Checking gpg mail signatures with Sylpheed−Claws

by Iznogood

<iznogood/at/iznogood−factory.org>

About the author:

Involved in GNU/Linux for a while, I'm now running a Debian system. Despite electronic studies, I've mostly done a french translation work for the GNU/Linux community available on Iznogood−Factory.

Abstract:

I will try to show how to install a gpg plugin and check a mail signature within Sylpheed−Claws using some bash pipes commands.

_____ _____ _____

Why check signatures?

I received an email from a friend who ask me : "Why have you send me a email with a virus program attached ?" Huuu! Someone had caught my email address and sent him a email with my address... He was lucky because the virus was detected. But what would have happened if there was only a date for a meeting in a town, 150 kms far from his house, as we are used to do... or a patch for a program under development. It would be a bad day!

From this time I always sign my emails. And I verify the email signature when the email have one. One more security against intruders. But sometimes, I receive a email from a new person with an gpg signature I haven't yet checked. Since I'm a very lazy guy and I don't want to open a xterm, write the gpg command to have the public key on my computer and then verify the signature for each new email address. That's why I have done it as an action in Sylpheed−Claws.

About Sylpheed

Sylpheed is a light, fast graphical GTK mailer and news reader. It is released in two flavours: Sylpheed, the main branch and Sylpheed−Claws, the bleeding edge application. Sylpheed−Claws support GPG with a plugin named PGP/MIME.
You need to have sylpheed−claws, sylpheed−claws−plugins, sylpheed−claws−pgpmime and gpg compiled on you machine. For Debian Sarge users, it's easier with aptitude, you just have to download the packages above (among others but make a search) or you make an

```
apt-get install sylpheed-claws sylpheed-claws-plugins sylpheed-claws-pgpmime gpg
```

To make it working, you need to go to Configuration –> Plugins then Load Plugin named pgpmime.so as shown on the images (of course, you can choose some others plugins to help you using Sylpheed–Claws).
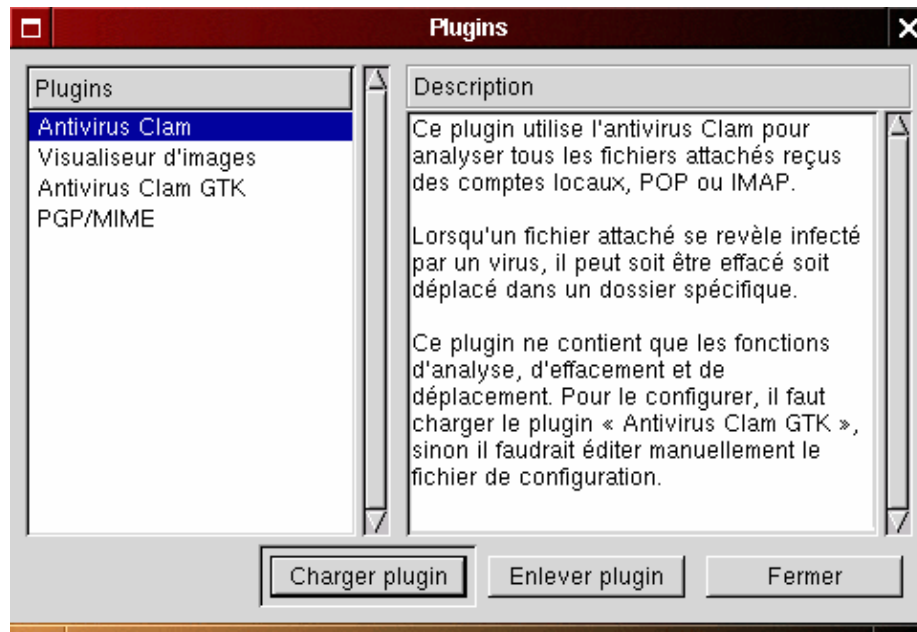
This will show you PGP/MIME on the left. Now, you can close the window. Then, go to Preferences in the Configuration menu.
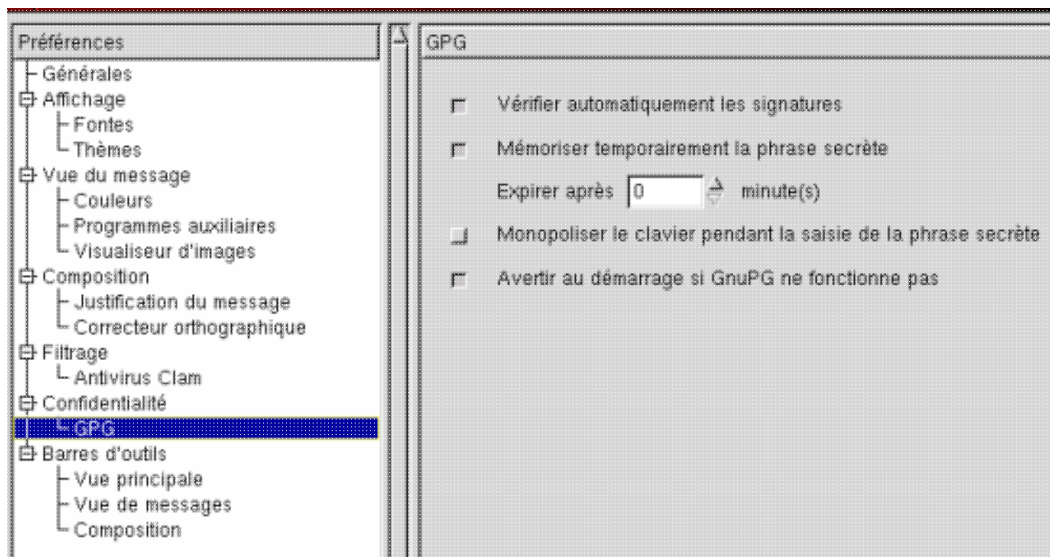
Then, go to Preferences in the Configuration menu. On the left you have Confidentiality –> GPG. Clicking on it will show 4 check boxes. You need to quote at least the first one (Automatic signature check). Check your messages. The others are intersting if you sign yours messages: the second keep your passphrase in memory during the session, the third gives the focus on the keyboard and the last one warns you if gpg doesn't work.

