University of Essex | Online

TrueCrypt: Peer Responses

Course: MSc Computer Science

Module: Secure Software Development (Computer Science)

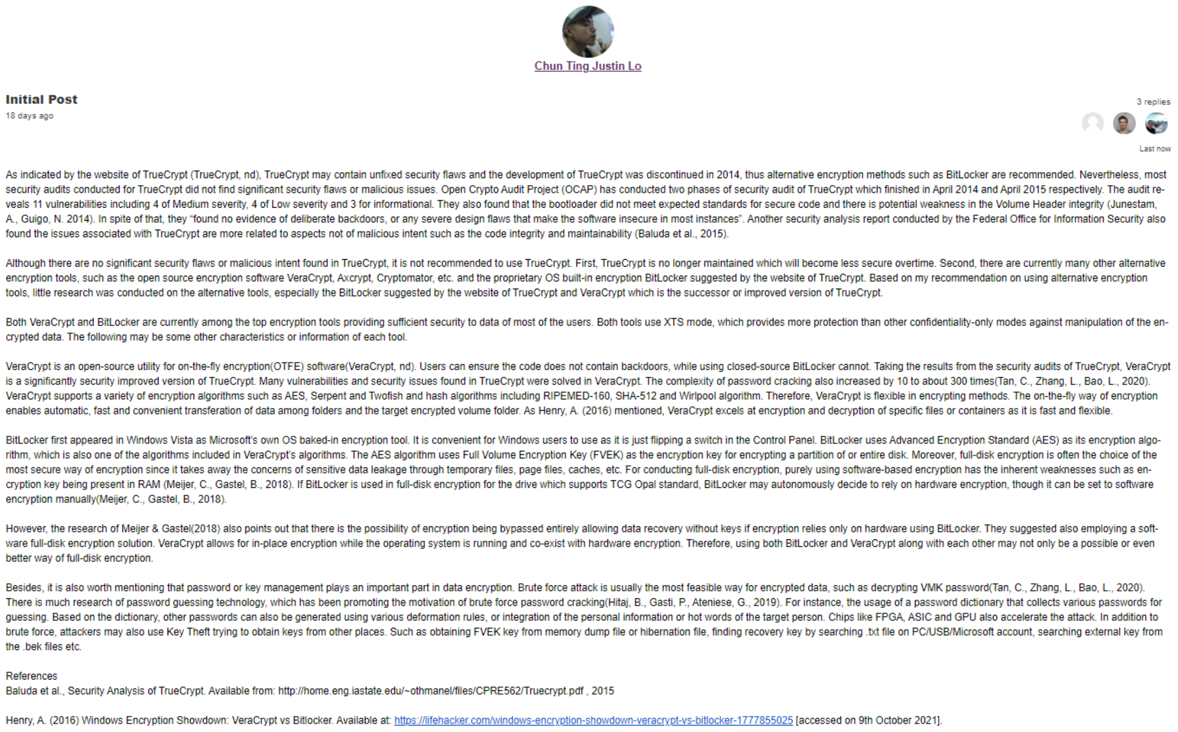
Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Peer Response 1:

In response to:



Chun Ting Justin Lo

Initial Post

18 days ago

3 replies

Last now

As indicated by the website of TrueCrypt (TrueCrypt, nd), TrueCrypt may contain unfixed security flaws and the development of TrueCrypt was discontinued in 2014, thus alternative encryption methods such as BitLocker are recommended. Nevertheless, most security audits conducted for TrueCrypt did not find significant security flaws or malicious issues. Open Crypto Audit Project (OCAP) has conducted two phases of security audit of TrueCrypt which finished in April 2014 and April 2015 respectively. The audit reveals 11 vulnerabilities including 4 of Medium severity, 4 of Low severity and 3 for informational. They also found that the bootloader did not meet expected standards for secure code and there is potential weakness in the Volume Header integrity (Junestam, A., Guigo, N. 2014). In spite of that, they "found no evidence of deliberate backdoors, or any severe design flaws that make the software insecure in most instances". Another security analysis report conducted by the Federal Office for Information Security also found the issues associated with TrueCrypt are more related to aspects not of malicious intent such as the code integrity and maintainability (Baluda et al., 2015).

