Truly deniable encrypted volumes in TurboCrypt

First published: July 2008

Global IP Telecommunications, Ltd. & PMC Ciphers, Inc. - Josephsburgstr. 85, 81673 Munich, Germany
Tel. +49 89 235 1468-0

Truly deniable encrypted volumes in TurboCrypt

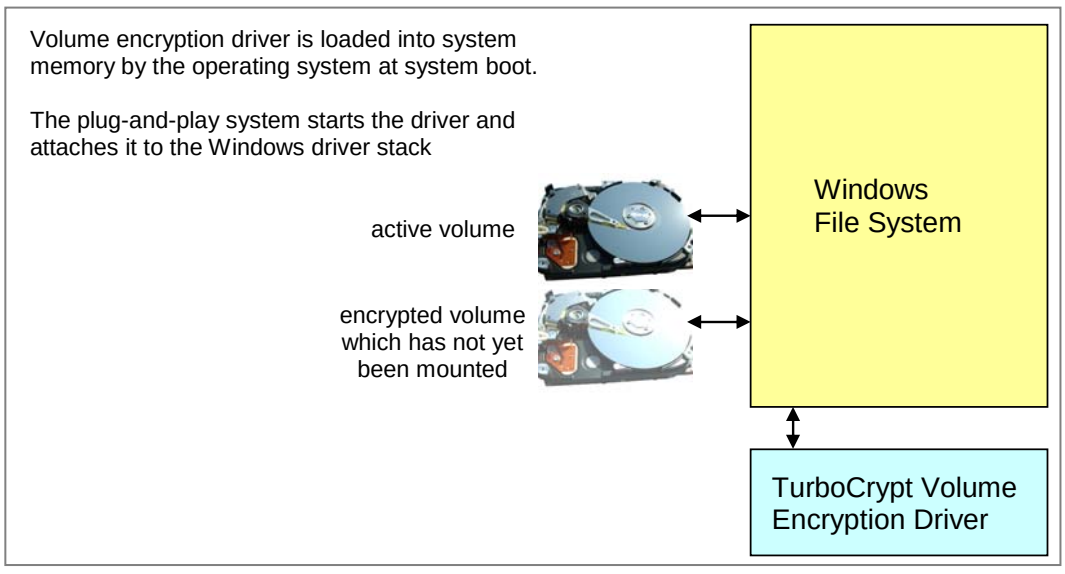
General paper

For the latest information, please see http://www.pmc-ciphers.com

Introduction

The idea dates back to the 90s when Julian Assange had the idea of a file system that enables for more than just one possible interpretation of data stored on that file system. In other words, password 1 reveils totally boring data while password 2 enables to read much more interesting things.
The TurboCrypt OTFE (On-the-Fly Encryption) disk encryption software enables users to deny the existence of more than just one interpretation of data stored in an encrypted volume. In TurboCrypt, data that has been encrypted with password 2 can be stored at almost arbitrary positions in a volume image file.

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. 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.



The TurboCrypt encryption driver is capable of providing an additional disk drive to the user. Data that is written to or read from an encrypted TurboCrypt volume is actually read or written to a physical disk device like an internal hard disk, an external disk drive or a USB stick.

Deniable volumes in TurboCrypt

In case you're forced by an adversary to reveal your password, TurboCrypt provides 100% plausible deniability through hidden volumes.

It should be explicitly noted that, although TurboCrypt volumes cannot be identified as a TurboCrypt volume, an adversary can still be sure that you're using encryption software because all encrypted volume files contain "noise". TurboCrypt volumes do not contain any file header or anything else that might identify them as a TurboCrypt volume. Although competitors sometimes pretend that adversaries cannot prove that encryption is used, they can very well do so.
TurboCrypt although can hide volumes in Windows Bitmap files (.BMP) and Audio files (.WAV). TurboCrypt containers (file-hosted volumes) further can have any file extension you like (e.g. .iso, .jpg, .mp3, etc.).

For extremely tough situations, that is when a TurboCrypt user is forced by somebody else to reveal the password to an encrypted volume, TurboCrypt provides users with the ultimate solution:

The photo show a real hard disk drive. Enormous amounts of data can be stored on the disk surfaces. Data is stored on individual tracks from the outside to the inside of a disk. Each track is divided into sectors. Sectors are the smallest unit of a disk. A sector is a group of 512 bytes.

The operating system computes for each disk access the sector number and subsequently performs read and write on the selected sector.

