Peer Response 1:

Collaborative Discussion 2: Cryptography case study - TrueCrypt

In reply to Anda Ziemele

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Your review of TrueCrypt effectively underscores the significant issues associated with using outdated encryption software.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 is in line 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 (2024), who emphasize how outdated technologies can expose vulnerabilities.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 ontology.

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.