# Truecrypt "The Joys Thereof."

 $\mathbf{n}$ m a m



## "Truecrypt."

- •Wh What ?
- Why Why?
   How How?

 $\mathbf{n}$ n  $\mathbf{a}$ m a m a u m



#### "What?"

"TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device)."

n a m



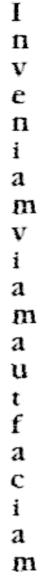
### "Truecrypt."

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed (pre-boot authentication).

n m a m  $\mathbf{a}$ 



## Demo.





## Why?

- Protection of IP
- Paranoia (USA Act)
- Protection of personal information



#### "The final straw."

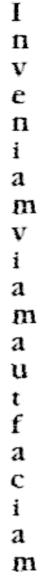
#### Plausible Deniability

- 1) Hidden volume (steganography) and hidden operating system.
- 2) No TrueCrypt volume can be identified (volumes cannot be distinguished from random data).

m



## Demo.





\* No data stored on an encrypted volume can be read (decrypted) without using

the correct password/keyfile(s) or correct encryption keys

the correct password/keyfile(s) or correct encryption keys.

\* Encryption algorithms: AES-256, Serpent, and Twofish. Mode of operation: XTS

m



## **Encryption Algorithms**

- · AES-256
- Serpent
- Twofish

 $\mathbf{n}$ m



## **Hashing Algorithms**

- Ripemd-160sha-512
- whirlpool

m



#### Shortfalls.

Doesn't support multi-boot configurations where a bootloader is installed in the MBR (grub / lilo)

When encrypting an entire drive you can't create any logical partitions

n m a u



## **Real World Application.**

- Full disc encryption for mobile users (laptop / r-drive)
- · Full disc encryption for remote servers in hostile environments
- · Safe storage of data off site (backups / configuration files)



## Thank you for your attention

