IETF
Internet-Draft
Intended status: Informational
Expires: April 5, 2020

A. Vesely
October 3, 2019

DNSWL Email Authentication Method Extension
draft-vesely-authmethod-dnswl-09

Abstract

This document describes an additional Email Authentication Method compliant with RFC 8601. The method consists in looking up the sender's IP in a DNS whitelist.

This document does not consider black lists.

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 April 5, 2020.

Table of Contents

1. Introduction

One of the many checks that mail servers carry out is to query DNS whitelists (DNSWL, [RFC5782]). The lookup is based on the connecting client's IP address, so this check can occur very early in an SMTP transaction. The result can be used to counterweight policies that typically occur at early stages too, such as the Sender Policy Framework (SPF, the last paragraph of Appendix D.3 of [RFC7208] is illustrated in Appendix A). In addition, the result of a DNSWL lookup can also be used at later stages; for example, a delivery agent can use it to learn the trustworthiness of a mail relay in order to estimate the spamminess of an email message. The latter possibility needs a place to collect query results for downstream use, which is precisely what the Authentication-Results header field aims at providing.

Results often contain additional data, encoded according to DNSWL-specific criteria. The present method considers only whitelists --one of the major branches considered by [RFC5782]. In case of DNSxL, the boundary MTA (see [RFC5598]) which carries out the check and possibly stores the result, has to be able to discern at least the color of "x", which is required to make accept/reject decisions.

Data conveyed in A and TXT records can be stored as result's parameters. In effect, they are tantamount to local policies, albeit outsourced. Downstream agents need to know DNSWL-specific encoding to understand the meaning of that data. In order to smooth operations, this document endorses a usage of TXT fields consistent with other authentication methods. Namely, to serve the domain name in the TXT record.

2. Method Details

The following ptype.property items define the relevant parameters where additional data can be stored. They augment the "pass" result with information about the entry found.

dns.zone: DNSWL query root domain, which defines the meaning of the result. Note that an MTA can use a local mirror with a different name. The name stored here has to be the best available reference for all foreseeable downstream consumers. If the message is handed outside the internal network, dns.zone had better be the global zone.

policy.ip: The bit mask value received in type A response, in dotted quad. Multiple entries can be arranged in a comma-separated list.

policy.txt: The TXT record, if any. Multiple records are concatenated in the usual way (explained, for example, in Section 3.3 of [RFC7208]). See Section 3 for the resulting content and query options.

dns.sec: This is a generic property stating whether data was retrieved using DNSSEC ([RFC4033]). It has three possible values:

ad: Authenticated data. The AD bit is set in the DNS response, indicating DNSSEC validation.

no: The AD bit is not set in the DNS response, although it was requested, thereby indicating that the zone is not signed.

na: Not applicable. The lookup is not run through a security-aware DNS resolver. In particular, "na" is used if the data was downloaded in bulk and then loaded on a local nameserver --which is the case of a producer querying a local zone different from the reported dns.zone. Temporary validation errors can also report "na".

The result of the method states how the query did, up to the interpretation of the result. In particular, some DNSBLs are known to return special codes to signal over quota, for example 127.0.0.255. If the result producer cannot interpret that value, that case results in a false positive.

pass: The query successfully returned applicable records. The sender is whitelisted, up to differing interpretation.

none: The query worked but yielded no record, or returned NXDOMAIN, so the sender is not whitelisted.

temperror: The DNS evaluation could not be completed due to some error that is likely transient in nature, such as a temporary DNS error, e.g., a DNS RCODE of 2, commonly known as SERVFAIL, or other error condition resulted. A later attempt may produce a final result.

permerror: The DNS evaluation cannot work because test entries don't work, that is, DNSWL is broken, or because queries are overquota, e.g., a DNS RCODE of 5, commonly known as REFUSED, or a DNSWL-specific policy.ip was returned. A later attempt is unlikely to produce a final result. Human intervention is required.

3. TXT Record Contents

According to [RFC5782], TXT records describe the reason why IP addresses are listed in a DNSWL. The TXT record is useful if it contains the domain name(s). The domain name would correspond to the DNS domain name used by or within the ADMD operating the relevant MTA, sometimes called the "organizational domain". In that case, the authentication provided by this method is equivalent to a DKIM signature ([RFC6376]) or an SPF check host ([RFC7208]).

According to a DNSWL's policy, attributing responsibility of an IP address to an organization may require something more than a mere PTR record consistency. If no domain names can be responsibly associated to a given IP, for example because the IP was added without direct involvement of the organization concerned, DNSWLs can use a subdomain of .INVALID ([RFC2606]) where the leftmost label hints at why an address is whitelisted. For example, if the address 192.0.2.38 was added by the list managers solely based on their knowledge, the corresponding TXT record might be AUTOPROMOTED.INVALID, so as to avoid to explicitly identify an entity who didn't opt-in.

Following the example of Multicast DNS (see the second paragraph of Section 16 of [RFC6762]) names containing non-ASCII characters can be encoded in UTF-8 [RFC3629] using the normalization form canonical composition (NFC) as described in Unicode Format for Network Interchange ([RFC5198]). Inclusion of unaltered UTF-8 TXT values in the header entails an environment compatible with EAI [RFC6530].

