Network Working Group
Internet-Draft
Intended status: Informational
Expires: 19 June 2023

H. Marques
B. Hoeneisen
pEp Foundation

16 December 2022

pretty Easy privacy (pEp): Mapping of Privacy Rating
draft-pep-rating-00

Abstract

In many Opportunistic Security scenarios end-to-end encryption is automatized for Internet users. In addition, it is often required to provide the users with easy means to carry out authentication.

Depending on several factors, each communication channel to different peers may have a different Privacy Status, e.g., unencrypted, encrypted and encrypted as well as authenticated. Also each message from/to a single peer may have a different Privacy Status.

To display the actual Privacy Status to the user, this document defines a Privacy Rating scheme and its mapping to a traffic-light semantics. A Privacy Status is defined on a per-message basis as well as on a per-identity basis. The traffic-light semantics (as color and symbol rating) allows for a clear and easily understandable presentation to the user in order to optimize User Experience.

This rating system is most beneficial to Opportunistic Security scenarios and is already implemented in several applications of pretty Easy privacy (pEp).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In many Opportunistic Security [RFC7435] scenarios end-to-end encryption is automatized for Internet users. In addition, it is often required to provide the users with easy means to carry out authentication.

Depending on several factors, each communication channel to different identities may have a different Privacy Status, e.g.

* unreliable

* encrypted

* encrypted and authenticated

* mistrusted

Also each message from or to a single peer may have a different Privacy Status.

To display the actual Privacy Status to the user, this document defines a Privacy Rating scheme and its mapping to a traffic-light semantics, i.e., a mapping to different color codes as used in a traffic-lights:

* red

* yellow

* green

* no color

Note: While "yellow" color is used in the context of traffic-lights (e.g., in North America), in other parts of the world (e.g., the UK) this is generally referred to as "orange" or "amber" lights. For the scope of this document, "yellow", "amber", and "orange" refer to the same semantics.

A Privacy Status is defined on a per-message basis as well as on a per-identity basis. The traffic-light semantics (as color and symbol rating) allows for a clear and easily understandable presentation to the user in order to optimize the User Experience (UX). To serve also (color-)blind Internet users or those using monochrome displays, the traffic light color semantics may also be presented by simple texts and symbols for signaling the corresponding Privacy Status.

The proposed definitions are already implemented and used in applications of pretty Easy privacy (pEp) [I-D.pep-general]. This document is targeted to applications based on the pEp framework and Opportunistic Security [RFC7435]. However, it may be also used in other applications as suitable.

Note: The pEp [I-D.pep-general] framework proposes to automatize the use of end-to-end encryption for Internet users of email and other messaging applications and introduces methods to easily allow authentication.

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.

1.2. Terms

The following terms are defined for the scope of this document:

* pEp Handshake: The process of one user contacting another over an independent channel in order to verify Trustwords (or fingerprints as a fallback). This can be done in-person or through established verbal communication channels, like a phone call. [I-D.pep-handshake]

* Trustwords: A representation of 16-bit natural numbers (0 to 65535) as natural language words: For each natural language a fixed number-to-word map can be defined as convention and registered with IANA. Trustwords are generated from the combined public key fingerprints of a both communication partners. Trustwords are used for verification and establishment of trust (for the respective keys and communication partners). [I-D.pep-trustwords]

* Trust On First Use (TOFU): cf. [RFC7435], which states: "In a protocol, TOFU calls for accepting and storing a public key or credential associated with an asserted Identity, without authenticating that assertion. Subsequent communication that is authenticated using the cached key or credential is secure against an MiTM attack, if such an attack did not succeed during the vulnerable initial communication."

* Man-in-the-middle (MITM) attack: cf. [RFC4949], which states: "A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association."

  Note: Historically, MITM has stood for '_Man_-in-the-middle'. However, to indicate that the entity in the middle is not always a human attacker, MITM can also stand for 'Machine-in-the-middle' or 'Meddler-in-the-middle'.

2. Per-Message Privacy Rating

2.1. Rating Codes

To rate messages (cf. also Appendix A.1), the following 12 Rating codes are defined as scalar values (decimal):

Rating code	Rating label
-3	under attack
-2	broken
-1	mistrust
0	undefined
1	cannot decrypt
2	have no key
3	unencrypted
5	unreliable
6	reliable
7	trusted
8	trusted and anonymized
9	fully anonymous

Table 1

(Code 4 could be used for the rating label "unencrypted for some", but it SHOULD NOT be used as having messages encrypted only for certain people means that the message gets leaked for sure, thus providing a wrong sense of protection.)

