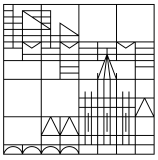
Universität Konstanz



#efail – What's gone wrong with e-mail and encryption?

Throughout the last few days, many of you night have heard or read about a problem in the media: encrypted e-mails are no longer safe? What going on here?

Problem 1:
Most e-mail clients (programs we use to read e-mails) interpret "active contents" in the text body of mails, e.g. to "nicely format" html-encoded text, to automatically load images that have been included as links by the sender, and so on. Automatically decrypting encrypted mail text also belongs to those "convenience features" that now turn out to cause trouble.

Problem 2:
The so-called MIME standard (Multi-purpose Internet Mail Extensions), which allows, among others, to include arbitrary attachments in e-mails, triggers some actions in your e-mail client as well.

Problem 3:
Even though the underlying cryptographic algorithms used for encrypted mail transfer are still considered safe, their use in handling e-mails opens up plenty of opportunities for attackers to-relatively easily-modify encrypted messages. Therefore, a "man-in-the-middle" attack during mail transfer from the sender to the receiver might remain undetected. (Both e-mail encryption frameworks, S/MIME and PGP/GPG share this problem, even though somewhat more pronounced in S/MIME.)

The combination of these three problems allows for rather simple attacks on encrypted e-mails, in particular getting access to the cleartext of encrypted e-mails. In the simplest case, an attacker able to modify the encrypted message during transport (Problem 3) uses the MIME standard (Problem 2) to "wrap" the cyphertext in such a way that, immediately after the automatic decryption by the receiver's e-mail client (Problem 1), an image is loaded from a machine under the attackers control (Problem 1), providing the whole cleartext as a "parameter" of the URL loading the image. As a result, the attacker has access to the cleartext message without even having to break the encryption, because the receiver's e-mail client was kind enough to do that for the attacker.

What can/shall we do?

1. If you're receiving encrypted mails every once in a while or on a regular basis, you should react:

a) Disable active interpretation of e-mail contents in your e-mail client.

It is good practice anyway to configure your e-mail client to display messages as "plain text only" (or "simple HTML", "View" menu in Thunderbird), since this prevents a lot of tracking/"phone home" functionality allowing senders to collect information from you. Most e-Mail clients are at least configurable to disallow loading of external content.
(In Thunderbird, for example, remove the check mark on „allow external content in messages" and don't click on „show external content", if you read an encrypted mail.)

b) You can also disable automatic decryption of encrypted messages (at least by disabling the corresponding plug-in or removing your key pair). By doing so, you're safes from this kind of attacks at the expense of extra work for decrypting encrypted mails: you need to copy the cyphertext to a separate tool for decryption (and make sure that this other tool does not interpret "active contents").

2. If you never (or hardly ever) receive encrypted mails, you are not affected by those problems.

3. If you only read mails using SOGo, you are not affected either (but cannot read or send encrypted mail anyway).

4. All e-mail clients need to be (substantially) fixed by the vendors, but this will take some time.

Additional hints:

- Continue using encrypted mails, if you have done so until now. This is much safer than sending unencrypted, where every "man-in-the-middle" can see cleartext right away.
- Do not send html-formatted messages via e-mail. Mail has never been designed to transfer formatted text, so it is no surprise that html-formatted e-mails have been a constant source of trouble.
- Keep your software updated! Some e-mail clients and/or encryption tools/plug-ins have been fixed or are being fixed in the near future, at least for the most obvious #efail attacks (enigmail for Thunderbird has been provided with an initial, but not complete, fix).