Secure Software Development (Computer Science) November 2021

Home / / My courses/ / SSDCS_PCOM7E November 2021 / / Unit 8 /

/ Collaborative Discussion 2: Cryptography case study: TrueCrypt /

Collaborative Discussion 2: Cryptography case study: TrueCrypt

This discussion will last for 3 weeks covering units 8, 9 and 10. Ensure you include appropriate citations and references in all your posts (this is not included in the word count for each week's post/submission).

Discussion Topic

TrueCrypt was a popular and well-respected operating system add-on that could create encrypted volumes on a Windows and/or Linux system. In addition, it was also designed to create a complete, bootable volume that could encrypt the entire operating system and data for a Windows XP system. It was discontinued in 2014.

Case Study: Read the TrueCrypt cryptanalysis by Junestam & Guigo (2014) (link is in the reading list) and then answer the following questions:

- The (anonymous) TrueCrypt authors have said "Using TrueCrypt is not secure as it may contain unfixed security issues" (**http://truecrypt.sourceforge.net/**, 2014). Does the cryptanalysis provided above prove or disprove this assumption?
- Would you be prepared to recommend TrueCrypt to a friend as a secure storage environment? What caveats (if any) would you add?

Remember to save this to your e-portfolio.

Present an ontology design which captures the weaknesses of TrueCrypt, and organise them according to their severity. Expand the ontology design by considering the factors which will cause each weakness to become an issue from a user's perspective. For example, if a user wishes to encrypt a disk storing bank details using TrueCrypt, which weakness of the software might cause this specific user goal to be negatively impacted?

Learning Outcomes

- Identify and manage security risks as part of a software development project.
- Critically analyse development problems and determine appropriate methodologies, tools and techniques (including program design and development) to solve them.
- Design and develop/adapt computer programs and to produce a solution that meets the design brief and critically evaluate solutions that are produced.

Assignment Guidance

- Your initial posting should respond to the question and be at least 200 words long. This should be labelled as '**Initial Post**'
- You will then respond to **at least 2 of your peers' posts** in unit 2 (each labelled as '**Peer Response**'). To guide your responses, look at the guidelines for the peer review process on the **Department's homepage**. Focus on the possible measures that could have been put in place in order to prevent the incidents highlighted by your peers. Please try to limit your response posts to **200-300 words maximum**, so that others may be encouraged to reflect on, and respond to your ideas.

- In Unit 3, you should provide a summary post based on your initial post, the feedback from your peers and the content of the three units. Please label this as '**Summary Post**'. It should be **300** words.
- Referencing: When you have referred to other authors thoughts, ideas and opinions in your posts, you must reference the author as you would in an academic assignment using the UoEO Harvard reference style.
- You will be not be assessed on your contribution to this forum throughout the module, but the tutor will post group feedback via a module announcement.
- This activity forms a component of your e-portfolio which you will submit in unit 12. All e-portfolio activities are intended to demonstrate your ability and strengths through evidence and reflection.

4 discussions

Add a new discussion

Search

Recent

Sort

Michael Botha

Initial Post

18 days ago

6 replies

Last 23 hours ago

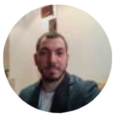
Thien Liu

Initial Post

6 days ago

1 reply

Last 2 days ago



Gennaro Coppola

Initial Post

12 days ago

4 replies

Last 7 days ago

Neelam Pirbhai-Jetha

Initial Post

27 days ago

5 replies

Last 7 days ago

Manage forum subscriptions

Secure Software Development (Computer Science) November 2021

Home / / My courses/ / SSDCS_PCOM7E November 2021 / / Unit 8 /

/ Collaborative Discussion 2: Cryptography case study: TrueCrypt / / Initial Post /

« Collaborative Discussion 2: Cryptography case study: TrueCrypt

Michael Botha

Initial Post

18 days ago

6 replies

Last 23 hours ago

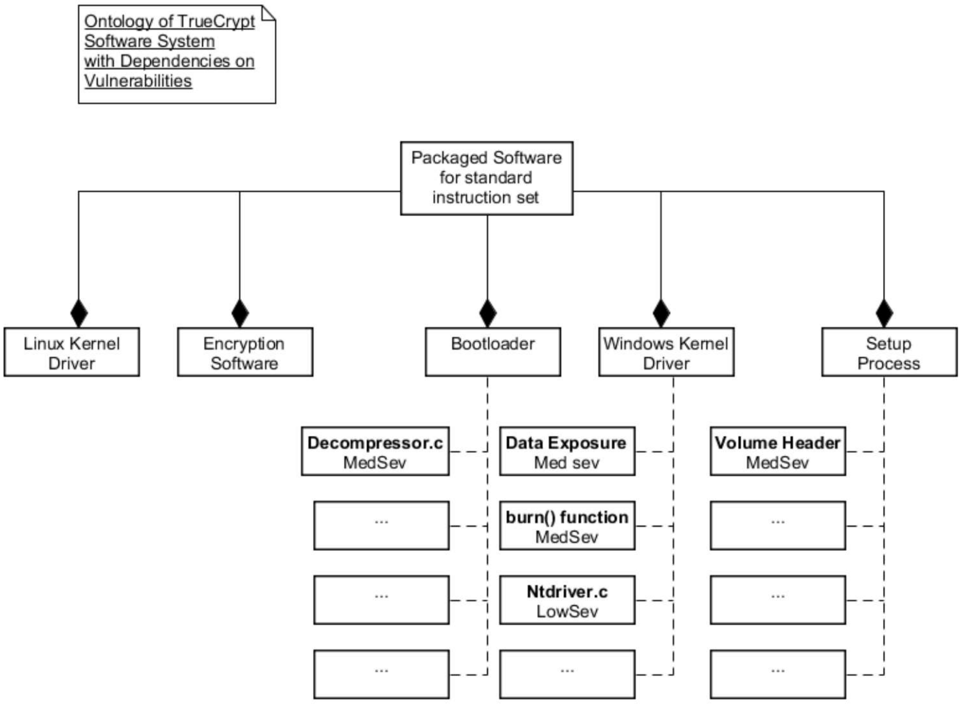
Perusing the provided references yielded the following thought-provoking questions to be contemplated and researched (Pillai, 2017):

