Journal of Computer Science 10 (9): 1692-1702, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1692.1702 Published Online 10 (9) 2014 (http://www.thescipub.com/jcs.toc)

A USER PROTECTION MODEL FOR THE TRUSTED COMPUTING ENVIRONMENT

Marwan Ibrahim Alshar'e, Rossilawati Sulaiman, Mohd Rosmadi Mukhtar and Abdullah Mohd Zin

Research Center for Software Technology and Management (Softam),
Faculty of Information Science and Technology, National University of Malaysia, Malaysia

Received 2013-04-12; Revised 2013-07-16; Accepted 2014-04-15

ABSTRACT

Information security presents a huge challenge for both individuals and organizations. The Trusted Computing Group (TCG) has introduced the Trusted Platform Module (TPM) as a solution to end-users to ensure their privacy and confidentiality. TPM has the role of being the root of trust for systems and users by providing protected storage that is accessible only within TPM and thus, protects computers against unwanted access. TPM is designed to prevent software attacks with minimal consideration being given toward physical attacks. Therefore, TPM focus on PIN password identification to control the physical presence of a user. The PIN Password method is not the ideal user verification method. Evil Maid is one of the attacking methods where a piece of code can be loaded and hidden in the boot loader before loading TPM. The code will then collects confidential information at the next boot and store it or send it to attackers via the network. In order to solve this problem, a number of solutions have been proposed. However, most of these solutions does not provide sufficient level of protection to TPM. In this study we introduce the TPM User Authentication Model (TPM-UAM) that could assist in protecting TPM against physical attack and thus increase the security of the computer system. The proposed model has been evaluated through a focus group discussion consisting of a number of experts. The expert panel has confirmed that the proposed model is sufficient to provide expected level of protection to the TPM and to assist in preventing physical attack against TPM.

Keywords: TPM, Biometrics, Authentication, Security, Privacy, Virtualization, Xen

1. INTRODUCTION

Computer security has been a research issue of computer science since the early 1960's (MacKenzie and Pottinger, 1997). Information risks and threats have become a critical issue for both IT users and professionals. Information security attacks are considered a major concern for all IT users. The number of weaknesses, types of possible and unwanted risks has motivated the information industry and experts to develop various solutions to protect information against attack (Ping An, 2010). In the environment of distributed systems, security issues should be given more attention in order to have more secure systems, where the threats comes from different sources including the local workplace or network, especially since the broad use of the Internet and the increased number of users. IT users now hope for a more secure and efficient platform, which was promised by the invention of the trusted platform (Shen *et al*., 2010).

The idea of trusted computing was introduced in order to respond to the users' concern on whether their data is protected while they are connected to a network and to make them confident with three major aspects: To protect their data, to ensure their platform is trustworthy and to allow them to decide if it is reasonable for them to trust other networks (Pearson, 2005).

Corresponding Author: Marwan Ibrahim Alshar'e, Research Center for Software Technology and Management (Softam), Faculty of Information Science and Technology, National University of Malaysia, Malaysia

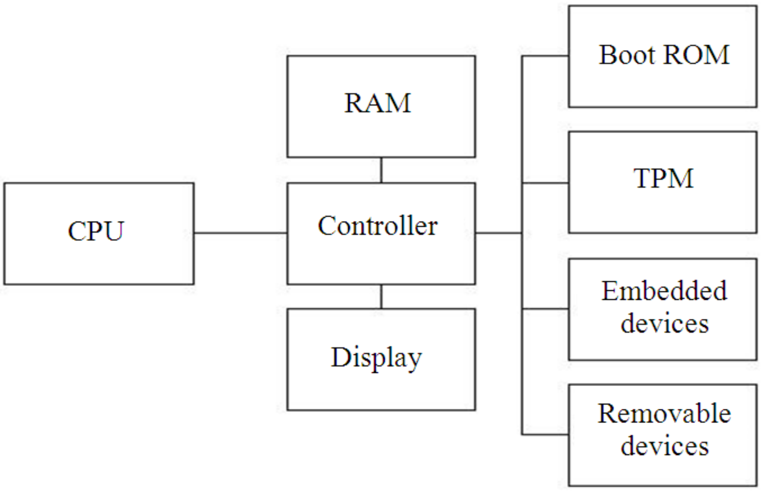

Fig. 1. Reference PC Platform Containing a TCG Trusted Platform Module (TPM), Source (TCG, 2010)

TPM is a platform that includes additional hardware and software to increase the security level of the systems hosted on the platform. The current implementation of TPM is a small chip placed on the main board, which can store cryptographic keys and other security critical information. In addition, TPM provides cryptographic functions like asymmetric encryption and signature schemes, **Fig. 1** shows a Reference PC Platform containing a TCG Trusted Platform Module (TPM). As shown in **Fig. 1**, TPM module is connected to the motherboard controller of the PC.

