Secure Storage with TrueCrypt

Introduction

This document is a brief guide on how to install and set up TrueCrypt, a free and open source file encryption tool. Use this tool to encrypt (lock with a password) and hide your sensitive files.

I: Installation

1. Go to *http://www.truecrypt.org/downloads* and download the version of TrueCrypt for your operating system.
2. Save and install on your computer or extract to your portable device such as a USB (Note: extracting to a USB is available for Windows but not Mac OS).

II: Create a Standard Container

1. Open TrueCrypt, and select **Create Volume** to launch the creation wizard
2. Select **create an encrypted file container** and then click **next**
3. Select **standard truecrypt volume** and click **next**
4. **Select file** to choose the name and location of the container. Be careful: do not select an existing file—it will be overwritten! Check **never save history** and click **next**
5. Under **encryption options** you can use the default settings. All options are considered secure. Click **next**.
6. Type in the **volume size** you would like for the container. This cannot be changed later, so be sure to make it big enough! (But if you would like to backup the volume on a USB or CD later, keep the size small enough to do so).
7. Type in a unique and strong password that you will not forget but will be difficult for others to guess. If your password is not safe enough, you will see a message recommending that you change it. Click **next** if the message does not appear.
8. The standard file system type is fine for format options. Click **next**
9. On the Volume Format screen, move your mouse around the screen as randomly as possible as your container encrypts. The longer you move it, the better the strength of the encryption. Click **format** when you are done.

III: Open your Volume

1. In the main TrueCrypt window, select **slot 1** (or any slot) for mounting your volume
2. Click **select file,** select the standard container you just created, and click **Open**
3. Click **mount**, and enter your password when prompted.
4. Your volume should now appear in slot one. Double click to open.
5. Select **volume tools** if you want to change the password for this volume
   a. **NOTE**: When your volume is open, anything that you save, copy, or move to the volume is automatically encrypted.
   b. This is called *on-the-fly encryption*
6. When you are done using your container, select it and click **dismount** and **close** TrueCrypt.

7. Next time you want to access a file on your TrueCrypt volume, you will have to mount it again.

Check: After you dismount your volume, find it on your computer (or wherever you saved it), and try opening it. What happens? What does the file look like?

IV: Back up your Volume

1. Always back up your volumes. Make sure your volume is not mounted before you begin.
2. Navigate to your volume file on your computer or device.
3. Select the file, and save it to an external memory device such as a USB or CD.
   a. Make sure the device size corresponds to the size of your volume!

V: Create a Hidden Container

A hidden container is located inside a normal file container. The purpose is to store "fake" secret files in the normal container, and the "real" secret files within the hidden container..

1. Go through the same steps as under Section II, except select **Hidden TrueCrypt volume**.
2. Enter a password for the **Outer Volume** and continue with setup to create the Outer Volume.
3. Open the Outer Volume and place some "fake secret" documents in it.
   Remember: The purpose of creating the hidden volume is to protect the files inside it by placing fake secrets in the Outer Volume. Place fake secrets in the Outer Volume that would satisfy anyone demanding to see your encrypted files!
4. Click **Next** to create the **Hidden Volume**, and follow the steps to set up.
5. Create a different password for the Hidden Volume.
6. A confirmation message will show that the Hidden Volume has been successfully created and will not be detectable.
7. To open your Hidden Volume click "Select File…" and open the Container of the volume
   a. To open the hidden volume: enter the password for the hidden volume
   b. To open the outer volume: enter the password for the outer volume.
8. When entering the password for the outer volume, click "options" and select "protect hidden volume when mounting outer volume" to make sure your Hidden Volume is not overwritten when changes are made to the Outer volume.
9. Remember to dismount and back up!