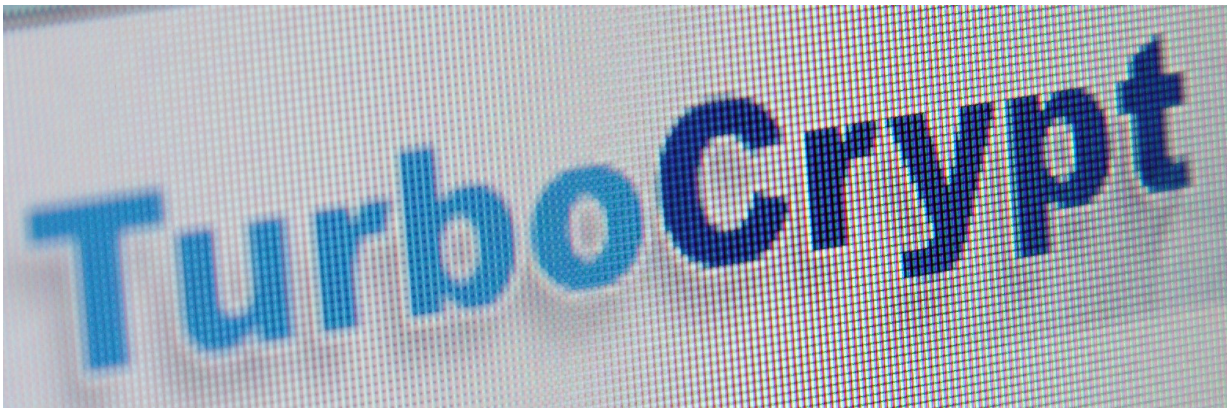

TurboCrypt 2008

FACT SHEET

General Description

TurboCrypt is an OTFE (On-the-Fly Encryption) disk encryption software that makes ultra-secure encrypted file hosted volumes available to users of all levels.
TurboCrypt drives are mounted at system start. To these drives can encrypted TurboCrypt volumes be mounted at any time.
TurboCrypt encrypted logical volumes are fast, seamless, integrated, and come with ultra-high security 1024 PMC encryption or alternatively FIPS-197 compliant AES encryption using four separate 256 bit AES engines.
All the structures needed by your operating system to recognise a file system of a particular type, such as FAT or NTFS, are made available through the TurboCrypt encryption driver. The plug-and-play TurboCrypt encryption driver has been programmed especially for Windows Vista 64, Vista 32 Operating Systems and is backward-compatible with Windows XP.

TurboCrypt is the only commercially available disk encryption software that is immune to Mount Control Code Attack and Backup Attack. It is further the only commercially available disk encryption software that allows for totally secure password entry. The built-in Trojan-Horse-proof Virtual Keyboard prevents malicious software like Trojan Horses and Computer Viruses from reconstructing user entry from mouse movements and screen logs.

TurboCrypt has been redesigned entirely so that:

- asymmetric ciphers prevent Trojan Horses from tapping data exchange between user interface and encryption driver
- even short passwords are comparably safe when the 1024 bit Polymorphic Cipher is used
- the existence of hidden volumes can be plausibly denied by users
- typical security holes like master keys, buffering of password data, weak encryption, fast generation of crypto context and likewise are avoided.

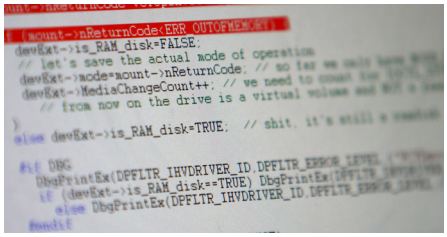

Fig. 1 Fotograph of source code snippet

Features

- Ultra-secure On-the-Fly Disk Encryption for Windows operating systems
- 'Type 1' 1024 bit Polymorphic Cipher with giant crypto context and extra-long crypto context setup running natively on 32 bit and 64 bit microprocessors.
- Additional AES Rijndael implementation if reduced data security is tolerated by the user
- Design hardened against attacks from malicious software that might even have infected the operating system (e.g. Mount Control Code Attack, Trojan-Horse-proof Virtual Keyboard)
- Trojan-Horse-proof Virtual Keyboard that prevents malicious software from logging password information
- Provision of two TurboCrypt drives that encrypted volumes are mounted to and that act as ramdisks in idle state
- Secure wipe of unused disk space using three different methods: Fast wipe, DoD 5220.22-M and Gutmann.
- Up to 2 Tb size of encrypted virtual volumes
- Full NTFS / FAT12 / FAT16 / FAT32 support
- Truly deniable encrypted volumes