TPM provides three main roots of trust, which are, Root of Trust for Measurement (RTM), Root of Trust for Storage (RTS) and Root of Trust for Reporting (RTR). RTM is responsible for taking platform integrity measurements, RTS securely stores different integrity measurements and RTR is responsible for reliably reporting values stored in the RTS. At the same time TPM supports other functions such as cryptographic key generation, data sealing and binding (Sadeghi *et al*., 2006).

TPM contains protected storage which is accessible only within TPM and it is protected against physical attack. The storage included in the TPM are, Platform Configuration Registers (PCRs) and volatile and non-volatile storage spaces (Aaraj *et al*., 2007).

Although TPM provides some methods and functions to control the physical presence of the user, there are still issues related to TPM. For instance, getting access to TPM and calling certain functions within TPM will require TPM to request the user to provide some keys and commands to prove his identity. In the case of rejection or cancellation, the TPM is forced to free the registers from the loaded TPM functions and shutdown the PC. However a serious problem could occur if a user could load software using the OS before the TPM started to work. The software could stay within the boot loader and from there it can collect keys and security information during the next boot and store it somewhere or even send the information via the network to the attacker. This situation is confirmed in the case of Evil Maid attack (Schneier, 2009).

In order to solve the problem, this study proposes a model for verifying and authenticating users before they are able to use the TPM. The use of this approach will increase the security level and the protection by ensuring the identity of the users before loading the TPM functions to the registers.

2. RELATED WORK AND BACKGROUND OF THE STUDY

According to Peng and Han (2006), trusted computing based on TPM has been classified based on four main perspectives of trust, which are: Trust of user, trust in platform, trust of application and trust between platforms.

A TPM user depends on the TPM to confront intrusion attempts of an identity theft. This is performed by providing users with the ability to create credential keys, which are encrypted and stored inside the chip. TPM prevents any software attempt to reach the TPM and acquire the stored information (Klenk *et al*., 2009).

According to George (2004) TCG did not take into account security from the users’ perspective, instead, the model is directed and focused on the platform. Peng and Han (2006) reported that, based on the Trusted Computing architecture, trust in the user can be found listed and discussed, but it does not really undertake security from the users’ point of view since the trusted computing model focused on the platform security and only fundamental concentration was given to user identification and authentication mechanisms.

In addition, TPM (2007) mentioned that TCG has not concentrated on the platform users and instead, focused on the platform’s owner and the operator, where these were the only two identities that TCG has confirmed via TPM as the users with administrative rights over TPM. Thus, TCG does not define user authentication but defines ownership authentication instead. This means TPM “authenticates” these users as the owner and they are authorised to use the TPM. Mechanisms for authentication and identification are still fairly rudimentary.

Klenk *et al*. (2009) reported that TPM authentication alone is not a significant solution to confirm and verify users’ identities. Furthermore, the general implementation of TPM administrative tools to authenticate users is still based on the normal password authentication methods. Hence, TPM is still exposed to all possible threats and weaknesses of password-based authentication, such as easy to guess, subject to dictionary attack, easy to snoop or lose and easy to share with others.

There are a number of researches and studies that have been conducted to overcome TPM’s weakness against physical attack. The main idea was centred on user authentication where the main risk starts, when an (authorized or unauthorised) user can request access to the platform. Some of the methods are described here.

2.1. Smart Card-Based User Authentication

According to George (2004), the user's ability to demonstrate knowledge of confidential information between the owner and the platform is proof of ownership of the platform. If the user has proven his knowledge it indicates and proves his identity. George (2004) suggested a solution using Smart Card-Based User Authentication to authenticate attempts to access to the secure platform by users. This solution suggests recording user authentication data on a smart card, where the user can introduce this card to request authentication to access a certain platform (this card protects users and the platform from a number of threats, especially dictionary attack).

The solution then suggested using a PIN to obtain access to specific information once the user was already authorized on that platform in order to reach higher level of security. This model caters for issues related to the process of user credential storage on the platform, which leads to storage spaces issues and confidential information theft or loss.

The assumption of the Smart Card-Based User Authentication as stated by George (2004), is to try to maximise the benefits and advantages of using smart card techniques combined with TPM to reach two-factor authentication; tamper-resistance storage to protect authentication data and personal information; isolation of security-critical computations; portability of credentials and other private information between computers.