Although there are no significant security flaws or malicious intent found in TrueCrypt, it is not recommended to use TrueCrypt. First, TrueCrypt is no longer maintained which will become less secure overtime. Second, there are currently many other alternative encryption tools, such as the open source encryption software VeraCrypt, Axcrypt, Cryptomator, etc. and the proprietary OS built-in encryption BitLocker suggested by the website of TrueCrypt. Based on my recommendation on using alternative encryption tools, little research was conducted on the alternative tools, especially the BitLocker suggested by the website of TrueCrypt and VeraCrypt which is the successor or improved version of TrueCrypt.

Both VeraCrypt and BitLocker are currently among the top encryption tools providing sufficient security to data of most of the users. Both tools use XTS mode, which provides more protection than other confidentiality-only modes against manipulation of the encrypted data. The following may be some other characteristics or information of each tool.

VeraCrypt is an open-source utility for on-the-fly encryption(OTFE) software(VeraCrypt, nd). Users can ensure the code does not contain backdoors, while using closed-source BitLocker cannot. Taking the results from the security audits of TrueCrypt, VeraCrypt is a significantly security improved version of TrueCrypt. Many vulnerabilities and security issues found in TrueCrypt were solved in VeraCrypt. The complexity of password cracking also increased by 10 to about 300 times(Tan, C., Zhang, L., Bao, L., 2020). VeraCrypt supports a variety of encryption algorithms such as AES, Serpent and Twofish and hash algorithms including RIPEMED-160, SHA-512 and Wirlpool algorithm. Therefore, VeraCrypt is flexible in encrypting methods. The on-the-fly way of encryption enables automatic, fast and convenient transferation of data among folders and the target encrypted volume folder. As Henry, A. (2016) mentioned, VeraCrypt excels at encryption and decryption of specific files or containers as it is fast and flexible.

BitLocker first appeared in Windows Vista as Microsoft's own OS baked-in encryption tool. It is convenient for Windows users to use as it is just flipping a switch in the Control Panel. BitLocker uses Advanced Encryption Standard (AES) as its encryption algorithm, which is also one of the algorithms included in VeraCrypt's algorithms. The AES algorithm uses Full Volume Encryption Key (FVEK) as the encryption key for encrypting a partition of or entire disk. Moreover, full-disk encryption is often the choice of the most secure way of encryption since it takes away the concerns of sensitive data leakage through temporary files, page files, caches, etc. For conducting full-disk encryption, purely using software-based encryption has the inherent weaknesses such as encryption key being present in RAM (Meijer, C., Gastel, B., 2018). If BitLocker is used in full-disk encryption for the drive which supports TCG Opal standard, BitLocker may autonomously decide to rely on hardware encryption, though it can be set to software encryption manually(Meijer, C., Gastel, B., 2018).

However, the research of Meijer & Gastel(2018) also points out that there is the possibility of encryption being bypassed entirely allowing data recovery without keys if encryption relies only on hardware using BitLocker. They suggested also employing a software full-disk encryption solution. VeraCrypt allows for in-place encryption while the operating system is running and co-exist with hardware encryption. Therefore, using both BitLocker and VeraCrypt along with each other may not only be a possible or even better way of full-disk encryption.

Besides, it is also worth mentioning that password or key management plays an important part in data encryption. Brute force attack is usually the most feasible way for encrypted data, such as decrypting VMK password(Tan, C., Zhang, L., Bao, L., 2020). There is much research of password guessing technology, which has been promoting the motivation of brute force password cracking(Hitaj, B., Gasti, P., Ateniese, G., 2019). For instance, the usage of a password dictionary that collects various passwords for guessing. Based on the dictionary, other passwords can also be generated using various deformation rules, or integration of the personal information or hot words of the target person. Chips like FPGA, ASIC and GPU also accelerate the attack. In addition to brute force, attackers may also use Key Theft trying to obtain keys from other places. Such as obtaining FVEK key from memory dump file or hibernation file, finding recovery key by searching .txt file on PC/USB/Microsoft account, searching external key from the .bek files etc.

