

Forum:[Hack Forums](#)

Thread: [How safe is veracrypt?](#)

bobermaner51 - August 8, 2024, 9:59 am

I was thinking of veracrypt FDE and to which extent it's unbreachable. ?

Most sources online say that once the device is encrypted it's secure, and don't go into more detail, most of them being guides or explaining basic encryption.

The thing is that there are methods like cold boot attacks, evil maid, dma, side-channel, and many other forms of attacks that might gain access to the key or bypass certain things.

There are certain methods like secure boot, bootloader verification, bios password, disabling external boot devices, encryption in pre-boot environment, that might help against certain attacks, but I was wondering if it's possible to make it unbreachable. If there was some sort of security measure that would make it so that no matter how much time an expert has with the drive or entire PC physically accessible to them, the security would be too airtight to exploit.

There are trusted encryption methods for that sort of thing, but the vulnerability starts with veracrypt, since it's not just encrypting data, it's also storing keys and gatekeeping and entire system instead of just having encrypted text/data, making the attack surface much larger.

TLDR: Is there a way to make veracrypt FDE fully airtight and unable to exploit regardless of expertise or time or physical access? If not are there other methods, like FDE + Encrypted hidden volumes for windows? What about on linux? Is there a method where forensics experts just sit there and think "well fuck it's over we can't continue without the key and we can't get the key"?

DramaKing - August 8, 2024, 10:21 am

Is this a laptop or desktop? Laptop with soldered DRAM and no physical TPM is best. Those keys are encrypted by a key in the TPM if not using a password, so it's very secure.

If you want to use Linux, try LUKS encryption. Make your password unique and 12+ characters, and no one will be able to crack the key until doomsday.

globalroot - August 8, 2024, 10:49 am

I heard that VeraCrypt encrypts the in-memory encryption keys (somehow?) so you shouldn't be vulnerable to cold boot attacks.

All attacks you listed require physical access and time to do. Just make sure to keep your computer in a safe place. Or cover it with some kind of plastic, so it will be obvious when someone removes and touches it. Or put a sticker to screw fields.

If someone knocks the door (you know who it is) and you shut down the computer immediately, you still got chances.

As long as you do everything as said in VeraCrypt's website, you are safe.

Yokobovich - August 10, 2024, 9:40 am

VeraCrypt should be safe. (Why, i can't say).

The most prominent cryptographers in the world seem to be on board with Vera, so it should be

safe compared to TrueCrypt. (What the hell happened there?)

peeman - August 13, 2024, 6:02 pm

can i encrypt html page with veracrypter?

DramaKing - August 14, 2024, 4:26 am

(Aug 13, 2024 06:02 PM)peeman Wrote: [\[CITE\]](#) can i encrypt html page with veracrypter?
For what reason??

SovietBastard - August 16, 2024, 1:28 am

(Aug 8, 2024 09:59 AM)bobermaner51 Wrote: [\[CITE\]](#) I was thinking of veracrypt FDE and to which extent it's unbreachable. ?

Most sources online say that once the device is encrypted it's secure, and don't go into more detail, most of them being guides or explaining basic encryption.

The thing is that there are methods like cold boot attacks, evil maid, dma, side-channel, and many other forms of attacks that might gain access to the key or bypass certain things.

There are certain methods like secure boot, bootloader verification, bios password, disabling external boot devices, encryption in pre-boot environment, that might help against certain attacks, but I was wondering if it's possible to make it unbreachable. If there was some sort of security measure that would make it so that no matter how much time an expert has with the drive or entire PC physically accessible to them, the security would be too airtight to exploit.

There are trusted encryption methods for that sort of thing, but the vulnerability starts with veracrypt, since it's not just encrypting data, it's also storing keys and gatekeeping and entire system instead of just having encrypted text/data, making the attack surface much larger.

TLDR: Is there a way to make veracrypt FDE fully airtight and unable to exploit regardless of expertise or time or physical access? If not are there other methods, like FDE + Encrypted hidden volumes for windows? What about on linux? Is there a method where forensics experts just sit there and think "well fuck it's over we can't continue without the key and we can't get the key"?
very safe...

dobroy_000 - August 17, 2024, 6:48 am

i guess the safest out there, as i know...