Independent Submission
Request for Comments: 8904
Category: Informational
ISSN: 2070-1721

A. Vesely

September 2020

DNS Whitelist (DNSWL) Email Authentication Method Extension

Abstract

This document describes an email authentication method compliant with RFC 8601. The method consists of looking up the sender's IP address in a DNS whitelist. This document provides information in case the method is seen in the field, suggests a useful practice, and registers the relevant keywords.

This document does not consider blacklists.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8904.

Table of Contents

1. Introduction

One of the many checks that mail servers carry out is to query DNS whitelists (DNSWLs). That method is fully discussed in [RFC5782]. The DNS [RFC1034] lookup is based on the connecting client's IP address, IPv4 or IPv6, and returns zero or more A records. The latter are IPv4 IP addresses in the range 127.0.0.0/8. Depending on the query, TXT records with varying content can also be retrieved. Query examples are given in Appendix A.

Since the IP address is known as soon as the connection is accepted, this check can occur very early in an SMTP transaction. Its 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 also illustrated in Appendix A). In addition, the result of a DNSWL lookup can 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 to provide.

Results often contain additional data, encoded according to DNSWL-specific criteria. The method described in this document considers only whitelists -- one of the major branches described by [RFC5782]. There are also blacklists/blocklists (DNSBLs) and combined lists. Since they all have the same structure, the abbreviation DNSxL is used to mean any. The core procedures of a Mail Transfer Agent (MTA) tend to be quite general, leaving particular cases to be handled by add-on modules. In the case of combined lists, 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 each entry, as that is required to make accept/reject decisions. This document provides for storing the result when the DNSxL record to be reported is a whitelisting one.

Data conveyed in A and TXT records can be stored as properties of the method. The meaning of such data varies widely at the mercy of the list operator; hence, the queried zone has to be stored as well. Mail site operators who configure their MTAs to query specific DNWSLs marry the policies of those lists, as, in effect, they become tantamount to local policies, albeit outsourced. Downstream agents who know DNSWL-specific encoding and understand the meaning of that data can use it to make delivery or display decisions. For example, a mail filter that detects heuristic evidence of a scam can counterweight such information with the trustworthiness score encoded in the A response so as to protect against false positives. Mail User Agents (MUAs) can display those results or use them to decide how to report abusive messages, if configured to do so.

This document describes a usage of TXT fields consistent with other authentication methods, namely to serve the domain name in the TXT record. That way, a downstream filter could also consider whether the sending agent is aligned with the author domain, with semantics similar to [RFC7489].

At the time of this writing, this method is implemented by Courier-MTA [Courier-MTA]. An outline of the implementation is given in Appendix B.

2. Method Details

The result of the method states how the query did, up to the interpretation of the returned data.

The method has four possible results:

pass: The query successfully returned applicable records. This result is usually accompanied by one or both of the policy properties described below. Since the list is configured as a DNSWL, agents unable to interpret list-specific properties can still derive a positive value from the fact that the sender is whitelisted.

none: The query worked but yielded no A 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. 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 over quota (reported by a DNS RCODE of 5, commonly known as REFUSED, or by a DNSWL-specific property (policy.ip, defined below) with the same meaning). A later attempt is unlikely to produce a final result. Human intervention is required.

Note that there is no "fail" result.

The following ptype.property items define how the data provided by the whitelist lookup can be saved.

dns.zone: DNSWL query root domain, which defines the meaning of the policy.ip property below. 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. Setting dns.zone to the global zone makes the result intelligible even if the message is handed outside of the internal network.

policy.ip: The bit mask value received in type A response, in dotted quad notation. Multiple entries can be arranged in a quoted, comma-separated list (quotes are necessary because commas are not allowed in a token).

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 the relevant data was validated using DNSSEC [RFC4033]. For the present method, the relevant data consists of the reported policy properties above or, if the method result is "none", its nonexistence. This property has three possible values:

yes: DNSSEC validation confirms the integrity of data. Section 5.2 considers how that is related to the DNS response.

no: The data is not signed. See Section 5.2.

na: Not applicable. No DNSSEC validation can be performed, possibly because the lookup is run through a different means than a security-aware DNS resolver. This does not necessarily imply less security. In particular, "na" is used if the data was downloaded in bulk and then loaded on a local nameserver, which is the case of an MTA querying a local zone different from the reported dns.zone. DNS errors, including validation errors, can also report "na". This is also the value assumed by default.

3. TXT Record Contents

According to [RFC5782], TXT records describe the reason why IP addresses are listed in a DNSWL. An example of a DNSWL whose TXT records contain the domain name of the organization assignee of the sending IP is given in Appendix B. The domain name would correspond to the DNS domain name used by or within the Administrative Management Domain (ADMD) operating the relevant MTA, sometimes called the "organizational domain". In that case, the authentication provided by this method is equivalent to a DomainKeys Identified Mail (DKIM) signature [RFC6376] or an SPF check host [RFC7208], if the DNSWL is trusted.

