                   DMARC Failure reporting Interval tag
                      draft-davids-dmarc-fi-tag-01

Abstract

   This document extends the DMARC (RFC7489) record format by defining
   an additional tag. This new tag, the "fi" tag, is to be used in
   conjunction with the "ruf" tag used for message-specific failure
   reporting. It provides a Domain Owner with a simple way of
   requesting limitation of the rate at which such reports are sent.

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 May 28, 2017.

the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

   DMARC [RFC7489] enables Domain Owners to request for detailed failure
   reports for individual messages by means of the "ruf" tag. There may
   be various reasons to permanently configure such a "ruf" tag. For
   example to facilitate reputation management, monitoring or simply for
   research or operational purposes.

   Failure reports are normally generated and sent almost immediately
   after the Mail Receiver detects a DMARC failure. These reports are
   useful for quickly notifying the Domain Owners of an authentication
   failure, without waiting for an aggregate report. However, under
   certain circumstances this property can potentially lead to an
   undesirably high volume of reports. Especially when a Domain Owner's
   name is spoofed and abused in a large-scale phishing or other
   impersonation attack.

   DMARC [RFC7489] Section 7.3 leaves it to the discretion of
   participating Mail Receivers and report generators if and how they
   take measures against sending high volumes of failure reports.
   However, what a Mail Receiver or report generator considers
   acceptable may exceed the capacity of the receiving Domain Owner.
   The lack of a mechanism for a Domain Owner to influence the volume of
   reports constitutes an obstacle to deployment of the "ruf" tag
   feature.

   This document updates [RFC7489] by defining the "fi" tag, a mechanism
   that allows the Domain Owner to request the limitation of failure

reports of no more than one failure report per report generator per
time interval.

2. Conventions Used In This Document

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] when they
appear in ALL CAPS. These words may also appear in this document in
lower case as plain English words, absent their normative meanings.

The following terms are used, as defined in DMARC [RFC7489].

Domain Owner and Mail Receiver.

Also the term "report generator" is applied here the same way as in
DMARC [RFC7489].

3. Extension to the General Record Format

The following tag is introduced as an additional valid DMARC tag for
use in conjunction with the Reporting URI for Failure ("ruf") tag:

fi:
   Interval requested between message-specific failure reports
   (plain-text 32-bit unsigned integer; OPTIONAL; if not defined or
   0, then there is no rate limitation requested). Indicates a
   request to report generators to send message-specific failure
   reports at an interval of approximately the requested number of
   seconds.

Any intermediate remaining reports SHOULD NOT be sent and MAY be
discarded, if generated at all. But discarding message-specific
failure reports as a consequence of this tag, SHALL NOT affect the
completeness of information in the aggregated feedback reports.

A report generator MAY include in the message-specific failure report
an indication of the number of reports discarde since the last issued
report. Where AFRF [RFC6591] is used, the Abuse Reporting Format
[RFC5965] optional "Incidents"-field may be used to indicate the
number of discarded reports.

Report generators that choose to adhere to the "ruf" tag option,
SHOULD also adhere to the requested "fi" tag setting defined here.
This tag's content SHALL be ignored if a "ruf" tag is not also
specified, or if the syntax of the "fi" integer is invalid.

   Report generators that implement this feature MUST be able to support
   the entire interval range from 0-86400 and MAY support longer
   intervals.

4. Formal Definition

   The formal definition of the "fi" tag format, using ABNF [RFC5234],
   is as follows:

   Introduced:

                dmarc-finterval = "fi" *WSP "=" *WSP 1*DIGIT

   Which changes the dmarc-record definition to:

        dmarc-record   = dmarc-version dmarc-sep
                           [dmarc-request]
                           [dmarc-sep dmarc-srequest]
                           [dmarc-sep dmarc-auri]
                           [dmarc-sep dmarc-furi]
                           [dmarc-sep dmarc-adkim]
                           [dmarc-sep dmarc-aspf]
                           [dmarc-sep dmarc-ainterval]
                           [dmarc-sep dmarc-finterval]
                           [dmarc-sep dmarc-fo]
                           [dmarc-sep dmarc-rfmt]
                           [dmarc-sep dmarc-percent]
                           [dmarc-sep]
                           ; components other than dmarc-version and
                           ; dmarc-request may appear in any order

5. Domain Owner Example

   The DMARC policy record with the "fi" tag might look like this when
   retrieved using a common command-line tool:

        % dig +short TXT _dmarc.example.com.
        "v=DMARC1; p=none; rua=mailto:dmarc-feedback@example.com;
         ruf=mailto:auth-reports@example.com; fi=300;"

