in build updates for PSD DMARC capable software.

Names of PSDs participating in PSD DMARC must be registered this new registry. New entries are assigned only for PSDs that require use of DMARC. The requirement has to be documented in a manner that satisfies the terms of Expert Review,per [RFC5226]. The Designated Expert needs to confirm that provided documentation adequately describes PSD policy to require domain owners to use DMARC or that all domain owners are part of a single organization with the PSO.

The initial set of entries in this registry is as follows:

PSD	Status
.bank	current
.insurance	current
.gov.uk	current
.mil	current

B.3. DMARC PSD PSL Extension

[psddmarc.org] provides a PSL like file to enable to facilitate identification of PSD DMARC participants. Contents are functionally identical to the IANA like registry, but presented in a different format.

When using this approach, the input domain of the extension lookup is supposed to be the output domain of the regular PSL lookup, i.e. the organizational domain. This alternative data approach is potentially useful since DMARC implementations already need to be able to parse the data format, so it should be easier to implement.

Appendix C. Implementations

There are two known implementations of PSD DMARC available for testing.

C.1. Authheaders Module

The authheaders Python module and command line tool is available for download or installation from Pypi (Python Packaging Index).

It supports both use of the DNS based query service and download of the CSV registry file from [psddmarc.org].

C.2. Zdkimfilter Module

The zdkimfilter module is a separately available add-on to Courier-MTA.

Mostly used for DKIM signing, it can be configured to also verify, apply DMARC policies, and send aggregate reports. For PSD DMARC it uses the PSL extension list approach, which is available from from [psddmarc.org]

Acknowledgements

Thanks to the following individuals for their contributions (both public and private) to improving this document. Special shout out to Dave Crocker for naming the beast.

Kurt Andersen, Seth Blank, Dave Crocker, Heather Diaz, Tim Draegen, Zeke Hendrickson, Andrew Kennedy, John Levine, Dr Ian Levy, Craig Schwartz, Alessandro Vesely, and Tim Wicinski

Author's Address

Scott Kitterman
fTLD Registry Services
600 13th Street, NW, Suite 400
Washington, DC 20005
United States of America

Phone: +1 301 325-5475
Email: scott@kitterman.com