Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 13, 2018

E. Foudil

Y. Shafranovich
Nightwatch Cybersecurity
February 09, 2018

A Method for Web Security Policies
draft-foudil-securitytxt-03

Abstract

When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. security.txt defines a standard to help organizations describe the process for security researchers to disclose security vulnerabilities securely.

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 August 13, 2018.

Copyright Notice

Table of Contents

1. Introduction

1.1. Motivation

Many security researchers encounter situations where they are unable to responsibly disclose security issues to companies because there is no course of action laid out. security.txt is designed to help assist

in this process by making it easier for companies to designate the preferred steps for researchers to take when trying to reach out.

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

In this document, we propose a richer, machine-parsable and more extensible way for companies to communicate information about their security disclosure policies, which is not limited to email and also allows for additional features such as encryption.

1.2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119].

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

security.txt is a text file that SHOULD be located under the /.well-known/ path ("/.well-known/security.txt") [RFC5785] for web properties. If it is not possible to place the security.txt file in the /.well-known/ path or setup a redirect, web-based services MAY place the file in the top-level path as a fall back option. For web-based services, the instructions MUST be accessible via the Hypertext Transfer Protocol [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]. For file systems and version control repositories a .security.txt file SHOULD be placed in the root directory.

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:"). Directives are case-insensitive. The "value" comes after the directive ("https://example.com/security"). A "field" always consists 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 you need a separate line for every field. One MUST NOT chain multiple values for a single directive. Everything MUST be in a separate field.

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.

```
# 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.
http://192.0.2.0/.well-known/security.txt

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

3.1. Comments

Comments can be added using the # symbol:

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

You MAY use one or more comments as descriptive text immediately before the field. Parsers can then associate the comments with the respective field.

3.2. Separate Fields

A separate line is required for every new value and field. You MUST NOT chain everything into a single field. Every line MUST end either with a carriage return and line feed characters (CRLF / %x0D %x0A) or just a line feed character (LF / %x0A).

3.3. Contact:

Add an address that researchers MAY use for reporting security issues. The value can be an email address, a phone number and/or a contact page with more information. The "Contact:" directive MUST always be present in a security.txt file. URIs SHOULD be loaded over HTTPS. Security email addresses SHOULD use the conventions defined in section 4 of [RFC2142], but there is no requirement for this directive to be an email address.

The value MUST follow the general syntax described in [RFC3986]. This means that "mailto" and "tel" URI schemes MUST be used when specifying email addresses and telephone numbers.

The precedence is in listed order. The first field is the preferred method of contact. In the example below, the e-mail 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

3.4. Encryption:

This directive allows you to point to an encryption key that you want security researchers to use for encrypted communication. You MUST NOT directly add your key to the field, instead the value of this field MUST be a URI pointing to a location where the key can be retrieved from. If the key is being retrieved from a website, then the key MUST be loaded over HTTPS.

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 signature file referenced in Section 3.5.

Example of a PGP key available from a web server:

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

Example of a PGP key available from an OPENPGPKEY DNS record under "security@example.com" (as per [RFC7553] and [RFC7929]):

Encryption: dns:5d2d3ceb7abe552344276d47d36._openpgpkey.example.com?type=OPENPGPKEY

3.5. Signature:

In order to ensure the authenticity of the security.txt file one SHOULD use the "Signature:" directive, which allows you to link to an external signature by specifying the full URI where the signature is located as per [RFC3986]. External signature files SHOULD be named "security.txt.sig" and also be placed under the /.well-known/ path. External signature files SHOULD be loaded over HTTPS.

When it comes to verifying the authenticity of the file, it is always the security researcher’s responsibility to make sure the key being specified is indeed one they trust.

Here is an example of an external signature file.

Signature: https://example.com/.well-known/security.txt.sig

3.6. Policy:

With the Policy directive, you can link to where your security policy and/or disclosure policy is located. This can help security researchers understand what you are looking for and how to report security vulnerabilities.

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

3.7. Acknowledgments:

This directive allows you to link to a page where security researchers are recognized for their reports. The page SHOULD list individuals or companies that disclosed security vulnerabilities and worked with you to remediate the issue.

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

3.8. Hiring:

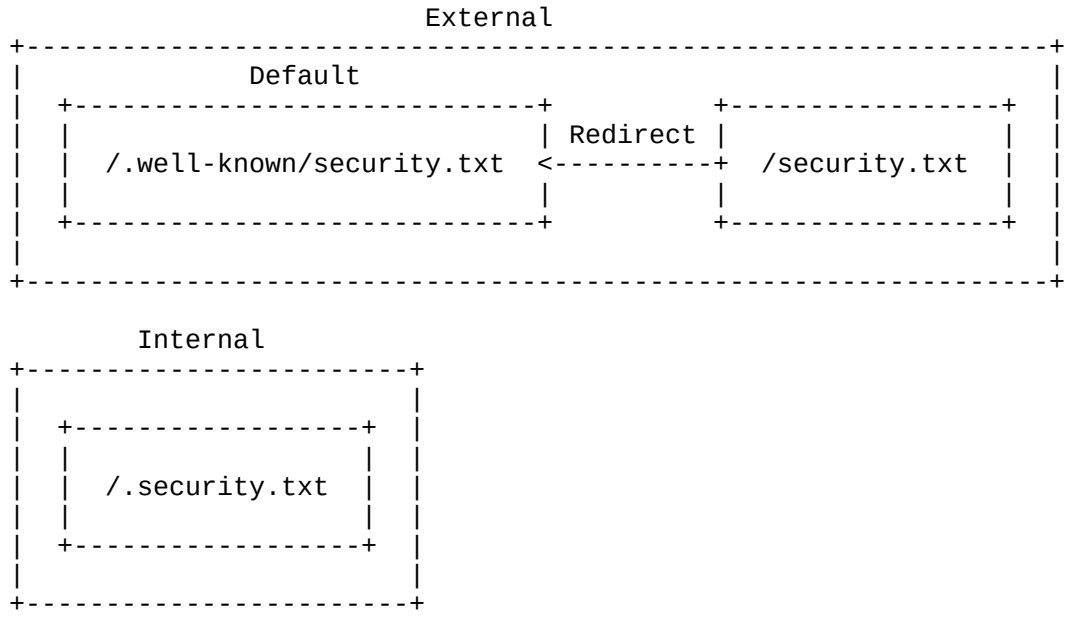
The "Hiring" directive is for linking to the vendor’s security-related job positions.

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

3.9. Example

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

# Our PGP 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

# Verify this security.txt file
Signature: https://example.com/.well-known/security.txt.sig
```

