TCTEMP
USER'S GUIDE

Version 1.7

Contents

General Information

TCTEMP automates the process of using TrueCrypt[1] to on-the-fly encrypt the Windows paging (swap) file, temporary files, and print spooler files.

TCTEMP creates new random keys and a new random password for a TrueCrypt volume during Windows startup. It then mounts the TrueCrypt volume and initializes the volume's file system. The mounted TCTEMP TrueCrypt volume is suitable for temporary files and for print spooler files.

The file system is initialized by copying the contents of an image file to the TrueCrypt volume. Only those sectors are copied to the TrueCrypt volume which are required to replicate the file system. The initialization procedure should therefore be as fast as using quick-format.

Caution: Moving the paging file to the TCTEMP volume is still experimental. It is known for the current TCTEMP version that a STOP error (blue screen) can occur during Windows shutdown after the paging file has been moved to the TCTEMP volume.

System Requirements

Supported operating systems:	Windows Vista/XP/2000/2003 and Windows Vista/XP/2003 x64 Edition
Required TrueCrypt version:	4.3a

Latest Version

The latest TCTEMP version can be downloaded from the TCTEMP project homepage[2]. The authenticity of the downloaded files can be checked with the public project key[3].

Licensing Information

TCTEMP may be used, modified and/or distributed under the terms of the TrueCrypt Collective License Version 1.2 (see *License.txt*).

Copyright Information

1 Based on TrueCrypt, freely available at http://www.truecrypt.org/
2 TCTEMP project homepage: http://www.tctemp.80t.com
3 Fingerprint of the TCTEMP project key: 75EB 6BC2 01B7 F6E7 4BD7 CC58 4A5F C393 19EE 6E69

Technical Description of TCTEMP

TCTEMP is started early in the boot process (just after the hard disks have been checked) and works as follows:

1. TCTEMP fills its entropy pool with the contents of the CPU time stamp counter
2. TCTEMP fills its entropy pool with volatile system information
3. [32-bit Windows only:] TCTEMP fills its entropy pool with 64 bytes from the VIA CPU RNG if a VIA CPU RNG is present and enabled
4. TCTEMP fills its entropy pool with the contents of the CPU time stamp counter
5. TCTEMP processes the command line arguments
6. TCTEMP fills its entropy pool with the contents of the CPU time stamp counter
7. TCTEMP fills its entropy pool with the last access time of the image file
8. TCTEMP fills its entropy pool with the contents of the CPU time stamp counter
9. TCTEMP reads the encrypted header of the unmounted TCTEMP TrueCrypt volume
10. TCTEMP fills its entropy pool with the contents of the CPU time stamp counter
11. TCTEMP fills its entropy pool again with volatile system information
12. TCTEMP fills its entropy pool with the contents of the CPU time stamp counter
13. TCTEMP creates new volume keys and a new password for the TCTEMP TrueCrypt volume with the same key deriving function which is later used to derive the header keys. The 2nd 64-byte-block of the encrypted header is used as salt, and the entropy pool is used as password.
14. TCTEMP initializes a buffer for the new volume header with zeros and copies the new volume keys to the header buffer
15. TCTEMP encrypts the salt of the header buffer with the new volume keys using 0xfffffffffffffff8 as start index for LRW mode
16. TCTEMP derives the header keys and encrypts the header buffer
17. TCTEMP replaces the header of the TCTEMP TrueCrypt volume with the header buffer and mounts the TrueCrypt volume.
18. TCTEMP copies the contents of an image file to the sectors of the mounted TrueCrypt volume in order to restore the file system.

If a weak key (or password) is detected after calling the key deriving function, then one salt byte is incremented and the key deriving function is called again (up to 254 times). TCTEMP aborts its operation if it cannot create a non-weak key or password. In this case, the TCTEMP TrueCrypt volume is not available for the system.

Installing TCTEMP

Note that the installation procedure will replace the registry value

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\
> BootExecute

with the default Windows value. A further entry is then appended to this value in order to start TCTEMP during system startup.

