Transparent Encryption Technique for Trusted Computing

Gushelmi1,2*, Abdullah Mohd Zin1

1Faculty of Computer Science & Technology, Universiti Kebangsaan Malaysia
2Faculty of Computer Science, Universitas Putra Indonesia YPTK

*gushelmi@upiyptk.ac.id

Abstract. Trusted computing is a technology that has been developed to make a computer safer and more trustworthy. The main purpose of trusted computing is to ensure that only authorized user will be able to use and access information stored inside the computer. Although the current trusted computing technology is capable of providing the level of trustworthiness required, it is still subjected to physical attack. In order to solve this problem, the TPM-UAM model has been proposed. However, in order to provide better protection, it is important that data inside the computer to be encrypted whenever it is not used and decrypted whenever it needs to be used. A number of encryption techniques are available such as RSA, AES, DES / 3DES, Twofish, Blowfish, IDEA, SEAL, RC4. However, time taken for encrypting and decrypting data by using these techniques is huge. This paper describes a research work that is currently undertaken in order to develop a new encryption mechanism that can provide very fast and transparent encryption and decryption services for trusted computers.

1. Introduction
Information risks and threats have been a studied issue since the early 1960s [1] and it has been main concern for all IT users. This issue has suggest information security experts to proposed several solutions to protect information against attack [2]. One of the ideas that have been proposed is trusted computing. This idea is to response and protect user data while the user a computer connected to a network [3].

Although the current trusted computing technology is capable of providing the level of trustworthiness required, it is still subjected to physical attack. In order to solve this problem, the TPM-UAM model has been proposed. This paper describes a technique to improve TPM-UAM model in order to ensure further security of a trusted computer.

2. Trusted computing
Trusted computing is defined as “an IT environment or an area” within it, in which a user, IT administrator or business partner can have “trust”. Trusted computing group (TCG) defines trust as “an expectation that a device will behave in a particular manner for a specific purpose”.

"Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI."
The concept of trusted computing is not new. The specification has been released in 2001. These specifications determine the core components of trusted computing, called the Trusted Platform Module (TPM).

TPM is a small chip which store cryptographic key. TPM not only a hardware but also a software. This TPM connected to a controller in motherboard PC. TPM provides three main roots of trust [4]:

- The root of Trust for Measurement (RTM) - is responsible for taking platform integrity measurements
- The root of Trust for Storage (RTS) - securely stores different integrity measurements and
- Root of Trust for Reporting (RTR) n- responsible for reliably reporting values stored in the RTS.

TPM is supports for cryptographic key generation, data sealing and binding [5]. The storage protected using TPM and only accessible with the TPM and the storage is protected from physical treats. The storage included in the TPM is Platform Configuration Registers (PCRs) and volatile and nonvolatile storage spaces [6].

Although some methods and functions provided TPM to control the user’s physical presence, it can still prone to physical attacks. One of these attacks is known as the Evil Maid attack [7]. This type of attack can happen if an attacker could load software using the OS before the TPM started to work. The software will exist with the boot loader and collect keys and security information during the next boot. TPM will save and send the information to the attacker via the network.

3. TPM-UAM Model

TPM-UAM model was developed based on three consider ations. By using virtualization concept, the first consideration develop a second platform on the same computer. The second assure the user’s identity and authority using biometric authentication method, and the third is to ensure user privacy. In order to achieve the three considerations above, the TPM-UAM model employs three techniques: (1) Use of Virtualization; (2) Use of biometrics and (3) Use of Privacy Protection Mechanism. Several virtual machine are split from a single physical machine. These process called virtualization. By using shared resources hardware from the physical machine, every virtual machine will run in different operating systems [8]. In TPM-UAM, the concept of virtualization allows a user to have two platforms: a secured platform and a normal platform. The use of virtualization is shown in Figure 1.

![Figure 1. Use of Virtualization in TPM-UAM.](image-url)
Since the secured platform is slow, a user can still use the normal platform like internet browsing for activities that do not require a high level of security.

ID/PIN methods are less reliable and secure method than Biometrics[9]. Thus, to scale up the security level, the model should combine user authentication using biometrics technique. This combination is to identity instead of the normal ID/PIN method. The Face Detection and Fingerprints are most popular biometric techniques.

A user privacy means precaution peeking from any third party at the monitor and view information clasification when using the PC, thus user needs to observe people who come in the background and view the monitor and then to take handle this problem.