References
Baluda et al., Security Analysis of TrueCrypt. Available from: http://home.eng.iastate.edu/~othmanel/files/CPRE562/Truecrypt.pdf , 2015

Henry, A. (2016) Windows Encryption Showdown: VeraCrypt vs Bitlocker. Available at: https://lifehacker.com/windows-encryption-showdown-veracrypt-vs-bitlocker-1777855025 [accessed on 9th October 2021].

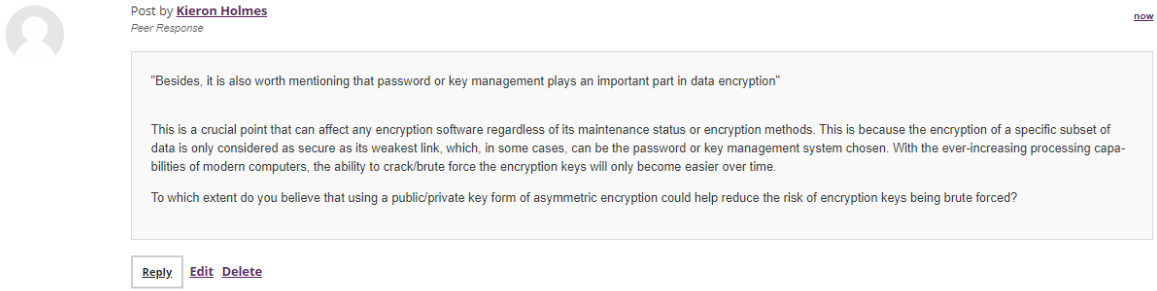
Post:

"Besides, it is also worth mentioning that password or key management plays an important part in data encryption"

This is a crucial point that can affect any encryption software regardless of its maintenance status or encryption methods. This is because the encryption of a specific subset of data is only considered as secure as its weakest link, which, in some cases, can be the password or key management system chosen. With the ever-increasing processing capabilities of modern computers, the ability to crack/brute force the encryption keys will only become easier over time.

To which extent do you believe that using a public/private key form of asymmetric encryption could help reduce the risk of encryption keys being brute forced?

Screenshot:



Post by Kieron Holmes

Peer Response

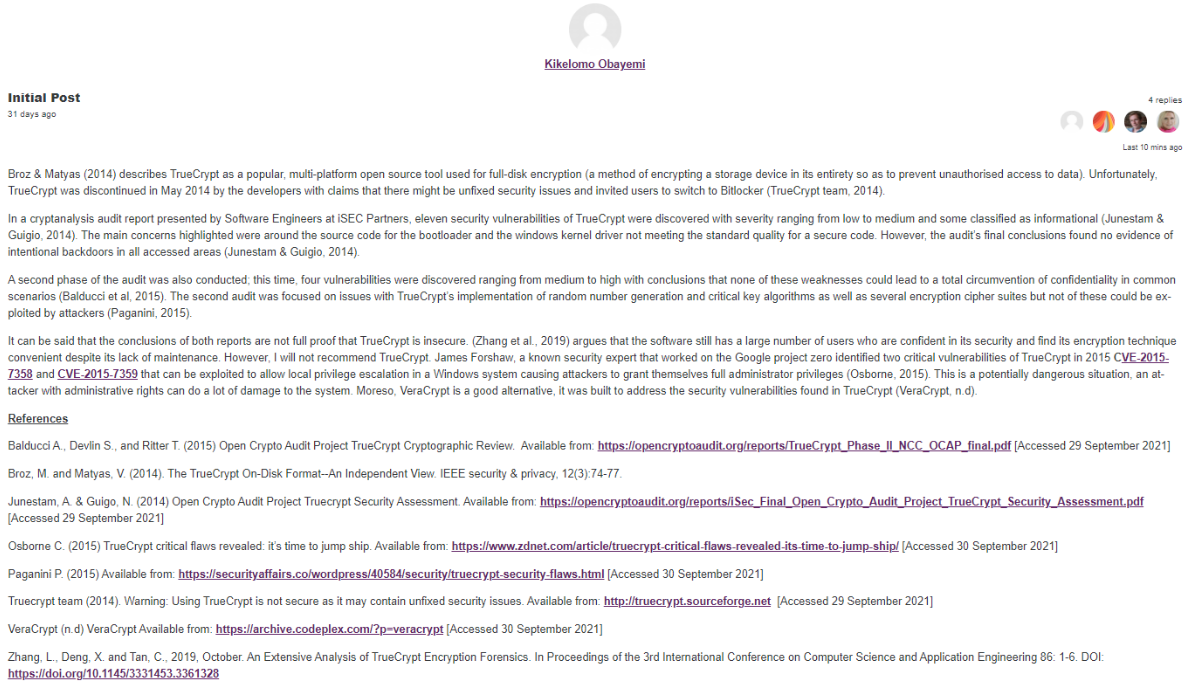
"Besides, it is also worth mentioning that password or key management plays an important part in data encryption"