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. A security.txt file located under the top-level path SHOULD either redirect to the security.txt file under the /.well-known/ path or be used as a fall back.

4.2. Filesystems

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

```
user:/$ l
.security.txt
example-directory-1/
example-directory-2/
example-directory-3/
example-file
```

4.3. Internal hosts

A .security.txt file SHOULD be placed in the root directory of an internal host to trigger incident response.

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 headers fields as defined in Section 7.2. Any fields registered via that process MUST be considered optional. To encourage extensibility and interoperability, implementors MUST ignore any fields they do not explicitly support.

5. File Format Description

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                    = *line (contact-field eol) *line

   line                    = *1(field / comment) eol

   eol                     = *WSP \[CR\] LF

   field                   = contact-field /
                             encryption-field /
                             acknowledgments-field /
                             ext-field

   fs                      = ":"

   comment                 = "#" *(WSP / VCHAR / %xA0-E007F)

   contact-field           = "Contact" fs SP (email / uri / phone)

   email                   = <Email address as per {{RFC5322}}>

   phone                   = "+" *1(DIGIT / "-" / "(" / ")" / SP)

   uri                     = <URI as per {{RFC3986}}>

   encryption-field        = "Encryption" fs SP uri

   signature-field         = "Signature" fs SP uri

   policy-field            = "Policy" fs SP uri

   acknowledgments-field   = "Acknowledgments" fs SP uri

   hiring-field            = "Hiring" fs SP uri

   ext-field               = field-name fs SP unstructured

   field-name              = <as per section 3.6.8 of {{RFC5322}}>

   unstructured            = <as per section 3.2.5 of {{RFC5322}}>
```

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

6. Security considerations

Organizations creating security.txt files will need to consider several security-related issues. These include exposure to sensitive information and attacks where limited access to a server could grant the ability to modify the contents of the security.txt file or affect

how it is served. Organizations SHOULD also monitor their security.txt files regularly to detect tampering.

To ensure the authenticity of the security.txt file, organizations SHOULD sign the file and include the signature using the "Signature:" directive.

As stated in Section 3.4 and Section 3.5, both encryption keys and external signature files SHOULD be loaded over HTTPS.

Websites MUST reserve the security.txt namespace to ensure no third-party can create a page with the "security.txt" name.

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 [RFC5785]):

URI suffix: security.txt

URI suffix: security.txt.sig

Change controller: IETF

Specification document(s): this document

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 "Specification Required" guidelines as described in section 4.6 of [RFC8126]. Any new field thus registered is considered optional by this specification unless a new version of this specification is published.

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

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

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: Acknowledgment
Description: link to page where security researchers are recognized
Multiple Appearances: Yes
Published in: this document
Status: current

Field Name: Contact
Description: contact information to use for reporting security issues
Multiple Appearances: Yes
Published in: this document
Status: current

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

Field Name: Signature
Description: signature used to verify the authenticity of the file
Multiple Appearances: No
Published in: this document
Status: current

Field Name: Policy
Description: link to security policy page
Multiple Appearances: No
Published in: this document
Status: current

8. Contributors

The editors would like to acknowledge the help provided during the development of this document by Tom Hudson, Joel Margolis, Jobert Abma, Gerben Janssen van Doorn, Austin Heap, Justin Calmus, and Casey Ellis.

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>.

[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>.

[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>.

[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>.

[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>.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, DOI 10.17487/RFC5785, April 2010, <https://www.rfc-editor.org/info/rfc5785>.

[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>.

[RFC7553] Faltstrom, P. and O. Kolkman, "The Uniform Resource Identifier (URI) DNS Resource Record", RFC 7553, DOI 10.17487/RFC7553, June 2015, <https://www.rfc-editor.org/info/rfc7553>.

[RFC7929] Wouters, P., "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP", RFC 7929, DOI 10.17487/RFC7929, August 2016, <https://www.rfc-editor.org/info/rfc7929>.

9.2. Informative References

[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 fall back 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)

Full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt-03

Authors' Addresses

Edwin Foudil

Email: contact@edoverflow.com

Yakov Shafranovich
Nightwatch Cybersecurity

Email: yakov+ietf@nightwatchcybersecurity.com