TurboCrypt Design Goals

First published: August 2008

TurboCrypt Design Goals

General Paper

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

Introduction

Privacy is an important human right. We've always tried to protect privacy in the best possible way by hardening our data encryption software as much as possible and as much as ever reasonable.

Unfortunately have the early years of this millennium turned out to be very unfavourable for people who try to keep a little bit of privacy.

All in all it's simply high time to improve data security for companies, public organizations and private persons.
As a software programmer who is good in programming software solutions that help to protect privacy, it's a duty to help and to provide a good and inexpensive (or even free) solution.

Biggest problem: Hackers and assigned organizations are obviously targetting everybody these days. All at a sudden there's a great interest in what internet pages we visit, how we pay for things and what we store on our harddisks.

It is thus pretty likely that tampered versions of operating systems contain a number of trojan horses that report back to hackers all the data that has been gathered in the past.
Some clever pieces of malicious software can only be used extremely rarely as they would otherwise be found too easily by independent security experts. A good example is readout of logs during immigration into a country. Laptops can be confiscated by border authorities. There have been cases that laptops were returned by immigration officers after 12 entire months!!! Plenty of time to read out logs, to copy entire harddisks and to try and break passwords. No network trace would ever expose such a trojan horse!

Certain sponsors spend huge amounts of money on intelligence. It doesn't take much imagination to realize that such an adversory is ultimately powerful.

As the potential adversary might have plenty of money, security measures of traditional encryption software are totally insufficient. Poorly constructed USB tokens, manual password entry, etc. are an invitation for a powerful adversary.

Inadequacies of commercially available disk encryption software are primary design goals for TurboCrypt

Disk encryption has recently become very important for protecting privacy. On this market not every product really keeps what the manufacturer promises.

Fig. 1 Ultimate security is not possible to guarantee with fingerprint sensors (high False Acception Rate)

Fig. 2 Not ultimate as well: USB tokens and code-protected USB sticks (code protection, not data encryption)

Design goal	TurboCrypt with Polymorphic Cipher	Competitor products
Ultra-secure encryption algorithm	**1024 bit Polymorphic Cipher Engine that compiles the actual worker cipher from the password.**	**Use of DES (broken in 1997), TripleDES (stronger than DES, but not favoured by most experts) and AES (128 bit cipher that lacks safety margin and that was broken in 1999 in a smart card application)**
NO master password(s)	For many companies this feature is an absolute requirement. **Such kind of backdoor does not exist and will never be implemented in TurboCrypt.**	**Almost all products make a master key available. If an employee gets fired, data on his laptop computer can easily be accessed.**
Secure entry of passwords	Before 2008, all versions of TurboCrypt have **NOT** been trojan-horse-proof. **It is highly recommended to update all existing TurboCrypt installations!** **All new versions (since 2008) feature an invention of which we are very proud of: The Trojan-Horse-Proof Virtual Keyboard.**	**No competitor product known to us that features any kind of method to securely enter passwords.**
NO fingerprint sensors and NO USB tokens	As we cannot guarantee ultimate security with such devices, we don't support them.	**Fingerprint sensors use templates to compare against a previous scan. They are useless for deniable encryption as users will be asked to put their finger on a sensor.** **USB tokens: Hardware can be reverse-engineered and analyzed, e.g. by secondary electron microscopes.** **=> Too dangerous !!!**
Peer review	Experts are free to visit us at any time. **All sources can thus be freely reviewed.**	**Except for one open-source project, no peer review seems to be possible.** **Many conventional OTFE software products might be susceptible to Backup Attack and Mount IOCTL Attack. Please proceed to www.pmc-ciphers.com to read the corresponding white papers.**
Security enhancements for short passwords (extremely long key setup time)	**An absolute minimum of 1.000.000 transistor equivalents per PMC block and more than 100ms key setup time on a modern microprocessor make comparably short passwords safe against Brute Force Attacks.** Extremely long key setup time extends energy consumption multiplied by the time needed for Brute Force by at least factor 2.000.000 compared with AES. **Less than approx. 50.000 PMC blocks can be copied on an 8''wafer. The advantage over AES is better than 2^{21} (!!!).**	Less than 50.000 transistor functions are required to build an AES block in dedicated hardware. **Approx. 1.000.000 AES blocks can run in parallel on an 8'' wafer (45nm feature size) to try and break a code with Brute Force. <1µs key setup time enable an adversory to try at least 2^{40} key combinations per second. 40 bit per wafer and second do not leave any security margin.**
Use of customized ciphers	**For the Polymorphic cipher engine in TurboCrypt there cannot exist fast code-breaking hardware.** The design uses by far more resources than conventional ciphers and key setup time is extremely long. **The cipher does NOT exhibit a static structure.**	**As fast key setup must be a design goal for smart card applications but not for a disk encryption software nor for telephony software, use of AES or similar algorithms does not make sense.**
Encrypted communication with encryption driver	**Encryption driver and control panel application (user interface) exchange vital information through an encryption protocol similar to SSL.** Trojan horses can thus NOT get hold of password information.	**The entire communication between driver and control panel software (user interface) is carried out in the clear (as plaintext)!**
Use of provably secure encryption technology	**1024 bit Polymorphic Cipher built into TurboCrypt features largely provable security. Key size and block size are designed to keep a safety margin of 768 bit (an attack thus may reduce effective keysize from 1024 bit to 256 bit).** Please proceed to www.pmc-ciphers.com for more information.	**AES, Twofish, etc. have undergone extensive peer review, but none of the underlying concepts are provably secure. Although DES is similar to Luby-Rackoff, weakness solely stems from weak S-boxes and S-box size / key size.**

