**TrueCrypt is more secure than thought (Initial Post) by Gianluca Cannone**

There are three main use cases for TrueCrypt:

- Information protection through system encryption

- Information protection through encrypted volumes

- Confidentiality and information protection through hidden volumes.

- The primary goal is to protect the confidentiality of data in a TrueCrypt volume.

- In addition to the primary protection goal, there are other goals, such as integrity protection or deniability.

According to Frauenhofer SIT, headed by Prof. Dr. Eric Bodden, TrueCrypt is more secure than previous assessments have suggested (Baluda et al, 2015).

Two noticeable vulnerabilities have been discovered in Google Project Zero's TrueCrypt. One of them is very concerning. The gap allows attackers who already have access to the running computer to gain advanced system privileges via malicious code. However, granting an attacker access to encrypted data takes work. To exploit the vulnerability, the attacker would already have extensive access to the computer, for example, via a Trojan. According to the Fraunhofer experts, TrueCrypt offers good protection, especially when data is stored offline on encrypted drives. TrueCrypt does what it is supposed to do relatively well but cannot protect the data during operation.

I recommend a friend TrueCrypt only when he wants to store data offline on a hard drive. However, if it comes to storing data online, I would not recommend it (Frauenhofer SIT, 2015).

**References**

Baluda, M.; Fuchs, A., Holzinger, P., Nguyen, L., Othmane, L. b., Poller, A., Repp, J., Späth, J., Steffan, J., Triller, S. & Bodden, E. (2015) Sicherheitsanalyse TrueCrypt, Darmstadt: Bundesamt für Sicherheit in der Informationstechnik.

Frauenhofer SIT (2015) TrueCrypt ist sicherer als gedacht. Available from: [**https://www.sit.fraunhofer.de/de/presse/details/news-article/show/truecrypt-ist-sicherer-als-gedacht/**](https://www.sit.fraunhofer.de/de/presse/details/news-article/show/truecrypt-ist-sicherer-als-gedacht/) [Accessed 7 November 2022].

Replay by Mustafa Sibai

Hi Gianluca,

While I do agree with your assessment, I disagree with using TrueCrypt even for offline data. The reason for this is if someone important used TrueCrypt to encrypt their extremely important and sensitive data and were targeted by an attacker, the attacker will be able to steal this data if the user of the device plugs in malicious USB into the device or if the attacker somehow had access to the device. The attacker can transfer a malicious payload which instructs the computer to copy important and sensitive data like PDF files, Word documents, Images, Videos, etc... from the device to the USB drive.

After the transfer is complete, the attacker can brute force their way into TrueCrypt encryption and decrypt the files. When it comes to data, high security and strong encryption should always be used regardless of whether the data is online or offline. Always assume that the device is unsecure and the data is vulnerable.