2.2. Trust of User using U-Key on Trusted Platform

Peng and Han (2006) introduced the Trust of User using U-Key on Trusted Platform to solve the issue of user authentication on top of secure platforms. The U-Key is a USB token, which contains a built-in smart card that provides secure storage and processing of sensitive data. This means users’ information, credentials, digital certificate and private keys are stored securely at the U-Key only. Using this method, if the user needs to get access, read or decrypt any document, all the required cryptographic functions will be performed by the microprocessor on the smart card. Since all information related to the keys and cryptographic functions are stored in the U-Key, this will assure that no third party will be listening to the confidential information.

However, this mechanism still requires an authentication process for users to access the platform. The authors suggested using a normal password authentication to confirm authenticity as we can see at BIOS where only a user with the correct password can guarantee access to the PC; this does not satisfy the required level of security.

Thus, they suggested a dual mode of authentication; one happens at the platform level via the TPM chip with the related password to authorise users and two, the U-Key for user authentication. Therefore, only an authorised user with the correct U-Key and PIN can boot the system.

2.3. Preventing Identity Theft with Electronic Identity Cards and the Trusted Platform Module

Klenk *et al*. (2009) reported that TPM authentication alone is not a significant solution to achieve verified identities. They suggested a new system called TPMIdent to attain better confidence using TPM based authentication with the help of eIDs (electronic identity card) to resist identity theft. Inside eIDs is an identify key that is a user specific, PIN protected and non-migratable key. The cryptographic operations for the authentication at the user’s side happen inside the TPM chip. The author suggests that all authentications should not occur without TPM access since the identity key cannot be transferred to another platform. This will guarantee that identity theft can be avoided.

The OpenID provider gets the public key certificate using a digital signature which works by combining public key and identity to prove user identity and then the authenticated certificate is sent to the Relaying Party. After the identity has been authenticated successfully, the OpenID Provider proceeds with the OpenID Protocol, signs the authentication result and sends it via browser redirect to the Relying Party. Note that this protocol works even without Verified Identities. It enables Unverified Identities and Pseudonyms, because it guarantees that the same user/device combination always authenticates with this protocol. Device independent authentication with verified identities requires a secure mechanism to gain trust that the key belongs to a specific identity and cannot be compromised.

The next step is to establish trust to ensure the execution environment is secure and cannot be modified. This is done through assured integrity measurement for security, which implies that the host runs only unmodified and authorised codes, TPM provides a perfect solution and answer for this case through an operation called remote attestation

2.4. Unicorn: Two-Factor Attestation for Data Security

Mannan *et al*. (2011) tried to benefit from the TPM software attack resistance without relying on the TPM for authentication attestation, where TPM can assure the software integrity throughout the root of trust based on the hardware, which is more difficult for the attacker to deal with than the root of trust of a given software or OS and on the other hand to use security tokens which have the capability to implement one time user passwords and are able to respond to cryptographic functions. Thus, the password has been protected against phishing using the security tokens, but passwords are still vulnerable to malware during the active session, so TPM and its root of trust will be responsible for protecting the passwords and other credentials from malware attack so user data are protected by attestation factors.

As a result, the author introduces the use of a new technique they call UNICORN, where they combine security tokens and trusted computing. A Personal Security Device (PSD) which is like a security token keeps user authentication and credentials then this information will be verified from the user’s computer by the TPM. PSD is implemented by an Android smart phone and Intel TXT with TPM as the trusted computing implementation. Unicorn example Applications (uApp) is used to secure access to remote data services and encrypted local data. When a user tries to access secure data, the UNICORN will start to work by requesting a boot order from the TPM at the user PC. TPM will be used to boot and measure a uApp. As a result the TPM will generate attestation and the uApp can access the secure information only when the PSD combines the attestation with the stored authentication credentials in the PSD.

The security token and the PSD are subject to various threats and weaknesses that can affect the desired protection level of the user authentication data and credentials.

2.5. Critical Study of Related Work

This section discusses the disadvantages associated with the four mechanisms mentioned at the previous section. Smart Card authentication has numerous advantages to be used as effective solutions for authentication. On the other hand, smart card authentication suffers some serious issues which have to be considered concerning the desired level of security for systems.

