threadreaderapp.com /thread/995967487140298752.html

183 views

Robert J. Hansen

@robertjhansen

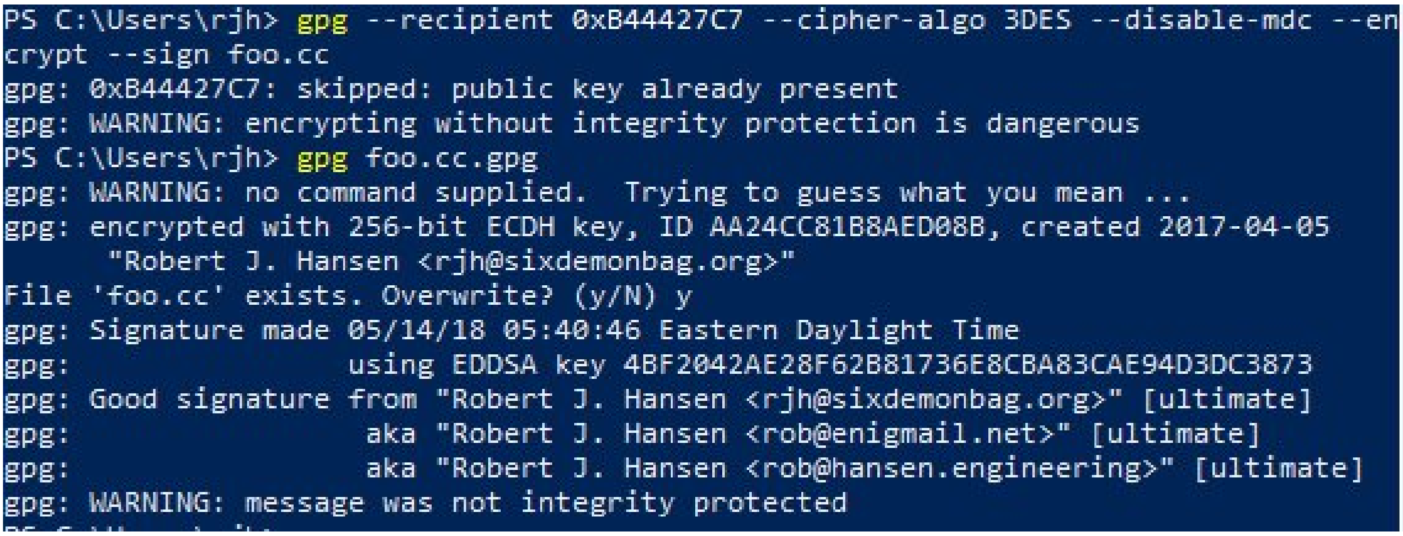
4 years ago, 10 tweets, 2 min read Read on Twitter

Long thread. If you want to know the high-level details of the Efail attack, read. Yes, it was embargoed; yes, we were respecting the embargo; but links to the paper are now easy to get, so... here goes. 1/

This is at its heart a malleability attack on OpenPGP's cipher feedback mode. These attacks aren't new. The IETF OpenPGP Working Group first knew about them in 1999. By September 2000, GnuPG had a defense. 2/

The defense is called a Modification Detection Code, or MDC. Originally MDCs were optional. Today they're the default. The Efail attack requires an MDC either be missing or be invalid. 3/

You *can* manipulate a message with MDC into being one without MDC. The Efail authors are right there. So let's see what happens when GnuPG sees a message without an MDC.



```
PS C:\Users\rjh> gpg --recipient 0xB44427C7 --cipher-algo 3DES --disable-mdc --en
crypt --sign foo.cc
gpg: 0xB44427C7: skipped: public key already present
gpg: WARNING: encrypting without integrity protection is dangerous
PS C:\Users\rjh> gpg foo.cc.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: encrypted with 256-bit ECDH key, ID AA24CC81B8AED08B, created 2017-04-05
      "Robert J. Hansen <rjh@sixdemonbag.org>"
File 'foo.cc' exists. Overwrite? (y/N) y
gpg: Signature made 05/14/18 05:40:46 Eastern Daylight Time
gpg:                using EDDSA key 4BF2042AE28F62B81736E8CBA83CAE94D3DC3873
gpg: Good signature from "Robert J. Hansen <rjh@sixdemonbag.org>" [ultimate]
gpg:                 aka "Robert J. Hansen <rob@enigmail.net>" [ultimate]
gpg:                 aka "Robert J. Hansen <rob@hansen.engineering>" [ultimate]
gpg: WARNING: message was not integrity protected
```

As you can see in the last line, you get a very clear message. "WARNING: Message was not integrity protected."

After that, it's up to your email client to do the right thing. 5/

Your email client should refuse to render the message. If it ignores the warning or does the wrong thing in response to it, then yes, the Efail attack is very real. So it's really more fair to say this is an attack on poorly-written clients, not OpenPGP. 6/

The OpenPGP spec does technically allow for non-MDCed messages. It has to for backwards compatibility reasons. But no modern OpenPGP client should silently ignore missing/malformed MDCs. No modern email client should ignore the OpenPGP client's warnings. 7/

GnuPG has given warnings on missing/malformed MDCs for years. And although the Efail authors did find some problems in Enigmail -- for which we're deeply sorry, and plead that we're only human -- we fixed them months ago. 8/

If you're using a recent GnuPG and Enigmail 2.0 or later, you should be fine. If you're not, consider this an object lesson in the importance of upgrading your security-critical software. 9/

I encourage you to read the Efail paper. I've also shown you some GnuPG commands and outputs: please check me. As always, we welcome your feedback. If you're a trainer or working with vulnerable people, please DM/email with your questions. 10/10 (end)