If there is one with a signature, you will see a logo on the right of the message body:
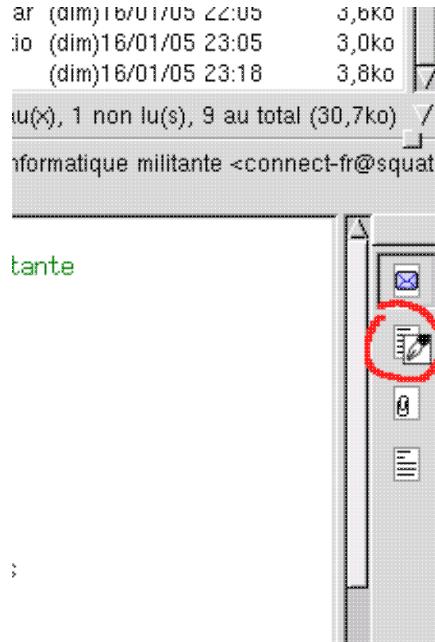
This icon with a pen shows gpg control is active but the author isn't in your database or the signature is wrong.

How to make a signature checker?

In Sylpheed−Claws, you can do actions with Tools −> Actions when you are on the email you want to check. But, first, you must program it in Configuration −> Actions. You open it:
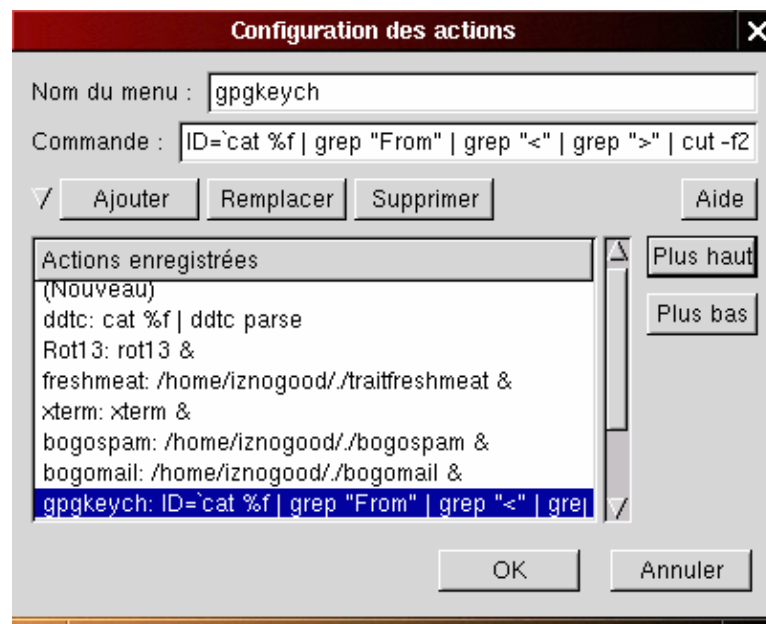
On menu name, you put the command name (you can choose the one you wan) and the command in Command (very difficult!) and you Add it. Here is the command piped to do the gpg check:

```
ID=`cat %f | grep "From" | grep "<" | grep ">" | cut -f2 -d\< | cut -f1 -d\> `;
xterm -e gpg --keyserver wwwkeys.ch.pgp.net --search-key $ID
```

in one line. The normal gpg command is :

```
gpg --keyserver servername --search-key email-address
```

with sylpheed−claws, we open it in a xterm with "xterm −e" because we always need to choose one name option. To have the email−address, the $ID:
 • we read the message with the cat %f
 • we search the From line with "<" and ">"
 • we keep everything before "<" and after ">"

and we have the address. When we check an email address with Actions, it goes on the wwwkeys.ch.pgp.net keyserver but you can replace it by yours or have two different actions with two different keyservers, as I do. You will have this xterm:


Choose the right address and the xterm window exits. You just have to check again the icon on the right that will open a button on the bottom to reverify. It's done! You will have this icon window:

If not, that mean the signature is wrong and you can put it in Trash.

If you have this icon box that mean the sender is a friend or a trusted person on your gpg database because he/she needs to have been trusted by you.
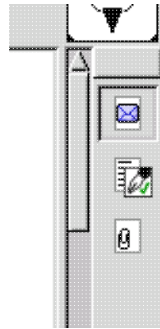
You will only have to do it one time for a new email identity then all emails will be automatically checked and your security will be improved.

Conclusion

It will be easy to adapt the bash pipes commands to another mailer graphical or not. It is quite easy to check your emails automatically. One other advantage: theses controlled emails don't need to pass the spam process because you have checked the address one time and, as far as I know, spams don't use gpg signature. There is undoubtedly a way to put a control over signed mails directly in the input with procmail to validate them directly but it will be another story you will find on Iznogood−Factory.

You can find more informations about gpg and email signatures on:

http://www.gnupg.org/

and for Sylpheed−Claws, it is here.

2005−04−09, generated by lfparser_pdf version 2.51