Some assumptions impair smart card authentication, Bezakova *et al*. (2000) discussed a number of the weaknesses associated with smart card authentication such as:

- Data and information stored in a smart card is prone to erasure or modification by an unusual voltage supply
- Heating the controller to high temperature or applying UV light to the card will cause removal of the security lock
- Physical attack can be harmful when the card is cut and the processor removed, then the chip can be reversed engineered

- Using certain methods such as Differential Power Analysis (DPA) which is a statistical attack on a cryptographic algorithm often capable of extracting an encryption key from a smart card, as well as Simple Power Analysis (SPA), the direct analysis of the recorded power data to determine actions and data

Clarke (2012) also reported some issues regarding smart cards such as:

- They can easily be lost, since smart cards are small and lightweight make them prone to loss
- Possible Risk of Identify Theft, a smart card is meant to store large amount of information, this makes it subject to identity theft especially as some printers are capable of printing a smart card's contents
- Security, smart cards are not secure as users think and this gives a false sense of security and some users might not protect their card and the information it holds properly

From the above mentioned issues and others, smart card authentication still cannot be considered as the most reliable technique to secure users' credentials and authentication data and then to provide a secure authentication process. On the execution side, TPM handles the execution and the encryption of the authorisation data, but in such cases TPM deals with provided authentication data regardless of the real identity of the user.

As a result unauthorised users can still gain access to an account they do not own or have access to. Feld and Pohlmann (2011) report that despite the high level of secure authentication that has been bought using OpenID and eID, a number of flaws and weaknesses have been recorded associated with these authentication techniques.

According to Feld and Pohlmann (2011) phishing and profiling are major threats related to OpenID and eID techniques, where phishing is possible by a Relying Party (RP), for example a malicious RP does not forward the user to the "correct" OpenID Provider (OP), but to an impersonating OP which is also under the control of the attacker. The OP can be copied using proxying which means that the user enters his credentials into the fake OP and then the phishing happens.

Another major threat addressed by Feld and Pohlmann (2011) is profiling, the authors suggest that creating the user accounts using OpenID is a critical issue since an OP can monitor the users' activities on the internet which is something that cannot be avoided where an RP will communicate OP to complete user's authentication visiting different locations on the internet. On the other hand, using this technique always requires direct access to the internet. The user needs internet access every time he/she needs to use a PC with TPM to authorise himself, meaning a dropdown of the network leaves the user without authentication and thus cannot get access to the TPM platform.

Using Security Tokens (Hardware Token) to find an effective solution to manage private and secure data is reasonable and can have a high impact doing what it was designed for, but a number of drawbacks associated with these tokens could prevent it from being the perfect solution and there is still a need to find a more reasonable solution to better serve users more effectively.

Khan and Zahid (2010) reports that tokens are vulnerable to being stolen, forgotten or shared with unauthorised users. In this case, using a mobile device can suffer some of those issues if stolen or lost, which exposes security data to the risk of being attacked. From the literature review we found that the tools have managed to achieve their objectives, however these mechanisms have to include third party devices to participate in the authentication process, which are vulnerable to various issues such as theft, loss or damage. In addition, extra budget will be needed to equip PC's with the required devices.

Therefore we propose a model that makes use of the virtualisation concept to perform the authentication process on different platform on the same machine, which will keep TPM secure and provide the best use of available resources without having to use additional equipment or being vulnerable to the above mentioned risks, **Fig. 2** shows the concept of the virtualization.

3. PROPOSED MODEL

As explained in the problem statement, allowing the user to interact directly with the TPM on the first interaction with the PC could lead to serious damage. This model takes the first interaction and the user authorisation process into a new stage and another level.

3.1. Development Considerations

There are three considerations when developing the model:

- To provide a second platform on the same PC by using means of virtualisation concept
- To use a biometric authentication method to assure the user's identity and authority
- To ensure user privacy

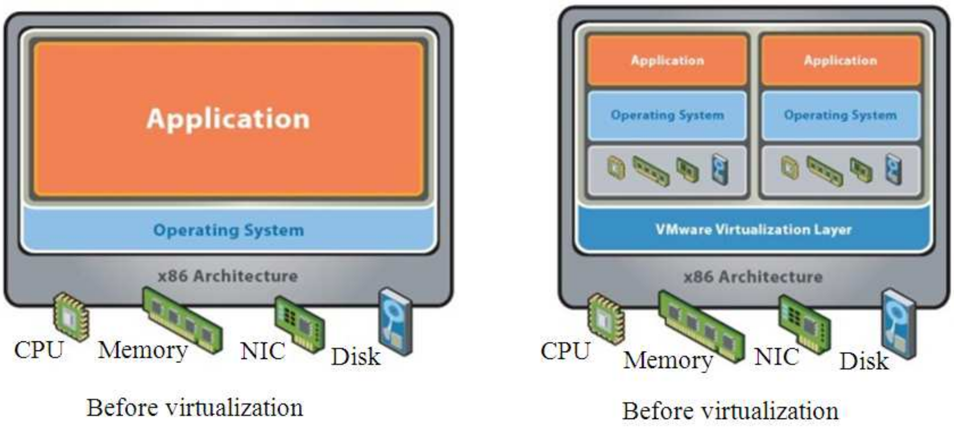

Fig. 2. Hardware resources before and after virtualisation (VMware, 2006)

3.1.1. Use of Virtualization

Virtualization is a process where a single physical machine can be split into a number of virtual machines. As shown in **Fig. 2**, each of this virtual machine may run different operating systems using shared hardware resources provided by the physical machine. Hypervisor that is a thin layer between the hardware resources and the virtual machines, guarantee fair distribution of the resources between the virtual machines (Muditha and Chamath, 2011). Hypervisor also guarantee that there is no interference between the resources after the creation of the logical components and each virtual machine runs independently (Hegan, 2008).