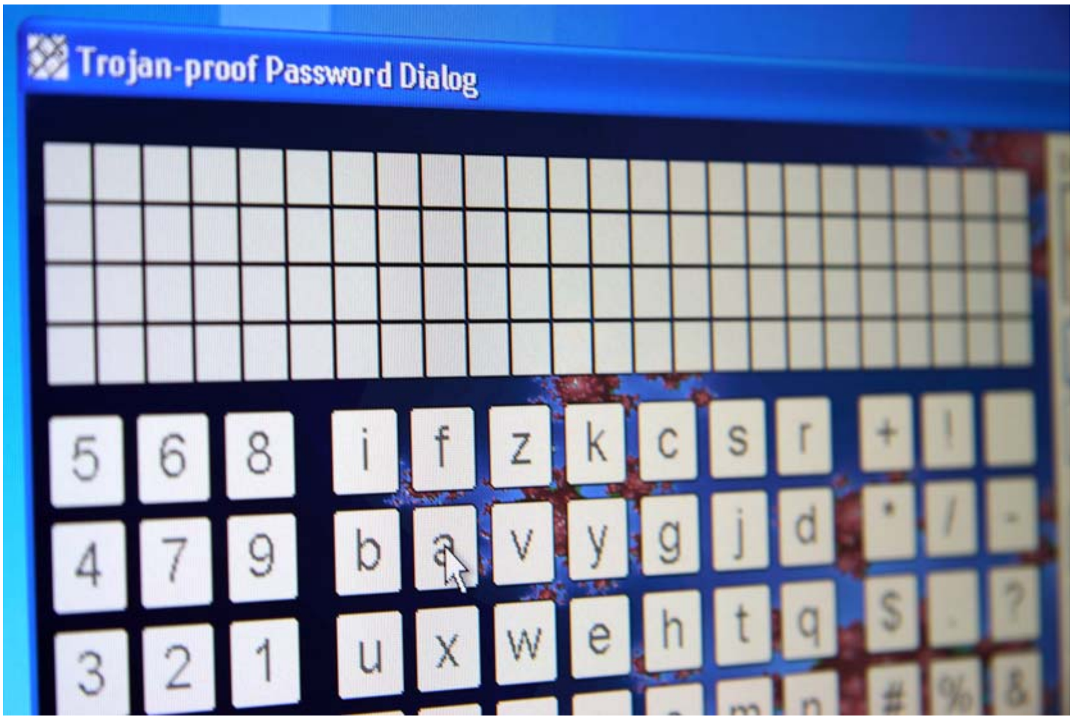
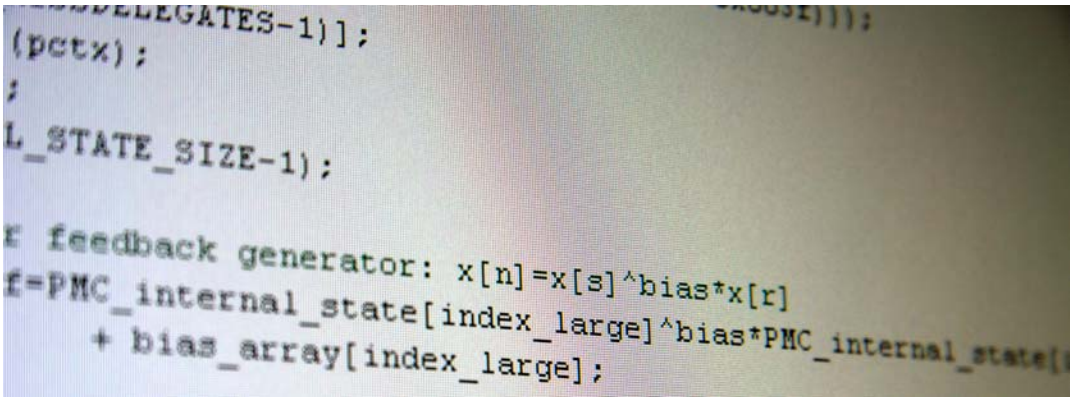