TCTEMP can be installed as follows:

1. Start *INSTALL\INSTALL.CMD*
2. If Windows notifies you that an unidentified program (namely *TCTEMP Setup.exe*) wants access to your computer, then press *Allow*.
3. [If TCTEMP is already installed:] Enter *1* to re-install TCTEMP
4. Enter *1* to *9* to change the TCTEMP settings. Please mind the following restrictions:
   - **Iteration count:** It is usually the best choice for most users to set the iteration count multiplier to 1. If this value is set too high, the computer might appear to be not bootable because it is busy with deriving the new keys and password. You can check how long it takes for TCTEMP to create the new keys and password by installing the TCTEMP DEBUG version. The time between displaying the command line and the text “Restoring file system…” is used to create the new keys and should be proportional to the iteration count multiplier.
   - **Volume name:** If you want to use an encrypted partition instead of a container file you must specify the TCTEMP volume with the nomenclature ***__*D*__*evice*__*H*__*arddisk0*__*P*__*artition2*. Be aware that the device/partition name is case sensitive, and make sure that you use correct values for the hard disk number and the partition number (*TrueCrypt.exe* can be used to find the right values).
5. Enter *i* to install TCTEMP

TCTEMP can be upgraded (or downgraded) by installing the new TCTEMP version without uninstalling a previously installed TCTEMP version.

Changing the Location of the Print Spooler Files

The location of the print spooler files can be redirected as follows (see also [6] and [1]):

1. Open *Control Panel*
2. Open *Printers*
3. Select menu item *File→Server Properties*
4. Select *Advanced*
5. Enter a new location for the print spooler files

Changing the Location of the Paging File

The location of the paging file can be redirected to the TCTEMP TrueCrypt volume as follows (see also [6] and [7]):

1. Right-click *My Computer*
2. Select *Properties*
3. Select *Advanced*
4. Press *Performance Options...*
5. Press *Change...*
6. Select the drive letter of the TCTEMP TrueCrypt volume, enter the values for *Initial size* and *Maximum size* and press *Set*
7. Select all other drive letters, remove the values and press *Set*
8. Press *OK* (as often as possible)

Caution: Moving the paging file to the TCTEMP volume is still experimental. It is known for the current TCTEMP version that a STOP error (blue screen) can occur during Windows shutdown after the paging file has been moved to the TCTEMP volume.
However, the occurrence of this STOP error can be reduced by changing the system's paging behavior (see [8], [9] and [10]), and by loading the TrueCrypt driver as soon as possible. These optimizations are optionally made during the installation procedure of TCTEMP.

Security Precautions

The automatically generated keys are possibly less secure than keys generated by TrueCrypt because the system offers less entropy sources during startup.

Troubleshooting

Disabling TCTEMP

A native startup application has always the potential to make the operating system unbootable. In this case TCTEMP can be disabled as follows:

1. Boot from Windows setup disk
2. Select *Repair Console*
3. Enter the administrator password
4. Enter *cd system32*
5. Enter *del tctemp.exe*

Frequently Asked Questions

Q: ***What was the reason of using an image file and not using quick-format instead?***

A: *The reason for using an image file is that the operating system cannot be asked during the boot process to quick-format a drive (the necessary libraries are Win32 DLLs), and using an image file seemed to be the easiest, fastest and most flexible way to obtain the same result.*

Q: ***Is it possible to store the hibernation file on the TCTEMP volume?***

A: *No, unfortunately it is impossible to store a hibernation file on the TCTEMP volume, because the password and the keys of the TCTEMP volume are lost when the system is powered off.*

Uninstalling TCTEMP

TCTEMP can be uninstalled as follows:

1. Start *INSTALL\INSTALL.CMD*
2. Enter *3* to select menu item *Uninstall TCTEMP*

Version History

1.7

- Updated: Documentation.

