**TrueCrypt - not recommended! (Initial post) By Etkin Getir**

TrueCrypt cryptanalysis by Junestam & Guigo (2014) evidently shows that there are a number of vulnerabilities ranging from high-severity to low-severity and informational ones. From my point of view, the most important vulnerabilities that TrueCrypt is susceptible to are:

* Volume Header key derivation algorithm
* Sensitive information might be paged out from kernel stacks

Because, an attacker can easily access the keys and decrypt the volume by performing a brute-force or a dictionary attack by exploiting these vulnerabilities. Even though, as demonstrated by Davies (2014), using a strong password with a salt of 2512increases the time required to carry out a brute force or a dictionary attack, the aforementioned vulnerabilities are still worrisome when considering the project is no longer maintained since 2014 and there are no recent studies which prove TrueCrypt is still a secure option.

As a result, I wouldn’t recommend TrueCrypt to a friend. However, if a friend of mine has to use it, I’d advise him/her to set a strong password in combination with a salt of 2512 to decrease the possibility of a brute attack, as mentioned above.

Here is an ontology I created for the vulnerabilities mentioned above:

Diagram

Description automatically generated

Replay by Mustafa Sibai

Hello Etkin,

I completely agree with your post. I would not be able to recommend TrueCrypt to anyone in 2022, mainly because the development ceased back in 2014. Even if the software had no vulnerabilities, I would be hard-pressed to recommend it. GPUs have become one of the best ways to brute force password unlocking and decode encrypted data today. With their tens of thousands of cores, they are ideal for encryption breaking. No matter how strong the encryption algorithm used in TrueCrypt, it would not last for very long with the immense power of today's GPUs.

Software must be regularly updated in order to stay secure that is why banks and institutions that deal with the general public's sensitive information update their encryption algorithms every few years to keep up with the growing power of today's CPUs, GPUs, and not to mention quantum computers and the specialized ASIC (Application-Specific Integrated Circuit) hardware.