Is enabling TRIM on an encrypted SSD a security risk?

▲
772
▼

I recently installed Ubuntu 13.10 on an SSD drive using the "encrypt the new Ubuntu installation for security" option. I wanted to enable TRIM, so was following the guide provided here.

One step says to add the `discard` option to `/etc/crypttab`. However, the crypttab man page somewhat vaguely states:

> *WARNING: Assess the specific security risks carefully before enabling this option. For example, allowing discards on encrypted devices may lead to the leak of information about the ciphertext device (filesystem type, used space etc.) if the discarded blocks can be located easily on the device later.*

What exactly are the security risks of enabling TRIM on an encrypted SSD partion/drive?

security

2 Answers   5475 Views

2 Answers

Voted

falconer

Best Answer

2014-01-04T04:31:47+08:00

The warning just want to say, that if you enable the discard option, the firmware of your SSD will zero out the unused blocks on your drive. And these zeroed blocks can be easily identified and analyzed for a pattern.

Obviously the zeroed blocks will show the attacker the unused space and because of that he will know what is the used space. So if he want to crack the encryption he will have to deal with a smaller encrypted data, because he won't care about the unused blocks. And from the pattern of the unused blocks the attacker may be able to guess the filesystem type and the filesystem parameters, which may help him in cracking the encryption.

I'm not a cryptographer nor a cryptoanalyst but these informations are likely just a minimal help for the attacker. I think the warning is just there because in cryptology every minimal leaked information about the encrypted data can lead to the break of the encryption. So the authors of this encrypting software wanted to inform you that you have better security without enabling that feature, but how much better is not really known, because we can't know how much these leaked information help the attacker in breaking of the encryption. Obviously if the authors thought that the enabling of this feature would lead to a bigger than minimal risk for the encryption then this feature wouldn't be present in the software.

If you want to know more about this topic I advise you to read this article from Milan Broz and the comments on that page which also contain some good links. From that good article I paste here his conclusions:

> - If there is a strong requirement that information about unused sectors must not be available to attacker, TRIM must be always disabled.
> - TRIM must not be used if there is a hidden device on the disk. (In this case TRIM would either erase the hidden data or reveal its position.)
> - If TRIM is enabled and executed later (even only once by setting option and calling fstrim), this operation is irreversible. Discarded sectors are still detectable even if TRIM is disabled again.
> - In specific cases (depends on data patterns) some information could leak from the ciphertext device. (In example above you can recognize filesystem type for example.)
> - Encrypted disk cannot support functions which rely on returning zeroes of discarded sectors (even if underlying device announces such capability).
> - Recovery of erased data on SSDs (especially using TRIM) requires completely new ways and tools. Using standard recovery tools is usually not successful.

▲ 6 ▼

K7AAY

2014-01-03T17:10:44+08:00

The key here is the phrase

> *if the discarded blocks can be located easily on the device later.*

So, make sure /tmp /var and other directories used by encryption are really in memory which will be cleared when they system shuts down. That minimizes risk.

I found a good explanation here.