Collaborative Discussion 2

Initial post

TrueCrypt, as an encryption tool, can protect data via encrypting a whole or part of a disk. A security assessment (Junestam, A. & Guigo, N, 2014) concluded that TrueCrypt, a security software without obviously insecure holes or backdoors, could let an attacker quickly take advantage of it. The report listed 11 vulnerabilities, and no one ranked as a critical level. From the paper, no substantial evidence to support the statement - "Using TrueCrypt is not secure as it may contain unfixed security issues".

However, I would not recommend taking TrueCrypt as your secure storage solution. Because of

1. The project had been discontinued. The software will not be improved or enhanced as OS, hardware, or another technology evolves. Some assumptions could be valid but not true in the future. For example, in 1995, 75-bit encryption was considered to offer adequate safety even for data in an intelligence agency (Blaze, M., Diffie, W., Rivest, R.L., Schneier, B. and Shimomura, T., 1996), but by 2002, 128-bit encryption started as a safety standard, and 75-bit was deprecated.

2. Severe new issues be disclosed. Although the audit report had not found any serious security flaws, in 2015, security researchers found two vulnerabilities that allow attackers to execute any code and privilege escalation via DLL hijacking (Lucian Constantin, 2015).

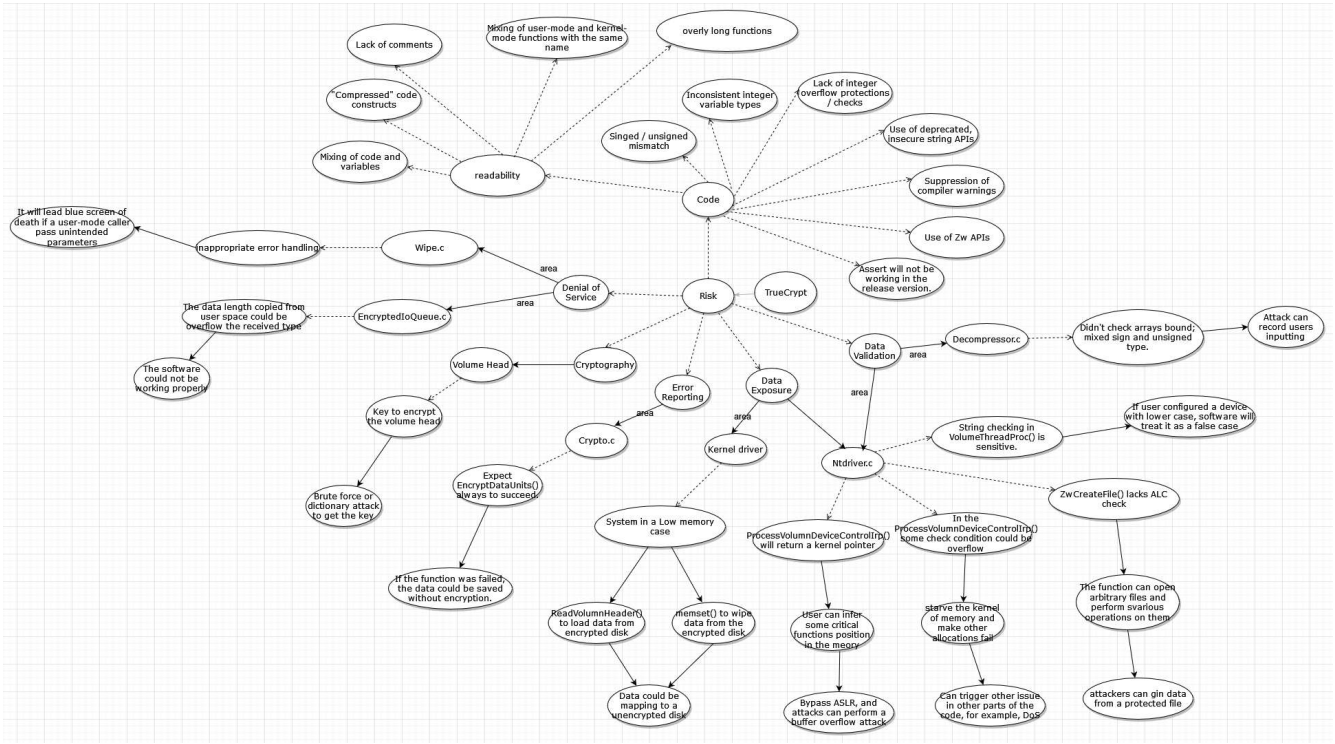
3. TrueCrypt requires users to follow many security requirements and precautions to achieve high security, which could overburden clients. In addition, TrueCrypt can't secure data if a computer has installed malware or an attacker can physically access the target computer.

reference:

Junestam, A. and Guigo, N., 2014. Open crypto audit project truecrypt.

Blaze, M., Diffie, W., Rivest, R.L., Schneier, B. and Shimomura, T., 1996. Minimal key lengths for symmetric ciphers to provide adequate commercial security. A Report by an Ad Hoc Group of Cryptographers and Computer Scientists. INFORMATION ASSURANCE TECHNOLOGY ANALYSIS CENTER FALLS CHURCH VA.

