Encrypting Files via OpenPGP

V1.5, 2019-04-16, Thomas Pronk

Contents

Introduction

This is a manual for storing files in a relatively secure manner. The manual consists of three parts: preparation, execution, and cleaning.

Disclaimer: <u>This manual does not offer protection against all possible adversaries.</u> The practices described in this manual are limited in the level of security that they provide, since they are aimed to be relatively easily performed by moderately skilled computer users on devices of their own choosing.

1. Preparation

In order to prepare each device (laptop or desktop computer), the following steps need to be undertaken:

1a. Required Materials

Before starting, you'll need the following:

1. A file with a public key, the name of which starts with **public-key** and ending with **asc**
2. An e-mail address to send an encrypted file to as a test run.
3. A device where you can install new software on.

1b. Basic Security

Please ensure the following of the device that you intend to use:

1. Is the operating system (Windows or MacOS) up-to-date?
2. Is it equipped with a properly configured firewall and virus-shield?
3. Has it been recently scanned for viruses and other malware?
4. Can the device be safely stowed during the project?
5. I recommend using **Google Chrome** as a web-browser. Please ensure that Chrome is up-to-date as well.

1c. Install and Configure GnuPG

GnuPG is software for encrypting files. Please install in configure it by performing the following steps:

1. Download **GnuPG** via the following web-page. Pick the version corresponding to your operating system below the header "GnuPG binary releases". Also note that the installer has different names depending on your operating system. Windows users should pick the file "Gpg4Win": https://www.gnupg.org/download/index.html
2. Install the application. When installing, be sure to enable the installation of the GPA (GNU Privacy Assistant).
3. Start the GPA. During startup, the application will ask you whether you'd like to create a private key; this isn't needed.
4. Once the GPA application has started up, import the file **public-key-608272CC.asc** via the "Import" button that can be found in the top ribbon. This file contains the public key used to encrypt the files you want to transmit.

1d. Install and Configure a File Wiper

When cleaning up, we'll use a *file wiper* to remove traces of files from the devices:

1. For Windows users, download **BitKiller** here: https://sourceforge.net/projects/bitkiller/files/BitKiller2.0.zip/download
2. For Mac users, I'm less sure what a good wiper application is, but I suspect **MacClean** should do the trick: https://www.imobie.com/macclean/

1e. Designate a Temporary Folder

Designate a **temporary folder** on the hard drive of your device. Any files collected before being transmitted should be stored here.

1f. Test Encrypting a File

During these steps we'll test if everything is set up correctly by encrypting and sending a file:

1. Please obtain a file with a picture of a kitten, *don't forget to download it directly to the **temporary folder***, for instance, by right-clicking the picture and selecting "Save image as" in Chrome on Windows. In this tutorial we'll use the file name *kitten.jpg* as example.
2. Start the GPA application.
3. Click the "Files" button at the top ribbon to start the File Manager.
4. In the File Manager, click the "Open" button at the top ribbon.
5. In the file picker that opens, select the file with the picture of the kitten.
6. Returning to the File Manager, click the "Encrypt" button at the top ribbon.
7. In the Encrypt documents window, select the key with Key ID **608272CC** and click OK.
8. A new file with the extension ".gpg" has been created in the temporary folder. For example: *kitten.jpg.gpg*
9. Please e-mail the gpg file to your technician.

1g. Test Wiping Temporary Folder

During these steps we'll test wipe the temporary folder. Step-by-step instructions are only provided for BitKiller:

1. Startup the application.
2. Click "Add Folder" and select the temporary folder.
3. Select "DOD 7 pass (very strong)" from the options on the left
4. Click "Shred Files"

2. Execution

Whenever collecting or transmitting a file for secure storage, take the following steps:

1. If you are using a website to collect the files, be sure you are connected via secure HTTP; the website address should start with "https" (e.g. https://web.whatsapp.com) also indicated via a little lock icon and the text "Secure" left to the website address when visiting it.
2. *Don't forget to download any files directly to the **temporary folder***
3. Encrypt the file using the steps outlined in Section 1d
4. Transmit the encypted file (the one ending in gpg)

3. Cleaning

Once you are done with collecting and transmitting files, it's time to remove traces from the hard drive via the file wiper. Perform the steps described in section 1g in order to do so.

4. Version History

- v1.5. Removed workflow elements that were part of an earlier project.