4. Encryption and Decryption

Encryption is the process of translating data known as plaintext into a representation that appears to be random and meaningless, known as ciphertext. Decryption is the process of converting ciphertext back to plaintext. The purpose of encryption is to ensure that data are protected. A number of encryption techniques are available such as RSA, AES, DES / 3DES, Twofish, Blowfish, IDEA, SEAL, RC4.

5. Transparent Encryption

The main aim of transparent encryption is to hide the complexities of encrypting and decrypting of data. Transparent encryption includes four main operations:

- Transparent deployment
- Transparent encryption operation
- Transparent authentication mechanism
- Transparent key management

A number of transparent encryption systems have been developed. Some of them are shown in Table 1 below.

| Name     | Source            | Description                                                                                   |
|----------|-------------------|-----------------------------------------------------------------------------------------------|
| CFS      | (Blaze, 2004)[10]| Implemented in user space as an NFS server.                                                   |
|          |                   | The confidential files should be encrypted in local or remote file system by the user.       |
|          |                   | The mount point is a special directory that required authenticated user to attach the confidential files by using CFS daemon. |
|          |                   | To encrypt files, a DES encryption algorithm in hybrid ECB and OFS operation modes needed by CFS. |
| EncFS    | (Gough,2008) [11]| The EncFs uses a FUSE library to provide an interface of file system on the userspace.       |
|          |                   | The userspace daemon is improved to assign transparent encryption and decryption for all files.|
|          |                   | The files are encrypted using a volume key.                                                   |
|          |                   | EncFS uses standard OpenSSL cryptographic libraries and supports AES and Blowfish block ciphers.|
| CryptoFS | (Hohmann,2006)[12]| Use Linux Userland File System (LUFS) and the File System in User Space (FUSE).               |
|          |                   | The AES, DES, Blowfish, Twofish, Arcfour, and CAST5 using the CFB mode can be used to assist in several |
encryption algorithms.

| ImgFS          | (Khassan et al, 2014) [13]                  | The main goal of restricting the protection mainly to the spatial images. Makes the system much more convenient to the user. Efficient security is ensured by using strong encryption algorithms and authentication methods. |

6. Discussion

TPM-UAM model has provided a good mechanism to protect the trusted computer from physical attack. In using a trusted computer, a user may have to leave the machine for a short while that may provide an opportunity for an attacker to obtain sensitive data. In order to provide better protection, it is important that data inside the computer to be encrypted whenever it is not used and decrypted whenever it needs to be used.

A number of encryption techniques are available. However, time taken for encrypting and decrypting data by using these techniques is huge. In order to solve this problem, research needs to be carried out to find very fast and transparent encryption and decryption services for trusted computers.

7. Conclusion

This paper describes a proposed technique to improve the security of trusted computing. It is based on TPM-UAM model that was proposed in order to protect the trusted computer from physical attack.

References

[1] Mackenzie D and Pottinger G 1997 Mathematics, technology, and trust: Formal verification, computer security, and the U.S. Military IEEE Ann. Hist. Comput. 19 41–59
[2] Wang P A 2010 Information Security Knowledge and Behavior: An Adapted Model of Technology Acceptance V2-365 364–7
[3] Pearson S 2005 Trusted Computing : Strengths , Weaknesses and Further 305–6
[4] Sun H, He R, Zhang Y, Wang R, Ip W H and Yung K L 2018 eTPM: A trusted cloud platform enclave TPM scheme based on intel SGX technology Sensors (Switzerland) 18 1–23
[5] Sadeghi A, Selhorst M, St C, Wachsmann C, Winandy M and Horst G 2006 TCG Inside ? - A Note on TPM Specification Compliance
[6] Aaraj N, Raghunathan A, Ravi S and Jha N K 2007 Energy and Execution Time Analysis of a Software-based Trusted Platform Module *
[7] Alshar’e M I, Sulaiman R, Mukhtar M R and Zin A M 2014 A user protection model for the trusted computing environment J. Comput. Sci. 10 1692–702
[8] vmware 2007 A Performance Comparison of Hypervisors A Perform. Comp. Hypervisors 22
[9] Khushk K P and Iqbal A A 2005 An overview of leading Biometrics Technologies used for human identity 2005 Student Conf. Eng. Sci. Technol. SCONEST
[10] Blaze M 2004 A cryptographic file system for UNIX 9–16
[11] Gaugh V 2008 EncFS Encrypted File System(online)
[12] Hohmann C 2006 CryptoFS (online)
[13] A Khassan O, Zin A M and Sundarrajan A E 2014 Performance study of selective encryption in comparison to full encryption for still visual images J. Zhejiang Univ. Sci. C 15 435–44