This is a crucial point that can affect any encryption software regardless of its maintenance status or encryption methods. This is because the encryption of a specific subset of data is only considered as secure as its weakest link, which, in some cases, can be the password or key management system chosen. With the ever-increasing processing capabilities of modern computers, the ability to crack/brute force the encryption keys will only become easier over time.

To which extent do you believe that using a public/private key form of asymmetric encryption could help reduce the risk of encryption keys being brute forced?

Peer Response 2:

In response to:



Kikelomo Obayemi

Initial Post

31 days ago

4 replies

Last 10 mins ago

Broz & Matyas (2014) describes TrueCrypt as a popular, multi-platform open source tool used for full-disk encryption (a method of encrypting a storage device in its entirety so as to prevent unauthorised access to data). Unfortunately, TrueCrypt was discontinued in May 2014 by the developers with claims that there might be unfixed security issues and invited users to switch to Bitlocker (TrueCrypt team, 2014).

In a cryptanalysis audit report presented by Software Engineers at iSEC Partners, eleven security vulnerabilities of TrueCrypt were discovered with severity ranging from low to medium and some classified as informational (Junestam & Guigio, 2014). The main concerns highlighted were around the source code for the bootloader and the windows kernel driver not meeting the standard quality for a secure code. However, the audit's final conclusions found no evidence of intentional backdoors in all accessed areas (Junestam & Guigio, 2014).

A second phase of the audit was also conducted; this time, four vulnerabilities were discovered ranging from medium to high with conclusions that none of these weaknesses could lead to a total circumvention of confidentiality in common scenarios (Balducci et al, 2015). The second audit was focused on issues with TrueCrypt's implementation of random number generation and critical key algorithms as well as several encryption cipher suites but not of these could be exploited by attackers (Paganini, 2015).

It can be said that the conclusions of both reports are not full proof that TrueCrypt is insecure. (Zhang et al., 2019) argues that the software still has a large number of users who are confident in its security and find its encryption technique convenient despite its lack of maintenance. However, I will not recommend TrueCrypt. James Forshaw, a known security expert that worked on the Google project zero identified two critical vulnerabilities of TrueCrypt in 2015 CVE-2015-7358 and CVE-2015-7359 that can be exploited to allow local privilege escalation in a Windows system causing attackers to grant themselves full administrator privileges (Osborne, 2015). This is a potentially dangerous situation, an attacker with administrative rights can do a lot of damage to the system. Moreso, VeraCrypt is a good alternative, it was built to address the security vulnerabilities found in TrueCrypt (VeraCrypt, n.d).

References

Balducci A., Devlin S., and Ritter T. (2015) Open Crypto Audit Project TrueCrypt Cryptographic Review. Available from: https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf [Accessed 29 September 2021]

Broz, M. and Matyas, V. (2014). The TrueCrypt On-Disk Format--An Independent View. IEEE security & privacy, 12(3):74-77.

Junestam, A. & Guigo, N. (2014) Open Crypto Audit Project Truecrypt Security Assessment. Available from: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 29 September 2021]

Osborne C. (2015) TrueCrypt critical flaws revealed: it's time to jump ship. Available from: https://www.zdnet.com/article/truecrypt-critical-flaws-revealed-its-time-to-jump-ship/ [Accessed 30 September 2021]

Paganini P. (2015) Available from: https://securityaffairs.co/wordpress/40584/security/truecrypt-security-flaws.html [Accessed 30 September 2021]

Truecrypt team (2014). Warning: Using TrueCrypt is not secure as it may contain unfixed security issues. Available from: http://truecrypt.sourceforge.net [Accessed 29 September 2021]

