TCGINA
USER'S GUIDE

Version 1.28

Contents

General Information

TCGINA allows the use of TrueCrypt[1] to on-the-fly encrypt a Windows user profile. A Windows user profile usually contains user registry files, user documents and settings, temporary files, etc. TCGINA detects whether a user profile is encrypted (stored on a TrueCrypt volume) and mounts the corresponding TrueCrypt volume before continuing the Windows log on procedure.

TCGINA is implemented as a stub GINA[2] and works together with the original Windows GINA (MSGINA DLL) or with a custom GINA.

Note: A more secure and more reliable method to encrypt user profiles is to encrypt the system partition. TCGINA is only then a preferable method if system encryption is not an option.

System Requirements

Supported operating systems:	Windows XP/2000 SP4/2003 and Windows XP/2003 x64 Edition
Required TrueCrypt version:	7.0a or 7.0

Latest Version

The latest TCGINA version can be downloaded from the TCGINA project homepage[3]. The authenticity of the downloaded files can be checked with the public project key[4].

Licensing Information

TCGINA 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 A GINA is a graphical identification and authentication library (see also http://en.wikipedia.org/wiki/Graphical_identification_and_authentication)

3 TCGINA project homepage: http://www.tcgina.t35.com

4 Fingerprint of the TCGINA project key: 294B A769 4A0A CC05 DAE6 00DD FF47 8C72 4097 67CE

Technical Description of TCGINA

TCGINA intercepts the communication between WINLOGON and the original/custom GINA, and performs its actions upon following system events:

System Startup

TCGINA mounts all TrueCrypt volumes which are specified via the registry value *Automount*.

User Logon

TCGINA considers a user profile to be encrypted, if either the user's registry hive cannot be found, or if there is already another interactive session running which belongs to the same user and which has an encrypted profile. TCGINA returns control back to the standard logon procedure if it could find the user's registry hive.

If TCGINA finds an unmounted TrueCrypt volume for the user profile (see registry value *TCFileName* and *TCPath*), then TCGINA tries to mount this volume with the intercepted password. If the volume cannot be mounted, then a dialog box is displayed and the user is asked to enter the password for the TrueCrypt volume.

If TCGINA cannot find a TrueCrypt volume for the user profile (i.e. if *TCFileName* is not defined and if the corresponding TrueCrypt container *username.tc* does not exist), then TCGINA tries to mount all partitions with the intercepted password until the one encrypted partition is found which contains the user's registry hive. If TCGINA could not find an encrypted partition for the user profile, then a dialog box is displayed and the user is asked to enter the password for the encrypted partition.

User Logoff

TCGINA performs no actions if the profile of the user who is logging off is not encrypted, or if another interactive session is running which belongs to the same user.

If the profile is encrypted, and if no further interactive session is running which belongs to the user, then TCGINA wipes the password cache and dismounts all unprotected[5] TrueCrypt volumes, and all volumes which were mounted by TCGINA for the user session, forcibly.

5 An unprotected TrueCrypt volume (in the context of TCGINA) is a volume which was not mounted by TCGINA or prior to TCGINA, and also not protected by registry value *ProtectedDrives*.

Installing TCGINA

TCGINA can be installed as follows:

1. Start *INSTALL\SETUP.EXE*
2. Select *Install TCGINA*
3. Select a TCGINA flavor:

   TCGINA LITE: This version contains the basic functionality of TCGINA.

   TCGINA FULL: This version contains all functions of TCGINA LITE, and additionally, support for *Windows Terminal Services*, network support, password file support and support for automatically mounted volumes which are mounted before the initial logon dialog box is displayed.

   TCGINA DEBUG: This version contains all functions of TCGINA FULL, and additionally maintains the log file *%SystemDrive%\TC.LOG*.
4. Press OK
5. Optionally disable the generation of LAN Manager hashes with *LANMAN\DISABLE_LAN_MANAGER_HASHES.CMD* if Windows user passwords are reused for TrueCrypt volumes (see chapter *Security Precautions* for further information, p. 20)
6. Optionally install the *User Profile Hive Cleanup Service* (see section *Resolving Logon Error Message* for further information, p. 21)
7. Optionally encrypt a user profile (see chapter *Encrypting User Profiles* for further information, p. 4).
8. Optionally run TrueCrypt with each encrypted user profile and disable all auto-dismount events (Settings → Preferences)

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

Encrypting User Profiles

Recommendations for User Profile Encryption

- Only newly created user accounts should be encrypted.
- A user with an encrypted profile should be only a member of restricted user groups in order to prevent that confidential information is stored unintentionally to unencrypted locations.
- The administrator account should not be encrypted in order to be able to log on if there is a problem with an encrypted user profile.

Limitations of User Profile Encryption

- The profile of the current user might not be completely copyable if an application or a system service has locked a data file (e.g. Outlook).
  Both *SETUP.EXE* and *TCUSER.CMD* prevent the encryption of the current user profile. However, the current user profile can be encrypted by first creating a temporary administrator account, followed by encrypting the user profile while being logged on with the temporary administrator account. The temporary administrator account can then be deleted afterwards.
- Applications and system services might already have created references to the unencrypted profile path which are no longer valid after the user profile has been redirected to the encrypted storage location. Some of these references might be found in the registry and can possibly be redirected manually to the encrypted user profile.
  If this limitation is unacceptable, the user profile can be encrypted with a reparse point instead (see below, p. 5).