Applications

- Protection of valuable data on notebook computers
- Parental control
- Data storage for Advocats, medical practitioners, scientists, etc.
- Countering of white-collar criminality

Mode of operation of TurboCrypt

TurboCrypt makes so-called file hosted encrypted volumes available to users. Such volumes are similar to a USB memory stick. Instead of being physical devices, file-hosted volumes are files that can reside on almost any storage medium.

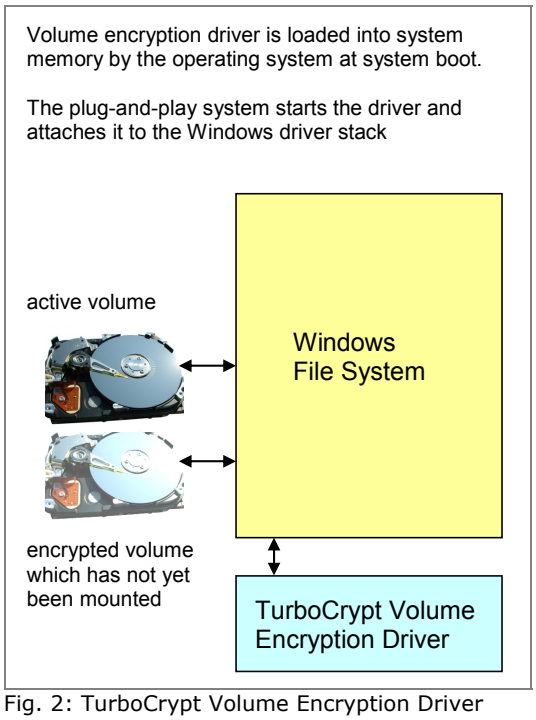

Fig. 2: TurboCrypt Volume Encryption Driver

In order to make these encrypted volumes available to users, TurboCrypt takes advantage of a software driver which translates disk input-output into read and write operations on mounted encrypted volumes.

Significantly enhance privacy with TurboCrypt

Privacy of existing software installations in offices is generally poor. Notebook computers can further get lost. Vital financial data or technical details of new developments can thus potentially be stolen.
By storing important data of your company on an encrypted TurboCrypt volume, the immanent risk potential is minimized.

Travellers might further take advantage of a unique feature of TurboCrypt – hidden volumes:
In case you're forced by an adversary to reveal your password, TurboCrypt provides 100% plausible deniability through hiding data in unused parts of a volume file. Existence of this data can be denied as it is absolutely impossible to even guess that there's additional data hidden in unused areas of an encrypted TurboCrypt volume.

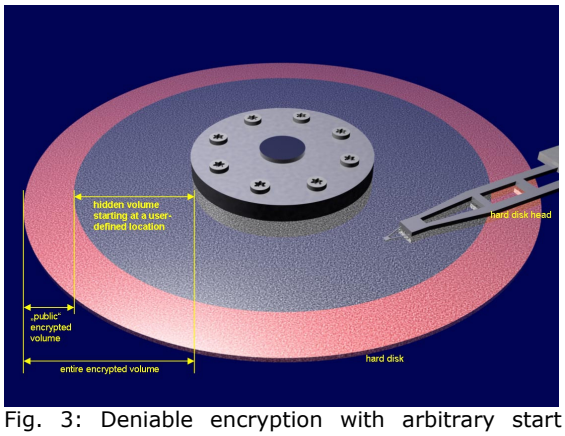

Fig. 3: Deniable encryption with arbitrary start sector

Secure password entry with the Trojan-Horse-Proof Virtual Keyboard

The photo below shows our invention of a virtual keyboard that allows for totally secure password entry. Conventional OTFE (On-The-Fly-Encryption) software - or encryption software in general - only allow for password entry by keyboard (or by smart cards and other authentication methods that are not suitable for guaranteeing perfect secrecy).