Trojan-proof Password Dialog
5 6 8 i f z k c s r + !
4 7 9 b a v y g j d * / -
3 2 1 u x w e h t q $. ?
m n # % &

Fig. 3 Trojan Horse-proof Virtual Keyboard



```
DELEGATES-1)];                              ]));
(pctx);
;
L_STATE_SIZE-1);

r feedback generator: x[n]=x[s]^bias*x[r]
f=PMC_internal_state[index_large]^bias*PMC_internal_state[
    + bias_array[index_large];
```

Fig. 4 Code snippet taken from the novel 1024 bit Polymorphic Encryption Algorithm implemented in TurboCrypt

Additional design goals

New attack scenarios makes a couple of additional product features mandatory:

Design goal	TurboCrypt	Competitor products
Camuflaging volume image files as multimedia files (music or images)	From 2008 all new TurboCrypt versions can create WAV and BMP files. **Playback of WAV files bigger than 4GB is possible.**	A few products support WAV files.
No product-specific header that might identify a volume file to be an encrypted volume.	From 2008 all TurboCrypt versions support this feature.	A few products support this feature.
Reset of file creation-, access- and write time	From 2008 all new TurboCrypt versions support this feature.	A few products support this feature.
Volumes that are hidden in bigger volume files	From 2008 all new TurboCrypt versions support this feature. **Start of file of the inner (hidden) volume is variable.**	A few products support this feature, but usually the start of file of the inner (hidden) volume is fixed.
No security holes	**Thorough analysis of possible leaks in competitor products as well as tough quality control during the programming of TurboCrypt ensures best possible design.**	**Two security holes in commercial competitor products and conceptually similar products have been identified by us.** For more information: Please visit www.pmc-ciphers.com.

Deniable encryption

Figure 5 and 6 show two real harddisk drives. Enormous amounts of data are stored on the disk surfaces. Sometimes two or more disks are stacked in order to increase capacity. Data is stored on individual tracks from the outside to the inside of a disk. Each track is divided into sectors. Sectors the smallest units of a disk. A sector is a group of 512 bytes.

