

Lab 8: DLP - Disk/Email Encryption

Outline demo: <https://youtu.be/dob5emKJa3o>

1 PGP Encryption

An import element in data loss prevention is encrypted emails. In this part of the lab we will use an open source standard: PGP.

On your main desktop, install GPG from:

<http://gpg4win.org/download.html>

No	Description	Result
1	<p>From the console on your Windows desktop (C:\Program Files (x86)\GNU\GnuPG), create a key pair with (RSA and 2,048 bit keys):</p> <p>gpg --gen-key</p> <p>Now export your public key using the form of:</p> <p>gpg --export -a "Your name" > mypub.key</p> <p>Now export your private key using the form of:</p> <p>gpg --export-secret-key -a "Your name" > mypriv.key</p>	<p>How is the randomness generated?</p> <p>Outline the contents of your key file:</p>
2	<p>Now send your lab partner your public key in the contents of an email, and ask them to import it onto their key ring:</p> <p>gpg --import theirpublickey.key</p>	<p>Which keys are stored on your key ring and what details do they have:</p>

	<p>Now list your keys with:</p> <pre>gpg --list-keys</pre>	
3	<p>Create a text file, and save it. Next encrypt the file with their public key:</p> <pre>gpg -e -a -u "Your Name" -r "Your Lab Partner Name" hello.txt</pre>	<p>What does the –a option do:</p> <p>What does the –r option do:</p> <p>What does the –u option do:</p> <p>Which file does it produce and outline the format of its contents:</p>
4	<p>Send your encrypted file in an email to your lab partner, and get one back from them.</p> <p>Now create a file (such as myfile.asc) and decrypt the email using the public key received from them with:</p> <pre>gpg -d myfile.asc > myfile.txt</pre>	Can you decrypt the message:
5	<p>Next using this public key file, send Bill (w.buchanan@napier.ac.uk) a question (http://asecuritysite.com/public.txt):</p> <pre>-----BEGIN PGP PUBLIC KEY BLOCK----- Version: BCPG C# v1.6.1.0 mQENBFTvF+gBCACkpcMPybSe1NTE1hDg86gPcQqoT8kd9oS/ankGwbB4R5zT+3Ny MZWZwT431L99R7sfkluglwvkqko74Lemy9pBF/rbweweV6mCR3z1V3yTTv3zP1V5</pre>	Did you receive a reply:

	tLcz3K65f1RHPQU/FzxqH1T4kaH6dDiL/UuKKcyYMxxNnqERitJPU7ZJVhqeM3gi 4cG4znKY5fw8bdSpNC//pgkDzEaWYJFdyq/KqCwRK5r/Egj7FVHalGC371DgZKR5 dBoIvaOTfxYkJLe3Vc3dIv9LU58U3YHqsc/w6X4E5R/eEnp0IwKyb7oXdrFOM5ud DSoJ7aT24IqZW678vNtufGdr4OD+BF5r2UZpABEBAAG0GHcuYnVjaGFuYW5hQG5h cG11ci5hYy51a4kBHAQQAQIABgUCV08X6AAKCRBOV4Uk9xMsXJgNB/4jfAnXLHjZ +I4z3Hhqn9UMOKu6Q4cQtrGX0he1ymKZTMXNoSkhT5fb9GB1IIbwMkZHxCUNmUB PuAwq+RAhFqtrRkcH3x1a5eNBhEvcfi9hs21s43gsrxjMzekY6dyzD/ePM7HvihJ vrsQNZNI7ZIaP5vICZFgQqmwyQA1LCrEy/xpSXBNrqr0wuti+2+xeZsswityLAZA ryDMgCG9GPusfkmvatYJJr15QAhj1p0FKERhL1/h3bh18i8L1h1K9teBxIJf4ZIy ivV1bx5G36jci0rKCLi7/m6xhHh86brRQA++qwudXU/3MMqvRwuins09NYevcf6Y v66cJqTgdR1F =uiw7 -----END PGP PUBLIC KEY BLOCK-----	
6	Next send your public key to Bill (w.buchanan@napier.ac.uk).	

2 TrueCrypt

Now go to the DFET Napier Cloud, and you should have a Kali instance.

