Truecrypt
“The Joys Thereof.”

Inveniamviamautfaciam

“Truecrypt.”

- Wh
- Why ?
- How ?

- What ?
- Why ?
- How ?

Invenimamviamautfaciam

“What ?”

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

Inveniamviamautfaciam

“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).

Invenia mviam autfaciam

Demo.

Why ?

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

Inveniamviamautfaciam

“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).

Inveniamviamaut faciam

Demo.

How ?

* Encryption is automatic, real-time (on-the-fly) and transparent.

* No data stored on an encrypted volume can be read (decrypted) without using
  the correct password/keyfile(s) or correct encryption keys.

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

Encryption Algorithms

- AES-256
- Serpent
- Twofish

Invenimvviamautfaciam

Hashing Algorithms

- Ripemd-160
- sha-512
- whirlpool

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

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)

Invenia m v ia m au t f ac ia m

Thank you for your attention

Inveniamviamautfaciam