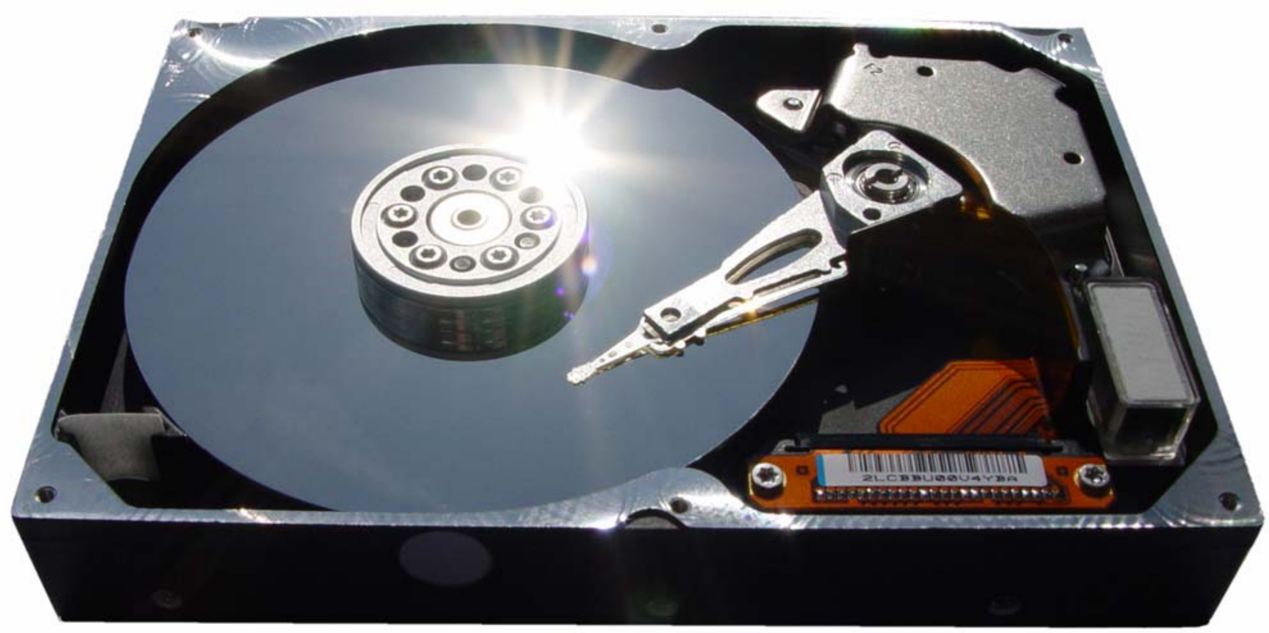


Fig. 5 Photo of a modern harddisk

Fig. 6 Closeup on magnetic harddisk head

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 deniable encryption. The harddisk symbolizes an entire volume. The volume is protected 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) on it. 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 in the outer volume (in red) not be sufficient. 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 !!!**