The concept of virtualization will be used as follows:

- Launch a first interaction platform which the user should interact with before getting access to the TPM. Here, we keep the TPM closed even there is a user who starts to interact with the PC
- All authorization and identity confirmation processes should be completed on this platform, because it should work as a separate platform and ensure there is no interaction with the TPM yet
- A case of success authentication only will allow the user to start and deal with the TPM which is under the control of the second platform
- Since TPM is considered a slow response platform due to the number of encryption/decryption processes running there, the second platform still can be used as fast platform that the user can use to practise normal processes which do not need a high level of protection, such as surfing the internet

3.1.2. Use of Biometric

Biometrics are a far more reliable and secure method than ID/PIN methods (Khushk and Iqbal, 2005). Thus, in order to increase the security level, the model should incorporate the use of biometrics technique to authenticate user identity instead of the normal ID/PIN method. Two of the most popular biometric techniques are Face Detection and Fingerprints.

3.1.3. To Ensure User Privacy

When using the PC, a user privacy means of protection should be available to prevent any third party from peeking at the monitor and view classified information, thus we need to monitor people who might appear in the background and view what is displayed on the monitor and then to take action to handle this problem.

3.2. State Machine Representation of the Model

Figure 3 shows the model in the state machine representation. The description of **Fig. 3** is as follows:

- State 0: User interacts with the machine to switch it from the OFF to the ON state
- State One is to verify the number of users in front of the PC (one user is allowed to interact with the system per account)
- In the case of multiple objects, the system goes back to the OFF State
- In the case of a single user, the system goes to State Two to verify user identity via Face Detection
- State Two will allow three attempts to detect the user's face

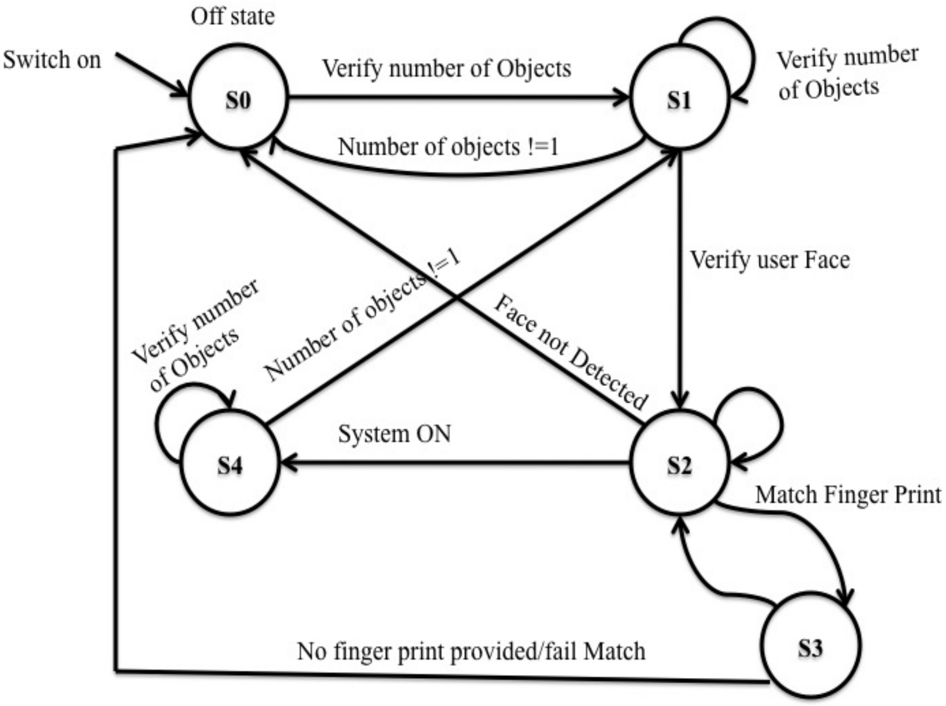

Fig. 3. TPM-UAM model

State Three: In case of failure to detect the face, the user has to provide a fingerprint scan to ensure he/she is the authorized user before the system allows another attempt at face detection due to false positive issues related to face recognition processes. A case of false positive is a common issue with face recognition systems, the issue of false positive means that the user is an authorised person but the system cannot detect him because of several reasons, such as shadows and lights, age, using or not using glasses, growing beards or hair changes. etc., thus, this model allows another chance for the user before moving to the OFF state. In addition, to ensure the safety of the system, the user has to go through the fingerprint again to prove his identity, only then does he have the chance for another attempt to scan his face again.

