Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 22, 2020

E. Foudil

Y. Shafranovich
Nightwatch Cybersecurity
November 19, 2019

A Method for Web Security Policies
draft-foudil-securitytxt-08

Abstract

When security vulnerabilities are discovered by independent security researchers, they often lack the channels to report them properly. As a result, security vulnerabilities may be left unreported. This document defines a format ("security.txt") to help organizations describe the process for security researchers to follow in order to report security vulnerabilities.

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 May 22, 2020.

Table of Contents

1. Introduction

1.1. Motivation, Prior Work and Scope

Many security researchers encounter situations where they are unable to report security vulnerabilities to organizations because there is no course of action laid out and no way indicated to contact the owner of a particular resource.

As per section 4 of [RFC2142], there is an existing convention of using the <SECURITY@domain> email address for communications regarding security vulnerabilities. That convention provides only a single, email-based channel of communication for security vulnerabilities per domain, and does not provide a way for domain owners to publish information about their security disclosure policies.

There are also contact conventions prescribed for Internet Service Providers (ISPs) in section 2 of [RFC3013], for Computer Security Incident Response Teams (CSIRTs) in section 3.2 of [RFC2350] and for site operators in section 5.2 of [RFC2196]. As per [RFC7485], there is also contact information provided by Regional Internet Registries (RIRs) and domain registries for owners of IP addresses, autonomous system numbers (ASNs) and domain names. However, none of these address the issue of how security researchers can locate disclosure policies and contact information for organizations in order to report security vulnerabilities.

In this document, we define a richer, machine-parsable and extensible way for organizations to communicate information about their security disclosure policies, which is not limited to email and also allows for additional features such as encryption. This format is designed to help assist with the security disclosure process by making it easier for organizations to designate the preferred steps for researchers to take when trying to reach out to them with security vulnerabilities.

Other details of vulnerability disclosure are outside the scope of this document. Readers are encouraged to consult other documents such as [ISO.29147.2018] or [CERT.CVD].

1.2. Terminology

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. Note to Readers

> *Note to the RFC Editor:* Please remove this section prior to publication.

Development of this draft takes place on Github at: https://github.com/securitytxt/security-txt

3. The Specification

This document defines a text file to be placed in a known location that provides information for security researchers to assist in disclosing security vulnerabilities.

The file is named "security.txt", and this file SHOULD be placed under the /.well-known/ path ("/.well-known/security.txt") [RFC8615] of a domain name or IP address for web properties. For legacy compatibility, a security.txt file might be placed at the top level path (see Section 4.1).

For web-based services, the file MUST be accessible via the Hypertext Transfer Protocol (HTTP) [RFC1945] as a resource of Internet Media Type "text/plain" with the default charset parameter set to "utf-8" per section 4.1.3 of [RFC2046], and it MUST be served with "https" (as per section 2.7.2 of [RFC7230]). For file systems and version control repositories a "security.txt" file SHOULD be placed in the root directory of a particular file system or source code project.

This text file contains multiple directives with different values. The "directive" is the first part of a field all the way up to the colon ("Contact:") and follows the syntax defined for "field-name" in section 3.6.8 of [RFC5322]. Directives are case-insensitive (as per section 2.3 of [RFC5234]). The "value" comes after the directive ("https://example.com/security") and follows the syntax defined for "unstructured" in section 3.2.5 of [RFC5322].

A "field" MUST always consist of a directive and a value ("Contact: https://example.com/security"). A security.txt file can have an unlimited number of fields. It is important to note that each field MUST appear on its own line. Unless specified otherwise by the field definition, multiple values MUST NOT be chained together for a single directive. Unless otherwise indicated in a definition of a particular field, any directive MAY appear multiple times.

3.1. Scope of the File

A "security.txt" file MUST only apply to the domain in the URI used to retrieve it, not to any of its subdomains or parent domains. A "security.txt" file that is found in a file system or version control repository MUST only apply to the folder or repository in which it is located, and not to any of its parent or sibling folders, or repositories. However, it will apply to all subfolders.

