Free Open source disk encryption with strong security for the Paranoid

3-4 minutes

Plausible Deniability

In case an adversary forces you to reveal your password, VeraCrypt provides and supports two kinds of plausible deniability:

1. Hidden volumes (see the section Hidden Volume) and hidden operating systems (see the section **Hidden Operating System**).
2. Until decrypted, a VeraCrypt partition/device appears to consist of nothing more than random data (it does not contain any kind of "signature"). Therefore, it should be impossible to prove that a partition or a device is a VeraCrypt volume or that it has been encrypted (provided that the security requirements and precautions listed in the chapter Security Requirements and Precautions are followed). A possible plausible explanation for the existence of a partition/device containing solely random data is that you have wiped (securely erased) the content of the partition/device using one of the tools that erase data by overwriting it with random data (in fact, VeraCrypt can be used to securely erase a partition/device too, by creating an empty encrypted partition/device-hosted volume within it). However, you need to prevent data leaks (see the section Data Leaks) and also note that, for system encryption, the first drive track contains the (unencrypted) VeraCrypt Boot Loader, which can be easily identified as such (for more information, see the chapter System Encryption). When using system encryption, plausible deniability can be achieved by creating a hidden operating system (see the section Hidden Operating System).

   Although file-hosted VeraCrypt volumes (containers) do not contain any kind of "signature" either (until decrypted, they appear to consist solely of random data), they cannot provide this kind of plausible deniability, because there is practically no plausible explanation for the existence of a file containing solely random data. However, plausible deniability can still be achieved with a file-hosted VeraCrypt volume (container) by creating a hidden volume within it (see above).

Notes

- When formatting a hard disk partition as a VeraCrypt volume (or encrypting a partition in place), the partition table (including the partition type) is *never* modified (no VeraCrypt "signature" or "ID" is written to the partition table).
- There are methods to find files or devices containing random data (such as VeraCrypt volumes). Note, however, that this should *not* affect plausible deniability in any way. The adversary still should not be able to *prove* that the partition/device is a VeraCrypt volume or that the file, partition, or device, contains a hidden VeraCrypt volume (provided that you follow the security requirements and precautions listed in the chapter Security Requirements and Precautions and in the subsection Security Requirements and Precautions Pertaining to Hidden Volumes).

Next Section >>