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 address, for example, because the IP address 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 explicitly identifying an entity that 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 C [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 Email Address Internationalization (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 brought a result of "none".

4. IANA Considerations

IANA maintains the "Email Authentication Parameters" registry with several subregistries. IANA has made the assignments set out in the following sections.

4.1. Email Authentication Methods

IANA has created four new entries in the "Email Authentication Methods" registry as follows.

Method	Definition	ptype	property	Value	Status	Version

dnswl	RFC 8904	dns	zone	DNSWL publicly accessible query root domain	active	1
dnswl	RFC 8904	policy	ip	type A response received (or a quoted, comma-separated list thereof)	active	1
dnswl	RFC 8904	policy	txt	type TXT query response	active	1
dnswl	RFC 8904	dns	sec	one of "yes" for DNSSEC authenticated data, "no" for not signed, or "na" for not applicable	active	1

Table 1

4.2. Email Authentication Property Type

IANA has created a new entry in the "Email Authentication Property Types" registry as follows.

ptype	Definition	Description
dns	RFC 8904	The property being reported belongs to the Domain Name System.

Table 2

4.3. Email Authentication Result Names

IANA has created four new entries in the "Email Authentication Result Names" registry as follows.

Auth Method	Code	Specification	Status
dnswl	pass	RFC 8904	active
dnswl	none	RFC 8904	active
dnswl	temperror	RFC 8904	active
dnswl	permerror	RFC 8904	active

Table 3

5. Security Considerations

5.1. Over-Quota Signaling

Some DNSWLs that provide for free access below a given quota are known to return special codes to signal that the quota has been exceeded (for example, 127.0.0.255). If the MTA cannot interpret that value, that case results in a false positive. It can accept

messages that it would otherwise reject. A DNSWL-specific module would realize this fact and call for human intervention.

Returning an RCODE 5 (REFUSED) conveys the concept that the query is "unauthorized" and human intervention required.

5.2. Security of DNSSEC Validation

The dns.sec property is meant to be as secure as DNSSEC results. It makes sense to use it in an environment where the DNSSEC validation can succeed.

Section 7 of [RFC4033] examines various ways of setting up a stub resolver that either validates DNSSEC locally or trusts the validation provided through a secure channel. For a different class, it is possible to set up a dedicated, caching, DNSSEC-enabled resolver reachable by the mail server through interprocess communication on 127.0.0.1. In such cases, the property dns.sec=yes corresponds to the Authenticated Data (AD) bit in the DNS response header.

When the response contains no DNSSEC data, a security-aware resolver seeks a signed proof of the nonexistence of a DS record at some delegation point. If no error is returned, the zone is unsigned and dns.sec=no can be set. The Security Considerations section of [RFC3225] states:

> The absence of DNSSEC data in response to a query with the DO bit set MUST NOT be taken to mean no security information is available for that zone as the response may be forged or a non-forged response of an altered (DO bit cleared) query.

If the application verifies the DNSSEC signatures on its own, it effectively behaves like a validating resolver and hence can set dns.sec correspondingly.

When the data is downloaded in bulk and made available on a trusted channel without using DNSSEC, the application sets dns.sec=na or not at all. For example, consider DNSWLs that publish bulk versions of their data duly signed using OpenPGP [RFC4880]. It is the responsibility of system administrators to authenticate the data by downloading and validating the signature. The result of such validation is not reported using dns.sec.

5.3. Inherited Security Considerations

For DNSSEC, the considerations of Section 12 of [RFC4033] apply.

All of the considerations described in Section 7 of [RFC8601] apply. That includes securing against tampering all the channels after the production of the Authentication-Results header field.

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 actionable and their format compatible with the computing environment.

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>.

[RFC3225] Conrad, D., "Indicating Resolver Support of DNSSEC", RFC 3225, DOI 10.17487/RFC3225, December 2001, <https://www.rfc-editor.org/info/rfc3225>.

[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>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[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>.

[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>.

[RFC8460] Margolis, D., Brotman, A., Ramakrishnan, B., Jones, J., and M. Risher, "SMTP TLS Reporting", RFC 8460,

DOI 10.17487/RFC8460, September 2018,
<https://www.rfc-editor.org/info/rfc8460>.

[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>.

[Courier-MTA]
"Courier Mail Server", <https://www.courier-mta.org/>.

[DNSWL] "dnswl.org - E-Mail Reputation - Protect against false positives", <https://www.dnswl.org/>.

[NFC] Whistler, K., Ed., "Unicode Normalization Forms", Unicode Standard Annex 15, February 2020, <https://www.unicode.org/reports/tr15/tr15-50.html>.