Some examples appear below:

```
# The following only applies to example.com.
https://example.com/.well-known/security.txt

# This only applies to subdomain.example.com.
https://subdomain.example.com/.well-known/security.txt

# This security.txt file applies to IPv4 address of 192.0.2.0.
https://192.0.2.0/.well-known/security.txt

# This security.txt file applies to IPv6 address of 2001:db8:8:4::2.
https://[2001:db8:8:4::2]/.well-known/security.txt

# This file applies to the /example/folder1 directory and subfolders.
/example/folder1/security.txt
```

3.2. Comments

Any line beginning with the "#" (%x30) symbol MUST be interpreted as a comment. The content of the comment may contain any ASCII or Unicode characters in the %x21-7E and %x80-FFFFF ranges plus the tab (%x09) and space (%x20) characters.

Example:

```
# This is a comment.
```

One or more comments MAY be used as descriptive text immediately before the field. Parsers SHOULD associate the comments with the

respective field. Only the line most immediately preceding a field SHOULD be associated with that field.

3.3. Line Separator

Every line MUST end either with a carriage return and line feed characters (CRLF / %x0D %x0A) or just a line feed character (LF / %x0A).

3.4. Digital signature

It is RECOMMENDED that a security.txt file be digitally signed using an OpenPGP cleartext signature as described in section 7 of [RFC4880]. When digital signatures are used, it is also RECOMMENDED that implementors use the "Canonical" directive (as per Section 3.5.2), thus allowing the digital signature to authenticate the location of the file.

When it comes to verifying the key used to generate the signature, it is always the security researcher's responsibility to make sure the key being used is indeed one they trust.

3.5. Field Definitions

3.5.1. Acknowledgments

This directive indicates a link to a page where security researchers are recognized for their reports. The page being referenced SHOULD list individuals or organizations that reported security vulnerabilities and collaborated to remediate them. Organizations SHOULD be careful to limit the vulnerability information being published in order to prevent future attacks.

If this directive indicates a web URL, then it MUST begin with "https://" (as per section 2.7.2 of [RFC7230]).

Example:

Acknowledgments: https://example.com/hall-of-fame.html

Example security acknowledgments page:

We would like to thank the following researchers:

(2017-04-15) Frank Denis - Reflected cross-site scripting
(2017-01-02) Alice Quinn - SQL injection
(2016-12-24) John Buchner - Stored cross-site scripting
(2016-06-10) Anna Richmond - A server configuration issue

3.5.2. Canonical

This directive indicates the canonical URI where the security.txt file is located, which is usually something like "https://example.com/.well-known/security.txt". If this directive indicates a web URL, then it MUST begin with "https://" (as per section 2.7.2 of [RFC7230]). The purpose of this directive is to allow a digital signature to be applied to the location of the "security.txt" file.

This directive MUST NOT appear more than once.

Canonical: https://example.com/.well-known/security.txt

3.5.3. Contact

This directive indicates an address that researchers should use for reporting security vulnerabilities. The value MAY be an email address, a phone number and/or a web page with contact information. The "Contact:" directive MUST always be present in a security.txt file. If this directive indicates a web URL, then it MUST begin with "https://" (as per section 2.7.2 of [RFC7230]). Security email addresses SHOULD use the conventions defined in section 4 of [RFC2142].

The value MUST follow the URI syntax described in [RFC3986]. This means that "mailto" and "tel" URI schemes MUST be used when specifying email addresses and telephone numbers, as defined in [RFC6068] and [RFC3966]. When the value of this directive is an email address, it is RECOMMENDED that encryption be used (as per Section 3.5.4).

The precedence SHOULD be in listed order. The first field is the preferred method of contact. In the example below, the email address is the preferred method of contact.

Contact: mailto:security@example.com
Contact: tel:+1-201-555-0123
Contact: https://example.com/security-contact.html

3.5.4. Encryption

This directive indicates an encryption key that security researchers SHOULD use for encrypted communication. Keys MUST NOT appear in this field - instead the value of this field MUST be a URI pointing to a location where the key can be retrieved. If this directive indicates a web URL, then it MUST begin with "https://" (as per section 2.7.2 of [RFC7230]).

When it comes to verifying the authenticity of the key, it is always the security researcher's responsibility to make sure the key being specified is indeed one they trust. Researchers MUST NOT assume that this key is used to generate the digital signature referenced in Section 3.4.

Example of an OpenPGP key available from a web server:

Encryption: https://example.com/pgp-key.txt

Example of an OpenPGP key available from an OPENPGPKEY DNS record:

Encryption: dns:5d2d37ab76d47d36._openpgpkey.example.com?type=OPENPGPKEY

Example of an OpenPGP key being referenced by its fingerprint:

Encryption: openpgp4fpr:5f2de5521c63a801ab59ccb603d49de44b29100f

3.5.5. Hiring

The "Hiring" directive is used for linking to the vendor's security-related job positions. If this directive indicates a web URL, then it MUST begin with "https://" (as per section 2.7.2 of [RFC7230]).

