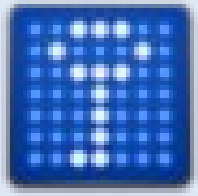
Introduction to TrueCrypt

WELCOME

11 January 2012

SLUUG - St. Louis Unix Users Group

http://www.sluug.org/



A Very Basic Tutorial and Demonstration

By Stan Reichardt

stanr@sluug.org

Introduction to TrueCrypt

DEFINITIONS

- Encryption
- Secrecy
- Privacy
- Paranoia
- Human Rights
- Self-determination

See http://www.markus-gattol.name/ws/dm-crypt_luks.html#sec1

Introduction to TrueCrypt

WHO

Who uses TrueCrypt?

- Who here has NOT used TrueCrypt?
- Who here has used TrueCrypt?

Introduction to TrueCrypt

WHO ELSE

Used by

- Businesses
- Military forces
- Government agencies
- Suspects (Possibly Bad people)
- Freedom Fighters (Against Bad Governments)
- Everyday People (That Want Privacy or Security)

Introduction to TrueCrypt

WHO WATCHES

Who watches the watchmen?

- http://en.wikipedia.org/wiki/Quis_custodiet_ipsos_custodes%3F

Introduction to TrueCrypt

WHAT

What is it?

GENERAL

- TrueCrypt is powerful encryption software for your personal data. It works by creating creating a virtual hard drive within a file and mounts it, so your computer treats it as a real hard drive. You can choose to encrypt an entire hard drive, certain folders, or removable media such as a USB flash drive.
- Encryption is automatic, real-time and transparent, so all the hard work is handled for you. It also provides two levels of plausible deniability, and supports various encryption algorithms depending on your needs, including AES-256, Serpent, and Twofish.

Introduction to TrueCrypt

WHAT IT DOES

What can it do?

The capabilities of TrueCrypt (taken from Users Guide, Introduction on page 6):

- TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data are automatically encrypted or decrypted right before they are loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g.., file names, folder names, contents of every file, free space, meta data, etc).
- Files can be copied to and from a mounted TrueCrypt volume just like they are copied to/from any normal disk (for example, by simple drag-and-drop operations).

Introduction to TrueCrypt

WHAT ELSE

The capabilities of TrueCrypt (taken from Users Guide, Security Model on page 83):

What does it do:

- Secure data by encrypting it before it is written to a disk
- Decrypt encrypted data after it is read from the disk

What doesn't it do?

- TrueCrypt files are **NOT** invisible
- Does **NOT** protect you from the system administrator
- Does **NOT** protect you from a compromised system
- And a large list of other things (2½ pages)...

Introduction to TrueCrypt

WHERE

Where can you use it?

PLATFORMS

Works on various Operating Systems:

- MS Windows (where it started)
- Linux (features were later added to MS Windows version)
- Mac OS X (added with TrueCrypt version 5 in February 2008)

Introduction to TrueCrypt

WHEN

When should it be used?

- When you are transporting data on a thumbdrive
- When you have sensitive data on a laptop
- When you have sensitive data on a desktop

When NOT to use?

- When visiting some foreign countries
- Possibly, when returning from foreign countries
- ?

Introduction to TrueCrypt

WHY

Why Use it?

- Free
- Security
  - Privacy
  - Retain Control over data (lost, seized, or stolen)
  - Prevent Identity Theft
- Multi-platform
  - runs on different Operating Systems
  - Encrypted files work across platforms
- If it was the norm, would reduce irrational association of guilt

Introduction to TrueCrypt

WHY NOT

Why avoid using it?

- Risk (Why you might want to avoid using it)
  - You may become a person of interest
    - Alligations of guilt
    - Easy target of further alligations
    - Instituionalized process
- Failure (You might shoot yourself in foot)
  - You might **forget** password
  - You don't follow additional recommended security precautions listed in documentation
  - http://www.truecrypt.org/docs/?s=security-requirements-and-precautions

Introduction to TrueCrypt

HOW

Downloading from http://www.truecrypt.org/downloads

MS Windows 7/Vista/XP/2000

- Download "***TrueCrypt Setup 7.1.exe***" (3.3 MB)

Mac OS X

- Download "***TrueCrypt 7.1 Mac OS X.dmg***" (9.8 MB)