1. What is the full functionality of the software?
2. What architectural components does the software comprise of?
3. How does the software achieve its goals?
4. Were all aspects mentioned above tested?
5. What testing techniques were used?
6. What evidence was produced?
7. What is the extent of the limitations created by the exposed vulnerabilities?

My initial consideration of the above questions would incline me to answer as per below for the discussion brief's questions (Junestam & Guigo, ,2014):

1. The audit does prove the assumption supplied by the TrueCrypt authors, but perhaps not to the degree which would encourage one not to use TrueCrypt at all, in any situation. For instance, only Windows aspects were investigated, not any related to Linux. Furthermore, the document seems to suggest that the risk analysis was performed on how the software encrypts an entire disk, or specific volumes on a disk, and not single files or folders within a partition. Additionally, not all vulnerabilities may cause a high impact for a user, or are easy to be exploited.
2. I would not recommend the software for encryption of complete disks, or entire volumes/partitions relying on a Windows OS, especially if the data is of a top secret nature. However, I may suggest the use of the software for encryption of individual folders or files on a Windows platform, or perhaps the complete use of the software for a Linux system.

It is difficult to map the system in its entirety due to a lack of knowledge of all its components. However, beneath is my attempt at an ontology representing the various elements within the problem domain, which aids in answering my initial questions (Arnaut et al., 2010).



References:

Arnaut, W., Oliveira, K., Lima, F. (2010) "OWL-SOA: A service oriented architecture ontology useful during development time and independent from implementation technology", *2010 Fourth International Conference on Research Challenges in Information Science (RCIS)*, 2010, pp. 523-532, doi: 10.1109/RCIS.2010.5507314.

Pillai, B. (2017) *Software Architecture with Python*. 1st Edition. Birmingham, UK: Packt Publishing.

Junestam, A., Guigo, N. (2014) *Open Crypto Audit Project TrueCrypt: Security Assessment*. iSEC Partners.

Reply

6 replies

1 Post by **Cathryn Peoples**

15 days ago

Re: Initial Post

Very relevant considerations in point 1, Michael, and I agree with these.

In relation to your ontology, good use of the hierarchy to capture the vulnerabilities associated with different aspects of the system.

Related to the way that this response has been written, it is not obvious which points are being supported using the related literature. For example, what is being referenced here?:

"Perusing the provided references yielded the following thought-provoking questions to be contemplated and researched (Pillai, 2017):"

This statement does not appear to need a reference. I also have the same comment for:

"My initial consideration of the above questions would incline me to answer as per below for the discussion brief’s questions (Junestam & Guigo, 2014):"

I would expect to see an argument such as, "Security is important" being supported using an academic literature source, a facutal statement, for which the reader is able to understand why the statement can be made with certainty.

Best wishes,

Cathryn

Reply

2

Reply to **Cathryn Peoples** from **Michael Botha** ↑

15 days ago

Re: Initial Post

Thank you for your response and comments - I will be sure to tighten up my argument in future.

Reply

3

Post by **Gennaro Coppola**

11 days ago

Peer response

Hello Michael,
were you aware of two critical vulnerabilities that have been found after the security assessment in 2014, specifically:
- **537 - Truecrypt 7 Derived Code/Windows: Incorrect Impersonation Token Handling EoP - project-zero (chromium.org)**
- **538 - Truecrypt 7 Derived Code/Windows: Drive Letter Symbolic Link Creation EoP - project-zero (chromium.org)**

do these findings if new change your evaluation given on the product?

Best regards,
Gennaro

Reply

4 Reply to Gennaro Coppola from Cathryn Peoples ↑

8 days ago

Re: Peer response

Hi Gennaro,
It would be great to supplement your post by explaining to Michael the reason(s) why you consider these critical vulnerabilities to be relevant within the context of his discussion. Try to help him along with your thought process as much as you can.

