Ubuntu-MD March 23, 2019 Meeting

Encryption

Our meeting today will focus on encrypting files, directories and messages on Ubuntu Linux systems. Ubuntu like many other Linux distributions comes with the gpg program installed that can be used rather easily from the command line. For example:
Let's create a file in your Documents directory called testencrpt.txt

- Open the terminal (Crtl+Alt T)
- cd Documents // change to your Documents directory
- touch testencrpt.txt // create the blank file
- gpg -c testencrpt.txt
- Enter a passphrase that will be needed to de-encrpyt
- A new file testencrpt.txt.gpg will be created that you can send to someone.
- You could send that file to a recipient and, as long as they have gpg installed, they can decrypt the file with the password you used for encryption. If they are a Windows user, they can always install Gpg4win.

To decrypt the file use:
gpg testencrpt.txt.gpg and enter the passphrase that was used to encrypt it.

If you want to use the GUI desktop for encrypting, do this:

- sudo apt install seahorse-nautilus
- Start the file manager
- Right click on the file you want to encrypt and click Encrypt
- You will then be prompted to add a gnugpg key

Creating a new key via command line

- sudo gpg –gen-key
- Prompted for Real Name, email and comment
- Select encryption type (RSA, DSA, etc)
- You will be given an option to edit your entries and then you can start the process.
- Enter your passphrase
- The key generation process takes a few minutes to complete.

After successfully generating a key certificate which will be stored in your ~/.gnupg directory you want to create a revocation certificate in the event your certificate is ever compromised:
gpg --output revoke.asc --gen-revoke <your@email.com>
When completed change the file permission:
sudo chmod 600 revoke.asc
Move the file to a safe place on your computer

Ubuntu-MD March 23, 2019 Meeting

Veracrypt

VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. It is based on TrueCrypt 7.1a.

VeraCrypt main features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).
- Encryption is **automatic**, **real-time**(on-the-fly) and **transparent**.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- More information about the features of VeraCrypt may be found in the **documentation**

`Download the linux file from the site, https://veracrpt.fr/en/ and extract the files. Start the GUI and add files or directories to encrypt.`