State Four allows the system to run and gives the user authority to use the system. State Four keeps on verifying the number of objects to ensure user privacy.

4. EVALUATION OF THE MODEL

The TPM-UAM model was evaluated through the focus group discussion. The suggested number of participants is from six to eight (Krueger and Casey, 2000). In our case, we invited seven participants who are experts in TPM. The discussion sessions lasted about three hours. There were five questions raised during the discussion:

- What is the opinion of the panel about the security level provided by the Trusted Platform Module (TPM)
- What are the weaknesses of the TPM
- Does the panel agree to the analysis of the TPM's weaknesses
- Does the proposed model solve the introduced problems
- Are there any aspects of the model which need improvement

The results from the discussion can be summarised as follows:

4.1. Security Level Provided by TPM

For Question 1, Participants confirmed that a large number of computers and personal devices now come equipped with TPM and benefit of the security level provided by TPM. The participants discussed a number of facts about TPM and its use including the following. TPM is a chip installed on the motherboard, which makes it work as hardware and software protection support for the machines that contain it. Computers running TPM are considered to have a trusted state, where TPM is used to encrypt encryption keys and store them within the TPM.

The TPM provides in place protection to machines containing it, where all information can be protected by encryption then store their encryption keys within the TPM, which make it impossible for any third party to benefit from this information without having the correct keys and proper access to the TPM. Even if an attacker can get the hard drive and run it on another machine, the attacker cannot gain access to the information as the keys are encrypted by the TPM and can only be opened by the TPM.

Participants also mentioned the new and latest trends for TPMs and their implementation within cloud computing, where, they say, the TPM work well and serve in this field to provide better security levels to authenticate different machines and software and can achieve the ultimate benefit of using the TPM over networks.

4.2. The Weakness of TPMs

For Question 2, this question asked the participants to share their opinions and experiences on issues and problems associated with the TPM, the participants declared that TPMs still suffer a number of issues and enhancements should be considered to improve the TPM’s performance. Participants mentioned a number of weaknesses mainly, *TPM still supports a single user per PC*, where each TPM affirms one administrator account called “owner,” and does not support creation of more than one account per TPM chip and they considered multiple accounts would be more advisable.

Participants also mentioned that TPM uses asymmetric cryptography for the encryption and decryption processes and they pointed out that the use of asymmetric cryptography for the encryption can cause low speed performance for platforms which have TPM, thus that might require more cores of CPU to reach the desired performance levels. The participants then recommended that symmetric cryptographic could be used to replace the asymmetric cryptographic within the TPM.

Participants also mentioned the TPM stands between the Hard Drive and OS, where any request to read encrypted information requires the TPM to confirm user identity and request verification codes (PIN Password), then the TPM will release the keys to decrypt the required information. Here, the man in the middle can listen to information transferred between the TPM and other Hardware through the OS, collect this information about keys and use it later to reach confidential information.

4.3. The Analysis of the TPM’s Weaknesses

For question 3, the weaknesses of TPMs were presented to the participants. In conclusion, participants agreed that there are weaknesses for TPMs, which are mainly:

Slow performance due to the use of asymmetric cryptographic by the TPM compared to a native OS without a TPM. Participants did mention that the TPM still uses asymmetric cryptography mechanisms to encrypt the encryption keys and they mentioned asymmetric is relatively slow compared to symmetric cryptography. On the other hand, the participants agreed that slow performance can affect the user’s acceptance to adopt and use TPM, which could ruin the chance to benefit from the high security levels provided by TPM.

Another weakness explained was the weak users’ authentication method implemented within TPM. Participants confirmed that TPM still works based on PIN password authentication and, despite of the advantage of using and implementing PIN password authentication as a dynamic and flexible authentication technique, they confirmed the *weakness of the PIN Password to protect TPM* and recommended the introduction of more reliable authentication methods. Participants agreed that, TPM is exposed to direct risk when collecting user passwords for authentication, where special software can be used to collect private keys, when the system is in the ON state and user information is running on the RAM. This is similar to the Evil Maid technique mentioned in the literature review section.

Participants also confirmed that expert attackers with proper software could collect information about and from, the TPM and later use it against the TPM.

4.4. Does the Proposed Model Solve the Problem

For Question 4, the proposed model was introduced to the participants and all states were explained. In conclusion participants agree to the sufficiency and importance of the model to overcome and solve the problems introduced and analysed earlier.