2.2. Color Codes

For an Internet user to understand what the available Privacy Status is, the following colors (traffic-light semantics) are defined:

Color code	Color label
-1	red
0	no color
1	yellow
2	green

Table 2

2.3. Surjective Mapping of Rating Codes into Color Codes

Corresponding User Experience (UX) implementations use a surjective mapping of the Rating Codes into the Color Codes (in traffic light semantics) as follows:

Rating codes	Color code	Color label
-3 to -1	-1	red
0 to 5	0	no color
6	1	yellow
7 to 9	2	green

Table 3

This mapping is used in current pEp implementations to signal the Privacy Status (cf. Section 6.2).

2.4. Semantics of Color and Rating Codes

2.4.1. Red

The red color MUST only be used in three cases:

* Rating code -3: A man-in-the-middle (MITM) attack could be detected.

* Rating code -2: The message was tempered with.

* Rating code -1: The user explicitly states he mistrusts a peer, e.g., because a Handshake [I-D.pep-handshake] mismatched or when the user learns the communication partner was attacked and might have gotten the corresponding secret key leaked.

2.4.2. No Color

No color MUST be shown in the following cases:

* Rating code 0: A message can be rendered, but the encryption status is not clear, i.e., undefined.

* Rating code 1: A message cannot be decrypted (because of an error not covered by rating code 2 below).

* Rating code 2: No key is available to decrypt a message (because it was encrypted with a public key for which no secret key could be found).

* Rating code 3: A message is received or sent out unencrypted (because it was received unencrypted or there's no public key to encrypt a message to a recipient).

* Rating code 5: A message is encrypted, but cryptographic parameters (e.g., the cryptographic method employed or key length) are insufficient.

Rating code 4 SHOULD not be used, but if it is used, this is its meaning:

* Rating code 4: A message is sent out unencrypted for some of the recipients of a group (because there's at least one recipient in the group whose public key is not available to the sender).

2.4.3. Yellow

* Rating code 6: Whenever a message can be encrypted or decrypted with sufficient cryptographic parameters, it's considered reliable. It is mapped into the yellow color code.

2.4.4. Green

* Rating code 7: A message is mapped into the green color code only if a pEp handshake [I-D.pep-handshake] was successfully carried out.

By consequence that means, that the pEp propositions don't strictly follow the TOFU (cf. [RFC7435]) approach, in order to avoid signaling trust without peers verifying their channel first.

In current pEp implementations (cf. Section 6) only rating code 7 is achieved.

The rating codes 8 and 9 are reserved for future use in pEp implementations which also secure meta-data (rating code 8), by using a peer-to-peer framework like GNUnet [GNUnet], and/or allow for fully anonymous communications (rating code 9), where sender and receiver don't know each other, but trust between the endpoints could be established nevertheless.

3. Per-Identity Privacy Rating

The same Color Codes (red, no color, yellow and green) as for messages (cf. Section 2.2) MUST be applied for identities (peers), so that a user can easily understand, which identities private communication is possible with.

The green color code MUST be applied to an identity whom the pEp handshake [I-D.pep-handshake] was successfully carried out with.

The yellow color code MUST be set whenever a public key could be obtained to securely encrypt messages to an identity, although a MITM attack cannot be excluded.

The no color code MUST be used for the case that no public key is available to engage in private communications with an identity.

The red color code MUST only be used when an identity is marked as mistrusted.

4. Security Considerations

Depending on how the rating system is implemented, a wrong sense of security can be created towards Internet users. User studies should be run to assess how Internet users interpret colors and symbols used.

Furtherly, denoting something as secure can be problematic if underlying cryptographic algorithms are disputed as being secure or even shown to be unsecure. To cover for this case, implementers are advised to use cryptographic libraries which are kept up to date including regular cryptographic refreshements.

5. IANA Considerations

This document has no actions for IANA.

6. Implementation Status

6.1. Introduction

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "[...] this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit."

6.2. Current software implementations of pEp

The following software implementations of the pEp protocols (to varying degrees) already exists:

* pEp for Outlook as add-on for Microsoft Outlook, release [SRC.pepforoutlook]

* pEp for iOS (implemented in a new MUA), release [SRC.pepforios]

* pEp for Android (based on a fork of the K9 MUA), release [SRC.pepforandroid]

* pEp for Thunderbird as an add-on for Thunderbird, release [SRC.pepforthunderbird]

Note: The former community project Enigmail/pEp as add-on for Thunderbird was discontinued and replaced by pEp's own add-on for Thunderbird [SRC.pepforthunderbird] in 2021.

pEp for Android, iOS, Outlook and Thunderbird are provided by pEp Security, a commercial entity specializing in end-user pEp implementations.

All software is available as Free and Open Source Software and published also in source form.