Encrypting User Profiles with SETUP.EXE

A user profile can be encrypted with *SETUP.EXE* as follows:

1. Optionally create a new user account (see [3] for further information)
2. Start *INSTALL\SETUP.EXE*
3. Select *Encrypt User Profile*
4. Select the name of the user account
5. Optionally create a new TrueCrypt volume for the user profile with *TRUECRYPT.EXE*
6. Mount a TrueCrypt volume for the user profile with *TRUECRYPT.EXE*
7. Select a TrueCrypt drive for the user profile

   (*SETUP.EXE* automatically detects whether the selected destination drive already contains a user profile for the selected user. In this case *SETUP.EXE* will only redirect the user profile to the encrypted location but no files will be copied.)

8. Press OK

The files of the original unencrypted user profile are only copied to the encrypted volume by *SETUP.EXE*. It is left to the administrator who encrypted the user profile to wipe these files securely with a tool like Eraser (see also [11]).

Encrypting User Profiles with Reparse Points

An alternative but **not recommended** method to encrypt a user profile is to move all files of a user profile to a TrueCrypt volume and to create a mount point (or more generally a reparse point) for the empty user profile folder in order to redirect the folder to the TrueCrypt volume. The command file *TCUSER.CMD* can be used to encrypt a user profile with a mount point (see *TCUSER.TXT* for further information).

> **CAUTION:** If a mount point (or reparse point) is used to redirect a user profile path to a mounted TrueCrypt volume, then the recycle bin should be disabled for the drive which hosts the user profiles (usually C:). Otherwise, files which are moved to the recycle bin might possibly be moved from the mounted TrueCrypt volume to unencrypted locations of the drive which hosts the user profiles (i.e. \RECYCLER*SID* where *SID* is the user's security identifier string).

Password Files

The keyfile editor *KFEDIT.EXE* can be used to create and edit password files. A password file can be used as storage for (the first part of) volume passwords and mount options (see *KFEDIT.TXT* for further information).

Mounting Outer Volumes with Hidden Volume Protection

Mounting outer volumes with hidden volume protection is supported by allowing the user to enter a concatenated password where the first part is the password of the outer volume, and the second part is the password of the hidden volume. Both passwords are separated by the first space character. The first space character is only used as a separator and does neither belong to the outer nor to the hidden volume password. Note that the hidden volume header is decrypted with the same keyfiles as the outer volume. A password with a space character is only considered to be a concatenated password if a mount attempt with all password characters has failed.

This approach has following advantage:

- Specifying both passwords is easier than clicking a button for the hidden volume password

And following disadvantages:

- The outer volume password must not contain a space character
- The length of both passwords must together not exceed 63 characters
- Mounting with hidden volume protection takes more time than necessary, because before considering the password to be a concatenated password, a previous mount attempt with all password characters must fail.
- An unsuccessful mount attempt without hidden volume protection takes twice as long if the password contains a space character (because then, also the concatenated password is used for a further mount attempt)

Mounting Multiple Volumes Automatically

Multiple volumes can automatically be mounted with the password of the volume which hosts the encrypted user profile by enabling the password cache (i.e. by setting the registry value *TCMountOptions* to 1). The volumes can then be mounted with a startup batch file like the following one:

```
@echo off
set TC="%ProgramFiles%\TrueCrypt\TrueCrypt.exe"
%TC% /q /l x /v d:\myvolume1.tc
%TC% /q /l y /v d:\myvolume2.tc
%TC% /q /l z /v d:\myvolume3.tc
%TC% /q /s /w
```

A slightly modified batch file is required if the TrueCrypt background task is enabled and if TrueCrypt is not started automatically upon Windows logon:

```
@echo off
rem ** This batch file works even if TrueCrypt's background task is enabled
set TC="%ProgramFiles%\TrueCrypt\TrueCrypt.exe"
%TC% start "Start TrueCrypt's background task" %TC% /q preferences
rem ** The following ping is used to wait for one second
ping -n 2 127.0.0.1 >nul
%TC% /q /l x /v d:\myvolume1.tc
%TC% /q /l y /v d:\myvolume2.tc
%TC% /q /l z /v d:\myvolume3.tc
%TC% /q /s /w
```

Further modifications are required if the volumes are stored at remote locations, because the TrueCrypt driver would not allow the *TrueCrypt.exe* process to terminate until the TrueCrypt volume with the remote container file is dismounted:

```
@echo off
rem ** This batch file works even if TrueCrypt's background task is enabled
rem ** and even if the TrueCrypt volumes are stored at remote locations
set TC="%ProgramFiles%\TrueCrypt\TrueCrypt.exe"
%TC% start "Start TrueCrypt's background task" %TC% /q preferences
rem ** The following ping is used to wait for one second
ping -n 2 127.0.0.1 >nul
start "Mount TrueCrypt volume 1" %TC% /q /l x /v \\server\share\vol1.tc
rem ** The following ping is used to wait for three second
ping -n 4 127.0.0.1 >nul
start "Mount TrueCrypt volume 2" %TC% /q /l y /v \\server\share\vol2.tc
rem ** The following ping is used to wait for three second
ping -n 4 127.0.0.1 >nul
start "Mount TrueCrypt volume 3" %TC% /q /l z /v \\server\share\vol3.tc
rem ** The following ping is used to wait for three second
```

```
ping -n 4 127.0.0.1 >nul
start %TC% /q /s /w
```

Alternatively, the desired volumes can once be mounted manually with TrueCrypt and saved as favorite volumes. These volumes can then be mounted automatically by enabling the options *Start TrueCrypt* and *Mount favorite volumes* of the preferences dialog box.