Best wishes,

Cathryn

Reply

5 Reply to Gennaro Coppola from Michael Botha ↑

5 days ago

Re: Peer response

Hi Gennaro,

Thank you for your response. No, I wasn't aware of further findings with regards to the TrueCrypt software. Considering whether my recommendations would now change; I did suggest that entire volumes should not be encrypted, but rather only files. Additionally, the sources you kindly provided seem to point to volume encryption vulnerabilities, and only within the Windows environment. Therefore, no, my original suggestions still stand. However, I have found it difficult to assess another source's findings pertaining to a system I have no real knowledge of. Especially, considering that there is low level code being quoted within a specific context, without the rest of the system's code available to suitably understand the implied context. Additionally, it is challenging to know what the TrueCrypt designers had thought when creating various code, and whether they perhaps planned to use another mechanism to secure the software outside of their immediate code. A full ontology of the system would definitely aid in having a better grasp of the systems components and functionality.

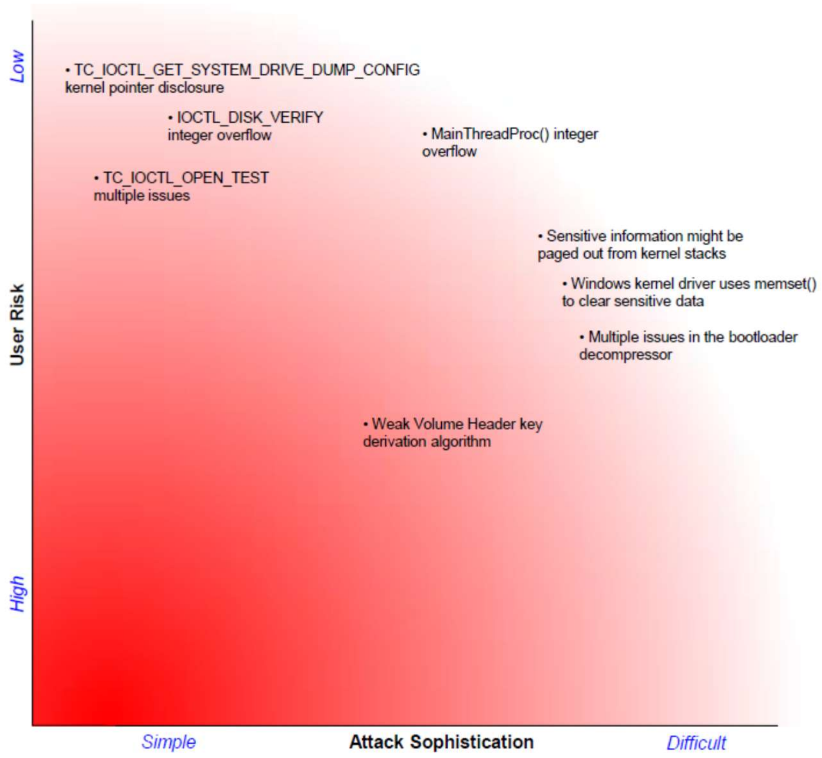
Reply

6 Post by Michael Botha

23 hours ago

Summary Post

In summary, it is difficult to analyse the findings holistically without some form of lucid ontological system representation supplied by the TrueCrypt software creators, or the auditors of the cited security assessment, where the full implications of systemic vulnerabilities are realised (Vega-Barbas et al., 2019). Furthermore, a reference to an auditing standard would increase the validity of the presented assessment, and inform a third party as to the level and style of analysis and testing performed on the software (CISQ, N.D). Additionally, quantitative risks would better inform a user regarding impacts, rather than the qualitative approach used (Volkan, 2021). However, if one were to take the audit at face value the supplied threat matrix chart is helpful in understanding the implications of each vulnerability found:



Threat Matrix Chart (Junestam & Guigo ,2014)

Considering the chart one can observe that the vulnerabilities which are easy to exploit have low risk (Junestam & Guigo, 2014). Furthermore, those vulnerabilities which have a medium severity to users are generally difficult to exploit (Junestam & Guigo, 2014). Therefore, it seems reasonable to suggest that one could use the system without an overall high risk. As a caveat one may advise a user to where possible, not use the TrueCrypt software to encrypt entire disks or volumes as the findings are specific to these use cases (Junestam & Guigo, 2014). However, the use of the software may be better for encrypting files and folders only.

References:

CISQ. (N.D) How to Measure and Quantify Software Risk. Available from: **https://www.it-cisq.org/use-cases/audit-and-certification.htm** [Accessed 07/02/2022].

E, Volkan. (2021) Qualitative vs. Quantitative Risk Assessment. Available from: **https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/qualitative-vs-quantitative-risk-assessment** [Accessed 07/02/2022].

Junestam, A., Guigo, N. (2014) *Open Crypto Audit Project TrueCrypt: Security Assessment*. iSEC Partners.

Vega-Barbas, M., Villagrá, V., Monje, F., Riesco, R, Larriva-Novo, X., Berrocal, J. (2019) Ontology-Based System for Dynamic Risk Management in Administrative Domains. *Applied Sciences* 9(21). DOI: https://doi.org/10.3390/app9214547.

Reply

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial Post