Protecting Private Information with TrueCrypt

NCTCUG – January 4, 2012

Lorrin R. Garson

© 2012 Lorrin R. Garson

What Kind of Information Should Be Encrypted?

- Anything you don't want someone else to see...
 - Passwords
 - Medical
 - Financial
 - Insurance
 - Sensitive correspondence



What is TrueCrypt?

- Free, easy to use encryption software (open source*)
- Available for Windows (XP, Vista, 7), Mac OS X and Linux
- Protects folders & files are by strong encryption
- Volumes ("Safes"/"Vaults") are virtual disk drives within physical drives

* For information about Open Source, see 🚺 🚺



Installing TrueCrypt



Opening TrueCrypt Setup 7.1.exe	x
You have chosen to open	
TrueCrypt Setup 7.1.exe	
which is a: Binary File (2.7 MB)	
from: http://www.truecrypt.org	
Would you like to save this file?	
Left-click ► Save File Canc	el



Downloads	
TrueCrypt Setup 7.1(1).exe 3.3 MB — truecrypt.org	3:31 PM
Double-left-click*	
<u>Clear List</u>	Search P

*It may be necessary to enter Administrator password



TrueCrypt Setup 7.1

Please read the license terms

You must accept these license terms before you can use, extract, or install TrueCrypt.

IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

TrueCrypt License Version 3.0

Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.

I. Definitions

1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and

✓ I accept the license terms < Check the box</p>

TrueCrypt Installer

< Back

Cancel

Next >

X

.

Left-click on "Next" A



TrueCrypt Setup 7.1

Wizard Mode

Select one of the modes. If you are not sure which to select, use the default mode.

○ Install ◀ Select this option

Select this option if you want to install TrueCrypt on this system.

C Extract

If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).

TrueCrypt Installer –

Help

< Back

Cancel

Next >

Left-click on "Next" A



TrueCrypt Setup 7.1		
Setup Options Here you can set various options to control the installation process.		
Please select or type the location where you want to install the TrueCrypt program files. If the specified folder does not exist, it will be automatically created.		
C:\Program Files\TrueCrypt\	Browse	
✓ Install for all users		
Add TrueCrypt to Start mend		
Associate the .tc file extension with TrueCrypt		
Create System Restore point		
TrueCrypt Installer		
Help < Back Install	Cancel	

Left-click on "Install" A



- You will notice numerous files being installed in C:\Program Files\TrueCrypt
- You will be asked to contribute a donation



1	TrueCrypt Setup 7.1	
	TrueCrypt has been successfully installed NOTE Please consider making a donation. You can dick Finish anytime to close the installer.	
	TrueCrypt Setup	
E	If you have never used TrueCrypt before, we recommend that you read the chapter Beginner's Tutorial in the TrueCrypt User Guide. Do you want to view the tutorial?	
	Yes No	6
	TrueCrypt Installer	



Creating a TrueCrypt Volume ("Safe"/"Vault")

- Invoke TrueCrypt
 - From a shortcut on the desktop
 - From an object on the Taskbar
 - Start → [key] TrueCrypt → [double-left-click]
 TrueCrypt



TrueCrypt	×
Volumes System Favorites Tools Settings Help	Homepage
Drive Volume Size Encryption algorith □ D: □ □ F: □ □ G: □ □ H: □ □ I: □ □ J: □ ○ K: □ ○ N: ○ ○ O: ○ ○ P: ○ ○ Q: R: ► Left-click on "Create Volume"	Im Type
Create Volume Volume Properties, V	Vipe Cache
✓ ✓ S ✓ Never save history Volume Tools	elect File
Mount Auto-Mount Devices Dismount All	Exit



TrueCrypt Volume Creation Wizard

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

C Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

C Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

Help

Next >

Cancel

X

Left-click on "Next"

< Back

TrueCrypt Volume Creation Wizard



Volume Type

Standard TrueCrypt volume Select this option

Select this option if you want to create a normal TrueCrypt volume.

C Hidden TrueCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

Help < Back Next > Cancel

Left-click on "Next"





х





Left-click on "Save"

TrueCrypt Volume Creation Wizard



Volume Location C: \Users \Lorrin \Documents \DEMO Select File... Never save history A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created. WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now. ▲ NOTE Warning

X



Left-click on "Next"

TrueCrypt Volume Creation Wizard	X
FIPS-approved cipher (Rijndael, published in 1998) that maused by U.S. government departments and agencies to proclassified information up to the Top Secret level. 256-bit ket 128-bit block, 14 rounds (AES-256). Mode of operation is X More information on AES Benchmark Hash Algorithm RIPEMD-160 Information on hash algorithms	/ be tect /, 'S.
Help < Back Next >	Cancel

Encryption Algorithms: AES, Serpent, Twofish + 5 combinations Hash Algorithms: RIPMD-160, SHA-512, Whirlpool

Left-click on "Next'



Left-click on "Next"

TrueCrypt Volume Creation Wizard



Colorest and Provide State

Left-click on "Next"

TrueCrypt Volume Creation Wizard	
Ld	Volume Format Options VOTE: FAT is the default Filesystem Cluster Default Dynamic
Ce	Random Pool: 38BE323DD783B2E15CD824223955F4CC Header Key: Master Key:
	Done Speed Left
H H	IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
	Help < Back Format Cancel

Left-click on "Format"

Move the mouse around as randomly as possible for awhile, then left-click on "Format"



Left-click on "Exit"



Left-click on "OK" 🔺

Using TrueCrypt: Demonstration

- **Opening a TrueCrypt volume ("Safe**"/"Vault")
 - DEMO, PW = <><>MySecretStuff3141
- Accessing the contents
- Adding a file or folder
- Deleting a file or folder
- Closing a TrueCrypt volume ("Safe"/"Vault")*

*Closing a TrueCrypt volume encrypts its contents



DEMO

Other Encryption Software

- Cryptainer; free to \$30, \$45 & \$70. See 🚺
- Folder Lock; free and \$40. See
- SensiGuard; free and \$39. See 🚺
- SafeHouse; free and \$30 & \$60 🚺
- CryptoForge; \$30 to \$40. See 🚺
- PGP (Pretty Good Privacy*); free 100

*For information on PGP and the criminal investigation of Phil Zimmermann see 1



What now?

Safety first...

Protect your private information with encryption!



The End Thank you!