VeraCrypt (n.d) VeraCrypt Available from: https://archive.codeplex.com/?p=veracrypt [Accessed 30 September 2021]

Zhang, L., Deng, X. and Tan, C., 2019, October. An Extensive Analysis of TrueCrypt Encryption Forensics. In Proceedings of the 3rd International Conference on Computer Science and Application Engineering 86: 1-6. DOI: https://doi.org/10.1145/3331453.3361328

Post:

Hi Kike,

You have produced a very in-depth post, focusing on the vulnerabilities identified by the independent audit on the TrueCrypt product. Not only is the product vulnerable from that perspective, but the lack of active maintenance could also be seen as a negative factor affecting organisations that were using the TrueCrypt product at the time it was discontinued.

The UK's National Cyber Security Centre (n.d.) considers two items that should be considered when working using obsolete software, namely:

- Reducing the likelihood of compromise

- Reduce the impact of compromise

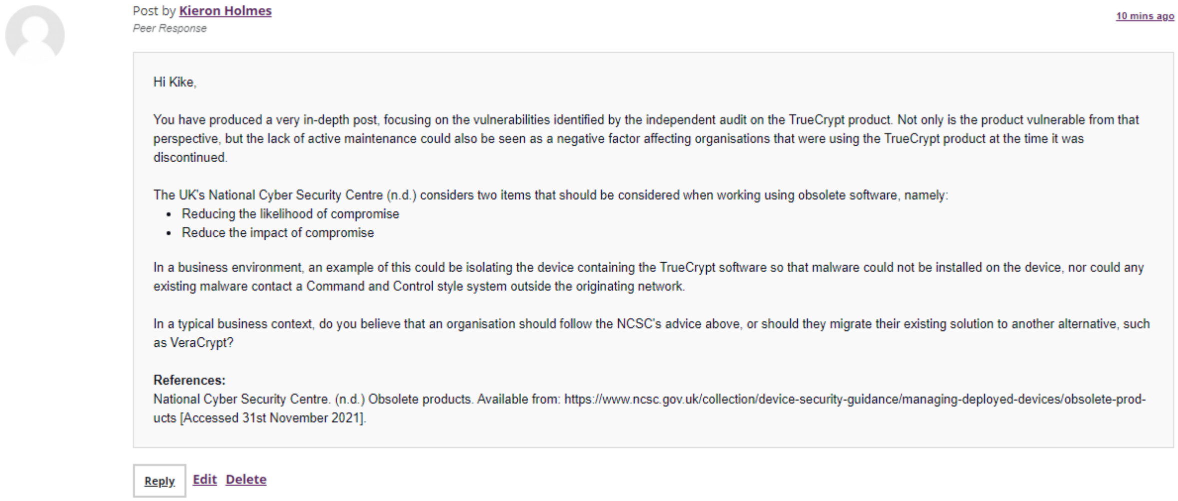
In a business environment, an example of this could be isolating the device containing the TrueCrypt software so that malware could not be installed on the device, nor could any existing malware contact a Command and Control style system outside the originating network.

In a typical business context, do you believe that an organisation should follow the NCSC's advice above, or should they migrate their existing solution to another alternative, such as VeraCrypt?

References:

National Cyber Security Centre. (n.d.) Obsolete products. Available from: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products [Accessed 31st November 2021].

Screenshot:



Post by Kieron Holmes
Peer Response

Hi Kike,

You have produced a very in-depth post, focusing on the vulnerabilities identified by the independent audit on the TrueCrypt product. Not only is the product vulnerable from that perspective, but the lack of active maintenance could also be seen as a negative factor affecting organisations that were using the TrueCrypt product at the time it was discontinued.

The UK's National Cyber Security Centre (n.d.) considers two items that should be considered when working using obsolete software, namely:

- Reducing the likelihood of compromise
- Reduce the impact of compromise

In a business environment, an example of this could be isolating the device containing the TrueCrypt software so that malware could not be installed on the device, nor could any existing malware contact a Command and Control style system outside the originating network.

In a typical business context, do you believe that an organisation should follow the NCSC's advice above, or should they migrate their existing solution to another alternative, such as VeraCrypt?

References:
National Cyber Security Centre. (n.d.) Obsolete products. Available from: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products [Accessed 31st November 2021].