Hiring: https://example.com/jobs.html

3.5.6. Policy

This directive indicates a link to where the security policy and/or disclosure policy is located. This can help security researchers understand what an organization is looking for and how to report security vulnerabilities. If this directive indicates a web URL, then it MUST begin with "https://" (as per section 2.7.2 of [RFC7230]).

Example:

Policy: https://example.com/security-policy.html

3.5.7. Preferred-Languages

This directive can be used to indicate a set of natural languages that are preferred when submitting security reports. This set MAY list multiple values, separated by commas. If this directive is included then at least one value MUST be listed. The values within this set are language tags (as defined in [RFC5646]). If this directive is absent, security researchers MAY assume that English is the default language to be used (as per section 4.5 of [RFC2277]).

The order in which they appear MUST NOT be interpreted as an indication of priority - rather these MUST be interpreted as all being of equal priority.

This directive MUST NOT appear more than once.

Example (English, Spanish and French):

Preferred-Languages: en, es, fr

3.6. Example of an unsigned "security.txt" file

```
# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html
```

3.7. Example of a signed "security.txt" file

```
----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

# Canonical URL
Canonical: https://example.com/.well-known/security.txt

# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2

[signature]
-----END PGP SIGNATURE-----
```

4. Location of the security.txt file

4.1. Web-based services

Web-based services SHOULD place the security.txt file under the /.well-known/ path; e.g. https://example.com/.well-known/security.txt as per [RFC8615]. For legacy compatibility, a security.txt file might be placed at the top-level path or redirect (as per section 6.4 of [RFC7231]) to the security.txt file under the /.well-known/ path.

If retrieval of a "security.txt" file from the top-level path results in a redirect (as per section 6.4 of [RFC7231]), the implementors MUST NOT follow that redirect if it leads to another domain or subdomain but SHOULD follow that redirect within the same domain name (but not different subdomain on the same domain).

The guidance regarding redirects SHOULD NOT apply to the resource locations that appear within the file.

4.2. Filesystems

File systems SHOULD place the "security.txt" file under the root directory; e.g., "/security.txt", "C:\security.txt".

Example file system:

```
/example-directory-1/
/example-directory-2/
/example-directory-3/
/example-file
/security.txt
```

4.3. Internal hosts

An internal host is "a host served by a NAT gateway, or protected by a firewall" (as per section 3 of [RFC6887]) and might not be accessible directly from the Internet. On such systems, a "security.txt" file SHOULD be placed in the root directory.

4.4. Extensibility

Like many other formats and protocols, this format may need to be extended over time to fit the ever-changing landscape of the Internet. Therefore, extensibility is provided via an IANA registry for directives as defined in Section 7.2. Any directives registered via that process MUST be considered optional. To encourage extensibility and interoperability, implementors MUST ignore any fields they do not explicitly support.

In general, implementors SHOULD "be conservative in what you do, be liberal in what you accept from others" (as per [RFC0793]).

5. File Format Description and ABNF Grammar

The expected file format of the security.txt file is plain text (MIME type "text/plain") as defined in section 4.1.3 of [RFC2046] and is encoded using UTF-8 [RFC3629] in Net-Unicode form [RFC5198].

The following is an ABNF definition of the security.txt format, using the conventions defined in [RFC5234].

```
body             =  signed / unsigned

signed           =  sign-header unsigned sign-footer

sign-header      =  < headers and line from section 7 of [RFC4880] >

sign-footer      =  < OpenPGP signature from section 7 of [RFC4880] >

unsigned         =  *line [can-field eol]
                    *line (contact-field eol)
                    *line [lang-field eol] *line
                    ; the order of elements is not important

line             =  (field / comment) eol

eol              =  *WSP [CR] LF

field            =  ack-field /
                    contact-field /
                    encryption-field /
                    hiring-field /
                    policy-field /
                    ext-field

fs               =  ":"

comment          =  "#" *(WSP / VCHAR / %x80-FFFFF)

ack-field        =  "Acknowledgments" fs SP uri

can-field        =  "Canonical" fs SP uri

contact-field    =  "Contact" fs SP uri

lang-tag         =  < Language-Tag from section 2.1 of [RFC5646] >
```

```
uri              =  < URI as per [RFC3986] >

encryption-field =  "Encryption" fs SP uri

hiring-field     =  "Hiring" fs SP uri

policy-field     =  "Policy" fs SP uri

lang-field       =  "Preferred-Languages" fs SP lang-values

lang-values      =  lang-tag *(*WSP "," *WSP lang-tag)

ext-field        =  field-name fs SP unstructured

field-name       =  < imported from section 3.6.8 of [RFC5322] >

unstructured     =  < imported from section 3.2.5 of [RFC5322] >
```

