Burner os & pgp encryption

By Tigeh

PERSISTENCE ON TAILS:

So now that you have your Tails USB working fine, there Maybe one more thing that you would need to do so you can use Tails properly. Remember how Tails is really Amnesic and forgets everything at shutdown? You have the option to set a space on the USB, where you can save your files and fully encrypt it with a passphrase. Doing this is what we call "Enabling Persistent" on Tails. After you enable Persistent, there will be a new folder called "Persistent". Files you place in this "persistent" folder will not be deleted at shutdown. With that being said, be careful about the type of files you save in the persistent folder. Files left anywhere else aside "Persistent" folder will be erased at shutdown. To enable Persistent,

1.first click on > applications > tails > configure persistent volume. "Setup Tails persistent volume" window will pop up. You can read about the dangers of enabling persistence on Tails.

2. Type in your passphrase and repeat. Make sure it’s a good strong passphrase, one that you will not forget.

3. Click on create. It may take a few minutes. Once it's done a new window will pop up. Tails persistence doesn't just enable you to keep your files from one session to another but you can also make save your application settings from one session to another as well. At the top of this list in the new popped up window is "personal data". This should be enabled by default. The remaining of the options are not enabled but you can enable them when needed. Example you can click on "GnuPG" to enable it, this means that you will be able to store your pgp encryption keys in tails, and they will not get deleted at shutdown. Same applies to Bitcoin client (to make btc transactions), pidgin(to chat with your contacts on jabber/xmpp)and the rest.You should put some thought into which of these applications you want to be persistent.

4. Click on "Save".

5. Reboot for persistence to take effect. Once it has been rebooted, you will have the option to unlock persistent volume with the passphrase you used in creating or start tails without persistence which is completely amnesic. That choice is yours to make.

PIDGIN FOR COMMUNICATION:

Observing a proper opsec, it is an important thing that you encrypt your chat messages from end-to-end. This is possible with OTR in the pidgin messenger.
What is OTR? OTR simply stands for Off The Record. It is an encryption protocol. All that it does is encryption and encryption only. It is not a chat app but instead existing chat apps that don't have encryption can be upgraded by adding OTR to them. Do not use pidgin plus OTR in Windows or Mac OS. This is because, while OTR makes it possible to send end to end messages, these two OS do not protect your anonymity. Therefore, anyone interested in finding your location can do so with ease. This is why I am encouraging pidgin plus OTR in Tails instead.
To start using pidgin plus OTR, you must first create an account with a jabber server. What is jabber? Jabber is an instant messaging program. It is also known as xmpp. Example of a jabber server is "jabber.calyxistitute.org" (the calyx institute based in california).
After you create an account with any of the numerous jabber servers(be sure to read about their privacy policy before signing up), you can now log in via the pidgin messenger. Done. Quick note: Make sure to enable OTR on all conversations.

PGP IN TAILS:

What is PGP?
PGP stands for pretty good privacy.
PGP is owned by the PGP corporation and symantec and was originally programmed by Phil Zimmerman and published in 1991. PGP allowed people to encrypt their emails and files, and it became a popular encryption tool in the 1990s. That is a brief description about PGP.
So right now you have got your Tails OS running and you want to start using PGP. First, you will need a key pair. Which is a public key and a private key.
Generating your own key pair:
1. Click on the clipboard icon located in the top right-hand corner of the Tails desktop screen. This is the tails PGP applet.

2. Select "manage keys". A window will pop up called "passwords and keys"

3. On "password and key" window, you will locate a button with a plus(+) sign. Click on it.

4. A new window will pop up "New item". Select "PGP key" from the drop down list and click on continue.

5. Fill the forms in the "New PGP key" pop up window. Make sure not give away your identity. Encryption type should remain RSA. Push key strength(bits) to 4096. You can set an expiry date if you want. After you checked everything and you feel OK about it, click create.

6. Put a strong passphrase and repeat.

7. Click OK. It will take a few seconds and congratulations you now own a key pair. To find your key pair

and that of your contacts, select "GnuPG keys".
You can now encrypt and decrypt texts(emails or whatever) and files with your PGP. You can also sign messages to your contacts or verify a signed message from your contacts. These are some of the uses of PGP.

Fingerprinted.
Leaking not
allowed.