Workgroup: intarea
Internet-Draft:
draft-dkg-intarea-dangerous-labels-02
Published: 27 July 2022
Intended Status: Informational
Expires: 28 January 2023
Authors: D. K. Gillmor
ACLU

Dangerous Labels in DNS and E-mail

Abstract

This document establishes registries that list known security-sensitive labels in the DNS and in e-mail contexts.

It provides references and brief explanations about the risks associated with each known label.

The registries established here offer guidance to the security-minded system administrator, who may not want to permit registration of these labels by untrusted users.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://dkg.gitlab.io/dangerous-labels/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-dkg-intarea-dangerous-labels/.

Discussion of this document takes place on the Internet Area Working Group mailing list (mailto:intarea@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/intarea/.

Source for this draft and an issue tracker can be found at https://gitlab.com/dkg/dangerous-labels.

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 28 January 2023.

Table of Contents

1. Introduction

The Internet has a few places where seemingly arbitrary labels can show up and be used interchangeably.

Some choices for those labels have surprising or tricky consequences. Reasonable admnistrators may want to be aware of those labels to avoid an accidental allocation that has security implications.

This document registers a list of labels in DNS and e-mail systems that are known to have a security impact. It is not recommended to create more security-sensitive labels.

Offering a stable registry of these dangerous labels is not an endorsement of the practice of using arbitrary labels in this way. A new protocol that proposes adding a label to this list is encouraged to find a different solution if at all possible.

1.1. Requirements Language

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. DNS Labels

Note that [RFC8552] defines the use of "underscored" labels which are treated differently than normal DNS labels, and often have security implications. That document also established the IANA registry for "Underscored and Globally Scoped DNS Node Names". That registry takes precedence to the list enumerated here, and any label in that list or with a leading underscore ("_") **MUST NOT** be included in this list.

Note also that Section 2.2 of [RFC8820] makes it clear that depending on specific forms of DNS labels in a given URI scheme in a protocol is strongly discouraged.

Below are some normal-looking DNS labels that may grant some form of administrative control over the domain that they are attached to.

They are mostly "leftmost" or least-significant labels (in the sense used in Section 8 of [RFC8499]), in that if foo were listed here, it would be because granting control over the foo.example.net label (or control over the host pointed to by foo.example.net) to an untrusted party might offer that party some form of administrative control over other parts of example.org.

Note: where "<key-tag>" occurs in Table 1, it indicates any sequence of five or more decimal digits, as described in [RFC8509].

DNS Label	Rationale	Reference
autoconfig	Hijack mail user agent autoconfiguration	[AUTOCONF]
autodiscover	Hijack Microsoft Exchange client configuration	[AUTODISCOVER]
imap	Hijack mail user agent autoconfiguration	[AUTOCONF]
imaps	Hijack mail user agent autoconfiguration	[AUTOCONF]
mta-sts	Set SMTP transport security policy	[RFC8461]
openpgpkey	Domain-based OpenPGP certificate lookup and verification	[I-D.koch-openpgp-webkey-service]
pop3	Hijack mail user agent autoconfiguration	[AUTOCONF]
pop3s	Hijack mail user agent autoconfiguration	[AUTOCONF]
root-key-sentinel-is-ta-<key-tag>	Indicates which DNSSEC root key is trusted	[RFC8509]
root-key-sentinel-not-ta-<key-tag>	Indicates which DNSSEC root key is not trusted	[RFC8509]
smtp	Hijack mail user agent autoconfiguration	[AUTOCONF]
smtps	Hijack mail user agent autoconfiguration	[AUTOCONF]
submission	Hijack mail user agent autoconfiguration	[AUTOCONF]
wpad	Automatic proxy discovery	[I-D.ietf-wrec-wpad-01]
www	Popular web browsers guess this label	FIXME: find a reference

Table 1: Dangerous DNS labels

3. E-mail Local Parts

Section 3.4.1 of [RFC5322] defines the local-part of an e-mail address (the part before the "@" sign) as "domain-dependent". However, allocating some specific local-parts to an untrusted party can have significant security consequences for the domain or other associated resources.

Note that all these labels are expected to be case-insensitive. That is, an administrator restricting registration of a local-part named "admin" **MUST** also apply the same constraint to "Admin" or "ADMIN" or "aDmIn".

[RFC2142] offers some widespread historical practice for common local-parts. The CA/Browser Forum's Baseline Requirements ([CABForum-BR]) constrain how any popular Public Key Infrastructure (PKI) Certification Authority (CA) should confirm domain ownership when verifying by e-mail. The public CAs used by popular web browsers ("web PKI") will adhere to these guidelines, but anyone relying on unusual CAs may still be subject to risk additional labels described here.

