

Forum:[Hack Forums](#)

Thread: [Encrypting portable hard disk](#)

f1kinHacker - April 1, 2021, 7:15 am

Hello everybody, yesterday I was thinking if it will be good idea to encrypt my portable hdd this way:

1. Hard disk can be unlocked only by fingerprint or password (Samsung Touch)
2. Files on the hard will be encrypted VeraCrypt container
3. Inside the encrypted container will be an .zip archive also with password in cyrillic.

My question is, is this going to work and if yes how long it will take for somebody to bruteforce the passwords ?

Thanks !

webdev77 - April 1, 2021, 5:52 pm

Password strength is the entire security factor. Never assume low cost biometric sensors are secure because they likely aren't against any serious attackers.

Layering up encryption is going to stop pretty much anyone from accessing your data unless it's known to contain something really bad and there is strong incentive to get access to it.

f1kinHacker - April 2, 2021, 7:50 am

(Apr 1, 2021 05:52 PM)webdev77 Wrote: [\[CITE\]](#) Password strength is the entire security factor. Never assume low cost biometric sensors are secure because they likely aren't against any serious attackers.

Layering up encryption is going to stop pretty much anyone from accessing your data unless it's known to contain something really bad and there is strong incentive to get access to it.

Yes, understood, but what if the password will be cyrillic ? How long it will take to somebody to crack it if he does not know its in cyrillic ?

Are there any problems if the data will be .zip archived with password -> then container encryption with veracrypt -> and then put on a portable HDD with fingerprint or password ?

webdev77 - April 2, 2021, 1:55 pm

(Apr 2, 2021 07:50 AM)f1kinHacker Wrote: [\[CITE\]](#) Yes, understood, but what if the password will be cyrillic ? How long it will take to somebody to crack it if he does not know its in cyrillic ?

Are there any problems if the data will be .zip archived with password -> then container encryption with veracrypt -> and then put on a portable HDD with fingerprint or password ?

Obviously if the attacker doesn't know the character set and picks the wrong one, it's safe. Using an archive file can be another layer of encryption.

f1kinHacker - April 3, 2021, 5:58 am

(Apr 2, 2021 01:55 PM)webdev77 Wrote: [\[CITE\]](#) Obviously if the attacker doesn't know the character set and picks the wrong one, it's safe. Using an archive file can be another layer of encryption.

Is this way of doing it (archive->encrypted container->hdd with pass) causing any harm to the data stored ? Like if once per week I have to "unlock" the data there to insert something extra and then "lock" it again?

webdev77 - April 3, 2021, 8:11 am

(Apr 3, 2021 05:58 AM)f1kinHacker Wrote: [\[CITE\]](#) Is this way of doing it (archive->encrypted container->hdd with pass) causing any harm to the data stored ? Like if once per week I have to "unlock" the data there to insert something extra and then "lock" it again?

You won't damage/corrupt the data. The only thing that will happen is you are going to spend a long time on decrypting and re-encrypting data.

f1kinHacker - April 3, 2021, 10:18 am

(Apr 3, 2021 08:11 AM)webdev77 Wrote: [\[CITE\]](#) You won't damage/corrupt the data. The only thing that will happen is you are going to spend a long time on decrypting and re-encrypting data.

Yep that's true, but there is something I have to highly encrypt so nobody can see. Thanks for the quick responses !