Linux - Download (as appropriate) **** NOT LIKELY IN YOUR DISTRO REPOSITORY***

- Standard - 32 bit (x86) (2.5 MB)
- Standard – 64 bit (x64) (2.5 MB)
- Console only – 32 bit (x86) (1.6 MB)
- Console only – 64 bit (x64) (1.6 MB)
- This will provide a **.tar.gz** file containing an executable setup file

Introduction to TrueCrypt

BACKGROUND

Quickly

- Developed by TrueCrypt Foundation
- First released 2 February 2004 (Groundhog Day)
- TrueCrypt Collective License

Introduction to TrueCrypt

LICENSE

IANAL – I Am Not A Lawyer

- Custom multi-part license (parts under GPL 2)
  - http://www.truecrypt.org/legal/license
    - TrueCrypt is and will remain open-source
    - TrueCrypt is and will remain free software
  - Confirmed on page 121 of Frequently Asked Questions
    - TrueCrypt User's Guide, version 7.1
    - Released by TrueCrypt Foundation on 1 Sept 2011
- License not officially recognized by Open Source Initiative
- Not free of licensing issues, per some Linux distributions

Introduction to TrueCrypt

VERSIONS

- TrueCrypt first released 2 February 2004
- History of versions
  - http://www.truecrypt.org/docs/?s=version-history
- The current stable TrueCrypt 7.1 version was released on 1 Sept 2011
  - New: Full compatibility with 64-bit and 32-bit Mac OS X 10.7 Lion
  - Minor improvements and bug fixes (MS Windows, Mac OS X, and Linux)
- There are functional differences between the platforms
  - Mainly because of issues with proprietary Operating Systems
- There will NEVER be a commercial version of TrueCrypt

Introduction to TrueCrypt

COMMUNITY:

Open Source

- Peer review possible (by real cryptographers)
- Independent reviewers have found bugs

Introduction to TrueCrypt

OPERATING SYSTEMS

- Works On:
  - Windows NT Based (XP†,Vista,Win7)
    - † Dealing with hibernation files not guaranteed!
  - Mac OS X (10.4+)
  - Linux (kernel 2.6+)
- Does NOT work on:
  - FreeBSD, OpenBSD, NetBSD, Dragonfly BSD
  - Pre-Windows NT (9x,) Windows Mobile/PocketPC

Introduction to TrueCrypt

LAYERS

Different TrueCrypt layers

- File (container)
- Partition
- Disk (non-system)

Above must be mounted as TrueCrypt volumes

- Whole Disk (system)

Introduction to TrueCrypt

FILE CONTAINER

File container

- Creates a virtual encrypted disk within a file
- Encrypted file container acts like a directory (folder)
- Mounted as a TrueCrypt volume
- Files are encrypted within that TrueCrypt file volume
    - Anything placed in container is encrypted
    - Anything removed from container is decrypted