1.6

- Changed: TCTEMP requires TrueCrypt 4.3a instead of TrueCrypt 4.3

1.5

- Changed: TCTEMP requires TrueCrypt 4.3 instead of TrueCrypt 4.2a
- Added: Support for Windows Vista

1.4a

- Fixed: Image file creation on Windows 2000 with TCTEMP 1.4 failed regularly with error code 21

1.4

- Fixed: Raw volume access is now done with more respect to the operating system

1.3a

- Improved: Setup makes further parameter validity checks

1.3

- Changed: TCTEMP requires TrueCrypt 4.2 instead of TrueCrypt 4.1
- New: Prepared to support volumes with a sector size of 512, 1024, 2048 or 4096 bytes (instead of supporting only a fixed sector size of 512 bytes)
- New: Support for the VIA CPU RNG on 32-bit Windows
- New: A higher value for the iteration count of the volume key and password derivation function can be specified (to increase the derivation complexity).
- Changed: Some (merely static) system information blocks are no longer added to the entropy pool. The 500 msec loop which reads only the CPU timestamp counter has been removed (it is more efficient to increase the password derivation complexity instead).

1.2a

- Fixed: File names are no longer limited to 15 characters (It is now possible to use a device-hosted TrueCrypt volume)

1.2

- Improved: Setup and image file creation procedure
- New: The CPU time stamp counter is used as a further entropy source
- Changed: The salt of the new volume header is now encrypted with the new volume keys (using LRW start index 0xfffffffffffffff8) in order to make it harder to find the previous contents of the volume header with forensic methods.

1.1

- Improved: Setup and image file creation procedure
- Changed: The stack is now wiped only once (just before terminating TCTEMP)

Acknowledgements

I would like to thank the TrueCrypt Foundation for its excellent free open-source disk encryption *TrueCrypt*. The interface to the device driver is taken from the source code of TrueCrypt 4.2a. The method to add values to the entropy pool is taken from the TrueCrypt keyfile applying algorithm.

I would like to thank Tom St Denis for his excellent portable ISO C cryptographic library *LibTomCrypt*. I have used his library for all hash functions, the PKCS #5 V2.0 key deriving function and for all ciphers but Serpent.

I would like to thank Wei Dai for his excellent comprehensive C++ class library *Crypto*++. I have used his library for Serpent.

I would like to thank Jason Perkins and the Premake Project for their free open-source build script generator *Premake*. I have used Premake to create all solution and project files.

I would like to thank Samuel Demeulemeester from *x86-secret.com* for testing the 32-bit VIA RNG code on a VIA C7 processor.

References

[1] How to Move the Spool Folder in Windows XP
http://support.microsoft.com/?kbid=308666

[2] How to Move the TEMP and TMP Directories
http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3Perf_ScalGuide/9214ee97-18e4-4754-937b-850f0045545a.mspx

[3] How to Change the Location of Temporary Internet Files
http://support.microsoft.com/?kbid=172949

[4] How to Move Event Viewer Log Files to another Location in Windows 2000 and in Windows Server 2003
http://support.microsoft.com/?kbid=315417

[5] [How to] Disable [the Eventlog Service]
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/bootcons_disable.mspx

[6] How to Move the Windows Default Paging File and Print Spooler to a Different Hard Disk
http://support.microsoft.com/?kbid=314105

[7] How to Move the Paging File in Windows XP
http://support.microsoft.com/?kbid=307886

[8] How to Stop the NT Executive from Paging to Disk
http://support.microsoft.com/?kbid=184419

[9] [Registry Value] DisablePagingExecutive
http://technet2.microsoft.com/WindowsServer/en/Library/3d3b3c16-c901-46de-8485-166a819af3ad1033.mspx

[10] Disable Paging of Kernel Stacks
http://technet2.microsoft.com/WindowsServer/en/Library/6a183942-57b1-45e0-8b4c-c546aa1b8c471033.mspx

[11] Inside Native Applications
http://www.microsoft.com/technet/sysinternals/information/nativeapplications.mspx

[12] Inside the Native API
http://wwwspies.informatik.tu-muenchen.de/lehre/praktika/SS02/bsprakt/inside_the_native_api.html

[13] M. E. Russinovich and D. A. Solomon, “Microsoft Windows Internals, 4th Edition: Microsoft Windows Server 2003, Windows XP, and Windows 2000,” Microsoft Press, 2005
http://en.wikipedia.org/wiki/Special:Booksources/0735619174

[14] G. Nebbett, “Windows NT/2000 Native API Reference,” Macmillan Technical Publishing, 2000
http://en.wikipedia.org/wiki/Special:Booksources/1578701996