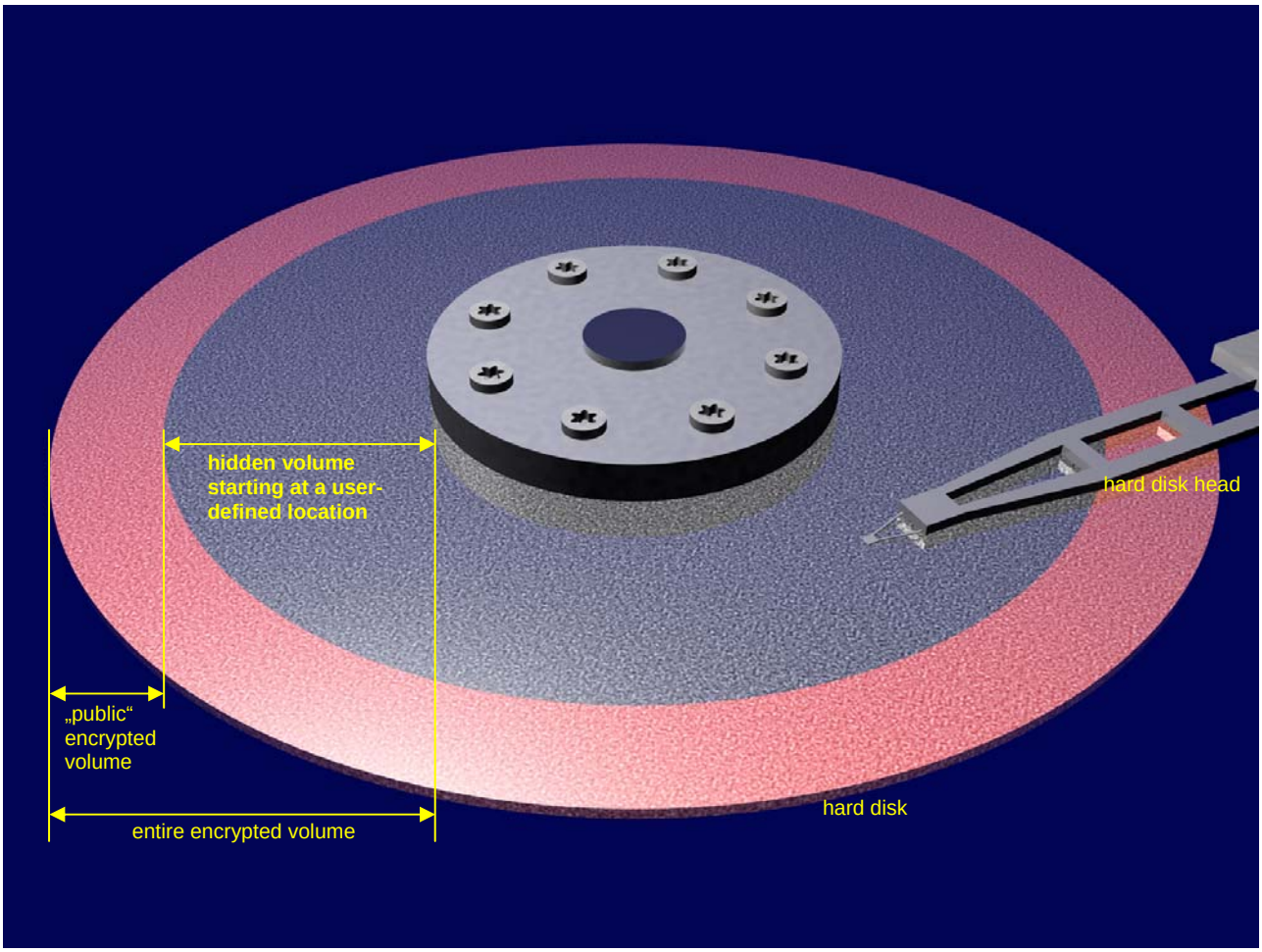
The following picture explains truly deniable encryption.

The hard disk symbolizes an entire volume. The volume is encrypted with a password that the user can give to anybody who asks for it. In other words, the user will store non-compromising information (e.g. pictures showing himself, Albert Einstein or his wife) there.

Within this "outer" volume is another volume stored. It's a hidden volume (shown in grey/blue color) – one that nobody would expect to find.

Sectors that don't overlap with this new "inner" volume belong to the outer volume only. They are shown in red. As most file systems write information from the start of a disk to the end incrementally, it is possible to occupy unused sectors for other purposes.

It should only be made sure that "unused" sectors of the outer volume don't get suddenly used. In this case would disk space of the outer volume (in red) be insufficient. The file system would simply write to sectors where information of the inner (hidden) volume (grey/blue color) is already stored! **Loss of data in the hidden volume would be the direct result.**
To an attacker the outer volume appears to contain noise. It is impossible for an attacker to identify the sheer existence of an inner and thus highly confidential volume. **During formatting, TurboCrypt writes to all data areas of virtual volumes that could possibly contain a hidden volume, data that looks like noise. Only this ensures TRUE deniability !!!**



TurboCrypt supports (almost) arbitrary start sectors for the inner (hidden) volume!
The lower limit for the start of sector of the hidden volume is the first data sector of the outer volume. If the start of the hidden volume was too close to the start of the outer volume, the outer volume would be corrupted.
The upper limit of the start sector is simply bound to the minimum size of the hidden volume, which is approximately 64Mb.

Users who want to take advantage of the unique feature of TurboCrypt to provide truly deniable hidden volumes must be aware that:

- they MUST remember the start sector they've chosen when they created the volume
- the password of the hidden volume should always be entered using the trojan-horse-proof virtual keyboard
- if they write too much data to the outer volume (which is not deniable and which thus should be secured with a very simple password), the start of the hidden volume CAN EASILY BE OVERWRITTEN !!! Loss of data is the direct result !!!

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

Global IP Telecommunications, Ltd. & PMC Ciphers, Inc. - Josephsburgstr. 85, 81673 Munich, Germany
Tel. +49 89 235 1468-0