The main points agreed by participants were firstly, the use of virtualisation to the benefit of available resources in creating a second platform to do the authentication. This can help to protect the TPM by keeping it closed until user verification is completed. Secondly, they agreed that, the new platform can be used or also seen as a native platform running at normal speed giving the user a faster platform to handle normal tasks or activities (tasks which do not require TPM use).

Thirdly, the use of biometrics as authentication methods can provide higher integrity in verifying users identity, which reduces the risk toward the TPM and toward users’ credentials, also the use of two attestation factors by joining face and fingerprint recognition which will add an extra level of security helping to confirm user identity and make the user authentication process more reliable and trustworthy. Finally participants agreed that hiding displayed information on the monitor is a good practice, as it will assist in protecting user privacy, preventing any other user from seeing what is displayed on the monitor as users deal with highly confidential information.

4.5. Model Improvements

For Question 5, participants were asked if any improvements could be added to the model. A suggestion by one of the participants was to add another dynamic verification and authentication PIN password from the machine to the model, like an account password, screen saver password or BIOS password and combine it into the model. Also for future work one participant suggested adding more biometrics to the model, like voice recognition and makes the user choose any two from many biometrics to authenticate him/her.

4.6. Conclusions

As discussed in section 2, previous researches had confirmed the importance of the TPM protecting and securing information and computer systems, also they discussed the weakness and the vulnerability of the TPM to physical attack, that where they took they use of TPM to another level to overcome that weakness. However, extra efforts and devices were included to meet the challenges and securing the TPM.

The result of the focus group, have comes to confirm the purpose of this research from both perspectives. Firstly, the panel has agreed to and confirmed on that the proposed model is sufficient to provide expected level of protection to the TPM and assist to prevent physical attack against TPM and the use of biometrics shall be the proper solution to replace the current PIN password authentication. Secondly, the use of virtualization and the implementation of two platforms, gives good solution to satisfy users with the use of safe and faster platforms, using available resources. Based on the recommendation from the panel, the proposed model can be consider as more appropriate and reliable than what had been introduced at section 2 background and related work responding to the problem.

5. DISCUSSION

The TPM-UAM model is meant to solve a critical issues associated with the implementation and the use of TPM in efficient way, using the available resources without adding any burden to equip computer systems with extra devices or peripherals which shall add cost and complexity, such as the case of including mobile phones at the verification processes, using smart cards and smart cards reader or the need to do verify computer systems over servers as mentioned at the background of this study.

As most of computer systems are equipped with webcams and big number also equipped with fingerprint scanner device which shall make it easy and more adequate to be adopted. Some computers may come without webcam or fingerprint scanner, for such case the low cost of these devices and easy to install features, makes it available to users to add them to their computer systems and have full benefit using TPM.

Meanwhile, using biometric for verification can be considered as more reliable and useful, as users carrying these features themselves all the time and where ever they go. Therefore, problem such as password theft or password lose might not appear here, which is main concern with the current user authentication technique within TPM, as well as smart card and tokens theft, lose, steel or damage issues as suggested by some researches as shown in section 2.

On the other hand, the virtualization concept help to create multiple platforms to separate the running platform with TPM from the platform that does the verification, in order to secure the TPM, also to create faster platform that could meet the user requirements, where TPM platform tends to be slow platform which leads to user dissatisfaction. The confirmation of these concepts has been approved by the focus group evaluation.

6. CONCLUSION

In this study we have presented the TPM-UAM model, which benefits from virtualisation concepts to create multiple platforms on the same physical machine, where this research shows different platforms are needed to authorise users and to run the TPM securely. A motion detection process is used to protect user’s privacy and keep confidential information safe from exposure. Biometric authentication techniques are used to confirm user identity and authority to use the TPM.

The limitations of this research can be introduced as this research work based on the use of Xen virtualization to benefit from Xen ability to modify the kernel of Linux OS and bring TPM to the virtual level, where we can force the use of TPM to be through our verification model always. As Xen works only with Linux OS, this required the users to have the willing and the familiarity to work with Linux systems as it will be used as authentication platform and the platform which should run the normal user's activities with normal level of security.

Our next step is to bring the proposed model into reality and build a working system prototype, which can prove the sufficiency of the proposed model solving the problems introduced and associated with TPMs. After that, to evaluate the prototype to confirm the model's functionality in responding to the stated problems.