7. Acknowledgements

The authors would like to thank the following people who have provided feedback or significant contributions to the development of this document: Leon Schumacher and Volker Birk

This work was initially created by pEp Foundation, and then reviewed and extended with funding by the Internet Society's Beyond the Net Programme on standardizing pEp. [ISOC.bnet]

8. References

8.1. Normative References

[I-D.pep-general]
Birk, V., Marques, H., and B. Hoeneisen, "pretty Easy privacy (pEp): Privacy by Default", Work in Progress, Internet-Draft, draft-pep-general-01, 21 October 2022, <https://www.ietf.org/archive/id/draft-pep-general-01.txt>.

[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>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[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>.

8.2. Informative References

[GNUnet] Grothoff, C., "The GNUnet System", 7 October 2017, <https://grothoff.org/christian/habil.pdf>.

[I-D.pep-handshake] Marques, H. and B. Hoeneisen, "pretty Easy privacy (pEp): Contact and Channel Authentication through Handshake", Work in Progress, Internet-Draft, draft-marques-pep-handshake-05, 8 July 2020, <https://www.ietf.org/archive/id/draft-marques-pep-handshake-05.txt>.

[I-D.pep-trustwords] Hoeneisen, B. and H. Marques, "IANA Registration of Trustword Lists: Guide, Template and IANA Considerations", Work in Progress, Internet-Draft, draft-birk-pep-trustwords-05, 9 January 2020, <https://www.ietf.org/archive/id/draft-birk-pep-trustwords-05.txt>.

[ISOC.bnet] Simao, I., "Beyond the Net. 12 Innovative Projects Selected for Beyond the Net Funding. Implementing Privacy via Mass Encryption: Standardizing pretty Easy privacy's protocols", June 2017, <https://www.internetsociety.org/blog/2017/06/12-innovative-projects-selected-for-beyond-the-net-funding/>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

[SRC.pepforandroid] "Source code for pEp for Android", December 2022, <https://pep-security.lu/gitlab/android/pep>.

[SRC.pepforios]
"Source code for pEp for iOS", December 2022, <https://pep-security.lu/gitlab/iOS/pep4ios>.

[SRC.pepforoutlook]
"Source code for pEp for Outlook", December 2022, <https://pep-security.lu/gitlab/win/pEpForOutlook>.

[SRC.pepforthunderbird]
"Source code for pEp for Thunderbird", December 2022, <https://pep-security.lu/gitlab/thunderbird/pEpForThunderbird>.

Appendix A. Excerpts from the pEp Reference Implementation

This section provides excerpts of the running code from the pEp reference implementation pEp engine (C99 programming language).

A.1. pEp rating

From the reference implementation by the pEp foundation, src/message_api.h:

```
typedef enum _PEP_rating {
    PEP_rating_undefined = 0,

    // no color

    PEP_rating_cannot_decrypt = 1,
    PEP_rating_have_no_key = 2,
    PEP_rating_unencrypted = 3,
    PEP_rating_unreliable = 5,

    PEP_rating_b0rken = -2,

    // yellow

    PEP_rating_reliable = 6,

    // green

    PEP_rating_trusted = 7,
    PEP_rating_trusted_and_anonymized = 8,
    PEP_rating_fully_anonymous = 9,

    // red

    PEP_rating_mistrust = -1,
    PEP_rating_under_attack = -3
} PEP_rating;
```

Appendix B. Document Changelog

[[RFC Editor: This section is to be removed before publication]]

* draft-pep-rating-00:

  - Update Terms

  - No longer mention "gray" color, use "no color"

  - Remove rating code 4

  - Update code example from reference implementation

  - Add Security Considerations

* draft-marques-pep-rating-03:

  - Updates terms and references; other minor changes

* draft-marques-pep-rating-02:

  - Add Privacy and IANA Considerations sections

  - Updated Terms

* draft-marques-pep-rating-01:

  - Update references

  - Minor edits

* draft-marques-pep-rating-00:

  - Initial version

Appendix C. Open Issues

[[RFC Editor: This section should be empty and is to be removed before publication]]

* Considering the SHA-1 attack, rating must be discussed when encryption is fine while the signature is not.

* Better explain usage of Color Codes in Per-Identity Privacy Rating

* Decide whether rating code scalars 6 and 7-9 should be raised to leave space for future extensions

* Add Security Considerations

* Add more source code excerpts to Appendix

* Add rating codes for secure cryptographic methods and parameters and reference them

Authors' Addresses

Hernani Marques
pEp Foundation
Oberer Graben 4
CH- 8400 Winterthur
Switzerland
Email: hernani.marques@pep.foundation
URI: https://pep.foundation/

Bernie Hoeneisen
pEp Foundation
Oberer Graben 4
CH- 8400 Winterthur
Switzerland
Email: bernie.hoeneisen@pep.foundation
URI: https://pep.foundation/