Unit 8

Blog Post – Case Study: TrueCrypt

The cryptanalysis report (Junestam & Guigo, 2014) regarding TrueCrypt disk encryption software concluded that several vulnerabilities exist that range from medium to low (according to the iSEC Partners Threat Matrix) with the software using deprecated functions and varying data types. TrueCrypt ensured integrity using the IEEE 1619 disk encryption algorithm known as XTS—based on the XEX mode of operation with CipherText Stealing feature that XORs plaintext before and after encryption (Alomari et al., 2009). The report highlights the causes of a vulnerability and how a hacker may attack the software and provides mitigation of specific vulnerabilities. However, from the report, almost all medium-level vulnerabilities require an attacker to force a low-memory situation or have knowledge of the workings of the TrueCrypt software. Therefore, it is agreeable that TrueCrypt contains “unfixed security issues” and should not be utilised. But such vulnerabilities do not seem so significant that they could not be corrected, with some users speculating about the software’s termination (Rozenzweig, 2014) being related to the audit performed on the code—which found no significant compromise the integrity of the program.

The anonymous authors of TrueCrypt (TrueCrypt, 2014) issue a warning regarding TrueCrypt, recommending BitLocker or Virtual Hard Disks instead. This point and the fact that Microsoft Windows supports BitLocker out of the box makes it irresponsible to recommend TrueCrypt since they will not address its security vulnerabilities. Fortunately, there are many replacements such as VeraCrypt, BitLocker, DiskCryptor, CipherShed or BoxCryptor. For BitLocker, caveats include reliance on a Trusted Platform Module (TPM) 1.2 or higher, a USB key if TPM is not supported, a UEFI compliant BIOS for use with TPM, and the need for two partitions—system integrity and verification occur separately. (Microsoft, 2021)

Lastly, another significant concern for disk encryption is the danger of forgotten passwords and, therefore, a greater emphasis on key/password management.

References

Alomari, M.A., Samsudin, K. and Ramli, A.R., 2009, May. A study on encryption algorithms and modes for disk encryption. In *2009 International Conference on Signal Processing Systems* (pp. 793-797). IEEE.

Junestam, A. & Guigo, N. (2014) Open crypto audit project truecrypt. Available from https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 04 Oct. 2021]

Microsoft (2021) BitLocker Overview and Requirements FAQ. Available from https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview-and-requirements-faq [Accessed 04 Oct. 2021]

Rosenzweig, P. (2014) The Strange Demise of TrueCrypt and What oIt Says About CyberSecurity. Available from https://www.lawfareblog.com/strange-demise-truecrypt-and-what-it-says-about-cybersecurity [Accessed 04 Oct. 2021]

TrueCrypt (2014) Migrating from TrueCrypt to BitLocker. Available from http://truecrypt.sourceforge.net/ [Accessed 04 Oct. 2021]