

## Initial Post

[◀ Initial Post](#)

## Summary Post ►

### Display replies in nested form

Settings ▾



### Initial Post

by [Anda Ziemele](#) - Sunday, 15 December 2024, 10:39 PM

TrueCrypt was a popular (Ratliff, 2016) data encryption programme, which was compatible with all major operating systems, however its development was discontinued in the light of multiple security issues and end of support for Microsoft XP (TrueCrypt, 2014), however multiple news organisations raised unusual circumstances (Hern, 2014).

Overall, I would not recommend a friend to use TrueCrypt. Firstly, given the developers abandoned the project over ten years ago, this is inherently a major security flaw. Software which is no longer kept up-to-date does not receive security updates, thus becomes vulnerable to new exploits. Additionally, the latest security mitigations are not carried, which results in exploitation being more successful and difficult to detect (NCSC, n.d.). Many organisations already use multiple outdated software packages with multiple vulnerabilities, exposing themselves to cyber attacks (Murciano-Goroff et al., 2024).

Additionally, although the report by Junestam & Guigo (2014) does not highlight any high-level vulnerabilities, only medium and low, a second report released by Balducci et al. (2015) highlights multiple high-severity issues which may cause significant failures in specific circumstances. For example, in one instance the random number generator for master encryption may fail, resulting in poorer encryption. The findings of the reports overall do not necessarily advise people against using TrueCrypt, but given these were produced a significant period of time ago, there is a high level of uncertainty as to their fit with current operating systems.

Figure 1 demonstrates an ontology of the findings based on the initial 2014 report, and adds vulnerabilities recorded in MITRE's CVE. Additional fields have been added to list requirements by users and which are affected by the listed vulnerabilities. The ontology could be expanded for the purposes of comprehensiveness and clarity. Some components of the ontology, such as 'hasVulnerability' has been demonstrated in the paper by Wang & Guo (2009).