Introduction to TrueCrypt

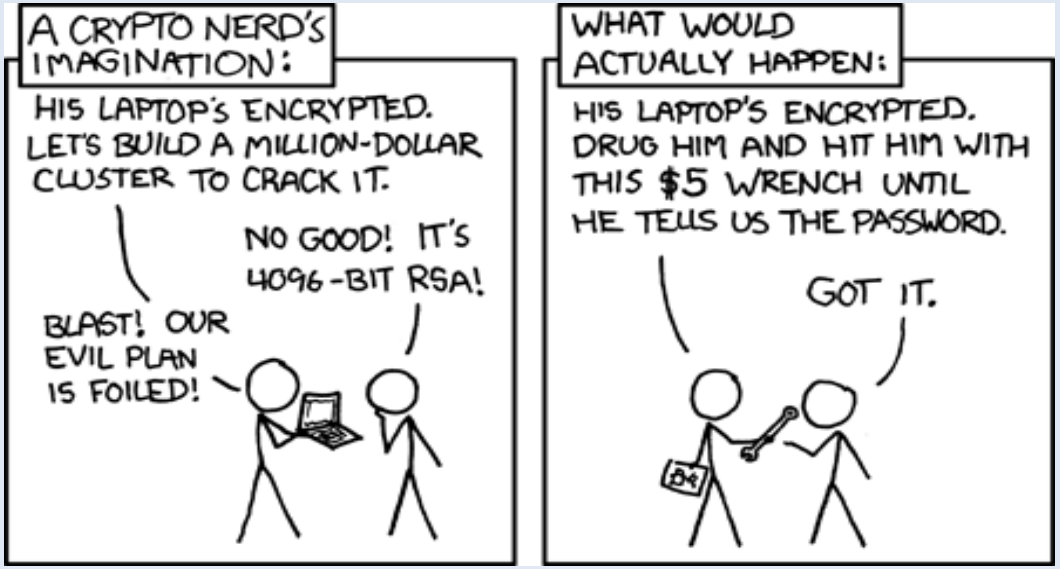
HIDDEN

Plausible Deniability

- Hidden Volume ***(a Volume Within a Volume)***
- Complex setup – ***lots of extra things to consider***
- http://www.truecrypt.org/hiddenvolume

Maybe NOT

- http://xkcd.com/538/



Introduction to TrueCrypt

PARTITION

Partition

- Encrypted partition mounted as a TrueCrypt volume
- Unmounted, it looks like it has not been formated
- Has to be encrypted before any data added

Introduction to TrueCrypt

DISK

Non-System Disk Encryption

- Non-system drives are mounted as TrueCrypt volumes
- Benefit:
    - Secure if stolen or lost
    - No Worry Disposal (You don't have to wipe it)

Introduction to TrueCrypt

WHOLE DISK

Whole Disk Encryption

- TrueCrypt can encrypt system drive (as of version 5)
- Requires CDROM/DVD burner to create recovery disc
- Includes Paging Files (Swap Files)
- Hibernation - added in version 5.1 (only on MS Windows?)
- Possibly improves response times
- Benefit:
    - Secure if stolen or lost
    - No Worry Disposal (You don't have to wipe it)

Introduction to TrueCrypt

PORTABLE MODE

Portable Mode

- Trust No One
  - Administrator account can track data
  - Can't compensate for a compromised system
  - May leave traces of activity
- Thumbdrive
  - TrueCrypt executable and driver requires Administrator access on host
  - TrueCrypt encrypted file container
  - Benefit:
    - Secure if stolen or lost
    - No Worry Disposal (You don't have to wipe it)

Introduction to TrueCrypt

HEADER

- Header data in each TrueCrypt volume
  - Not detectable
  - Contains a Master Key
  - Selected crypto algorithm (AES, Twofish,...)
- Master Key
  - Can backup header with initial password
  - Allows user to change password
  - If password lost, restore header (master key)

Introduction to TrueCrypt

FILE FORMATS

Portability of files

- You can copy and use TrueCrypt files across the different supported platforms.
- No discoverable distinct format for TrueCrypt files
  - No required naming convention or suffix
  - No detectable internal description
    - Run “man (5) magic” and see “magic” file
    - Run “file -s ” on the TrueCrypt file

Introduction to TrueCrypt

ALTERNATIVES

Some popular full disk encryption systems:

- Microsoft Bitlocker (proprietary)
- Apple FileVault (proprietary)
- McAfee Endpoint Encryption (SafeBoot) (proprietary)
- dm-crypt for Linux (GPL)

Other programs:

- http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

Introduction to TrueCrypt

COMPARISONS

See http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

Features To Compare:

- Hidden containers
- Pre-boot authentication
- Custom authentication (not clearly defined)
- Multiple keys
- Passphrase strengthening
- Hardware acceleration
- Trusted Platform Module
- Two-factor authentication

Introduction to TrueCrypt

FEATURES

See http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

Features that are in TrueCrypt:

- Hidden containers
- Pre-boot authentication (only in MS Windows)
- ~~Custom authentication~~ Does NOT Use (not clearly defined)
- ~~Multiple keys~~ Does NOT Use (not clearly defined)
- Passphrase strengthening
- Hardware acceleration
- ~~Trusted Platform Module~~ Does NOT Use – misleading ”security theater”
- Two-factor authentication

Introduction to TrueCrypt

INSTALLATION

Go get it

- Where can you get it? – Answered on ”HOW” slide.
  - Home Page
  - http://www.truecrypt.org/
- A few alternatives (**NOT recommended**):
  - The Open Disc Project (Free Open Source Software that runs on MS Windows)
    - http://www.theopendisc.com/
    - Does not have latest version.
  - File Hippo – Download Free Software site (MS Windows version only)
    - http://www.filehippo.com/software/security/

Introduction to TrueCrypt

DEMONSTRATION

Time for a demonstration?