TrueCrypt Volumes with Network Shares

TrueCrypt volumes with network shares must be mounted before the *LAN Manager Server* service is running. Otherwise, the network shares on the mounted TrueCrypt volume are not reestablished. However, the network shares can be reestablished at any time by restarting the *LAN Manager Server* service, e.g. with the following commands:

```
net /y stop lanmanserver
net start browser
[Windows 2000 Server only:] net start dfs
```

Note that the *Computer Browser* service is dependent on the *LAN Manager Server* service: Stopping the *LAN Manager Server* service also stops the *Computer Browser* service, and vice versa, starting the *Computer Browser* service also starts the *LAN Manager Server* service.

Usually, starting and stopping services requires administrator privileges. This restriction can be bypassed by writing a helper service which restarts a service on demand. Another method is to change the security attributes of the service.

If the TrueCrypt volumes which are mounted by TCGINA have network shares, then it is recommendable to change the startup type of the services *Server* and *Computer Browser* to manual, and to set the registry value *TCStopServices* to *lanmanserver*, and the registry value *TCStartServices* to *browser*. Note that this method is not supported by TCGINA LITE.

[Windows 2000 Server only:] If the TrueCrypt volumes which are mounted by TCGINA have network shares, then it is recommendable to change the startup type of the services *Server*, *Computer Browser* and *Distributed File System* to manual, and to set the registry value *TCStopServices* to *lanmanserver*, and the registry value *TCStartServices* to { *browser*, *dfs* }. Note that this method is not supported by TCGINA LITE.

Debugging Logon/Logoff Scripts

The execution order of a logon/logoff script and of TCGINA actions can be logged to the TCGINA log file by installing TCGINA DEBUG and by adding the line

```
echo START OF LOGOFF SCRIPT (%USERNAME%)>>%SystemDrive%\TC.LOG
```

at the beginning of the script, and the line

```
echo END OF LOGOFF SCRIPT (%USERNAME%)>>%SystemDrive%\TC.LOG
```

at the end of the script. The security attributes of the TCGINA log file (*%SystemDrive%\TC.LOG*) must be set correctly, otherwise the script might not have the necessary access rights to write to the log file.

Registry Settings

General TCGINA settings are stored at the registry key

> HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}

User settings are stored at the corresponding sub-key

> HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}*username*

where *username* is a placeholder for the user name. A user registry value is looked up in the general TCGINA registry key if it cannot be found in the *username* sub-key.

Optional alternative user settings, which are used for a remote session, are stored at the registry key

> HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}*username*\RemoteSession

Note that all *REG_MULTI_SZ* values can also be defined as *REG_SZ* values (which are limited to 1058 characters). In this case the entries are separated with a semicolon and optionally enclosed in double quotation marks. A single *REG_MULTI_SZ* string is limited to 259 characters, and the number of characters of a *REG_MULTI_SZ* value is limited to 1059-*N* where *N* is the number of strings.

General Settings for TCGINA LITE/FULL/DEBUG

TCGINA LITE/FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
GinaDLL (REG_SZ)	Name of the GINA DLL which is used for the GUI and for authentication (MSGINA.DLL)

TCGINA LITE/FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
HideGinaDLL (REG_DWORD)	If *HideGinaDLL* is not zero, then TCGINA hides all registry values with the name *GinaDLL* from all MSGINA.DLL procedures within the Winlogon process. This can be used to make Windows believe that no custom GINA is installed and that the Welcome Screen can be displayed. (0) **Caution:** The registry value *HideGinaDLL* should only be used for test purposes and not be set in a productive environment. The operating system is not expecting that a custom function interferes with the processing of an API function (even if the effect is limited to a single process). The operating system may therefore behave unexpectedly and undefined (which might include a catastrophic system failure or an unstable computer) after *HideGinaDLL* is set to a non-zero value. Note: Be careful with Fast User Switching (which is available via *WIN-L*, or by executing "*rundll32.exe user32.dll, LockWorkStation*", but not via the *Start* button due to the visibility of the *GinaDLL* registry value in the Explorer process), because unexpected effects, like a frozen Welcome Screen during a secondary logon (which should be repairable by pressing *CTRL-ALT-DEL*), can sometimes be experienced.
ProtectedDrives (REG_SZ)	Sequence of drive letters which are protected from being automatically dismounted on logoff. Note: The volumes which are mounted before TCGINA is running, and auto mounted volumes, and profile volumes (including auto mounted partitions) are automatically added to the protected drives list.

