TrueCrypt

TrueCrypt was discontinued in 2014 due to Microsoft discontinuing support for this in it's OS. At this point, the developers warned that "using TrueCrypt is not secure as it may contain unfixed security issues (TrueCrypt, 2014). Within the same year, Junestam and Guigo (2014) carried out analysis on TrueCrypt that indicated that there are concerns with how TrueCrypt operates.

Junestam and Guido indicated that the source code for TrueCrypt is difficult to review (2014). Because of this, it is difficult to debug the code and correct issues. While seeking secure methods of encryption, being able to appropriately review the applications that do this is essential for professionals and data controllers to be sure that data is being kept surely, which in turn ensures their compliance with all required data laws.

It was also identified during the analysis of TrueCrypt that there was insufficient iteration counts for passwords. This would allow attackers easier routes to guessing passwords, thus allowing access to data that they are not entitled to. The research by Junestam and Guigo (2014) assessed this as a medium risk, which would need to be addressed.

These two factors alone, along with others mentioned within the research, would lead me to not feel confident in recommending TrueCrypt as a storage solution. While it could potentially be useful for people who are not needing to secure sensitive information (for example, if they were wanting to encrypt a manuscript for a novel they are writing), but anything that requires storing sensitive or personal data should not be encrypted using TrueCrypt.

References

Junestam, D., & Guigo, S. (2014). Open Crypto Audit Project: TrueCrypt. iSec Partners.

TrueCrypt (2014) TrueCrypt. Available from: https://truecrypt.sourceforge.net/ [Accessed 20 October 2024].