DNS queries with a QTYPE of ANY may lead to inconsistent replies, depending on the cache status. In addition, ANY is not "all", and the provisions for queries that have QTYPE=ANY ([RFC8482]) don't cover DNSxLs. A mail server can issue two simultaneous queries, A and TXT. Otherwise, a downstream filter can issue a TXT query on its own, if it knows that an A query was successful and that the DNSWL serves useful TXT records. It is unlikely that TXT records exist if a query for QTYPE A failed.

4. IANA Considerations

There is a registry of Email Authentication Methods. The method described in this document is referred by Table 1, along with its ptype.property values.

Method	ptype	property	Value	Status	Version
dnswl	dns	zone	DNSWL publicly accessible query root domain	active	1
dnswl	policy	ip	type A response received (or comma-separated list thereof)	active	1
dnswl	policy	txt	type TXT query response	active	1
dnswl	dns	sec	one of "ad" for authenticated data, "no" for not signed, or "na" for not applicable	active	1

Table 1: Email Authentication Method

A new ptype, "dns" is introduced in Table 2. It is meant to be used for properties related to the Domain Name System (DNS [RFC1034]).

ptype	Definition	Description
dns	[this doc]	The property being reported belongs to the Domain Name System

Table 2: Email Authentication Property Type

This method reuses four of the values already defined in the Email Authentication Result Names associated registry. They are listed in Table 3.

Auth Method	Code	Specification	Status
dnswl	pass	Sender is whitelisted, up to returned code interpretation	active
dnswl	none	NXDOMAIN or no record, sender is not whitelisted	active
dnswl	temperror	Transient DNS error during the query	active
dnswl	permerror	Query cannot work, human intervention needed	active

Table 3: Email Authentication Result Names

5. Security Considerations

All of the considerations described in Section 7 of [RFC8601] apply.

In addition, the usual caveats apply about importing text from external online sources. Although queried DNSWLs are well known, trusted entities, it is suggested that TXT records be reported only if, upon inspection, their content is deemed actually actionable.

6. References

6.1. Normative References

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, DOI 10.17487/RFC2606, June 1999, <https://www.rfc-editor.org/info/rfc2606>.

[RFC5782] Levine, J., "DNS Blacklists and Whitelists", RFC 5782, DOI 10.17487/RFC5782, February 2010, <https://www.rfc-editor.org/info/rfc5782>.

[RFC8601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 8601, DOI 10.17487/RFC8601, May 2019, <https://www.rfc-editor.org/info/rfc8601>.

6.2. Informative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, DOI 10.17487/RFC5198, March 2008, <https://www.rfc-editor.org/info/rfc5198>.

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

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, DOI 10.17487/RFC6530, February 2012, <https://www.rfc-editor.org/info/rfc6530>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC8482] Abley, J., Gudmundsson, O., Majkowski, M., and E. Hunt, "Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY", RFC 8482, DOI 10.17487/RFC8482, January 2019, <https://www.rfc-editor.org/info/rfc8482>.

Appendix A. Example

```
Delivered-To: recipient@example.org
Return-Path: <sender@example.com>
Authentication-Results: mta.example.org;
  dkim=pass (whitelisted) header.i=@example.com
Authentication-Results: mta.example.org;
  dnswl=pass dns.zone=list.dnswl.example dns.sec=na
  policy.ip=127.0.10.1
  policy.txt="fwd.example https://dnswl.example/?d=fwd.example"
Received-SPF: fail (Address does not pass Sender Policy Framework)
  client-ip=192.0.2.1;
  envelope-from="sender@example.com";
  helo=mailout.fwd.example;
  receiver=mta.example.org;
Received: from mailout.fwd.example (mailout.fwd.example [192.0.2.1])
  (TLS: TLSv1/SSLv3,128bits,ECDHE-RSA-AES128-GCM-SHA256)
  by mta.example.org with ESMTPS; Thu, 03 Ocy 2019 19:23:11 +0200
  id 00000000005DC044.000000005702D87C.000007FC
```

Trace fields added at the top of the header by multiple agents at various stages during processing at the final MTA

The message went through a third party, fwd.example, which forwarded it to the final MTA. Such mail path was not arranged beforehand with the involved MTAs, it emerged spontaneously. This message would not have made it to the target without whitelisting, because:

- the author domain published a strict SPF policy (-all),
- the forwarder did not alter the bounce address, and
- the target usually honors reject-on-fail, according to Section 8.4 of [RFC7208].

However, the target also implemented the last paragraph of Appendix D.3 of [RFC7208]. Rather than rejecting the message outright before DATA, the MTA received it, recorded the SPF fail result, and indicated the local policy mechanism which was applied in order to override that result. Subsequent filtering detected no malware and verified DKIM [RFC6376]. It would still have been possible to reject the message, based on its content. It is at these later stages, after receiving the body and also during delivery, that a deeper knowledge of the policy values obtained from dnswl.example can allow weighting that score against other factors.

Author's Address

Alessandro Vesely
v. L. Anelli 13
Milano, MI 20122
IT

Email: vesely@tana.it