User Settings for TCGINA LITE/FULL/DEBUG

TCGINA LITE/FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
AutoRedirectionRepair (REG_DWORD)	If *AutoRedirectionRepair* is not zero, then TCGINA automatically restores a redirected profile image path of an encrypted user to its encrypted location (without user notification). Note that auto-repair requires *DisableRedirectionDetection* to be zero. (0)
DisableRedirectionDetection (REG_DWORD)	If *DisableRedirectionDetection* is not zero, then TCGINA does not verify whether the profile image path has been redirected

TCGINA LITE/FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
	from the encrypted location. This value can be set (on user request) by TCGINA. Note that this value should only be set either to 0 or 1 if set manually. (0)
EncryptedProfileImagePath (REG_EXPAND_SZ)	Location of the encrypted user profile. This value is required to detect whether Windows has redirected the profile image path. This value is created by *SETUP.EXE*.
ProfileImagePath (REG_EXPAND_SZ)	Original unencrypted location of the user profile. This value is created by *SETUP.EXE*.
SID (REG_SZ)	Original user SID. This value is used to identify the type of the user account. If this value is not defined, the type of the user account is unknown. If this value equals the SID of the current user, the user account is considered to be encrypted. If this value does not equal the SID of the current user, the user account is considered to be not encrypted, and the values *ProfileImagePath* and *EncryptedProfileImagePath* are considered to be invalid. This value is created by *SETUP.EXE*.
TCDrive (REG_SZ)	TrueCrypt drive name for a user profile which has been encrypted with *TCUSER.CMD* instead of *SETUP.EXE* (U:)
TCFileName (REG_SZ)	TrueCrypt volume name (%USERNAME%.tc). The placeholder %USERNAME% can be used for the user name. The value *TCPath* is ignored if *TCFileName* starts with a backslash or slash. *TCFileName* supports both file-hosted and device-hosted volumes. If *TCFileName* is not specified and if the default TrueCrypt container of the user profile does not exist, then all partitions are temporarily mounted with the password until an encrypted partition with the user's registry hive is found. TCGINA FULL and TCGINA DEBUG only: *TCFileName* supports UNC paths (\\server\sharename) and uses the intercepted user name and password to connect to the server.
TCFirstAutoMountDrive (REG_SZ)	TrueCrypt drive name of the first automatically mounted device-hosted volume. Automatically mounting of device-hosted volumes is disabled if *TCFirstAutoMountDrive* is empty or undefined.

TCGINA LITE/FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
TCKeyFileDrives (REG_SZ)	Sequence of drive letters which are used to search for the keyfiles on alternative drives. Note that only the drive letter of the first keyfile (and of those keyfiles which use the same drive letter as the first one) is replaced. Example: *TCKeyFileDrives* = "EFGH"
TCKeyFileNames (REG_MULTI_SZ)	Keyfile names Note 1: TCGINA does not support volumes which are not encrypted with a password. You can use password files instead. Note 2: Keyfiles are not supported for volumes which are defined to be mounted via the *Automount* registry value. For these volumes, you can use password files instead (which are defined via the registry values *KF*…).
TCKeyFileTimeout (REG_DWORD)	Timeout in ms for keyfile medium dialog box if *TCKeyFileTimeout* is non-zero (0)
TCMountOptions (REG_DWORD)	TrueCrypt mount options (0) 1: Enable password cache 2: Mount volume as read-only (This option is not available for the TrueCrypt volume which hosts the user profile) 4: Mount as removable media 8: Mount in shared mode 16: Don't preserve container file timestamps
TCOptions (REG_DWORD)	Options (0) 1: Display password 2: Disable mount attempt with user account password 4: Automount volume is mandatory. The boot procedure is not continued if a wrong password is entered. Instead, the password prompt dialog box is displayed again. 8: Disable wiping of password cache during log off 16: Disable dismounting of volumes during log off
TCPasswordTimeout (REG_DWORD)	Timeout in ms for volume password dialog box if *TCPasswordTimeout* is non-zero (the timeout counter is reset by a keystroke). (0)

TCGINA LITE/FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
TCPasswordTotalTimeout (REG_DWORD)	Total timeout in ms for volume password dialog box if *TCPasswordTotalTimeout* is non-zero. (0) Note that a timeout of 5 minutes will be used if *TCPasswordTotalTimeout* is both zero and belonging to an *Automount* registry sub-key.
TCPath (REG_MULTI_SZ)	Search path for TrueCrypt files. The placeholder %USERNAME% can be used for the user name (default profiles path)

Additional General Settings for TCGINA FULL/DEBUG

TCGINA FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
Automount (REG_MULTI_SZ)	Sub-key names for TrueCrypt volumes which are automatically mounted before the first logon dialog box is displayed.
AutomountMode (REG_DWORD)	Option to schedule the automatic mounting. (0) 0: Automount is performed after the SAS (CTRL+ALT+DEL sequence) 1: One automount attempt is performed before the SAS (CTRL+ALT+DEL sequence)
LogFileName (REG_EXPAND_SZ)	File name of the TCGINA log file (%SystemDrive%\TC.LOG)
MSCount (REG_DWORD)	Max. number of simultaneously running interactive sessions with an encrypted user profile. Support for Windows Terminal Services sessions is disabled, if *MSCount* is zero. (0)
MSOptions (REG_DWORD)	Options for multiple sessions (0) 1: Reject logon attempt for interactive sessions without an encrypted user profile, if there is already at least one interactive session with an encrypted user profile running. 2: Notify user who is about to log on with an encrypted user profile if there are already other running interactive sessions.