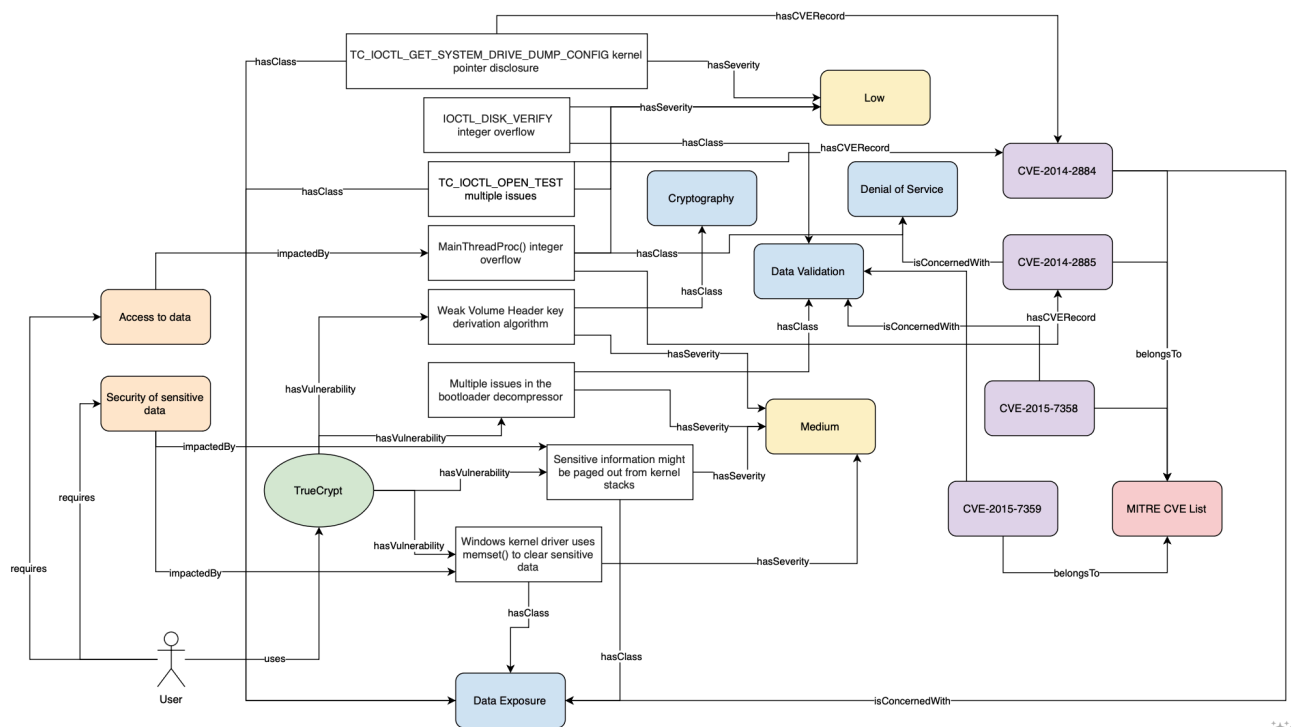


Figure 1. Initial ontology based on findings by Junestam & Guigo (2014).

### References:

Chat to us!

Balducci, A., Devlin, S. & Ritter, T. (2015) Open Crypto Audit Project Truecrypt Security Assessment. *Open Crypto Audit Project*. Available from: [https://opencryptoaudit.org/reports/TrueCrypt\\_Phase\\_II\\_NCC\\_OCAP\\_final.pdf](https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf) [Accessed 11 December 2024]

Hern, A. (2014) Encryption software TrueCrypt closes doors in odd circumstances. *The Guardian*. Available from: <https://www.theguardian.com/technology/2014/may/30/encryption-software-truecrypt-closes-doors> [Accessed 15 December 2024]

Junestam, A. & Guigo, N. (2014) Open Crypto Audit Project Truecrypt Security Assessment. *Open Crypto Audit Project*.

Murciano-Goroff, R., Zhuo, R. & Greenstein, S. (2024) Navigating Software Vulnerabilities: Eighteen Years of Evidence from Medium and Large US Organizations (No. w32696). *National Bureau of Economic Research*. Available from: <https://www.nber.org/papers/w32696> [Accessed 15 December 2024]

NCSC (n.d.) Obsolete products. *National Cyber Security Centre*. Available from: <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products> [Accessed 15 December 2024]

TrueCrypt (2014) Homepage. *TrueCrypt*. Available from: <https://truecrypt.sourceforge.net> [Accessed 11 December 2024]

Ratliff, E. (2016) The Strange Origins of TrueCrypt, ISIS's Favored Encryption Tool. *New Yorker*. Available from: <https://www.newyorker.com/news/news-desk/the-strange-origins-of-truecrypt-iss-favored-encryption-tool> [Accessed 15 December 2024]

Wang, J.A. & Guo, M. (2009) OVM: an ontology for vulnerability management. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (1-4).

[Permalink](#) [Reply](#)



Re: Initial Post

by [Cathryn Peoples](#) - Monday, 16 December 2024, 2:20 PM

Thanks very much for sharing this, Anda, and for the amount of effort which you have placed into its preparation. I feel that it is a little more like a flow diagram than an ontology - I wouldn't expect to see an actor in the ontology. I'm also finding it a little difficult to track the paths, I'll take a closer look with you in a video now:

[https://kaplanopenlearning.zoom.us/rec/share/8nngzi7TLADOBRvrcUi9BXCD1ouGwk3cO5zOswUzAeX3O7jrlpMZtNX3ivl8LRpN.epuypf5GOM\\_CEp1z](https://kaplanopenlearning.zoom.us/rec/share/8nngzi7TLADOBRvrcUi9BXCD1ouGwk3cO5zOswUzAeX3O7jrlpMZtNX3ivl8LRpN.epuypf5GOM_CEp1z)

Best wishes,  
Cathryn

[Permalink](#) [Show parent](#) [Reply](#)



Peer Response

by [Oi Lam Siu](#) - Tuesday, 24 December 2024, 6:32 AM

Dear Andy,

Thank you for bringing to our attention the second audit report on TrueCrypt by Balducci et al. (2015), which focuses specifically on the cryptographic implementation and usage within TrueCrypt. This report offers a deeper dive into the cryptographic aspects, building upon the audit report by Junestam and Guigo (2014). The audit report by Balducci et al. (2015) identified four vulnerabilities, including two high-severity issues.

Key vulnerabilities found:

- CryptAcquireContext may silently fail in unusual scenarios: This could lead to weak random number generation.
- AES implementation susceptible to cache-timing attacks: Potentially allowing attackers to recover encryption keys.
- Keyfile mixing is not cryptographically sound: There is a weakness in how keyfiles are combined with passwords.
- Unauthenticated ciphertext in volume headers: The lack of integrity checks could allow tampering with volume headers.

