Unit 8
Collaborative Discussion 2
Cryptography case study: TrueCrypt

- **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): (https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf)
- and then answer the following questions:

- Question 1: 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?

- Question 2: Would you be prepared to recommend TrueCrypt to a friend as a secure storage environment? What caveats (if any) would you add?
- Question 3: 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?

- Released by anonymous developers in February 2004, TrueCrypt was vastly used and considered a secure data storage encryption that even FBI hackers failed to crack (Korea IT Times, 2011). However, in 2014, its anonymous developers stopped its updates and development (Zhang et al, 2019), claiming that "TrueCrypt is not secure" (Anon, TrueCrypt website). Despite this, the latest version of the software, considered accessible, user-friendly and secure, still attracts users (Zhang et al, 2019; Hoffman, 2017).
- Yet, many security vulnerability issues of the software were raised in Junestam and Guigo's report: lack of comments, use of insecure functions, inconsistent variable types among others. The report posits that TrueCrypt source code is confusing, making it difficult to understand, read, review and maintain it, thus rendering future bugs harder to find and correct. TrueCrypt is also vulnerable to brute-force and/or dictionary attacks. There might be leakage of sensitive information as sensitive information is not consolidated to one single location and is not locked into memory. Furthermore, it is possible for an attacker to modify the TrueCrypt code to record and save the user's password while the user enters it. Information leakage is another problem as attackers can create a low memory situation on the user's machine, forcing key information that should have been securely wiped to be paged out to the unencrypted system disk (Junestam & Guigo, 2014).
- The security assessment of the TrueCrypt source code for the bootloader and Windows kernel driver by Junestam & Guigo (2014) seems to confirm that TrueCrypt does not meet the expected standards for secure code. If the vulnerabilities are not tackled and the software is not continuously maintained and patched, TrueCrypt cannot be recommended. It would be more judicious to turn to other encryption software such as VeraCrypt (Hoffman, 2017).
- The tables below, created by Junestam & Guigo (2014), give a summary of the 11 vulnerability issues found in TrueCrypt and their level of severity:

Vulnerability Summary

Total High severity issues	Zero (0)
Total Medium severity issues	Four (4)
Total Low severity issues	Four (4)
Total vulnerabilities identified	Eleven (11) (incl. three (3) Informational)

See Section 3.1 for descriptions of these classifications.

Category Breakdown:

Access Controls	0
Auditing and Logging	0
Authentication	0
Configuration	0
Cryptography	1 ■
Data Exposure	4 ■■■■
Data Validation	3 ■■■
Denial of Service	2 ■■
Error Reporting	1 ■
Patching	0
Session Management	0
Timing	0

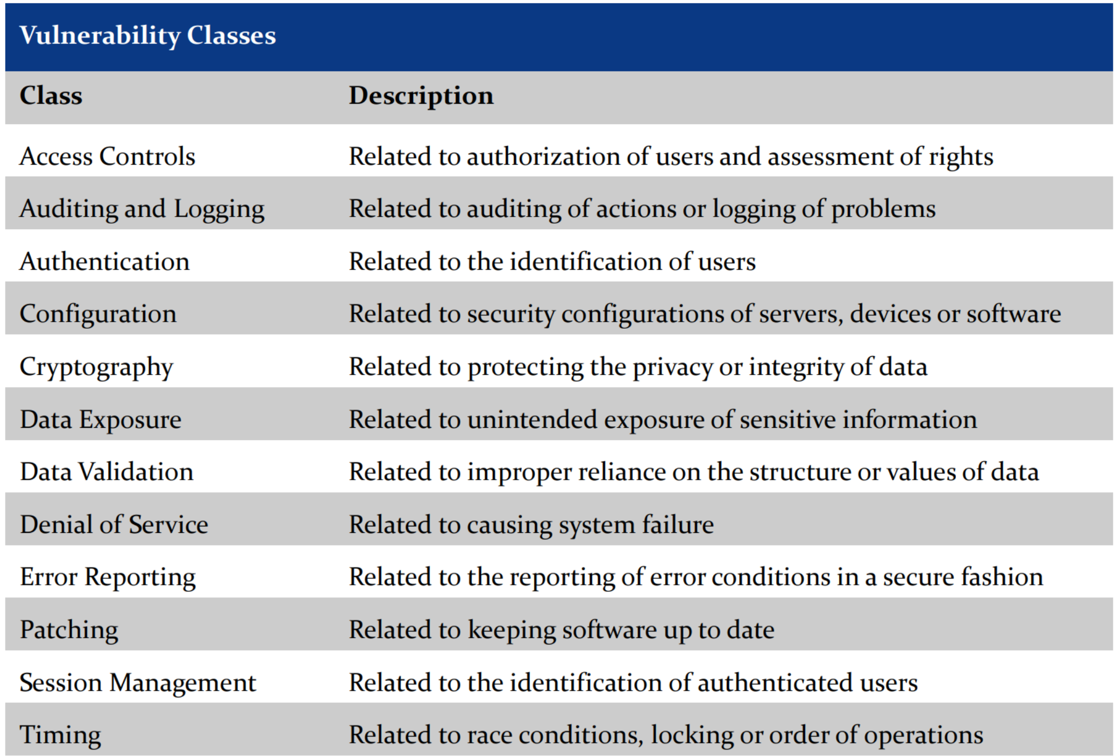
Severity Categories

Severity	Description
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or Defense in Depth
Undetermined	The extent of the risk was not determined during this engagement
Low	The risk is relatively small or is not a risk the customer has indicated is important
Medium	Individual user's information is at risk, exploitation would be bad for client's reputation, moderate financial impact, possible legal implications for client
High	Large numbers of users, very bad for client's reputation, or serious legal or financial implications