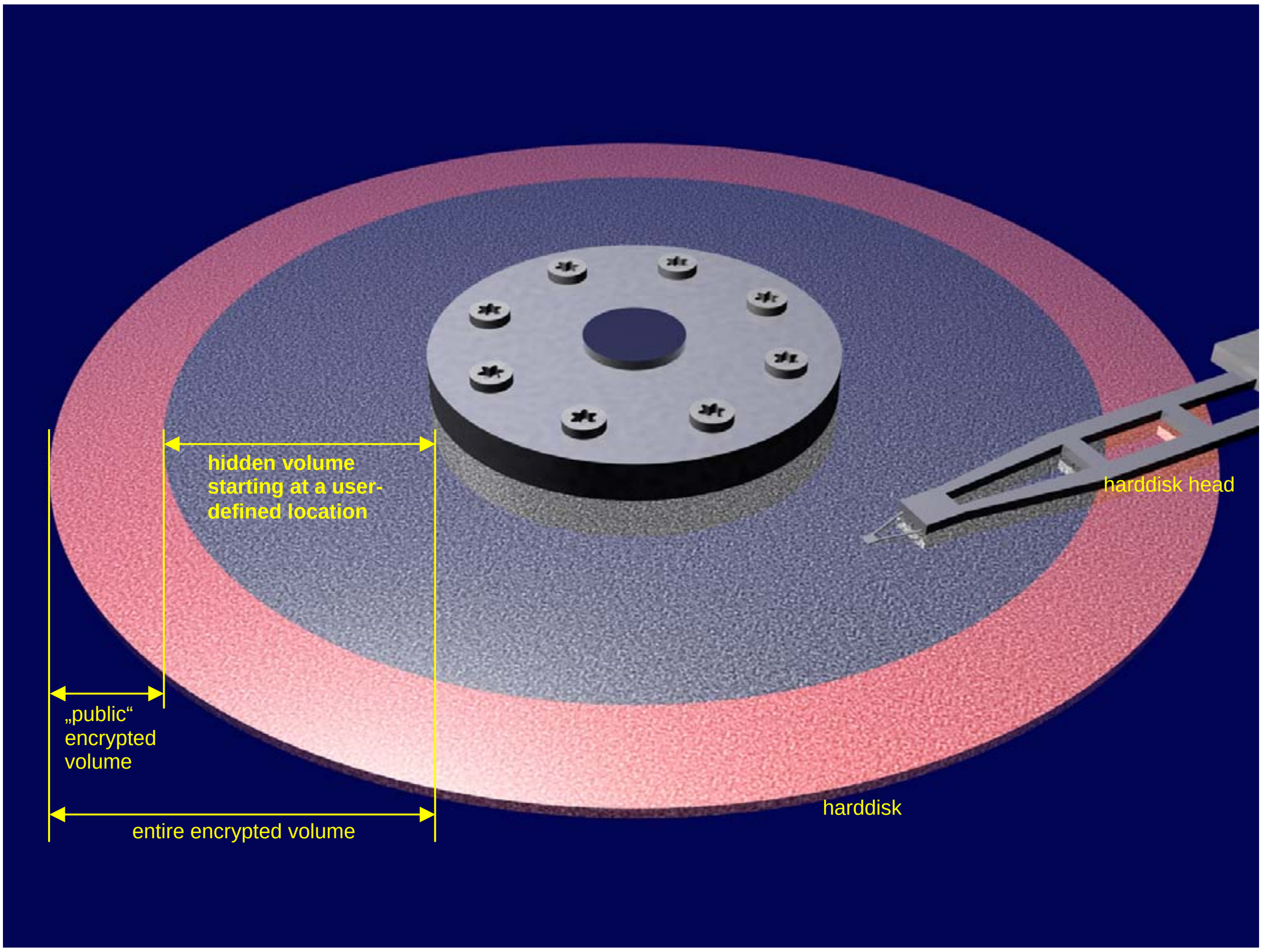
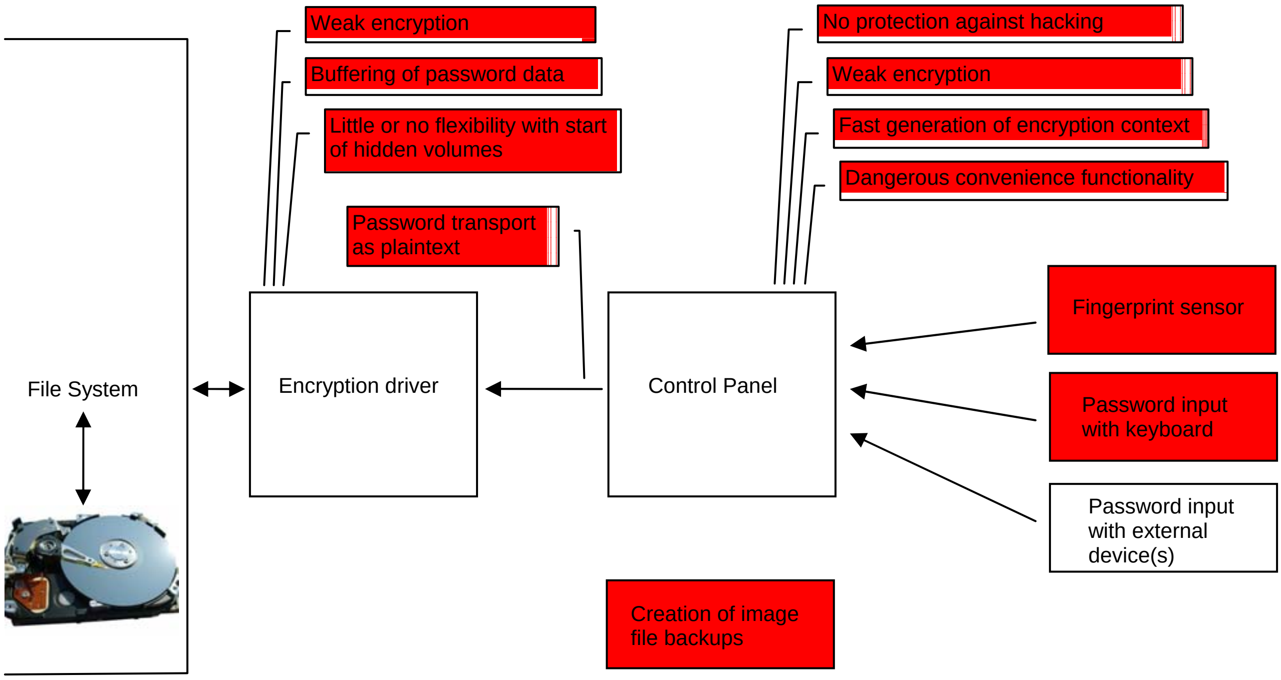

