Free Open source disk encryption with strong security for the Paranoid

12-15 minutes

Security Requirements and Precautions Pertaining to Hidden Volumes

If you use a hidden VeraCrypt volume, you must follow the security requirements and precautions listed below in this section. Disclaimer: This section is not guaranteed to contain a list of *all* security issues and attacks that might adversely affect or limit the ability of VeraCrypt to secure data stored in a hidden VeraCrypt volume and the ability to provide plausible deniability.

- If an adversary has access to a (dismounted) VeraCrypt volume at several points over time, he may be able to determine which sectors of the volume are changing. If you change the contents of a hidden volume (e.g., create/copy new files to the hidden volume or modify/delete/rename/move files stored on the hidden volume, etc.), the contents of sectors (ciphertext) in the hidden volume area will change. After being given the password to the outer volume, the adversary might demand an explanation why these sectors changed. Your failure to provide a plausible explanation might indicate the existence of a hidden volume within the outer volume.

  Note that issues similar to the one described above may also arise, for example, in the following cases:

  - The file system in which you store a file-hosted VeraCrypt container has been defragmented and a copy of the VeraCrypt container (or of its fragment) remains in the free space on the host volume (in the defragmented file system). To prevent this, do one of the following:
    - Use a partition/device-hosted VeraCrypt volume instead of file-hosted.
    - Securely erase free space on the host volume (in the defragmented file system) after defragmenting. On Windows, this can be done using the Microsoft free utility SDelete. On Linux, the *shred* utility from GNU coreutils package can be used for this purpose.
    - Do not defragment file systems in which you store VeraCrypt volumes.
  - A file-hosted VeraCrypt container is stored in a journaling file system (such as NTFS). A copy of the VeraCrypt container (or of its fragment) may remain on the host volume. To prevent this, do one the following:
    - Use a partition/device-hosted VeraCrypt volume instead of file-hosted.
    - Store the container in a non-journaling file system (for example, FAT32).
  - A VeraCrypt volume resides on a device/filesystem that utilizes a wear-leveling mechanism (e.g. a flash-memory SSD or USB flash drive). A copy of (a fragment of) the VeraCrypt volume may remain on the device. Therefore, do not store

hidden volumes on such devices/filesystems. For more information on wear-leveling, see the section Wear-Leveling in the chapter Security Requirements and Precautions.
    - A VeraCrypt volume resides on a device/filesystem that saves data (or on a device/filesystem that is controlled or monitored by a system/device that saves data) (e.g. the value of a timer or counter) that can be used to determine that a block had been written earlier than another block and/or to determine how many times a block has been written/read. Therefore, do not store hidden volumes on such devices/filesystems. To find out whether a device/system saves such data, please refer to documentation supplied with the device/system or contact the vendor/manufacturer.
    - A VeraCrypt volume resides on a device that is prone to wear (it is possible to determine that a block has been written/read more times than another block). Therefore, do not store hidden volumes on such devices/filesystems. To find out whether a device is prone to such wear, please refer to documentation supplied with the device or contact the vendor/manufacturer.
    - You back up content of a hidden volume by cloning its host volume or create a new hidden volume by cloning its host volume. Therefore, you must not do so. Follow the instructions in the chapter How to Back Up Securely and in the section Volume Clones.

- Make sure that *Quick Format* is disabled when encrypting a partition/device within which you intend to create a hidden volume.
- On Windows, make sure you have not deleted any files within a volume within which you intend to create a hidden volume (the cluster bitmap scanner does not detect deleted files).
- On Linux or Mac OS X, if you intend to create a hidden volume within a file-hosted VeraCrypt volume, make sure that the volume is not sparse-file-hosted (the Windows version of VeraCrypt verifies this and disallows creation of hidden volumes within sparse files).
- When a hidden volume is mounted, the operating system and third-party applications may write to non-hidden volumes (typically, to the unencrypted system volume) unencrypted information about the data stored in the hidden volume (e.g. filenames and locations of recently accessed files, databases created by file indexing tools, etc.), the data itself in an unencrypted form (temporary files, etc.), unencrypted information about the filesystem residing in the hidden volume (which might be used e.g. to identify the filesystem and to determine whether it is the filesystem residing in the outer volume), the password/key for the hidden volume, or other types of sensitive data. Therefore, the following security requirements and precautions must be followed:
    - *Windows*: Create a hidden operating system (for information on how to do so, see the section Hidden Operating System) and mount hidden volumes only when the hidden operating system is running. Note: When a hidden operating system is running, VeraCrypt ensures that all local unencrypted filesystems and non-hidden VeraCrypt volumes are read-only (i.e. no files can be written to such filesystems or VeraCrypt volumes).* Data is allowed to be written to filesystems within hidden VeraCrypt volumes. Alternatively, if a hidden operating system cannot be used, use a "live-CD" Windows PE system (entirely stored on and booted from a CD/DVD) that ensures that any data written to the system volume is written to a RAM disk. Mount hidden volumes only when such a "live-CD" system is running (if a hidden operating system cannot be used). In addition, during such a "live-CD"