Additional User Settings for TCGINA FULL/DEBUG

TCGINA FULL/DEBUG: Value Name (Value Type)	**Description** (Default Value Data)
KFDrives (REG_SZ)	Sequence of drive letters which is used to search for the password file on alternative drives. Example: *KFDrives* = "EFGH"
KFFileName (REG_SZ)	Password file name
KFFileOffset (REG_DWORD)	32 least significant bits of the offset of the first password file item (0)
KFFileOffsetHigh	32 most significant bits of the offset of the first password file

TCGINA FULL/DEBUG: **Value Name** (Value Type)	**Description** (Default Value Data)
(REG_DWORD)	item (0)
KFFileSize (REG_DWORD)	Size of all password file items if *KFFileSize* is non-zero (0)
KFID (REG_DWORD)	Password file item ID if KFID is non-zero (0)
KFMediumTimeout (REG_DWORD)	Timeout in ms for password file medium dialog box if *KFMediumTimeout* is non-zero. (0) Note that a timeout of 5 minutes will be used if *KFMediumTimeout* is both zero and belonging to an *Automount* registry sub-key.
KFNoPasswordDialog (REG_DWORD)	No password dialog box will be displayed if *KFNoPasswordDialog* equals 1 (0)
KFPassword (REG_SZ)	Password for password file item (logon password)
KFPasswordTimeout (REG_DWORD)	Timeout in ms for password file password dialog box if *KFPasswordTimeout* is non-zero (the timeout counter is reset by a keystroke). (0)
KFPasswordTotalTimeout (REG_DWORD)	Total Timeout in ms for volume password dialog box if *KFPasswordTotalTimeout* is non-zero. (0) Note that a timeout of 5 minutes will be used if *KFPasswordTotalTimeout* is both zero and belonging to an *Automount* registry sub-key.
NDLocalName (REG_SZ)	Local name for network drive
NDPassword (REG_SZ)	Password for network drive
NDRemoteName (REG_SZ)	Remote name for network drive
NDUserName (REG_SZ)	User name for network drive
~~TCPassword (REG_SZ)~~	~~Password for TrueCrypt volume which is mounted during system startup (see registry value *Automount*)~~ (This registry value is no longer supported. A password file can be used instead.)
TCStartServices (REG_MULTI_SZ)	Services which are started after the TrueCrypt volume has been mounted

TCGINA FULL/DEBUG: **Value Name** (Value Type)	**Description** (Default Value Data)
TCStopServices (REG_MULTI_SZ)	Services which are stopped before processing *TCStartServices*. Note that services, on which the service to stop depends, are stopped as well.

Security Precautions

Reusing Windows user passwords for TrueCrypt volumes weakens the password safety of the TrueCrypt volumes, because Windows passwords are stored as 128-bit MD4 hashes which are much faster to break with brute force than TrueCrypt passwords. Furthermore, care must be taken that the generation of LAN manager hashes is disabled (see also [2]).

Troubleshooting

Resolving Logon Error Message

Windows can occasionally fail to log on with an encrypted user profile. In this case the message *System could not allocate required space in a registry log* is displayed instead. This error message can be resolved by installing the *User Profile Hive Cleanup Service* (see [4] and [5]).

Disabling TCGINA

A custom GINA has always the potential to lock all users out. In this case TCGINA can be disabled as follows:

1. Boot in safe mode (You can boot in safe mode if you select *Safe Boot* from the boot menu. The boot menu is available if you press F8 twice after starting the computer.)
   Note that booting in safe mode already disables TCGINA temporarily. In order to disable TCGINA permanently, the Winlogon registry value *GinaDLL* must be removed (see steps 2 to 4).
2. Run *regedit*
3. Select the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
4. Remove the registry value *GinaDLL*

Resolving Logon Problems

A recommended approach to resolve logon problems is:

1. Check the registry key HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}*username* (where *username* is a placeholder for the name of the corresponding user account) for plausible entries
2. Check the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList*UserSID*\ProfileImagePath (where *UserSID* is a placeholder for the security identifier of the corresponding user account which can be looked up from HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}*username*\SID)
3. Install the TCGINA debug version
4. Try to logon and analyze the log file %SystemDrive%:\TC.LOG (usually C:\TC.LOG)

Frequently Asked Questions

Q: ***How do I correctly install TCGINA if I also want to use a custom GINA?***

A: *The custom GINA must already be installed before TCGINA is installed. The TCGINA setup program automatically detects a custom GINA and defines the corresponding TCGINA registry value (GinaDLL).*

Q: ***What went wrong if the installer displays "Cannot find installation files"?***

A: *The setup program cannot find the installation files if it is started from within an archiver window. The TCGINA archive must first be unpacked completely, and SETUP.EXE must then be started from the unpacked location.*

Q: ***Is it possible to enable the Welcome screen and Fast User Switching if TCGINA is installed?***

A: *No, both Welcome screen and Fast User Switching are automatically disabled by Windows if a stub GINA or a custom GINA is installed.*

Q: ***Sometimes I get the error message "System could not allocate required space in a registry log". How can I get rid of this error message?***

A: *See section Resolving Logon Error Message (page 21).*

Q: ***Is it possible to bypass the logon dialog box and to display the TCGINA password prompt directly after the computer is (re)started?***

A: *Yes, it is possible to bypass the logon dialog box. The easiest way is to install Tweak UI (see [6] and [7] for further information) and to use Tweak UI's "autologon" settings. If no password is used for the "autologon" user account, and if the logon dialog box is still displayed, then a password should be assigned for the "autologon" user account, and the "autologon" settings should be updated correspondingly.*

Q: ***Can I still use the auto-dismount options (like when "screen saver is launched" or when "power saving mode is entered") in TrueCrypt if I am logged on with an encrypted profile?***

A: *No, instead of using auto-dismount, you can alternatively use auto-logoff, e.g. with an auto-logoff capable screen saver like "WinExit" (see [8] and [9] for further information), or with a keyboard which has application shortcut keys, where one of these keys is used to start "PsShutdown.exe" (see [10]).*

Q: ***Can I run an application with "run as" in the context of a user whose profile is encrypted?***

A: *Yes, but unfortunately a GINA cannot intercept a secondary logon. Therefore, either the TrueCrypt volume of the encrypted user profile must be mounted manually (with the correct*

drive letter) before the application is started, or “runas.exe” must be started with the “/noprofile” switch.