   To publish such a record, the DNS administrator for the Domain Owner
   might create an entry like the following in the appropriate zone file
   (following the conventional zone file format):

```
   ; DMARC record for the domain example.com

  _dmarc  IN TXT ( "v=DMARC1; p=none; "
                  "rua=mailto:dmarc-feedback@example.com; "
                  "ruf=mailto:auth-reports@example.com; fi=300; " )
```

The request implies that the Domain Owner is willing to accept no
more than one message-specific failure report every 5 minutes from
any report generator. A report generator in this example would
typically honour the "fi" tag by sending out a report, storing a
'last report sent' timestamp for example.com in memory and
maintaining it as a 'do not sent' flag for a minimum of 300 seconds
during which period no consecutive reports are to be sent. After the
flag has cleared, a report may again be sent. The cycle then
repeats.

Intermediate, unsent reports are discarded. But they do add to
statistical counters as if they were sent. So their details are part
of any corresponding aggregated reports.

Any optionally defined indications for the maximum report size in the
URI will continue to work as defined in [RFC7489].

6. IANA Considerations

As per [RFC7489 p.17] Section 6.3 last paragraph, a new version of
DMARC is not required. Older implementations that consider the "fi"
tag as unknown, will ignore it.

However, this document requires an update to the IANA [RFC5226] DMARC
Tag Registry [1]:

```
        Tag Name | Description
        ---------+---------------------------
        fi       | Failure Reporting interval
```

7. Security Considerations

The Domain Owner should be aware that defining a "fi" tag involves a
trade-off between the benefit of preventing unmanageable incoming
report flows and the risk of not receiving potentially useful data.
A large scale attack that triggers reporting rate limitation, might
result in the non-dispatch of reports regarding other events
involving the same domain to the same Mail Receiver.

An attack can involve many different report generators. The Domain
Owner should be aware that the "fi" tag limits reporting by each
individual report generator. Multiple report generators might still

collectively generate a large volume of reports. Mail Receivers with
a farm or cluster of several report generators might choose to
synchronise the 'last sent' timestamp value accross their machines in
order to better comply with the wishes of Domain Owners and to reduce
the risk described above.

An attack can also involve multiple domains belonging to a single
Domain Owner. The "fi" tag applies to an individual domain, so the
deliberate abuse of multiple spoofed domains belonging to Domain
Owner, might still generate a high volumes of message-specific
failure reports.

It therefore it makes sense to define a relatively short TTL for
DMARC-records, to allow for the possibility of increasing the "fi"-
value on an ad hoc basis, or to remove the "ruf" (and "fi") tag
altogether in the even of a problem.

[TODO: mention the part hereafter, or is it out of scope for this
draft?] An attacker that enforces message-specific detailed failure
("ruf") reports that are larger than an optionally-defined maximum-
size specification, may leave the Domain Owner in the darks, because
no reports will be sent.

The security of the DMARC TXT-record, which the "fi" tag part of,
depends on the security of the underlying DNS infrastructure. In
that respect it is advisable to make use of DNSSEC.

8. Discussion

The DMARC virtual verification draft [draft-akagiri-dmarc-virtual-
verification] discusses possible values for the "ruf" tag. The
authors of that draft are kindly requested to take this draft into
consideration as part of their discussions.

9. Acknowledgments

The author would like to thank Elizabeth Zwicky, Moritz Mueller,
Maarten Wullink, Cristian Hesselman and Bart Knubben for their
valuable feedback.

10. References

10.1. 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,
           <http://www.rfc-editor.org/info/rfc2119>.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              DOI 10.17487/RFC5226, May 2008,
              <http://www.rfc-editor.org/info/rfc5226>.

   [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax
              Specifications: ABNF", STD 68, RFC 5234,
              DOI 10.17487/RFC5234, January 2008,
              <http://www.rfc-editor.org/info/rfc5234>.

   [RFC5965] Shafranovich, Y., Levine, J., and M. Kucherawy, "An
              Extensible Format for Email Feedback Reports", RFC 5965,
              DOI 10.17487/RFC5965, August 2010,
              <http://www.rfc-editor.org/info/rfc5965>.

   [RFC6591] Fontana, H., "Authentication Failure Reporting Using the
              Abuse Reporting Format", RFC 6591, DOI 10.17487/RFC6591,
              April 2012, <http://www.rfc-editor.org/info/rfc6591>.

10.2. Informative References

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

10.3. URIs

   [1] https://www.iana.org/assignments/dmarc-parameters/dmarc-
       parameters.xhtml

Author's Address

   Marco Davids
   SIDN
   Meander 501
   Arnhem 6825 MD
   NL

   Phone: +31 26 352 5500
   Email: marco.davids@sidn.nl