"ext-field" refers to extension fields, which are discussed in Section 4.4

6. Security Considerations

In addition to the security considerations of [RFC8615], the following considerations apply.

6.1. Compromised Files and Redirects

An attacker that has compromised a website is able to compromise the "security.txt" file as well or setup a redirect to their own site. This can result in security reports not being received by the organization or sent to the attacker.

To protect against this, organizations SHOULD digitally sign their "security.txt" files (as per Section 3.4), use the canonical directive to sign the location of the file (as per Section 3.5.2), and regularly monitor the file and the referenced resources to detect tampering.

Security researchers SHOULD check the "security.txt" file including verifying the digital signature and checking any available historical records before using the information contained in the file. If "security.txt" file looks suspicious or compromised, it SHOULD NOT be used.

To avoid redirect attacks, redirects for these files MUST NOT be followed when the file is placed in the top level path and they lead to a different domain (as per Section 4.1). This restriction is

because the top level path is potentially more likely to be compromised as opposed to the ".well-known" path.

6.2. Incorrect or Stale Information

If information and resources referenced in a "security.txt" file are incorrect or not kept up to date, this can result in security reports not being received by the organization or sent to incorrect contacts, thus exposing possible security issues to third parties. Not having a security.txt file may be preferable to having stale information in this file.

Organizations SHOULD ensure that information in this file and any referenced resources such as web pages, email addresses and telephone numbers are kept current, are accessible, controlled by the organization, and are kept secure.

6.3. Intentionally Malformed Files, Resources and Reports

It is possible for compromised or malicious sites to create files that are extraordinarily large or otherwise malformed in an attempt to discover or exploit weaknesses in parsing code. Implementors SHOULD make sure that any such code is robust against large and malformed files. The ABNF grammar (as defined in Section 5) SHOULD be used as a way to verify these files.

The same concerns apply to any other resources referenced within security.txt files, as well as any security reports received as a result of publishing this file. Such resources and reports may be hostile, malformed or malicious.

6.4. No Implied Permission for Testing

The presence of a security.txt file might be interpreted by researchers as providing permission to do security testing against that asset. This might result in increased testing against an organization by researchers. On the other hand, a decision not to publish a security.txt file might be interpreted by the organization operating that website to be a way to signal to researchers that permission to test that particular site or project is denied. This might result in pushback against researchers reporting security issues to that organization.

Therefore, implementors MUST NOT assume that presence or absence of a "security.txt" file grants or denies permission for security testing. Any such permission MAY be defined in a security or disclosure policy (as per Section 3.5.6) or a new directive (as per Section 4.4).

6.5. Multi-user Environments

In multi-user / multi-tenant environments, it may possible for a user to take over the location of the "security.txt" file. Organizations SHOULD reserve the "security.txt" namespace at the root to ensure no third-party can create a page with the "security.txt" AND "/.well-known/security.txt" names.

6.6. Protecting Data in Transit

To protect a "security.txt" file from being tampered with in transit, implementors MUST use HTTPS (as per [RFC2818]) when serving the file itself and for retrieval of any web URLs referenced in it (except when otherwise noted in this specification). As part of the TLS handshake, implementors MUST validate the provided X.509 certificate in accordance with [RFC6125] and the following considerations:

- Matching is performed only against the DNS-ID identifiers.
- DNS domain names in server certificates MAY contain the wildcard character '*' as the complete left-most label within the identifier.

The certificate MAY be checked for revocation via the Online Certificate Status Protocol (OCSP) [RFC6960], certificate revocation lists (CRLs), or similar mechanisms.

As an additional layer of protection, it is also RECOMMENDED that organizations digitally sign their "security.txt" file with OpenPGP (as per Section 3.4). Also, to protect security reports from being tampered with or observed while in transit, organizations SHOULD specify encryption keys (as per Section 3.5.4) unless HTTPS is being used.

However, the determination of validity of such keys is out of scope for this specification. Implementors MUST establish other secure means to verify them.