Lucian Constantin., 2015. Newly found TrueCrypt flaw allows full system compromise. [online] Available at: https://www.pcworld.com/article/423766/newly-found-truecrypt-flaw-allows-full-system-compromise.html [Accessed 8 Aug. 2022].



Peer Review to Roberto Cappiello

Thanks for your sharing, Roberto.

Based on the report, I don't think TrueCrypt can be considered an insecure solution to protect user data. There was no evidence to show any critical issue among the vulnerabilities listed in the peper. Change to other words, an attacker could be extremely hard to take advantage of this weakness to steal the information—it was possibly insecure in theory but not in an actual situation.

However, some codes that didn't meet the standard secure code, especially those allocated in the windows kernel driver layer, could bring huge risks. Insecure Kernel driver code took the central part of vulnerabilities for an OS (Chou, A., Yang, J., Chelf, B., Hallem, S. and Engler, D., 2001). Kernel drivers have more privilege than user space, which means if attackers can break from kernel space, the damage will be worse than usual, can bypass all elaborate safety checking.

TrueCrypt was a good solution to protect user data, but it had become obsolete because of its discontinued status. No software can avoid compromise, and only continuous improvement can survive the various attacks.

reference:

Chou, A., Yang, J., Chelf, B., Hallem, S. and Engler, D., 2001, October. An empirical study of operating systems errors. In Proceedings of the eighteenth ACM symposium on Operating systems principles (pp. 73-88).

Peer Review to Nicolas Haas

Thanks for sharing your point, Nicolas.

I agree that software could gain a security benefit from its openness characteristic.The book The Cathedral and the Bazaar advocates taking open source ways to eliminate bugs, and the principle can be written to "given enough eyeballs, all bugs are shallow" (Raymond, E.S., 1997). Hoepman and Jacobs consider open source code will make more secure than closed one (Hoepman, J.H. and Jacobs, B., 2007).

But I would make a reservation on recommending TrueCrypt because of its discontinued status. It could be considered a good choice in the software activity phase (2007-2014), and some stories have proved its good reputation. For example, a journalist was using it against the decoding effort of the government and said it "renders the material extremely difficult to access" (Reuters, 2013). However, as the project developers gave up, users could question the security as lacking continuous improvement. Meanwhile, many OSs have offered their native encryption solution to user files/disks, like BitLocker in windows, FileVault in MacOS, or VeraCrypt, which is the successor of TrueCrypt, can be used on multiple platforms.

reference:

Raymond, E.S., 1997. The cathedral and the bazaar.Hoepman,

J.H. and Jacobs, B., 2007. Increased security through open source. Communications of the ACM, 50(1), pp.79-83.

UK asked N.Y. Times to destroy Snowden material. (2013). Reuters. [online] 30 Aug. Available at: https://www.reuters.com/article/us-usa-security-snowden-nytimes-idUSBRE97T0RC20130830 [Accessed 14 Aug. 2022].

Summary Post

TrueCrypt was proven by its user stories and the security evaluation report, and it was considered a safety solution for protecting user data. However, as it was given up by developers, despite its good reputation, the software can't be a good choice in terms of security concerns because software in the non-maintenance status is a serious security risk (OWASP 2021), as Maja had pointed it out in her peer review. Furthermore, TrueCrypt revealed two more critical vulnerabilities not listed in the report, so I don't suggest using TrueCrypt in users' daily security practices.

However, people can still learn much about software security design and development. When studying the TrueCrypt report, I noted some vulnerabilities in the different areas that could have the exact cause - in the lower memory situation. Usually, people don't focus on function implementation, which supports working on extreme cases. Change other words, software/functions always rely on pre-defined assumptions to achieve the desired result. However, based on the security report, TrueCrypt didn't have an adequate mechanism to detect a false belief about sufficient memory in the running environment. When in design high-security software, people can't just take into consideration the software part, "If ... considers only the software, he or she is limited to production of general goals of the form X must not occur." (Haley, C.B., Laney, R.C., Moffett, J.D. and Nuseibeh, B., 2006). False assumption has been the majority cause of system failure, and it also plays an essential role in software security (Mamun, M.A.A. and Hansson, J., 2011). The most famous example in the assumption of software could be Thompson's compiler case. Recently, more and more supply chins attacks reflect people how much blind trust people place in software assumptions. When high-security software runs, it can minimize the security risks if broken assumptions can be detected.

reference:

1. OWASP (2021). A06 Vulnerable and Outdated Components - OWASP Top 10:2021. [online] owasp.org. Available at: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/.

2. Haley, C.B., Laney, R.C., Moffett, J.D. and Nuseibeh, B., 2006. Using trust assumptions with security requirements. Requirements Engineering, 11(2), pp.138-151.

3. Mamun, M.A.A. and Hansson, J., 2011. Review and challenges of assumptions in software development. In Second Analytic Virtual Integration of Cyber-Physical Systems Workshop (AVICPS).

4. Thompson, K., 1984. Reflections on trusting trust. Communications of the ACM, 27(8), pp.761-763.