Focusing specifically on the high-severity issue you mentioned in your initial post—weak random number generation by Balducci et al. (2015) also addresses recommendations that align with the Microsoft Learn Challenge (Microsoft, 2024). Calling CryptAcquireContext, it is advised to include the CRYPT\_VERIFYCONTEXT flag. This flag informs the function that no key

[Chat to us!](#)

container is needed and that it should not attempt to access one. Since TrueCrypt uses CryptAcquireContext exclusively for random number generation and does not need to store persistent keys, this flag prevents failures due to inaccessible key containers.

Other than that, it is also important to validate and test across different environments, ensuring that a wide range of system configurations and policies are covered.

By following these mitigations, TrueCrypt can ensure that it does not inadvertently operate with weak randomness, thereby enhance the security and integrity of cryptographic keys and operations.

Best regards,

Helen

#### Reference:

Balducci, A., Devlin, S. & Ritter, T. (2015) Open Crypto Audit Project Truecrypt – Cryptographic Review. Tech. rep., nccgroup.

Junestam, A. and Guigo, N. (2014) Open Crypto Audit Project Truecrypt – Security Assessment. Tech. rep., iSECpartners.

Microsoft. (2024) Microsoft Learn Challenge - CryptAcquireContext() use and troubleshooting. Available from: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/cryptacquirecontext-troubleshooting>

Maximum rating: -

[Permalink](#)

[Show parent](#)

[Reply](#)



Re: Peer Response

by [Oi Lam Siu](#) - Tuesday, 24 December 2024, 11:41 AM

Sorry to mistype your name, Anda.

Maximum rating: -

[Permalink](#)

[Show parent](#)

[Reply](#)



Peer Response

by [Andrius Busilas](#) - Tuesday, 7 January 2025, 8:05 PM

Hi Anda,

Your review of TrueCrypt effectively underscores the significant issues associated with using outdated encryption software. The focus on security vulnerabilities caused by the cessation of updates aligns with cybersecurity best practices (NCSC n.d.). The argument is further bolstered by referencing studies by Balducci et al. (2015) and Junestam and Guigo (2014), offering a historical context for the software's shortcomings.

The discussion of the software's incompatibility with modern operating systems and the potential failure of its random number generator illustrates the concrete risks of using obsolete encryption tools. This aligns with broader concerns about legacy software in organizational settings, as explored by Murciano-Goroff et al. (2024), who emphasize how outdated technologies can expose vulnerabilities.

It would be beneficial to elaborate on alternative encryption methods. For example, mentioning VeraCrypt, which improves upon TrueCrypt's foundation, while addressing many of its weaknesses, could be valuable. Presenting such options would enhance critique's constructiveness by providing readers with practical alternatives.

The ontology presented in Figure 1 offers a novel approach for classifying vulnerabilities. The inclusion of user requirements and their connection to specific weaknesses adds practical value. Further development of this framework, as suggested, could increase its applicability across various software analysis scenarios, potentially aiding proactive vulnerability management (Wang & Guo, 2009).

In summary, your critique is supported by credible sources. This discussion could be enriched by providing more recommendations for alternative encryption tools and exploring the potential applications of the proposed ont

[Chat to us!](#)

References

Balducci, A., Devlin, S. & Ritter, T. (2015) Open Crypto Audit Project Truecrypt Security Assessment. Open Crypto Audit Project.

Murciano-Goroff, R., Zhuo, R. & Greenstein, S. (2024) Navigating Software Vulnerabilities: Eighteen Years of Evidence. National Bureau of Economic Research.

NCSC (n.d.) Obsolete products. National Cyber Security Centre.

Wang, J.A. & Guo, M. (2009) OVM: An Ontology for Vulnerability Management. Cyber Security and Information Intelligence Research.

[Permalink](#) [Show parent](#) [Reply](#)

[◀ Initial Post](#) [Summary Post ▶](#)

You are logged in as Oi Lam Siu (Log out)

[Policies](#)

Powered by Moodle

[Site Accessibility Statement](#)  
[Privacy Policy](#)

© 2025 University of Essex Online. All rights reserved.



Chat to us!