Vulnerability	Class	Severity
1. Weak Volume Header key derivation algorithm	Cryptography	Medium
2. Sensitive information might be paged out from kernel stacks	Data Exposure	Medium
3. Multiple issues in the bootloader decompressor	Data Validation	Medium
4. Windows kernel driver uses memset() to clear sensitive data	Data Exposure	Medium
5. TC_IOCTL_GET_SYSTEM_DRIVE_DUMP_CONFIG kernel pointer disclosure	Data Exposure	Low
6. IOCTL_DISK_VERIFY integer overflow	Data Validation	Low
7. TC_IOCTL_OPEN_TEST multiple issues	Data Exposure	Low
8. MainThreadProc() integer overflow	Denial of Service	Low
9. MountVolume() device check bypass	Data Validation	Informational
10. GetWipePassCount() / WipeBuffer() can cause BSOD	Denial of Service	Informational
11. EncryptDataUnits() lacks error handling	Error Reporting	Informational

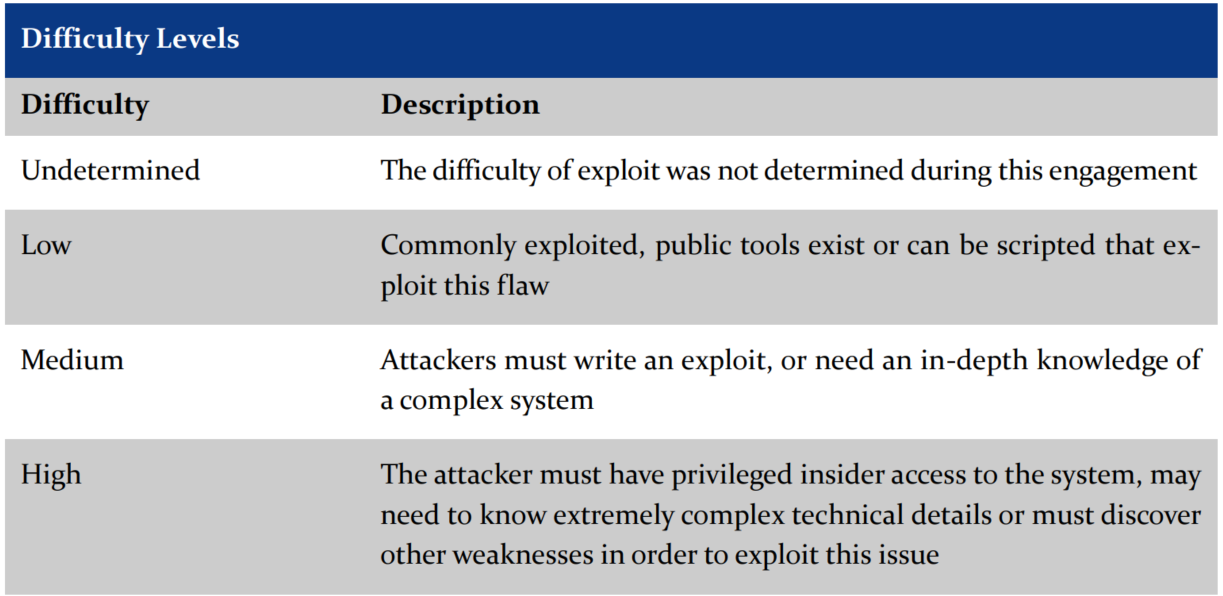
REFERNCES

- Anon, *TrueCrypt*, Available from: http://truecrypt.sourceforge.net/ [Accessed 11 January 2021]
- Hoffman, C (July 12, 2017) “Alternatives to the Now-Defunct TrueCrypt for your Encryption Needs ». Available from: https://www.howtogeek.com/203708/3-alternatives-to-the-now-defunct-truecrypt-for-your-encryption-needs/ [Accessed 11 January 2021]
- Junestam A. & Guigo, N. (2014) *Open Crypto Audit Project TrueCrypt Security Assessment*. iSEC Partners, Inc Available from: https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [Accessed 11 January 2021]
- Korea IT Times (February 28, 2011) FBI Hackers Fail to Crack TrueCrypt. Available from: http://www.koreaittimes.com/news/articleView.html?idxno=13278
- Zhang, L., Deng, X., & Tan, C. (2019). *An Extensive Analysis of TrueCrypt Encryption Forensics. Proceedings of the 3rd International Conference on Computer Science and Application Engineering – CSAE 2019.* Available from: doi:10.1145/3331453.3361328. [Accessed 11 January 2021]