No	Description	Result
1	<p>Go to your Kali instance. Now Create a new volume and use an encrypted file container (use tc_<i>yourname</i>) with a Standard TrueCrypt volume.</p> <p>When you get to the Encryption Options, run the tests and outline the results:</p>	<p>CPU (Mean)</p> <p>AES: AES-Twofish: AES-Two-Serpent Serpent -AES Serpent: Serpent-Twofish-AES Twofish: Twofish-Serpent:</p> <p>Which is the fastest:</p>

		Which is the slowest:
2	Select AES and RIPMD-160 and create a 100MB file. Finally select your password and use FAT for the file system.	What does the random pool generation do, and what does it use to generate the random key?
3	Now mount the file as a drive.	Can you view the drive on the file viewer and from the console? [Yes][No]
4	Create some files your TrueCrypt drive and save them. Next dismount your drive, and copy the file to the provided USB stick. Give the USB stick to your neighbour, and see if they can view the file contents.	Without giving them the password, can they read the file? With the password, can they read the files?

3 TrueCrypt Volumes

The following files have the passwords of “Ankle123”, “foxtrot”, “napier123”, “password” or “napier”. Determine the properties of the files defined in the table:

File	Size	Encryption type	Key size	Files/folders on disk	Hidden partition (y/n)	Hash method
http://asecuritysite.com/tctest01.zip						
http://asecuritysite.com/tctest02.zip						
http://asecuritysite.com/tctest03.zip						

Now with **truecrack** see if you can determine the password on the volumes. Which TrueCrypt volumes can truecrack?

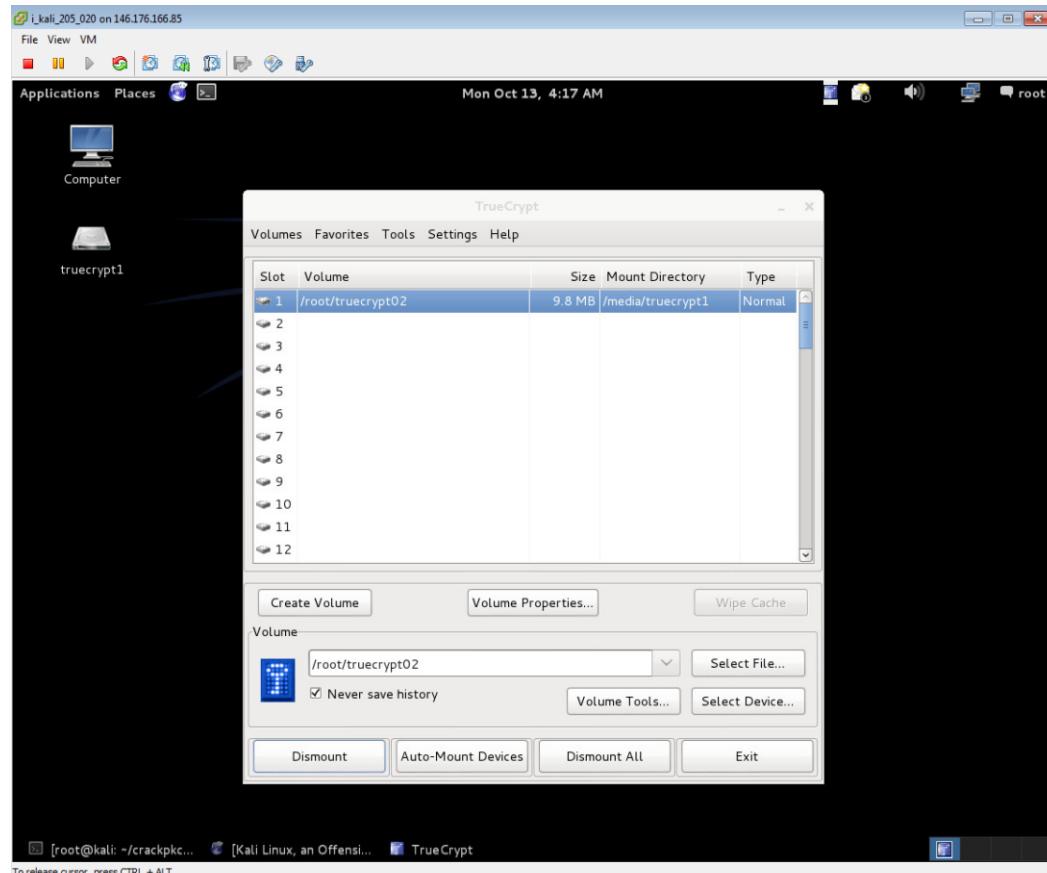


Figure 1: Kali mount

4 EFS

On your desktop, undertake the following.