hidden volume starting at a user-defined location
harddisk head
„public“ encrypted volume
harddisk
entire encrypted volume

Fig. 7 Deniable encryption. TurboCrypt supports arbitrary start sectors for the inner (hidden) volume

No security holes

Not only that we've located potential security holes in disk encryption software, we've additionally taken great care that each and every part of TurboCrypt is designed in a bulletproof way.

These are the neuralgic points for convential OTFE software:


Weak encryption
Buffering of password data
Little or no flexibility with start of hidden volumes
Password transport as plaintext
No protection against hacking
Weak encryption
Fast generation of encryption context
Dangerous convenience functionality
File System
Encryption driver
Control Panel
Fingerprint sensor
Password input with keyboard
Password input with external device(s)
Creation of image file backups

The entirety of the red boxes and the necessity to write code for a number of microprocessor platforms was actually the reason why TurboCrypt has been redesigned from scratch. Here's an explanation for each red box:

User interaction	Conventional OTFE Software	TurboCrypt with Polymorphic Cipher
Fingerprint sensors	Very convenient and good for general access control, but **the mode of operation makes such devices inacceptable to protect ultra-secure encrypted volumes.**	**No support for fingerprint sensors as our primary design goal is ultimate security.**
Password input with keyboard	Used to be no problem, but these days not only hackers try to do "phishing". **Organizations that have sufficient resources to spend millions or even billions on the development of viruses are on the radar screen these days.**	**TurboCrypt is equipped with a phantastic invention: The Trojan-Horse-proof Virtual Keyboard. Passwords are thus protected in the best possible way.**
Secure entry of passwords	Before 2008, all versions of TurboCrypt have **NOT** been trojan-horse-proof. **It is highly recommended to update all existing TurboCrypt installations!** **All new versions (since 2008) feature an invention of which we are very proud: The Trojan-Horse-proof Virtual Keyboard.**	**Wouldn't it be great to be able to enter passwords without giving any kind of trojan horse or virus any opportunity to log anything? To our knowledge, TurboCrypt is the ONLY OTFE encryption tool with such a useful feature!**
Password input with external devices	Potentially secure, but too expensive. As it's expensive, such mechanisms are only used in specialized applications like ATMs.	**TurboCrypt provides the user with a 100% secure and inexpensive alternative: the Trojan-Horse-proof Virtual Keyboard.**