6.7. Spam and Spurious Reports

Similar to concerns in [RFC2142], denial of service attacks via spam reports would become easier once a "security.txt" file is published by an organization. In addition, there is an increased likelihood of reports being sent in an automated fashion and/or as result of automated scans without human triage.

Organizations SHOULD weigh the advantages of publishing this file versus the possible disadvantages and increased resources required to triage security reports.

Security researchers SHOULD consult the organization's policy, if available, before submitting reports in an automated fashion or as resulting from automated scans.

7. IANA Considerations

example.com is used in this document following the uses indicated in [RFC2606].

192.0.2.0 and 2001:db8:8:4::2 are used in this document following the uses indicated in [RFC6890].

7.1. Well-Known URIs registry

The "Well-Known URIs" registry should be updated with the following additional values (using the template from [RFC8615]):

URI suffix: security.txt

Change controller: IETF

Specification document(s): this document

Status: permanent

7.2. Registry for security.txt Header Fields

IANA is requested to create the "security.txt Header Fields" registry in accordance with [RFC8126]. This registry will contain header fields for use in security.txt files, defined by this specification.

New registrations or updates MUST be published in accordance with the "Expert Review" guidelines as described in sections 4.5 and 5 of [RFC8126]. Any new field thus registered is considered optional by this specification unless a new version of this specification is published.

Designated Experts are expected to check whether a proposed registration or update makes sense in the context of this specification and provides value to the wider Internet community.

New registrations and updates MUST contain the following information:

1. Name of the field being registered or updated

2. Short description of the field

3. Whether the field can appear more than once

4. The document in which the specification of the field is published (if available)

5. New or updated status, which MUST be one of:

   * current: The field is in current use

   * deprecated: The field is in current use, but its use is discouraged

   * historic: The field is no longer in current use

6. Change controller

An update may make a notation on an existing registration indicating that a registered field is historical or deprecated if appropriate.

The initial registry contains these values:

Field Name: Acknowledgments
Description: link to page where security researchers are recognized
Multiple Appearances: Yes
Published in: this document
Status: current
Change controller: IESG

Field Name: Canonical
Description: canonical URL for this file
Multiple Appearances: No
Published in: this document
Status: current
Change controller: IESG

Field Name: Contact
Description: contact information to use for reporting vulnerabilities
Multiple Appearances: Yes
Published in: this document
Status: current
Change controller: IESG

Field Name: Encryption
Description: link to a key to be used for encrypted communication
Multiple Appearances: Yes
Published in: this document
Status: current
Change controller: IESG

Field Name: Hiring
Description: link to the vendor's security-related job positions
Multiple Appearances: Yes
Published in: this document
Status: current
Change controller: IESG

Field Name: Policy
Description: link to security policy page
Multiple Appearances: Yes
Published in: this document
Status: current
Change controller: IESG

Field Name: Preferred-Languages
Description: list of preferred languages for security reports
Multiple Appearances: No
Published in: this document
Status: current
Change controller: IESG

8. Contributors

The authors would like to acknowledge the help provided during the development of this document by Tom Hudson, Jobert Abma, Gerben Janssen van Doorn, Austin Heap, Stephane Bortzmeyer, Max Smith, Eduardo Vela and Krzysztof Kotowicz.

The authors would also like to acknowledge the feedback provided by multiple members of IETF's SAAG and SECDISPATCH lists.

9. References

9.1. Normative References

[RFC1945] Berners-Lee, T., Fielding, R., and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", RFC 1945, DOI 10.17487/RFC1945, May 1996, <https://www.rfc-editor.org/info/rfc1945>.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[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>.

[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>.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <https://www.rfc-editor.org/info/rfc2277>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[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>.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <https://www.rfc-editor.org/info/rfc3966>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[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>.

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

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

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <https://www.rfc-editor.org/info/rfc5646>.

[RFC6068] Duerst, M., Masinter, L., and J. Zawinski, "The 'mailto' URI Scheme", RFC 6068, DOI 10.17487/RFC6068, October 2010, <https://www.rfc-editor.org/info/rfc6068>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <https://www.rfc-editor.org/info/rfc6887>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[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>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

9.2. Informative References

[CERT.CVD] Software Engineering Institute, Carnegie Mellon University, "The CERT Guide to Coordinated Vulnerability Disclosure (CMU/SEI-2017-SR-022)", 2017.

