Statement on Efail research

Summary

On the 14th of May 2018, a group of researchers published a number of problems in mail applications on efail.de. Most mail clients supporting S/MIME are affected as well as a few clients supporting OpenPGP.

They have tested OpenPGP support with GpgOL (our Outlook Add-in) and it behaved well for supported versions of Outlook.

The bottom line is, that you can keep using Gpg4win while:

- You pay extra attention to the ability of your S/MIME recipients to handle crypto emails well, until the majority of other email clients has been updated.
- You never load external references in encrypted HTML emails, especially for S/MIME. Make sure that the default is still *off*.

The Gpg4win Initiative plans to release another minor version soon that takes further precautions, removes Outlook 2007 support, and improves some edge cases for its S/MIME support.

Details

On the 14th of May 2018, a group of academic researchers from Germany and Belgium published a paper called Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels (draft 0.9.0) on their website. They show a number of problems with how email encryption is currently implemented. A few mail clients supporting OpenPGP and most clients supporting S/MIME are affected.

"Direct exfiltration" in other clients

Two major email clients, Apple Mail and Thunderbird/Enigmail, have been found to be vulnerable to an attack called "direct exfiltration". **Gpg4win's Outlook-Plugin** and for example the Free Software ("Open Source") mailers Claws, Evolution, KMail, K9-Mail, Mailvelope, Mailpile and Mutt were **found to be immune.**

The attack is made possible if the email client concatenates different mail parts and interprets them together as HTML with external references. This can be used by an attacker: A manipulated encrypted email tricks the email client into sending decrypted plaintext to a webserver of choice, when fetching the references.

As this attack works on the sender and all recipients of an encrypted email, all the used email clients have to be safe for your communication to be safe.

Advice:

Make sure to only send encrypted emails to people that are using clients in a safe way. Put special attention to the vulnerable clients listed in the bottom of efail.de until fixed versions are widely available. Check updates from a computer emergency response team that feels responsible for you, e.g. CB-K18-0673 (Germany) and their "Efail" vulnerabilities - What you should know now or VU#122919 (USA).

Note:

Each communication partner already had the responsibility to keep contents coming from you confidential on an organisational and technical level. Right now some may just not be informed about the version of their product being vulnerable to this specific attack.

"crypto gadget" attack

If an email is only encrypted and not signed, an attacker can reorder, delete or insert data, which will be partly decrypted. The current OpenPGP protocol as it is widely used for about 15 years includes protection against this manipulation. Current S/MIME specifications also allow for protection, but this has not been deployed in practice. The manipulation can cause an insecure mail client to leak decrypted data to a remote attacker through a backchannel like an external reference. The attack does not work, if there is no usable backchannel.

OpenPGP

The GnuPG crypto-backend in Gpg4win detects such manipulations and issues an error to mail clients, unless the sender or receiver deliberately uses weak settings. Most mail clients using Gpg4win respect the errors issued by GnuPG. Especially Ggp4win's Outlook Add-in "GpgOL" will not display any data in this case which makes it **immune against the OpenPGP crypto gadget attack.**

The combination of GpgOL and Outlook 2010 or newer in addition does not load external links by default. Automatically loading links in mails is a privacy problem in itself and has long been discouraged for security reasons. Only some mail clients load external URLs by default.

An exception to this is GpgOL for Outlook 2007. Since Version 3.0 Gpg4win already shows a warning that this part of GpgOL is unmaintained. Users should stop using Outlook 2007 as it does not receive updates from its vendor anymore. Support for this version will be removed in the next Gpg4win revision.

S/MIME

Deployed standard S/MIME implementations do not have a way to detect the mentioned manipulations when using unsigned mails. This is described in the current S/MIME standard (RFC5751).

The problem arises if clients still show contents in case of a missing or bad signature for an encrypted mail and they are loading external references to open a backchannel.

Note that there is an S/MIME mode to GpgOL, which is disabled by default and has not been tested by the researchers. They tested the S/MIME mode of KMail which is also using GnuPG as an S/MIME backend and only found that a user can manually trigger a backchannel.

As a precaution against any S/MIME message modification attacks in Outlook the Gpg4win team **recommends to not load external references, e.g. images, in mails and refrain from using HTML-mails.**

Automatic download of images could have been enabled in Outlooks options under: "Trust Center->Automatic Download" The automatic download is disabled by default, thus **GpgOL is immune against the S/MIME crypto gadget attack**.

A rarely used feature of Gpg4win is to apply S/MIME crypto operations to files. When executing files users should always **ensure that it comes from a trustworthy source** by checking a signature.

Note: When receiving an email or file without a cryptographic signature you already had to be careful that the contents could have been manipulated and thus you should not use unsigned active contents, like executables, office macros and other scripts.

Media coverage of the larger picture

While the researchers have chosen an important topic to work on and their tests demonstrated important weaknesses in implementations and the need to update related standards, there is some concern in the Gpg4win team about how the findings got reported in some media.

The broken email clients allowing "direct extraction" are worrisome and may need broad media coverage to use reach their users, but it would have been better to wait with reporting until better fixes and instructions were available. It is a classic situation that is happening several times during the year that some implementations are found to be defect and updates are needed. It happens to many applications and does not indicate a more general problem.

The problem with S/MIME implementations missing integrity protection is serious and we hope that vendors will quickly agree on implementing RFC6476 or something similar. This seems to be the most interesting finding, as it cannot be resolved quickly and it reminds everybody to be careful with contents that can become active as a backchannel or exploit code.

The situation with OpenPGP is different: When used sensibly, the current OpenPGP specification, its implementations, and GnuPG itself continue to provide very reasonable protection. The integrity detection MDC is used for more than 15 years and GnuPG itself issues a clear indication for a manipulated email and even a hard failure since 2015.

On a general note: OpenPGP and S/MIME are protocols which are openly documented with several implementations and variants. OpenPGP is additionally designed to have a de-centralised structure. They need to consider backwards compatibility more than a single vendor, but they are also less vulnerable against a serious implementation defect in one product.

When considering other solutions for communicating in private our recommendation would be to also check if it is Free Software ("Open Source"), openly documented, de-centralised and has an understandable business model where users are the customers.

Security is a complicated matter and thus profits from calm reporting. A pressure to simplify and report quickly on the research findings may have caused more confusion than necessary. It is for us as readers

to honor a thorough style of journalism that may need more time to shine.

Bernhard Reiter, Andre Heinecke, Werner Koch