Collaborative Discussion 2

Initial post

TrueCrypt was a popular full disk encryption program released in 2004, and subsequently discontinued in 2014. Rumors persist that the shutdown may have occurred as a result of government intervention, however, other researchers have hypothesized that the security vulnerabilities present were too expensive to fix, and that shutting down was the more astute option (Hern, 2014).

Researchers have thoroughly analyzed the TrueCrypt software, and have found two critical vulnerabilities:

- CVE-2015-7358. This vulnerability allows an attacker to gain access to a running process and obtain administrative privileges, thus allowing for access to the decrypted data.

- CVE-2015-7359. This vulnerability allows the attacker to impersonate an authenticated user.

The open crypto audit project also discovered other flaws in coding, such as signed and unsigned mismatches, Inconsistent integer variable types and use of deprecated, insecure string APIs among others (Junestam & Guigo, 2014).

None of these issues were reported to have been exploited. The code also contained Suppression of compiler warnings, which prevented Microsoft compilers from showing these code errors (Junestam & Guigo, 2014).

Since TrueCrypt has been discontinued, and development ceased, it is inadvisable to continue using this program (“TrueCrypt,” n.d.). A subsequent project called VeraCrypt has been developed and has addressed the critical vulnerabilities that had plagued TrueCrypt. Another option for full disk encryption is Microsoft’s Bit locker, however this is a proprietary code and not an open source project, which should be taken into account when selecting a full disk encryption. (“TrueCrypt alternatives: 5 best services to encrypt your data today | PrivacySavvy,” 2021.).

References

Hern, A. (2014). Encryption software TrueCrypt closes doors in odd circumstances | Technology | The Guardian. Retrieved July 11, 2021, from https://www.theguardian.com/technology/2014/may/30/encryption-software-truecrypt-closes-doors

Junestam, A., & Guigo, N. (2014). Open Crypto Audit Project TrueCrypt. *ISECpartners*, (Security Assesment).

TrueCrypt. (n.d.). Retrieved July 11, 2021, from http://truecrypt.sourceforge.net/

TrueCrypt alternatives: 5 best services to encrypt your data today | PrivacySavvy. (n.d.). Retrieved July 11, 2021, from https://privacysavvy.com/security/safe-browsing/truecrypt-alternatives/

Summary Post

The research that I had conducted as well as input from my colleagues, has reaffirmed my initial stance that TrueCrypt is not a viable full disk encryption service. It should not be recommended for use (*TrueCrypt*, no date).

Grace pointed out that the cryptographic function used was not secure and could lead to watermark attacks. Upon further research into this method of attack, I discovered that patterns could be discovered using the ciphertext, thus revealing the existence of hidden volumes (Broz and Matyas, 2014).

Yohay mentioned quality control audit issues in his post, which raises a major concern about the validity of results during testing.

In addition, since the software has reached end of life, with no future support offered, there are several issues that may be present, such as:

- Security vulnerabilities as mentioned previously (Junestam and Guigo, 2014).
- Software incompatibility - TrueCrypt is unlikely to be fully compatible with newer operating systems (Spiceworks, 2016).
- Compliance issues- Since GDPR is now being enforced, it is unclear whether TrueCrypt would be compatible with newer regulations (Spiceworks, 2016).
- Poor reliability- Bugs would not be addressed by the developers, and usability would suffer (Spiceworks, 2016).

I conducted further research into the area of cloud encryption, as disk storage is quickly being replaced by cloud storage. The problem with companies encrypting their data prior to uploading to the cloud, is that customers do not have the decryption key, and when they download the data for use, they are unable to use it without being supplied the decryption key by the parent company, leading to possible security risks. A possible solution is using the cloud storage providers encryption, which would then allow for the data to be decrypted in the cloud and securely sent via TLS to the customers device (*Cloud Encryption: Challenges and Recommendations - business.com*, no date). This however puts a lot of unencrypted data in the hands of major tech companies such as google, amazon and apple. For the security conscious user, who prefers not to entrust their data with these companies, there are solutions such as nCrypted Cloud, Encrypto and Boxcryptor amongst others (Paul Bischoff, 2018).

References

Broz, M. and Matyas, V. (2014) ‘The trueCrypt on-disk format - An independent view’, *IEEE Security and Privacy*, 12(3), pp. 74–77. doi: 10.1109/MSP.2014.60.

Cloud Encryption: Challenges and Recommendations - business.com (no date). Available at: https://www.business.com/articles/cloud-data-encryption/ (Accessed: 17 July 2021).

Junestam, A. and Guigo, N. (2014) ‘Open Crypto Audit Project TrueCrypt’, *iSECpartners*, (Security Assesment).

Paul Bischoff (2018) *Best Free Apps to Encrypt Files & Data before Uploading to the Cloud*, *Comparitech*. Available at: https://www.comparitech.com/blog/cloud-online-backup/6-apps-to-encrypt-your-files-before-uploading-to-the-cloud/ (Accessed: 17 July 2021).

Spiceworks (2016) *End-of-life software: What are the dangers?* Available at: https://www.spiceworks.com/it-articles/end-of-life-software-dangers/ (Accessed: 17 July 2021).

TrueCrypt (no date). Available at: http://truecrypt.sourceforge.net/ (Accessed: 11 July 2021).