[ISO.29147.2018] International Organization for Standardization (ISO), "ISO/IEC 29147:2018, Information technology -- Security techniques -- Vulnerability disclosure", 2018.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, DOI 10.17487/RFC2196, September 1997, <https://www.rfc-editor.org/info/rfc2196>.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", BCP 21, RFC 2350, DOI 10.17487/RFC2350, June 1998, <https://www.rfc-editor.org/info/rfc2350>.

[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>.

[RFC3013] Killalea, T., "Recommended Internet Service Provider Security Services and Procedures", BCP 46, RFC 3013, DOI 10.17487/RFC3013, November 2000, <https://www.rfc-editor.org/info/rfc3013>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[RFC7485] Zhou, L., Kong, N., Shen, S., Sheng, S., and A. Servin, "Inventory and Analysis of WHOIS Registration Objects", RFC 7485, DOI 10.17487/RFC7485, March 2015, <https://www.rfc-editor.org/info/rfc7485>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Appendix A. Note to Readers

Note to the RFC Editor: Please remove this section prior to publication.

Development of this draft takes place on Github at https://github.com/securitytxt/security-txt

Appendix B. Document History

Note to the RFC Editor: Please remove this section prior to publication.

B.1. Since draft-foudil-securitytxt-00

- Moved to use IETF's markdown tools for draft updates
- Added table of contents and a fuller list of references
- Moved file to .well-known URI and added IANA registration (#3)
- Added extensibility with an IANA registry for fields (#34)
- Added text explaining relationship to RFC 2142 / security@ email address (#25)
- Scope expanded to include internal hosts, domains, IP addresses and file systems

- Support for digital signatures added (#19)

The full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt-01

B.2. Since draft-foudil-securitytxt-01

- Added appendix with pointer to Github and document history
- Added external signature file to the well known URI registry (#59)
- Added policy field (#53)
- Added diagram explaining the location of the file on public vs. internal systems
- Added recommendation that external signature files should use HTTPS (#55)
- Added recommendation that organizations should monitor their security.txt files (#14)

The full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt-02

B.3. Since draft-foudil-securitytxt-02

- Use "mailto" and "tel" (#62)
- Fix typo in the "Example" section (#64)
- Clarified that the root directory is a fallback option (#72)
- Defined content-type for the response (#68)
- Clarify the scope of the security.txt file (#69)
- Cleaning up text based on the NITS tools suggestions (#82)
- Added clarification for newline values
- Clarified the encryption field language, added examples of DNS-stored encryption keys (#28 and #94)
- Added "Hiring" field

B.4. Since draft-foudil-securitytxt-03

- Added "Hiring" field to the registry section
- Added an encryption example using a PGP fingerprint (#107)
- Added reference to the mailing list (#111)
- Added a section referencing related work (#113)
- Fixes for idnits (#82)
- Changing some references to informative instead of normative
- Adding "Permission" field (#30)
- Fixing remaining ABNF issues (#83)
- Additional editorial changes and edits

B.5. Since draft-foudil-securitytxt-04

- Addressing IETF feedback (#118)
- Case sensitivity clarification (#127)
- Syntax fixes (#133, #135 and #136)
- Removed permission directive (#30)
- Removed signature directive and switched to inline signatures (#93 and #128)
- Adding canonical directive (#100)
- Text and ABNF grammar improvements plus ABNF changes for comments (#123)
- Changed ".security.txt" to "security.txt" to be consistent

B.6. Since draft-foudil-securitytxt-05

- Changing HTTPS to MUST (#55)
- Adding language recommending encryption for email reports (#134)
- Added language handling redirects (#143)

- Expanded security considerations section and fixed typos (#30, #73, #103, #112)

B.7. Since draft-foudil-securitytxt-06

- Fixed ABNF grammar for non-chainable directives (#150)
- Clarified ABNF grammar (#152)
- Clarified redirect logic (#143)
- Clarified comments (#158)
- Updated references and template for well-known URI to RFC 8615
- Fixed nits from the IETF validator

B.8. Since draft-foudil-securitytxt-07

- Addressing AD feedback (#165)
- Fix for ABNF grammar in lang-values (#164)
- Fixing idnits warnings
- Adding guidance for designated experts

Full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt

Authors' Addresses

Edwin Foudil

Email: contact@edoverflow.com

Yakov Shafranovich
Nightwatch Cybersecurity

Email: yakov+ietf@nightwatchcybersecurity.com