E-mail local-part	**Rationale**	**References**
abuse	Receive reports of abusive public behavior	Section 2 of [RFC2142]
administrator	PKI Cert Issuance	Section 3.2.2.4.4 of [CABForum-BR]
admin	PKI Cert Issuance	Section 3.2.2.4.4 of [CABForum-BR]
hostmaster	PKI Cert Issuance, DNS zone control	Section 3.2.2.4.4 of [CABForum-BR], Section 7 of [RFC2142]
info	PKI Cert Issuance (historical)	[VU591120]
is	PKI Cert Issuance (historical)	[VU591120]
it	PKI Cert Issuance (historical)	[VU591120]
noc	Receive reports of network problems	Section 4 of [RFC2142]
postmaster	Receive reports related to SMTP service, PKI Cert Issuance	Section 5 of [RFC2142], Section 3.2.2.4.4 of [CABForum-BR]
root	Receive system software notifications, PKI Cert Issuance (historic)	[VU591120], FIXME: find a reference for root (software config docs?)
security	Receive reports of technical vulnerabilities	Section 4 of [RFC2142]
ssladministrator	PKI Cert Issuance (historical)	[VU591120]
ssladmin	PKI Cert Issuance (historical)	[VU591120]
sslwebmaster	PKI Cert Issuance (historical)	[VU591120]
sysadmin	PKI Cert Issuance (historical)	[VU591120]
webmaster	PKI Cert Issuance, Receive reports related to HTTP service	Section 3.2.2.4.4 of [CABForum-BR], Section 5 of [RFC2142]

E-mail local-part	Rationale	References
www	Common alias for webmaster	Section 5 of [RFC2142]

Table 2: Dangerous E-mail local-parts

4. Security Considerations

Allowing untrusted parties to allocate names with the labels associated in this document may grant access to administrative capabilities.

The administrator of a DNS or E-mail service that permits any untrusted party to register an arbitrary DNS label or e-mail local-part for their own use **SHOULD** reject attempts to register the labels listed here.

4.1. Additional Risks Out of Scope

The lists of security concerns in this document cover security risks and concerns associated with interoperable use of specific labels. They do not cover every possible security concern associated with any DNS label or e-mail localpart.

For example, DNS labels with an existing underscore are likely by construction to be sensitive, and are registered separately in the registry defined by [RFC8552].

Similarly, where humans or other systems capable of transcription error are in the loop, subtle variations of the labels listed here may also have security implications, due to homomgraphic confusion ([Homograph]), but this document does not attempt to enumerate all phishing, typosquatting, or similar risks of visual confusion, nor does it exhaustively list all other potential risks associated with variant encodings. See [UTR36] for a deeper understanding of these categories of security concerns.

Additionally, some labels may be associated with security concerns that happen to also commonly show up as DNS labels or e-mail local parts, but their risk is not associated with their use in interoperable public forms of DNS or e-mail. For example, on some systems, a local user account named backup has full read access to the local filesystem so that it can transfer data to the local backup system. And in some cases, the list of local user accounts is also aliased into e-mail local parts. However, permitting the registration of backup@example.net as an e-mail address is not itself an interoperable security risk -- no external third party will treat any part of the example.net domain differently because of

the registration. This document does not cover any risk entirely related to internal configuration choices.

5. IANA Considerations

This document asks IANA to establish two registries, from Table 1 and Table 2.

5.1. Dangerous DNS Labels Registry

The table of Dangerous DNS Labels (in Table 1) has three columns:

- *DNS Label (text string)
- *Rationale (human-readable short explanation)
- *References (pointer or pointers to more detailed documentation)

Note that this table does not include anything that should be handled by the pre-existing "Underscored and Globally Scoped DNS Node Names" registry defined by [RFC8552].

Following the guidance in [BCP26], any new entry to this registry will be assigned using Specification Required. The IESG will assign one or more designated experts for this purpose, who will consult with the IETF DNSOP working group mailing list or its designated successor. The Designated Expert will support IANA by clearly indicating when a new DNS label should be added to this table, offering the label itself, a brief rationale, and a pointer to the permanent and readily available documentation of the security consequences of the label. Updates or deletions of DNS Labels will follow the same process.

5.2. Dangerous E-mail Local Parts Registry

The table of Dangerous E-mail Local Parts (in Table 2 also has three columns:

- *E-mail local part (text string)
- *Rationale (human-readable short explanation)
- *References (pointer or ponters to more detailed documentation)

Following the guidance in [BCP26], any new entry to this registry will be assigned using Specification Required. The IESG will assign one or more designated experts for this purpose, who will consult with the IETF EMAILCORE working group mailing list or its designated successor. The Designated Expert will support IANA by clearly indicating when a new e-mail local part should be added to this

table, offering the local part itself, a brief rationale, and a pointer to the permanent and readily available documentation of the security consequences of the local part. Updates or deletions of of E-mail Local Parts will follow the same process.