Uninstalling TCGINA

Uninstalling TCGINA with SETUP.EXE

TCGINA can be uninstalled as follows:

1. Start *INSTALL\SETUP.EXE*
2. Select *Uninstall TCGINA*
3. Check one or more uninstall options:

   Remove TCGINA files: All files which are belonging to TCGINA will be removed (TCGINA*.DLL and TCGINA log files), and the GINA registry value will either be set to the custom GINA or be removed. This option cannot be disabled.

   Reset user profiles to their original unencrypted locations: If enabled, all user accounts with an encrypted profile, whose original unencrypted files have not been removed, will be redirected to the original unencrypted location. This option is only available if at least one encrypted user account exists whose original unencrypted files have not been removed.

   Remove TCGINA settings: If enabled, the TCGINA registry key and all its sub-keys will be removed. This option is only available if the TCGINA registry key exists.
4. Press OK

Uninstalling TCGINA Manually

Alternatively, TCGINA can also be uninstalled manually, and the user account with the encrypted profile can optionally be removed as follows:

1. Log on as administrator with an unencrypted user profile
2. Optionally delete the encrypted user account (see also [3])
3. Optionally wipe the TrueCrypt container file which has been selected during TCGINA setup with a tool like eraser (see [11]). Its name is stored at HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}*username*\TCFileName)
4. If the registry value HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-523603A5594D}\GinaDLL does not exist (i.e. no custom GINA like PGINA or NWGINA is installed), remove the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL.
   Otherwise, copy the *GinaDLL* registry value from HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL\{D47DF546-F16B-490b-A6D8-

523603A5594D}
to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

5. Remove the registry key HKEY_LOCAL_MACHINE\SOFTWARE\TCGINA DLL
6. Restart the computer
7. Remove all *TCGINA*.DLL* files in the system folder (usually *C:\Windows\System32* or *C:\WinNT\System32*)
8. Delete the TCGINA log file (*C:\TC.LOG*) if the TCGINA debug version was previously installed

Version History

1.28

- Changed: TCGINA requires TrueCrypt 7.0a/7.0 instead of TrueCrypt 6.3a/6.3

1.27

- Changed: TCGINA requires TrueCrypt 6.3/6.3a instead of TrueCrypt 6.2a

1.26

- Changed: TCGINA requires TrueCrypt 6.2/6.2a instead of TrueCrypt 6.1a

1.25

- Changed: TCGINA requires TrueCrypt 6.1a instead of TrueCrypt 6.1

1.24

- Changed: TCGINA requires TrueCrypt 6.1 instead of TrueCrypt 6.0/6.0a

1.23

- Changed: TCGINA requires TrueCrypt 6.0/6.0a instead of TrueCrypt 6.0

1.22

- Changed: TCGINA requires TrueCrypt 6.0 instead of TrueCrypt 5.1/5.1a
- New: The registry value *AutomountMode* can be used to schedule the automatic mounting

1.21

- Changed: TCGINA requires TrueCrypt 5.1/5.1a instead of TrueCrypt 5.1

1.20

- Changed: TCGINA requires TrueCrypt 5.1 instead of TrueCrypt 5.0/5.0a

1.19

- Changed: TCGINA requires TrueCrypt 5.0/5.0a instead of TrueCrypt 4.3a
- Changed: TCGINA mounts all volumes as standard volumes (instead of persistent volumes)
- Changed: The registry value *ProtectedDrives* can be used to protect certain volumes from being dismounted on log off.

1.18

- New: Option to disable the dismounting of the encrypted profile volume or disable wiping of the password cache (via registry value *TCOptions*).

1.17

- Changed: TCGINA requires TrueCrypt 4.3a instead of TrueCrypt 4.3
- New: Experimental option to enable the Welcome Screen (new registry value *HideGinaDLL*)
- New: Automount volumes can be declared (via registry value *TCOptions*) as mandatory
- Fixed (Windows x64 only): A local 32-bit variable was used to obtain a 64-bit result. This bug is present only in 64-bit TCGINA versions from version 1.8 to 1.16, but should have no side effects (at least for TCGINA 1.15/1.16; note that the machine code of versions 1.8 to 1.14 has not been checked for side effects).

1.16

- Changed: TCGINA requires TrueCrypt 4.3 instead of TrueCrypt 4.2a
- Fixed: The network registry values *ND*… are now also supported for volumes which are defined to be mounted via the *Automount* registry value.

1.15

- Changed: TCGINA requires TrueCrypt 4.2a instead of TrueCrypt 4.2
- New: Better timeout control (new registry values *TCPasswordTotalTimeout* and *KFPasswordTotalTimeout*)
- New: TCGINA supports alternative registry settings for remote sessions
- Fixed: The *Automount* registry value is now again processed after the first SAS notice has been displayed
- Fixed: SETUP.EXE does no longer display “ERROR: Invalid user name!” if the selected TrueCrypt Drive number equals the number of found user profiles

1.14

- Changed: TCGINA requires TrueCrypt 4.2 instead of TrueCrypt 4.1
- Changed: All volumes are mounted as persistent volumes

- Changed: All mounted volumes which are not mounted as system volume are dismounted upon system shutdown
- Removed: The registry value is no longer supported (persistent volumes can be used instead)
- Fixed: If necessary, an alternative method is used to find the user SID (by enumerating all sub-keys of the profile list registry key)

1.13

- New: All volumes which have been mounted after TCGINA has been loaded are forcibly dismounted by TCGINA on shutdown.
- Changed: All volumes which have been mounted before TCGINA has been loaded are protected from being dismounted by TCGINA.