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=2001:db8::2:1;
  envelope-from="sender@example.com";
  helo=mail.fwd.example;
  receiver=mta.example.org;
Received: from mail.fwd.example (mail.fwd.example [2001:db8::2:1])
  (TLS: TLSv1/SSLv3,128bits,ECDHE-RSA-AES128-GCM-SHA256)
  by mta.example.org with ESMTPS; Thu, 03 Oct 2019 19:23:11 +0200
  id 00000000005DC044.000000005702D87C.000007FC
```

Figure 1: Trace Fields at the Top of the Header

The message went through a third party, fwd.example, which forwarded it to the final MTA. The 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]. Its behavior hinges on the following DNS entries:

```
  1.0.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.b.8.2.0.0.1.
                                                      list.dnswl.example.
       IN  A    127.0.10.1
       IN  TXT  "fwd.example https://dnswl.example/?d=fwd.example"
```

Figure 2: DNS Resource Records for 2001:db8::2:1 (line breaks for editorial reasons)

If mail.fwd.example had connected from address 192.0.2.1, then the query name would have been "1.2.0.192.list.dnswl.example". See full

description in [RFC5782].

At connection time, because the remote IP address is whitelisted, the target MTA did not reject the message before DATA. Instead, it recorded the SPF fail result and indicated the local policy mechanism that was applied in order to override that result. Subsequent filtering verified DKIM [RFC6376].

At later stages, mail filters can reject or quarantine the message based on its content. A deeper knowledge of the policy values obtained from dnswl.example allows interpreting the values of policy.ip and weighing them against other factors so as to make better decisions.

Appendix B. Known Implementation

Implementation details mentioned in this section have been stable for several years. Yet, this description is necessarily superficial, version dependent, and subject to change.

Courier-MTA [Courier-MTA] can be configured to look up DNSBLs and DNSWLs, with similar command-line switches:

```
-block=zone[=displayzone][,var[/n.n.n.n][,msg]]
-allow=zone[=displayzone][,var[/n.n.n.n[,]]]
```

"zone" is the zone to be queried.

"displayzone" is only used for -allow; it is the value to be set in the dns.zone property.

"var" stands for the environment variable whose existence triggers a special action. The default variable names result in a conventional behavior implemented by Courier-MTA. By setting different environment variables, users can customize the behavior. Conventional behavior differs widely between -block and -allow. The former rejects the message; the latter produces Authentication-Results header fields.

The n.n.n.n IP address requires a precise A record response. If not given, any response results in setting the corresponding variable. If given, variables are set only if the response matches exactly. Such syntax provides for a very limited interpretation of the information encoded in A records. However, it is considered to be too complicated already. Even specifying a range, an enumeration of values, or a regular expression would require something beyond what a normal user would be willing to manage.

Finally, the trailing message, which overrides the 5xx SMTP reply for -block, is not used for -allow, except that its mere presence requires querying TXT records to be registered in policy.txt.

SPF is part of Courier-MTA’s core. It is configured separately and provides for an "allowok" keyword to indicate the choice to override rejection in case of SPF failure and -allow whitelisting.

A customary whitelist is defined by DNSWL.org [DNSWL]. It serves A records encoded as follows:

1st octet: 127.

2nd octet: 0.

3rd octet: Category of business, 15 values.

4th octet: Trustworthiness/score, 4 values.

They also serve TXT records containing the domain name followed by a URL pointing to further information about the relevant organization, such as what other IP addresses of theirs are being whitelisted. They don't use UTF-8.

DNSWL.org provides for free registration and free access below 100,000 queries per day. They use a special return code, 127.0.0.255 as exemplified above, to signal that the quota has been exceeded. Although Courier-MTA itself does not recognize this return code, it has a mail filter (zdkimfilter, named after its main usage) that hard codes recognition of this code and the code for trustworthiness in the 4th octet.

Appendix C. Future Possibilities of the 'dns' ptype

The description of the new ptype proposed in Section 4.2 says, "The property being reported belongs to the Domain Name System." That definition can broadly include any tag found in a domain's TXT record. For example, designers of authentication methods can agree that within a resinfo of a given method, any dns ptype refers to tags in the relevant DNS record, unless otherwise specified. So one could have, say:

```
Authentication-Results: example.com;
  spf=pass smtp.mailfrom=example.net dns.sec=y;
  dkim=pass header.i=@example.org header.b=jIvx30NG dns.s=tlsrpt
```

While dns.sec is defined above, albeit not for the spf method, the use of tlsrpt in the DKIM record is exemplified in Section 3 of [RFC8460]. The tag s= is part of the DKIM TXT record, not to be confused with the selector s=, which is part of a DKIM signature. Just like the latter can be reported as header.s because the DKIM header field is in the message header, it may make sense to report the former as dns.s because the DKIM DNS record is in the DNS.

NOTE: This is only a hint at what may become a consistent naming convention around the new ptype. In any case, any new property using this ptype requires its own formal definition. This document does NOT define the property dns.s=, let alone the service tlsrpt.

Author's Address

Alessandro Vesely
v. L. Anelli 13
20122 Milano MI
Italy

Email: vesely@tana.it