Network Working Group
Internet-Draft
Intended status: Experimental
Expires: November 28, 2019

S. Kitterman
fTLD Registry Services

May 27, 2019

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

draft-ietf-dmarc-psd-04

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. DMARC policies can be applied at the individual domain level or for a set of domains at the organizational level. The design of DMARC precludes grouping policies for a set of domains above the organizational level, such as TLDs (Top Level Domains). These types of domains (which are not all at the top level of the DNS tree) can be collectively referred to as Public Suffix Domains (PSDs). For the subset of PSDs that require DMARC usage, this memo describes an extension to DMARC to enable DMARC functionality for such domains.

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 November 28, 2019.

Copyright Notice

Table of Contents

1. Introduction

DMARC [RFC7489] provides a mechanism for publishing organizational policy information to email receivers. DMARC [RFC7489] allows policy to be specified for both individual domains and sets of domains within a single organization. For domains above the organizational

level in the DNS tree, policy can only be published for the exact domain. There is no method available to such domains to express lower level policy or receive feedback reporting for sets of domains. This prevents policy application to non-existent domains and identification of domain abuse in email, which can be important for brand and consumer protection.

As an example, imagine a country code TLD (ccTLD) which has public subdomains for government and commercial use (.gov.example and .com.example). Within the .gov.example public suffix, use of DMARC [RFC7489] has been mandated and .gov.example has published its own DMARC [RFC7489] record:

"v=DMARC1;p=reject;rua=mailto:dmarc@dmarc.service.gov.example"

at

_dmarc.gov.example.

This would provide policy and feedback for mail sent from @gov.example, but not @tax.gov.example and there is no way to publish an organizational level policy that would do so. While, in theory, receivers could reject mail from non-existent domains, not all receivers do so. Non-existence of the sending domain can be a factor in a mail delivery decision, but is not generally treated as definitive on its own.

This memo provides a simple extension to DMARC [RFC7489] to allow operators of Public Suffix Domains (PSDs) to express policy for groups of subdomains, extends the DMARC [RFC7489] policy query functionality to detect and process such a policy, describes receiver feedback for such policies, and provides controls to mitigate potential privacy considerations associated with this extension.

As an additional benefit, the PSD DMARC extension will clarify 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. PSD DMARC will help clarify that DMARC is not limited to organizational domains and their sub-domains.

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 [RFC7489] purposes. They require the same protections as DMARC [RFC7489] Organizational Domains, but are currently excluded.

- o 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 [RFC7489] 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 applicable to PSDs, since they (e.g., the ".gov.example" used above) do not send mail.

DMARC [RFC7489], by design, does not support usage by PSOs. For PSDs that require use of DMARC [RFC7489], an extension of DMARC reporting and enforcement capability is needed for PSO to effectively manage and monitor implementation of PSD requirements.

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". They are not available for private registration. In many cases the public portion of the DNS tree is more than one level deep. PSD DMARC includes all public domains above the organizational level in the tree, e.g., ".gov.uk".

2.3. Longest PSD

Organizational Domain (DMARC [RFC7489] Section 3.2) with one label removed.

2.4. Public Suffix Operator (PSO)

A Public Suffix Operator manages operations within their PSD.

2.5. 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 (the term Organizational Domains is defined in DMARC [RFC7489] Section 3.2). Depending on PSD policy, these will have one (e.g., ".com") or more (e.g., ".co.uk") name components.

2.6. Non-existent Domains

For DMARC [RFC7489] purposes, a non-existent domain is a domain name that publishes none of A, AAAA, or MX records that the receiver is willing to accept. 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. Section 6.1 DMARC Policy Record

PSD DMARC records are published as a subdomain of the PSD. For the PSD ".example", the PSO would post DMARC policy in a TXT record at "_dmarc.example".

3.3. Section 6.5. Domain Owner Actions

In addition to the DMARC [RFC7489] domain owner actions, PSOs that require use of DMARC ought to make that information available to receivers.

3.4. 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 2.3) of the Organizational Domain is one that the receiver has determined is acceptable for PSD DMARC, the Mail Receiver MUST query the DNS for a DMARC TXT record at the DNS domain matching the longest PSD (Section 2.3) 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.cctld", the query for PSD DMARC would use "compute.cloudcompany.com.cctld" as the longest PSD (Section 2.3). 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.cctld".

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 [RFC7489] policy. Specifically, this is not a mechanism to provide feedback addresses (RUA/RUF) when an Organizational Domain has declined to do so.

3.5. Section 7. DMARC Feedback

Operational note for PSD DMARC: For PSOs, feedback for non-existent domains is desired and useful. See Section 4 for discussion of Privacy Considerations.

4. Privacy Considerations

These privacy considerations are developed based on the requiremetns of [RFC6973]. The Privacy Considerations of [RFC7489] apply to this document.

4.1. Feedback leakage

Providing feedback reporting to PSOs can, in some cases, create leakage of information outside of an organization to the PSO. This leakage could be 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 it's 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 is best 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 ought to 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 12.5, 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 document does not require any IANA actions.

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/>.

[PSL] multiple, "Public Suffix List", April 2019, <https://publicsuffix.org/>.

[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. The Experiment

To mitigate the privacy concerns associated with Multi-organization PSDs that do not mandate DMARC usage, see Section 4.1, a mechanism to indicate which PSDs do not present this privacy risk is appropriate. There are multiple approaches that are possible.

The experiment is to evaluate different possible approaches. The experiment will be complete when there is rough consensus on a technical approach that is demonstrated to be operationally usable and effective at mitigating the privacy concern.

The mechanism needs the following attributes:

- Be reliably, publicly accessible
- Be under configuration control based on a public set of criteria
- List PSDs that either mandate DMARC for their registrants or for which all lower level domains are controlled by the PSO and that the relevant PSO has indicated a desire for the PSD to participate in PSD DMARC
- Have a small operational footprint (e.g. provide a documented, lightweight mechanism for developers and operators to retrieve the list of PSD DMARC participants)
- Not allow PSO to add PSDs to the PSD DMARC participants list without third party review

As of this writing, three approaches have been proposed. None of them are ideal:

- An extension to the Public Suffix List at [PSL]
- A dedicated registry queried via DNS - an example of such a service is described in Appendix B.1 below
- An IANA registry

Appendix B. DMARC PSD Registry Examples

To faciliate 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

Appendix C. Implementation

There is one known implementation 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].

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