Vulnerability Classes

Class	Description
Access Controls	Related to authorization of users and assessment of rights
Auditing and Logging	Related to auditing of actions or logging of problems
Authentication	Related to the identification of users
Configuration	Related to security configurations of servers, devices or software
Cryptography	Related to protecting the privacy or integrity of data
Data Exposure	Related to unintended exposure of sensitive information
Data Validation	Related to improper reliance on the structure or values of data
Denial of Service	Related to causing system failure
Error Reporting	Related to the reporting of error conditions in a secure fashion
Patching	Related to keeping software up to date
Session Management	Related to the identification of authenticated users
Timing	Related to race conditions, locking or order of operations

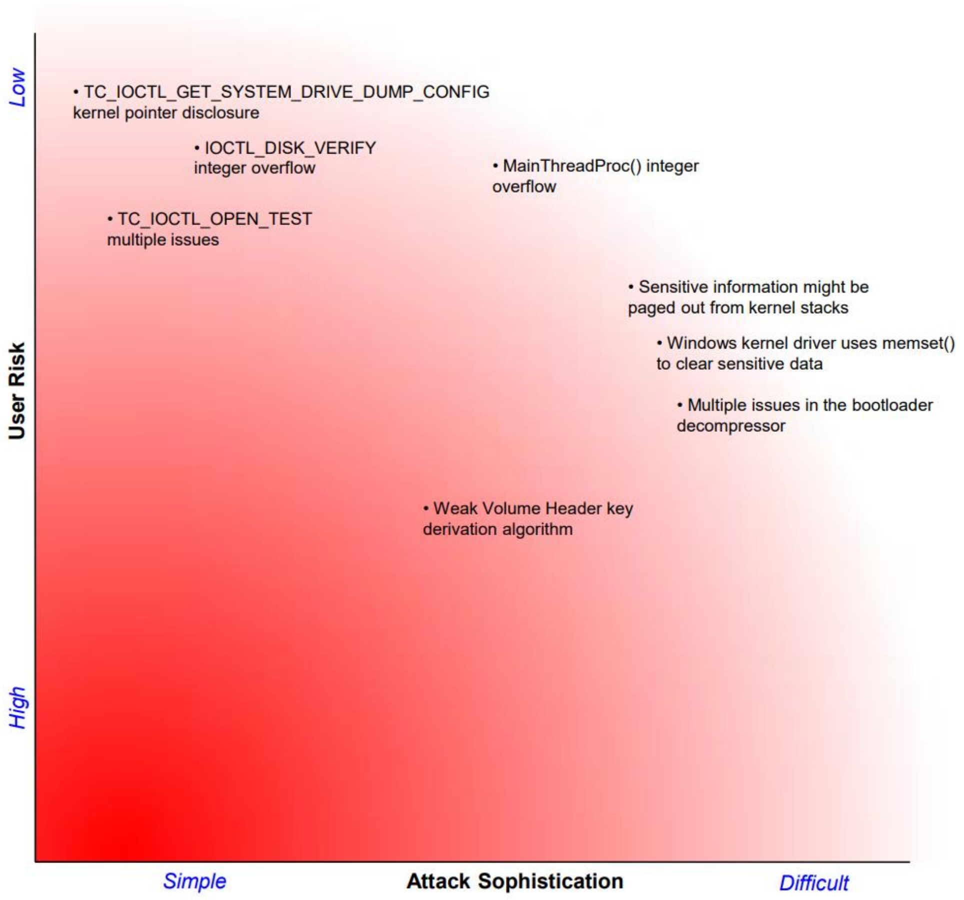


Difficulty Levels

Difficulty	Description
Undetermined	The difficulty of exploit was not determined during this engagement
Low	Commonly exploited, public tools exist or can be scripted that exploit this flaw
Medium	Attackers must write an exploit, or need an in-depth knowledge of a complex system
High	The attacker must have privileged insider access to the system, may need to know extremely complex technical details or must discover other weaknesses in order to exploit this issue

1.1 iSEC Risk Summary

The iSEC Partners Threat Matrix chart evaluates discovered vulnerabilities according to estimated user risk. The impact of the vulnerability increases towards the bottom of the chart. The sophistication required for an attacker to find and exploit the flaw decreases towards the left of the chart. The closer a vulnerability is to the chart origin, the greater the risk.


Low
• TC_IOCTL_GET_SYSTEM_DRIVE_DUMP_CONFIG kernel pointer disclosure
• IOCTL_DISK_VERIFY integer overflow
• MainThreadProc() integer overflow
• TC_IOCTL_OPEN_TEST multiple issues
• Sensitive information might be paged out from kernel stacks
• Windows kernel driver uses memset() to clear sensitive data
• Multiple issues in the bootloader decompressor
• Weak Volume Header key derivation algorithm
User Risk
High
Simple
Attack Sophistication
Difficult