1.12

- New: TCGINA supports Windows Terminal Services sessions and optionally rejects further log on attempts if there is already an interactive session with an encrypted user profile running. (Registry values *MSCount* and *MSOptions*)
- Changed: TrueCrypt volumes can be excluded from being dismounted on log off. (see registry value). All volumes which have been mounted by TCGINA before the log on dialog box was displayed, and all volumes which are mounted or protected by TCGINA within another session, are excluded from being dismounted as well.
- Changed: The *Automount* registry value is processed before the first SAS notice is being displayed.
- Changed: If the TCGINA dialog boxes are closed with "Cancel" (or aborted by Winlogon), then TCGINA performs all steps to log off the user in Winlogon's place. Otherwise, Winlogon might use the returned information about the user to redirect the user profile to a newly created one.
- Changed: TCGINA also redirects the function dispatch table in order to catch possible changes of the context pointer.
- Fixed: KFEDIT.EXE runs on Windows 2000

1.11a

- Fixed: Repair of user profile redirection was incomplete in version 1.11

1.11

- New: TCGINA detects optionally if the location of the profile image path of an encrypted user profile has been modified, and repairs it either on demand, or automatically without user notification. (Registry values: *AutoRedirectionRepair*, *DisableRedirectionDetection*, *EncryptedProfileImagePath*)
- New: SETUP.EXE analyzes the storage location of that TrueCrypt volume which is selected as

destination for an encrypted user profile, and notifies the user about possible issues if the volume is stored at a remote location, a network drive or inside another TrueCrypt volume.
- New: *TCFileName* also supports UNC paths (\\server\sharename). Note that UNC paths are not supported by TCGINA LITE, and that TCGINA uses the credentials of the authenticated user to connect to the server.
- New: Services can be (re)started automatically after a TrueCrypt volume has been mounted (to support services which require resources from mounted TrueCrypt volumes – like the LAN Manager Server service or data base server services)

1.10b

- New: General recommendation to use SETUP.EXE instead of TCUSER.CMD to encrypt user profiles
- Changed: The name of the log file can be specified with a registry value (*LogFileName*). The default name of the log file is now %SystemDrive%\TC.LOG instead of C:\TC.LOG.
- Changed: A mount attempt is considered as successful if the TrueCrypt drive is available after calling the TrueCrypt driver (possible error codes returned by the driver are only logged to the log file by TCGINA DEBUG).
- Changed: No additional access rights for the user profile are required. All file permissions which are sufficient to log on with an unencrypted user profile are also sufficient to log on with an encrypted user profile.

1.10a

- New: Recommendation to disable the recycle bin if user profiles are encrypted with TCUSER.CMD instead of SETUP.EXE
- Changed: The TCGINA DLL is installed with the same security attributes as MSGINA.DLL
- New option: Disable mount attempts with user account password (*TCOptions*)

1.10

- Fixed: TCGINA now waits until the TrueCrypt driver is running
- New: Display password check box
- New: Default setting for display password check box (*TCOptions*)

1.9a

- Fixed: The registry value *TCDrive* was not supported by version 1.9
- Changed: New version of TCUSER.CMD with better support for customization (see TCUSER.TXT for further information)

1.9

- Changed: TCGINA requires TrueCrypt 4.1 instead of TrueCrypt 4.0
- Fixed: Version 1.8 did not preserve the container file timestamps
- New: Support for optionally not preserving the container file timestamps
- New: Support for keyfiles (the filenames/paths are defined with a registry value)
- New: Support for mounting outer volumes with hidden volume protection by using a concatenated password where the password of outer and hidden volume are separated by the first space character (Note that the keyfiles of the outer volume are then also used to decrypt the header of the hidden volume)

1.8

- Changed: TCGINA requires TrueCrypt 4.0 instead of TrueCrypt 3.1a
- New: Support for Windows XP x64 Edition

1.7a

- Fixed: Now, the setup program also copies the security attributes when it copies a user profile to an encrypted location

1.7

- New: Setup program for TCGINA
- Changed: Smaller password dialog box
- Removed: Removed support for EXE interface

1.6a

- New version of KFEdit (1.0a)
- Fixed: Drive letters which are defined in a keyfile item are no longer ignored
- Removed: Removed support for registry value *TCPassword* (Volumes which are automatically mounted before the initial log on dialog box is displayed, should use a password file instead)
- New TCGINA flavor (TCGINA LITE)

1.6

- New: Support for password files
- New: Password dialog with timeout and keyboard layout/Caps Lock/Num Lock indicators
- New: All memory blocks which are used for passwords or key data remain in physical memory. A list of all secure memory blocks is maintained to defer *VirtualUnlock*() until all secure memory blocks which share the same memory pages are freed.