session, only filesystems that reside in hidden VeraCrypt volumes may be mounted in read-write mode (outer or unencrypted volumes/filesystems must be mounted as read-only or must not be mounted/accessible at all); otherwise, you must ensure that applications and the operating system do not write any sensitive data (see above) to non-hidden volumes/filesystems during the "live-CD" session.
    - *Linux*: Download or create a "live-CD" version of your operating system (i.e. a "live" Linux system entirely stored on and booted from a CD/DVD) that ensures that any data written to the system volume is written to a RAM disk. Mount hidden volumes only when such a "live-CD" system is running. During the session, only filesystems that reside in hidden VeraCrypt volumes may be mounted in read-write mode (outer or unencrypted volumes/filesystems must be mounted as read-only or must not be mounted/accessible at all). If you cannot comply with this requirement and you are not able to ensure that applications and the operating system do not write any sensitive data (see above) to non-hidden volumes/filesystems, you must not mount or create hidden VeraCrypt volumes under Linux.
    - *Mac OS X*: If you are not able to ensure that applications and the operating system do not write any sensitive data (see above) to non-hidden volumes/filesystems, you must not mount or create hidden VeraCrypt volumes under Mac OS X.
- When an outer volume is mounted with hidden volume protection enabled (see section Protection of Hidden Volumes Against Damage), you must follow the same security requirements and precautions that you are required to follow when a hidden volume is mounted (see above). The reason is that the operating system might leak the password/key for the hidden volume to a non-hidden or unencrypted volume.
- If you use an **operating system residing within a hidden volume** (see the section Hidden Operating System), then, in addition to the above, you must follow these security requirements and precautions:
    - You should use the decoy operating system as frequently as you use your computer. Ideally, you should use it for all activities that do not involve sensitive data. Otherwise, plausible deniability of the hidden operating system might be adversely affected (if you revealed the password for the decoy operating system to an adversary, he could find out that the system is not used very often, which might indicate the existence of a hidden operating system on your computer). Note that you can save data to the decoy system partition anytime without any risk that the hidden volume will get damaged (because the decoy system is *not* installed in the outer volume).
    - If the operating system requires activation, it must be activated before it is cloned (cloning is part of the process of creation of a hidden operating system — see the section Hidden Operating System) and the hidden operating system (i.e. the clone) must never be reactivated. The reason is that the hidden operating system is created by copying the content of the system partition to a hidden volume (so if the operating system is not activated, the hidden operating system will not be activated either). If you activated or reactivated a hidden operating system, the date and time of the activation (and other data) might be logged on a Microsoft server (and on the hidden operating system) but not on the decoy operating system. Therefore, if an adversary had access to the data stored on the server or intercepted your request to the server (and if you revealed the password for the decoy operating system to him), he might find out that the decoy operating system was activated (or reactivated) at a different time, which might indicate the existence of a hidden operating system on your computer.

For similar reasons, any software that requires activation must be installed and activated before you start creating the hidden operating system.

- When you need to shut down the hidden system and start the decoy system, do *not* restart the computer. Instead, shut it down or hibernate it and then leave it powered off for at least several minutes (the longer, the better) before turning the computer on and booting the decoy system. This is required to clear the memory, which may contain sensitive data. For more information, see the section Unencrypted Data in RAM in the chapter Security Requirements and Precautions.
- The computer may be connected to a network (including the internet) only when the decoy operating system is running. When the hidden operating system is running, the computer should not be connected to any network, including the internet (one of the most reliable ways to ensure it is to unplug the network cable, if there is one). Note that if data is downloaded from or uploaded to a remote server, the date and time of the connection, and other data, are typically logged on the server. Various kinds of data are also logged on the operating system (e.g. Windows auto-update data, application logs, error logs, etc.) Therefore, if an adversary had access to the data stored on the server or intercepted your request to the server (and if you revealed the password for the decoy operating system to him), he might find out that the connection was not made from within the decoy operating system, which might indicate the existence of a hidden operating system on your computer.

  Also note that similar issues would affect you if there were any filesystem shared over a network under the hidden operating system (regardless of whether the filesystem is remote or local). Therefore, when the hidden operating system is running, there must be no filesystem shared over a network (in any direction).

- Any actions that can be detected by an adversary (or any actions that modify any data outside mounted hidden volumes) must be performed only when the decoy operating system is running (unless you have a plausible alternative explanation, such as using a "live-CD" system to perform such actions). For example, the option '*Auto-adjust for daylight saving time*' option may be enabled only on the decoy system.
- If the BIOS, EFI, or any other component logs power-down events or any other events that could indicate a hidden volume/system is used (e.g. by comparing such events with the events in the Windows event log), you must either disable such logging or ensure that the log is securely erased after each session (or otherwise avoid such an issue in an appropriate way).

In addition to the above, you must follow the security requirements and precautions listed in the following chapters:

- Security Requirements and Precautions
- **How to Back Up Securely**

Next Section >>

---

* This does not apply to filesystems on CD/DVD-like media and on custom, untypical, or non-standard devices/media.