7. REFERENCES

Aaraj, N., A. Raghunathan, S. Ravi and N.K, Jha, 2007 . Energy and execution time analysis of a software-based trusted platform module. Proceeding of the Automation and Test in Europe Conference and Exhibition, Apr. 16-20, IEEE Xplore Press, Nice, pp: 1-6. DOI: 10.1109/DATE.2007.364446

Bezakova, I., O. Pashko and D. Surendran, 2000. Smart Card Technology and Security.

Clarke, L ., 2012. Advantages and disadvantages of using smart cards: Brief overview of smart card security and uses. Bright Hub. Ed. Rebecca Scudder.

Feld, S. and N. Pohlmann, 2011. Security analysis of OpenID, Followed by a Reference Implementation of an nPA-Based OpenID Provider. In: ISSE 2010 Securing Electronic Business Processes, Springer, ISBN: 978-3-8348-1438-8, pp: 13-25.

George, P., 2004. User authentication with smart cards in trusted computing architecture. Proceedings of the International Conference on Security and Management, Jun. 21-24, CSREA Press, Las Vegas, Nevada, USA, pp: 25-31.

Hegan, W.V., 2008. Professional Xen Virtualization. 1st Edn., Wiley India Pvt. Limited, ISBN-10: 812651597X, pp: 422.

Khan, U. and H. Zahid, 2010. Comparative study of authentication techniques. Int. J. Video Image Process. Netw. Security, 10: 9-13.

Khushk, K.P. and A.A. Iqbal, 2005. An overview of leading biometrics technologies used for human identity. Proceedings of Student Conference on the Engineering Sciences and Technology, Aug. 27-27, IEEE Xplore Press, Karachi, pp: 1-4. DOI: 10.1109/SCONEST.2005.4382869

Klenk, A., H. Kinkelin, C. Eunicke and G. Carle, 2009. Preventing identity theft with electronic identity cards and the trusted platform module. Proceedings of the 2nd European Workshop on System Security, Mar. 31-31, ACM, Nuremburg, Germany, pp: 44-51. DOI: 10.1145/1519144.1519151

Krueger, R.A. and M.A. Casey, 2009. Focus Groups: A Practical Guide for Applied Research. 1st Edn., SAGE Publications, Los Angeles, ISBN-10: 1412969476, pp: 219.

MacKenzie, D. and G. Pottinger, 1997. Mathematics, technology and trust: Formal verification, computer security and the U.S. military. Ann. History Comput., 19: 41-59. DOI: 10.1109/85.601735

Mannan, M., B.H. Kim, A. Ganjali and D. Lie, 2011. Unicorn: Two-factor attestation for data security. Proceedings of the 18th ACM Conference on Computer and Communications Security, ACM, USA, pp: 17-28. DOI: 10.1145/2046707.2046712

Muditha, P. and K. Chamath, 2011. A performance comparison of hypervisors. Proceedings of the International Conference on Advances in ICT for Emerging Regions, Sept. 1-2, IEEE Xplore Press, Colombo, pp: 120-120. DOI: 10.1109/ICTer.2011.6075037

Pearson, S., 2005. Trusted computing: Strengths, weaknesses and further opportunities for enhancing privacy. Proceedings of the 3rd International Conference on Trust Management, May 23-260, Springer, Paris, France, pp: 305-320. DOI: 10.1007/11429760_21

Peng, S. and Z. Han, 2006. Trust of user using U-Key on trusted platform. Proceedings of the 8th International Conference on Signal Processing, Nov. 16-20, IEEE Xplore Press, Beijing, DOI: 10.1109/ICOSP.2006.346076

Ping An, W., 2010. Information security knowledge and behavior: An adapted model of technology acceptance. Proceedings of the 2nd International Conference on Education Technology and Computer, Jun. 22-24, IEEE Xplore Press, Shanghai, pp: 364-367. DOI: 10.1109/ICETC.2010.5529366

Sadeghi, A.R., M. Selhorst, C. Stuble, C. Wachsmann and M. Winandy, 2006. TCG inside?: A note on TPM specification compliance. Proceedings of the 1st ACM Workshop on Scalable Trusted Computing, Oct. 30-Nov,03, ACM, Alexandria, VA, USA, pp: 47-56. DOI: 10.1145/1179474.1179487

Schneier, B., 2009. Evil Maid Attacks on Encrypted Hard Drives. Crypto-Gram Newsletter.

Shen, C., H. Zhang, H. Wang, J. Wang and B. Zhao *et al*., 2010. Research on trusted computing and its development. China Inform. Sci., 53: 405-433. DOI: 10.1007/s11432-010-0069-x

TCG, 2010. Black hat conference report about TPMs: TCG in Action.

TCG, 2007. TPM main, Part 1, design principles, specification version 1.2, Level 2 revision 103. Trusted Computing Group, Trust Computing Group.

VMware, 2006. Virtualization overview. VMware.