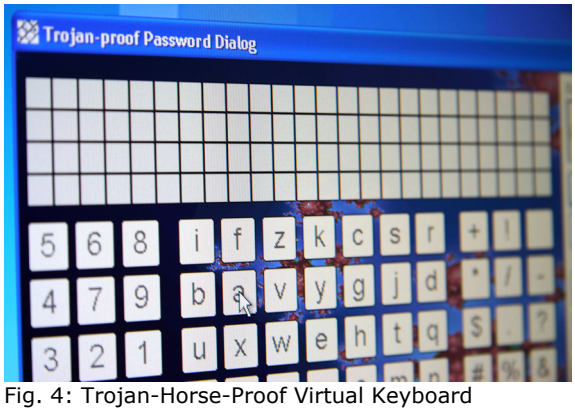

Fig. 4: Trojan-Horse-Proof Virtual Keyboard

Key characters are painted, deleted, painted again and deleted again. This sequence repeats itself several times per second. In order to keep highly intelligent trojan horses from taking a snapshot of the screen while all characters are visible, a characteristic that is inherent to the task scheduler, which is implemented in the core of the operating system, is exploited.

TurboCrypt is immune to Mount Control Code Attack

On-the-fly disk encryption software generally creates a virtual encrypted disk within a file and mounts it via a software driver as a real disk to the file system of a computer. In order to mount a virtual encrypted disk, a user interface application that is part of the software package, passes volume file path information, the selected encryption algorithm as well as the password to the software driver. By intercepting this so-called mount request, all required information to gain access to an encrypted volume is made available to an adversory in an extremely convenient way

TurboCrypt is immune to the Mount Control Code Attack by preventing Trojan Horses from tapping the data exchange between user interface and encryption driver.

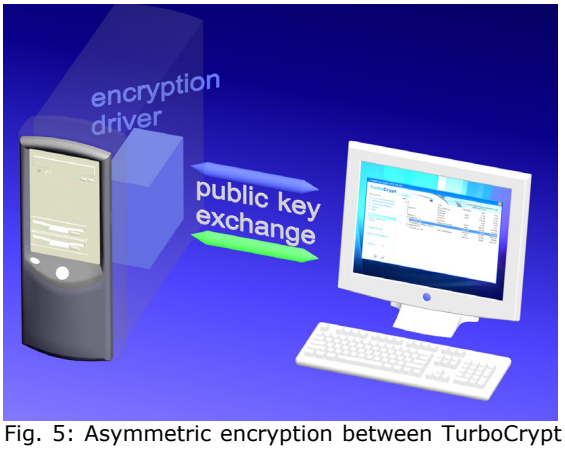

Fig. 5: Asymmetric encryption between TurboCrypt User Interface and the encryption driver

Prior to the execution of a task that requires optimum protection, both kernel-mode encryption driver and user-mode application (which controls the encryption driver) negotiate a key that subsequently remains private to both pieces of software. Password information, which is exchanged via the DeviceIoControl() kernel function, is thus totally inaccessible to the operating system.

Ease of use

Usability studies indicate that users are easily overwhelmed by complex interfaces. The new user interface is even easier to use compared with previous versions.
As an example, the encryption driver is automatically installed when the software is used for the first time. New versions automatically update the environment.

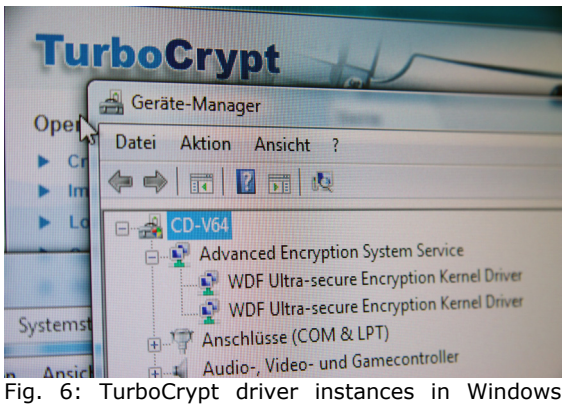

Fig. 6: TurboCrypt driver instances in Windows Device Manager

Certain security functionality although requires detailed knowlegde und understanding. For the Trojan-Horse-Proof Virtual Keyboard there's a test tool available in the program menu with which it is easy to adjust settings of the virtual keyboard.

For more information: http://www.pmc-ciphers.com