1.5

- New: Support for TrueCrypt volumes which are automatically mounted before the initial log on dialog box is displayed (Registry values *Automount*, *TCPassword*)

1.4

- New: Automatic mounting of all device/partition hosted volumes after a TrueCrypt volume of an encrypted user profile was successfully mounted (Registry value *TCFirstAutoMountDrive*)

1.3b

- Changed: Source code clean-up (strict usage of Hungarian Notation, warning level 4)

1.3a

- Changed: Now using the multithreaded RTL
- Changed: Linker switch /OPT:NOWIN98 to reduce the file size of TCGINA.DLL

1.3

- New: Support for an alternative GINA DLL
- New: Support for pre-mounted network drives to support encrypted user profiles which are stored on a network share
- New: The TrueCrypt volume is automatically dismounted before a new user is logged on, even if Windows fails to log on an encrypted user although the TrueCrypt volume could be mounted.

1.2

- New: Additional registry values (*TCDrive*, *TCFileName*, *TCMountOptions*, *TCPath*)
- New: Support for user dependent registry values
- New: Support for encrypted partitions
- New: Support for *.*tcuser* files

1.1

- New: Support for two TrueCrypt interfaces:
  1. Direct interface to the device driver (supported only for TrueCrypt 3.1a)
  2. Call of *TrueCrypt.exe*: The *TrueCrypt.exe* process is granted a maximum of 10 seconds to perform a mount or dismount operation. Furthermore, key stroke messages are sent every 500 ms to every main window of the *TrueCrypt.exe* process to prevent hanging of the process due to missing user input

- Changed: The location of the profiles folder is now taken from the registry
- New: The TrueCrypt file extension association is taken into account to find *TrueCrypt.exe*
- New: Support for encrypted user profiles with modified image path
- New: Password prompt if TrueCrypt volume password is different from user account password
- New: Dismount on log off is only done for sessions with an encrypted user profile
- New: Dismount on log off waits for exclusive access to the user's registry hive

Other Projects

TCGINA

Description: TCGINA allows the use of TrueCrypt to on-the-fly encrypt a Windows user profile. A Windows user profile usually contains user registry files, user documents and settings, temporary files, etc. TCGINA detects whether a user profile is encrypted (stored on a TrueCrypt volume) and mounts the corresponding TrueCrypt volume before continuing the Windows log on procedure. TCGINA is implemented as a stub GINA and works together with the original Windows GINA (MSGINA DLL) or with a custom GINA.

Project Start: March 2005

Fingerprint of the Public Project Key:
294B A769 4A0A CC05 DAE6 00DD FF47 8C72 4097 67CE

Project Homepage: http://tcgina.t35.com

TCTEMP

Description: TCTEMP automates the process of using TrueCrypt to on-the-fly encrypt 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 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.

Project Start: February 2006

Fingerprint of the Public Project Key:
75EB 6BC2 01B7 F6E7 4BD7 CC58 4A5F C393 19EE 6E69

Project Homepage: http://tctemp.t35.com

TCUSER

Description: TCUSER allows the use of TrueCrypt to on-the-fly encrypt a Windows user profile. A Windows user profile usually contains user registry files, user documents and settings, temporary files, etc.

Project Start: August 2008

Fingerprint of the Public Project Key:
B4B2 4F8B D691 335F B90C 1A64 FD5F 9D52 6EA4 7C3F

Project Homepage: http://tcuser.t35.com

Acknowledgements

I would like to thank the TrueCrypt Foundation for its excellent free open-source disk encryption *TrueCrypt*. The interface to the device driver, the notification of the operating system about added or removed drives, and the derivation of the password from keyfiles are taken from the source code of TrueCrypt.

I would like to thank Tom St Denis for his excellent portable ISO C cryptographic library *LibTomCrypt*. I have used (a slightly modified version of) his library for the password file support and for the SHA-1 function which is used by the setup program.

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.

References

[1] How To Change the Default Location of User Profiles and Program Settings
http://support.microsoft.com/?kbid=322014

[2] How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases
http://support.microsoft.com/?kbid=299656

[3] How To Create and Configure User Accounts in Windows XP
http://support.microsoft.com/?kbid=279783

[4] Troubleshooting Profile Unload Issues
http://support.microsoft.com/?kbid=837115

[5] User Profile Hive Cleanup Service
http://www.microsoft.com/downloads/details.aspx?FamilyId=1B286E6D-8912-4E18-B570-42470E2F3582

[6] Tweak UI 1.33 (Windows 2000)
~~http://download.microsoft.com/download/winme/Install/1.0/WinMe/EN-US/Tweakui.exe~~

[7] Microsoft PowerToys for Windows XP (incl. Tweak UI 2.10)
http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx

[8] How To Force Users to Quit Programs and Log Off After a Period of Inactivity in Windows XP
http://support.microsoft.com/?kbid=314999

[9] Windows Server 2003 Resource Kit Tools
http://www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD

[10] PsTools
http://www.microsoft.com/technet/sysinternals/utilities/PsTools.mspx

[11] Eraser
http://sourceforge.net/projects/eraser
http://www.heidi.ie/eraser/

[12] Security Briefs: Customizing GINA, Part 1
http://msdn.microsoft.com/en-us/magazine/cc163803.aspx

[13] Security Briefs: Customizing GINA, Part 2
http://msdn.microsoft.com/en-us/magazine/cc163786.aspx

[14] K. Brown, “Programming Windows Security,” Addison-Wesley, November 2000
http://en.wikipedia.org/wiki/Special:Booksources/0201604426

[15] 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