Backups	Conventional OTFE Software	TurboCrypt with Polymorphic Cipher
Secure function for the creation of backups	Conventional OTFE software leaves the creation of backups of volume files up to the user. We've been able to show that this is more than only dangerous as **information leaks easily without the need to know anything about the encryption key!** For more information: Please visit www.pmc-ciphers.com.	**TurboCrypt comes with a 100% secure function to create backups of image files.** For more information: Please visit www.pmc-ciphers.com.
Functionality to warn users when mounting old volume image files	**To our knowledge, no conventional OTFE software is known that warns users** (the underlying weakness was previously unknown or neglected)	**TurboCrypt can warn users if a copied image file is to be mounted.**

User interface	Conventional OTFE Software	TurboCrypt with Polymorphic Cipher
Protection against hacking	Hackers can decompile software and change functions calls or leave them out. Although usually only games are affected in order to surpass the license protection mechanism, **this method is very effective e.g. to limit passwords effectively to a few bits only. As the source code of a quite well-known open-source project is publically available (which is a plus for peer review), it is likely that weak versions are offered for download and installed by unsuspecting users.**	**TurboCrypt is protected against changes with a highly sophisticated multi-level protection scheme for the license as well as for the machine code.**
Weak encryption	**Algorithms like DES, which is a 56 bit cipher that can be cracked easily these days. AES is certainly much more secure with password lengths of 128, 192 and 256 bit, but it still remains a 128 bit block cipher that is not approved for use by U.S. government agencies for the encryption of classified information.**	**AES with 4x256 bit keys is available, but use of the proprietary 1024 bit Polymorphic Cipher is highly encouraged.**
Generation of encryption context	Fast generation of encryption context is usually seen as an advantage of small ciphers like DES, AES, Twofish, etc.. 8 bit microcontroller hardware like the famous 8051 (created in 1976), only tolerates small ciphers that compute round keys very quickly from the key. CPUs like the 8051 can be found in washing machines, toys, etc.. OTFE software like TurboCrypt although solely runs on CPUs like the Intel Pentium 4, Intel Core Duo, AMD Athlon64, etc.. Each of these target CPUs is more than a million times faster than an 8051. As a matter of consequence do modern microprocessors easily compute all round keys from a key (also called the crypto context) within a fraction of a microsecond. This fact can be exploited by novice hackers as well as by professionals to try each and every password combination. For some products there there are even more or less effective tools available! On www.lostpassword.com one can read that **"With 95% recovery rate for English words, password search speed is over 2,000,000 passwords per minute."**	Wouldn't it be better if the recovery rate was only 100 or 200 passwords per minute? **As the 1024 bit Polymorphic Cipher implemented in TurboCrypt is not intended to run on washing machines or likewise, one of the design goals was the use of as much chip space of 32 or 64 bit CPUs as possible and to maximize complexity as well as the amount of computations required to compute the crypto context from the key.** **=> Brute Force Attack runs several ten thousand times slower than with AES/SHA-1 or AES/SHA-256.**
Dangerous convenience functionality	**Everything that is related to "master passwords" or "forgotten user password recovery" is a potential weakness.**	**TurboCrypt is definitely free of any backdoors, even if this is sometimes very inconvenient to have to tell a customer that all his data is gone if he cannot remember his password.** **To us, security is more important than convenience.** Users who seek maximum convenience will find suitable software for his needs elsewhere.

