dm-crypt/Specialties - ArchWiki

3-4 minutes

Discard/TRIM support for solid state drives (SSD)

Solid state drive users should be aware that, by default, TRIM commands are not enabled by the device-mapper, i.e. block-devices are mounted without the `discard` option unless you override the default.

The device-mapper maintainers have made it clear that TRIM support will never be enabled by default on dm-crypt devices because of the potential security implications.[3][4] Minimal data leakage in the form of freed block information, perhaps sufficient to determine the filesystem in use, may occur on devices with TRIM enabled. An illustration and discussion of the issues arising from activating TRIM is available in the blog of a *cryptsetup* developer. If you are worried about such factors, keep also in mind that threats may add up: for example, if your device is still encrypted with the previous (cryptsetup <1.6.0) default cipher `--cipher aes-cbc-essiv`, more information leakage may occur from trimmed sector observation than with the current default.

The following cases can be distinguished:

- The device is encrypted with default dm-crypt LUKS mode:
  - By default the LUKS header is stored at the beginning of the device and using TRIM is useful to protect header modifications. If for example a compromised LUKS password is revoked, without TRIM the old header will in general still be available for reading until overwritten by another operation; if the drive is stolen in the meanwhile, the attackers could in theory find a way to locate the old header and use it to decrypt the content with the compromised password. See cryptsetup FAQ, section 5.19 What about SSDs, Flash and Hybrid Drives? and Full disk encryption on an ssd.
  - TRIM can be left disabled if the security issues stated at the top of this section are considered a worse threat than the above bullet.

  See also Securely wipe disk#Flash memory.

- The device is encrypted with dm-crypt plain mode, or the LUKS header is stored separately:
  - If plausible deniability is required, TRIM should **never** be used because of the considerations at the top of this section, or the use of encryption will be given away.
  - If plausible deniability is not required, TRIM can be used for its performance gains, provided that the security dangers described at the top of this section are not of concern.

Warning: Before enabling TRIM on a drive, make sure the device fully supports TRIM commands, or data loss can occur. See Solid State Drives#TRIM.

Besides enabling discard support in dm-crypt, it is also required to periodically run fstrim(8) or mount the filesystem (e.g. `/dev/mapper/root` in this example) with the `discard` option in `/etc/fstab`. For details, please refer to the TRIM page.