No	Description	Result
1	Go to your Windows 7 instance. Now create a folder named: My_Enc_yourname Add some files to the folder, and then right click on the folder and encrypt it.	How does the name of the folder change when it is encrypted?
2	Now use: Cipher /u	Which files are encrypted on your drive:
3	Using: Cipher /c <i>filename</i>	Which encryption type and key size has been used for the file encryption?
4	Make sure you can view your files. Now export your certificates with: Cipher /r: <i>filename</i>	Which are the names of the files created? View the CER and PFX file. What is the difference between the two files?
5	Go to Control Panel -> Internet Options Then click on the Content tab and select the Certificates button. Now view your EFS certificate.	Outline some of the details of the EFS certificate. When does it expire? What type of encryption does it use? What is the length of the encryption key?

		Who has signed it?
6	Now delete the EFS certificate from the store and reboot your instance.	After reboot, can you access your files? [Yes][No]
7	Now import the PFX certificate that you created.	Can you access your files? [Yes][No]

5 EFS (with USB)

Undertake the following, but this time mount a USB stick, and encrypt on the USB device. First delete your existing EFS certificate.

No	Description	Result
1	Go to your Windows 7 instance. Now create a folder named: My_Enc_yourname Add some files to the folder, and then right click on the folder and encrypt it.	How does the name of the folder change when it is encrypted?
2	Now use: Cipher /u	Which files are encrypted on your USB disk:
3	Using: Cipher /c <i>filename</i>	Which encryption type and key size has been used for the file encryption?

4	<p>Make sure you can view your files.</p> <p>Now export your certificates with:</p> <p>Cipher /r:<i>filename</i></p>	<p>Which are the names of the files created?</p> <p>View the CER and PFX file. What is the difference between the two files?</p>
5	<p>Go to Control Panel -> Internet Options</p> <p>Then click on the Content tab and select the Certificates button.</p> <p>Now view your EFS certificate.</p>	<p>Outline some of the details of the EFS certificate.</p> <p>When does it expire?</p> <p>What type of encryption does it use?</p> <p>What is the length of the encryption key?</p> <p>Who has signed it?</p>
6	Now delete the EFS certificate from the store and reboot your instance.	After reboot, can you access your files? [Yes][No]
7	Now import the PFX certificate that you created.	Can you access your files? [Yes][No]
8	<p>Now dismount your drive, and give the USB stick to your neighbour.</p> <ol style="list-style-type: none"> 1. Ask them to access the files on the USB disk without importing the certificate. 2. Ask them to access the files on the USB disk after importing the certificate. 	<p>Can they access your files before certificate import? [Yes][No]</p> <p>Can they access your files after certificate import? [Yes][No]</p>

6 Cracking digital certificates and file types

Undertake the following.

No	Description	Result
1	<p>Run Networksims.</p> <p>Now run Toolkit client (Figure 2).</p> <p>Goto the Encryption tab and select Digital Certificate from the left-hand menu. Next click on the Dictionary Search button, and load each of the following files (remember to extract to PFX):</p> <p>http://asecuritysite.com/log/fred.zip</p> <p>http://asecuritysite.com/log/sample01.zip</p>	What are the passwords for the PFX files?

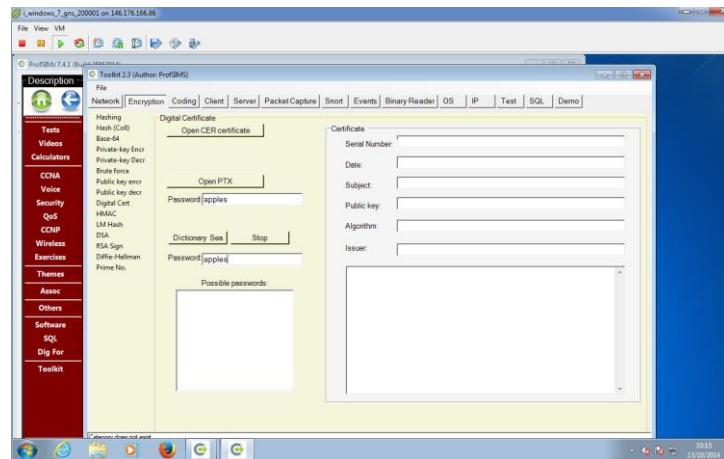


Figure 2: Dictionary search