Driver-related issues	Conventional OTFE Software	TurboCrypt with Polymorphic Cipher
Password transport as plaintext	It is very likely that there's not a single tool available that protects transport of the password to the encryption driver. Organizations who develop their own trojans and/or viruses will definitely spend a few bucks on enabling their trojan horse(s) to spy on the driver stack. OTFE software always passes the password down to the encryption driver when a volume is to be mounted. **If the password is transported in the clear, then there's no security at all. A well-programmed trojan-horse can intercept this data and as this is technically possible, it will be done.**	**TurboCrypt encryption driver and control panel exchange vital information through an encryption protocol similar to SSL. Trojan horses can thus NOT get hold of any password information.**
Weak encryption	See above	See above
Buffering of password data	Some drivers buffer passwords. There is a potential risk that parts of the kernel which operate at ring 0 (full access to any memory location) can exploit this feature. Risk is low but immanent.	**The TurboCrypt encryption driver does not buffer passwords. Password information is immediately processed and destroyed. Encryption context of the 1024 polymorphic encryption algorithm is several 100kB in size and it different for every block that is encrypted!!! Encryption contexts of AES and likewise are rarely bigger than 100 bytes.**
Flexibility for start of hidden volumes	**Conventional OTFE software usually uses a fixed start sector for hidden volumes. Adversories thus know exactly where to try a Brute Force Attack to uncover a hidden volume.**	**TurboCrypt tolerates arbitrary start of hidden volumes. A 1GB volume thus can potentially house approx. 2 million different hidden volumes (one hidden volume, but 2 million different and equally probable start sectors). Adversories need 2 million times more time and computing power to try and uncover a hidden TurboCrypt volume compared with conventional disk encryption!**

TurboCrypt features in comparison with competitor products

Functionality	TurboCrypt	Others
File Hosted Volumes	x	x
Encryption of entire Partitions	only old versions support this feature as most users didn't use this functionality	(x)
Pre-boot Authentication		very few products support this feature
Deniable (hidden) Volumes	x	(x)
Arbitrary Start of Hidden Volumes	x	
Hiding of Data in Multimedia Files	.bmp and .wav	(.wav)
Reliable Password Sniffing Protection	x	Products might be susceptible to Trojan Horses
Master Password		x THIS IS HIGHLY DANGEROUS
Password Recovery		x THIS IS HIGHLY DANGEROUS
Secure Disk Deletion	x	(x)
Disk Sharing	x	(x)
Recovery of Encrypted Data		x THIS IS HIGHLY DANGEROUS
USB Drive Support	x	x
Fingerprint Sensor Support		x THIS IS HIGHLY DANGEROUS
1024 bit Polymorphic Cipher	x	
Block Size of Encryption Algorithm	1024 bit	128 bit (maximum)
Protection against Code-breaking Hardware	x	Approx. 1.000.000 AES blocks can run in parallel on an 8’’ wafer and sieve 10^{12} keys per second
Availability of Customized Cipher	x (on request)	
Proofness against New Attacks on Effective Linearity of the Cipher	x	Potentially susceptible to future attacks that decrease effective key size
Reserve Key Size	768 bit	no reserve
AES Support	x	x
Cipher Stacking (Cascades)		x Susceptible to Meet-in-the-Middle Attack
Long Key Setup Time	x	Short passwords are susceptible to Brute-Force Attack (>500.000 keys per second)
No checksums	x	
Reset of file creation and access times	x	
Proofness against Backup Attack	x	Products might potentially be

		susceptible to Backup Attack
Proofness against MOUNT Control Code Attack	x	**Products might potentially be susceptible to MOUNT IOCTL Attack**

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

This is a preliminary document and may be changed substantially prior to final commercial release. This document is provided for informational purposes only and PMC Ciphers & Global IP Telecommunications make no warranties, either express or implied, in this document. Information in this document is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of PMC Ciphers or Global IP Telecommunications.

PMC Ciphers or Global IP Telecommunications may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from PMC Ciphers or Global IP Telecommunications, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.