Efail or OpenPGP is safer than S/MIME

Werner Koch wk at gnupg.org
Mon May 14 11:03:42 CEST 2018

- Previous message (by thread): Efail or OpenPGP is safer than S/MIME
- Next message (by thread): Efail or OpenPGP is safer than S/MIME
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Hi!

I digged in my mail archives and found a discussion with Sebastian
Schinzel about a work in progress thing which turned out to not being a
GnuPG problem.  Here is a timeline with my messages.

On 2017-11-24 we were asked for the encryption keys of the security at
gnupg.org address.  On the same day we received an advisory titled

  Efail: Full Plaintext Recovery in PGP via Chosen-Ciphertext Attack

with the notice

  We ask you kindly to keep this advisory and the information therein
  confidential until we find a nearby date for coordinated public
  disclosure!

A few hours later my reply went out:

--8<---------------cut here---------------start------------->8---
Thanks for sharing the paper with us.  I may have missed something but I
can't see that you considered the use of MDC as specified in RFC-4880,
5.13 (Sym. Encrypted Integrity Protected Data Packet (Tag 18)).  Here is
the timeline of the introduction of the MDC.

  AES conference March 2000

    * Meeting between PRZ, Jon Callas, and me to discuss how to make our
      encryption mode more robust without requiring signed content.

  GnuPG  1.0.3 (2000-09-18)

    * Twofish and MDC enhanced encryption is now used.  PGP 7 supports
      this.  Older versions of GnuPG don't support it, so they should be
      upgraded to at least 1.0.2

  GnuPG 1.0.7 (2002-04-29)

    * The MDC feature flag is supported and can be set by using
      the "updpref" edit command.

  GnuPG 1.1.92 (2002-09-11)

    * The use of MDCs have increased.  A MDC will be used if the
      recipients directly request it, if the recipients have AES,
      AES192, AES256, or TWOFISH in their cipher preferences, or if
      the chosen cipher has a blocksize not equal to 64 bits
      (currently this is also AES, AES192, AES256, and TWOFISH).
```

```
    * GnuPG will no longer automatically disable compression when
      processing an already-compressed file unless a MDC is being
      used.  This is to give the message a certain amount of
      resistance to the chosen-ciphertext attack while communicating
      with other programs (most commonly PGP earlier than version 7.x)
      that do not support MDCs.

  GnuPG 2.1.9 (2015-10-09)

    * gpg: Fail with an error instead of a warning if a modern cipher
      algorithm is used without a MDC.
```

Your attack should not work if the MDC is in use. And it is always in use for AES. In any case active content in mails should be discouraged in all mails (see my mail headers ;-).

We are slowly working in the WG on RFC4880bis to introduce a new encryption mode. Unfortunately there are heavy opinions on the use of OCB mode and thus we may need to come up with the choice of two new modes. Based on the experience with MDC I expect that the deployment of a new mode will take at least 3 years. Until then I hope that the MDC hack will serve us fine.
--8<---------------cut here---------------end--------------->8---

In response to that they said that they did a simple rollback to the non-MDC encryption. This is a pretty old thing which we are aware of and the reasons why a warning has always been printed in that case.

In a further response the same day they noted that gpg indeed returns an error code but that Enigmail still displays the message. My reply on that went out on 2017-11-26:

--8<---------------cut here---------------start------------->8---
Enigmail does something wrong the. Here is the respective code in GnuPG:

```
  else if (!result
           && !opt.ignore_mdc_error
           && !pkt->pkt.encrypted->mdc_method
           && openpgp_cipher_get_algo_blklen (c->dek->algo) != 8
           && c->dek->algo != CIPHER_ALGO_TWOFISH)
    {
      /* The message has been decrypted but has no MDC despite that a
         modern cipher (blocklength != 64 bit, except for Twofish) is
         used and the option to ignore MDC errors is not used: To
         avoid attacks changing an MDC message to a non-MDC message,
         we fail here.  */
      log_error (_("WARNING: message was not integrity protected\n"));
      if (opt.verbose > 1)
        log_info ("decryption forced to fail\n");
      write_status (STATUS_DECRYPTION_FAILED);
```

which was introduced with

```
  commit 625e292108cc0fd9077769587a8c22abe7805e33
  AuthorDate: Tue Oct 6 09:40:57 2015 +0200

    gpg: Fail decryption for AES etc message w/o MDC.

    * g10/mainproc.c (proc_encrypted): Fail for modern messages w/o MDC.
    --
```

```
    This change turns the missing MDC warning into an error if the message
    has been encrypted using a cipher with a non-64 bit block length cipher
    and it is not Twofish.

    We can assume that such messages are created by code which should have
    been able to create MDC packets.  AES was introduced with 1.0.3 on
    2000-09-18 shortly after MDC (1.0.2 on 2000-07-12).  We need to
    exclude Twofish because that might have been used before MDC.


GPGME based applications should get it correct because GPGME detects the
STATUS_DECRYPTION_FAILED and flags the result as failed.
--8<---------------cut here---------------end--------------->8---

On 2017-11-29 we got a short mail asking for a phone call.  It might be
that I did not reply to that but in any case my office phone number is
easy to lookup.  I did not get a phone call.

Since then we have not seen any more communication - not even about the
proposed coordinated public disclosure.  Thus I closed this issue in
December and forgot about it.

On 2018-04-27 I received another paper via a Kmail developer which had a
different title than the one from November

    *** DO NOT PUBLISH OR SHARE ON PUBLIC MAILING LISTS ***
    Efail: Breaking S/MIME and OpenPGP Email Encryption using
                        Exfiltration Channels

and no author names etc.  The GnuPG team discussed this but did not see
that any action was required.  In particular because due to the
redaction we were not able to contact and help the developers of other
MUAs which might be affected.


Shalom-Salam,

   Werner

--
#  Please read:  Daniel Ellsberg - The Doomsday Machine  #
Die Gedanken sind frei.  Ausnahmen regelt ein Bundesgesetz.
-------------- next part --------------
A non-text attachment was scrubbed...
Name: not available
Type: application/pgp-signature
Size: 227 bytes
Desc: not available
URL: <https://lists.gnupg.org/pipermail/gnupg-
users/attachments/20180514/6fbfaede/attachment-0001.sig>
```

- Previous message (by thread): Efail or OpenPGP is safer than S/MIME
- Next message (by thread): Efail or OpenPGP is safer than S/MIME
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the Gnupg-users mailing list