5.3. Shared Considerations

Having to add a new security-sensitive entry to either of these tables is likely to be a bad idea, because existing DNS zones and e-mail installations may have already made an allocation of the novel label, and cannot avoid the security implications. For a new protocol that wants to include a label in either registry, there is almost always a better protocol design choice.

Yet, if some common practice permits any form of administrative control over a separate resource based on control over an arbitrary label, administrators need a central place to keep track of which labels are dangerous.

If such a practice cannot be avoided, it is better to ensure that the risk is documented clearly and referenced in the appropriate registry, rather than leaving it up to each administrator to re-discover the problem.

6. References

6.1. Normative References

[BCP26] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, June 2017. <https://www.rfc-editor.org/info/bcp26>

[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>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[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>.

[RFC8552] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/info/rfc8552>.

6.2. Informative References

[AUTOCONF] Wolf, A., "Mail Client Auto-Configuration", 22 February 2021, <https://roll.urown.net/server/mail/autoconfig.html>.

[AUTODISCOVER] Microsoft, "Autodiscover for Exchange", 15 January 2020, <https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/autodiscover-for-exchange>.

[CABForum-BR] CA/Browser Forum, "CA/Browser Forum Baseline Requirements", 23 April 2022, <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.4.pdf>.

[Homograph] Gabrilovich, E. and A. Gontmakher, "The homograph attack", Communications of the ACM vol. 45, no. 2, pp. 128, DOI 10.1145/503124.503156, February 2002, <https://doi.org/10.1145/503124.503156>.

[I-D.hoffman-dns-special-labels] Hoffman, P., "IANA Registry for Special Labels in the DNS", Work in Progress, Internet-Draft, draft-hoffman-dns-special-labels-00, 1 October 2018, <https://www.ietf.org/archive/id/draft-hoffman-dns-special-labels-00.txt>.

[I-D.ietf-wrec-wpad-01] Perkins, C. E., Cohen, J., Dunsmuir, M., Gauthier, P. A., Cooper, I., and J. W. C. M.A., "Web Proxy Auto-Discovery Protocol", Work in Progress, Internet-Draft, draft-ietf-wrec-wpad-01, 29 July 1999, <https://www.ietf.org/archive/id/draft-ietf-wrec-wpad-01.txt>.

[I-D.koch-openpgp-webkey-service] Koch, W., "OpenPGP Web Key Directory", Work in Progress, Internet-Draft, draft-koch-openpgp-webkey-service-14, 13 May 2022, <https://www.ietf.org/archive/id/draft-koch-openpgp-webkey-service-14.txt>.

[RFC2142] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, DOI 10.17487/RFC2142, May 1997, <https://www.rfc-editor.org/info/rfc2142>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-

STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8509] Huston, G., Damas, J., and W. Kumari, "A Root Key Trust Anchor Sentinel for DNSSEC", RFC 8509, DOI 10.17487/RFC8509, December 2018, <https://www.rfc-editor.org/info/rfc8509>.

[RFC8820] Nottingham, M., "URI Design and Ownership", BCP 190, RFC 8820, DOI 10.17487/RFC8820, June 2020, <https://www.rfc-editor.org/info/rfc8820>.

[UTR36] Davis, M. and M. Suignard, "Unicode Security Considerations", n.d., <https://unicode.org/reports/tr36/>.

[VU591120] CERT Coordination Center, "Multiple SSL certificate authorities use predefined email addresses as proof of domain ownership", 7 April 2015, <https://www.kb.cert.org/vuls/id/591120/>.

Appendix A. Acknowledgements

Many people created these dangerous labels or the authorization processes that rely on them over the years.

Dave Crocker wrote an early list of special e-mail local-parts, from [RFC2142].

Paul Hoffman tried to document a wider survey of special DNS labels (not all security-sensitive) in [I-D.hoffman-dns-special-labels].

Rasmus Dahlberg, yuki, and Carsten Bormann reviewed this draft and gave feedback.

Tim Wicinski pointed out wpad.

Appendix B. Document Considerations

This section is to be removed before publishing as an RFC.

B.1. Other types of labels?

This document is limited to leftmost DNS labels and e-mail local-parts because those are the arbitrary labels that the author is familiar with. There may be other types of arbitrary labels on the

Internet with special values that have security implications that the author is not aware of. If you are aware of some other system with a similar pattern, please send feedback.

B.2. Document History

B.2.1. Substantive Changes from -01 to -02

* New dangerous DNS labels: WPAD, MS Exchange Autodiscover, common MUA autoconfig (originally from Mozilla Thunderbird)

B.2.2. Substantive Changes from -00 to -01

* explicitly define IANA tables

* indicate that the tables use Specification Required

* clarify scope

Author's Address

Daniel Kahn Gillmor
American Civil Liberties Union
United States of America

Email: dkg@fifthhorseman.net