- A few YouTube videos
  - How to install TrueCrypt on Linux Mint 12
  - JacksTech Tips#19 Encrypt your usb key
  - TrueCrypt on Ubuntu - tutorial
- Do we have time for live use examples?

Introduction to TrueCrypt

RESOURCES

TrueCrypt - Free Open-Source On-The-Fly Disk Encryption Software

for Windows ® Vista/XP/2000 and Linux

- http://www.truecrypt.org/

Wikipedia, the free encyclopedia

- http://en.wikipedia.org/wiki/TrueCrypt
- http://en.wikipedia.org/wiki/Disk_encryption
- http://en.wikipedia.org/wiki/Disk_encryption_software
- http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

Other

- http://otfedb.sdean12.org/ On-The-Fly Encryption: A Comparison
- http://www.markus-gattol.name/ws/dm-crypt_luks.html#sec1 (Interesting Essay)

Introduction to TrueCrypt

LEARNING RESOURCES

TrueCrypt Tutorial

- http://www.truecrypt.org/docs/

Painless Thumbdrive Backups

- http://www.linuxjournal.com/article/9311

eCryptfs: a Stacked Cryptographic Filesystem

- http://www.linuxjournal.com/search/node/TrueCrypt

Lockdown: Secure Your Files With TrueCrypt (PDF)

- http://www.makeuseof.com/pages/download-lockdown-secure-your-files-with-truecrypt
- Above PDF download requires password ”makeuseof”

Introduction to TrueCrypt

MORE RESOURCES

Gibson Research Corp • Security Now • Episode Archives (MP3 with PDF transcripts)

http://www.grc.com/SecurityNow

- Episode # 41, for May 25, 2006: TrueCrypt
- Episode # 133, for February 28, 2008: TrueCrypt 5
- Episode # 135, for March 13, 2008: IronKey
- Episode # 137, for March 27, 2008: RAM Hijacks
- Episode # 138, for April 3, 2008: Listener Feedback # 38
- Episode # 255, for June 30, 2010: Your questions, Steve's answers # 95
- Episode # 297, recorded April 20, 2011: Pass-Sentences

An Overview of Cryptography by Gary C. Kessler, 22 May 2011

http://www.garykessler.net/library/crypto.html

Introduction to TrueCrypt

FURTHER READING

Possibly relevant:

- **U. S. Constitution, Fourth Amendment**
  - **http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution**
- **Nineteen Eighty-Four** by George Orwell, 1949
  - http://en.wikipedia.org/wiki/Nineteen_Eighty-Four
  - Republished Plume (May 6, 2003) ISBN-10: 0452284236 or ISBN-13: 978-0452284234
- **Cryptonomicon** by Neal Stephenson, Avon Books Inc. NY,1999
  - ISBN-10: 0-380-97346-4
- **Daemon** by Daniel Suarez, Dutton/Penguin, 2009
  - ISBN-13: 978-0-525-95111-7 or ISBN-10: 0525951113
- **Freedom ™** by Daniel Suarez, Dutton/Penguin, 2010
  - ISBN-13: 9780525951575 or ISBN-10: 0525951571

Introduction to TrueCrypt

- CONSIDER THESE

- BILL OF RIGHTS DAY

  In memorium (15 December)

  http://en.wikipedia.org/wiki/United_States_Bill_of_Rights

- U. S. Constitution, Fifth Amendment

  http://en.wikipedia.org/wiki/Fifth_Amendment_to_the_United_States_Constitution

- Episode # 243, for April 8, 2010: State Subversion of SSL

  http://media.grc.com/sn/sn-243.mp3

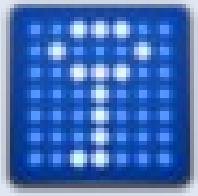
Introduction to TrueCrypt

QUESTIONS

http://www.truecrypt.org/faq

SLUUG - St. Louis Unix Users Group

http://www.sluug.org/



A Very Basic Tutorial and Demonstration

By Stan Reichardt

stanr@sluug.org