Journal of Theoretical and Applied Information Technology
20th November 2015. Vol.81. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATION OF THE TPM USER AUTHENTICATION MODEL FOR TRUSTED COMPUTERS

MARWAN ALSHAR'E, ABDULLAH MOHD ZIN, ROSSILAWATI SULAIMAN, MOHD ROSMADI MOKHTAR

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

Email: miaajo@yahoo.com

ABSTRACT

A number of previous researchers have discussed the vulnerability of TPM to physical attack and have proposed a number of solutions to solve these issues. Investigation have shown a number of flaws that these solutions suffers from. Trusted Platform Module User Authentication Model (TPM-UAM) is a model that was proposed and evaluated to overcome major safety issue that TPM found to be vulnerable to. A system prototype based on TPM-UAM was developed to prove the TPM-UAM ability to protect trusted computers protected by TPM. Expert review method depends on the understanding that experts are able to provide clear judgment and opinions from their experience and knowledge in their fields. The evaluation process consists of three sections, functionality evaluation, 'can you break it?' test and usability evaluation. Three experts in an individual expert review method were asked to evaluate the system prototype in order to confirm the system correctness of design and implementation and also to evaluate the prototype as a reflection of the TPM-UAM and confirm the model ability to protect trusted computers protected by TPM. The evaluation process was conducted as planed and the system prototype was successfully evaluated. The results confirmed on the system's correct design and implementation, also confirms the correct imitation and representation of the TPM-UAM model in a software prototype, as well as the system efficiency and ability to secure TPM. This paper describes the expert evaluation of software prototype based on TPM-UAM model. Three experts in the field of trusted computing and information security evaluated the system prototype individually in three evaluation sections includes functionality evaluation, 'can you break it' test and usability evaluation. The evaluation results confirms the system correct design, ability to protect TPM and the reflection of the TPM-UAM model that the prototype system intended to represent.

Keywords: *TPM, Expert Evaluation, Individual Expert Review, Heuristic Evaluation, Functional Evaluation.*

1. INTRODUCTION

Trusted Platform Module (TPM) had been developed by Trusted Computing Group (TCG) as platform that includes additional hardware and software to increase the security level of IT-systems. A Trusted Platform is "a computing platform that has a trusted component, probably in the form of built-in hardware, which it uses to create a foundation of trust for software processes" [1]. Despite the solid foundation that TPM provides to platforms that contains it, literature investigation suggests numbers of drawbacks and limitations with TPM as in [2], [3], [4] and [5] which are vulnerability to physical attack and weak authentication.

Therefore, Trusted Platform Module User Authentication Model (TPM-UAM) was proposed by [6] to solve the safety flaws of TPM. Later, the design and implementation of a software prototype based on the TPM-UAM was introduced to bring the model into practice and proves the model ability to protect the TPM, the software prototype was successfully implemented and tested using functionality testing technique, and the testing results confirm the system functionality and performance in accordance to the functionality suggested by the TPM-UAM model [7].

The term "expert review" is defined by [8] as " an informal method used by one or more expert usability professionals to evaluate a user interface". The method depends on the understanding that experts are able to provide clear judgment and opinions from their experience and knowledge in their fields.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The concept of individual expert review was introduced by [9]. In an individual expert review a single expert is to examine certain data about a product or service imitating the roles of a user to discover drawbacks in a system using various techniques such as individual walkthrough, interviews on users, review on product against certain heuristics and examination on the product from different perspectives. Conducting individual expert review might be done by combining aspects of various evaluation methods as in heuristic evaluations, perspective-based inspections, cognitive walkthroughs and informal usability testing (Wilson, 2014).

In this paper we present the individual expert review evaluation of the software prototype, to confirm the usefulness of the TPM-UAM model and the working prototype.

2. BACKGROUND

According to [10] TPM provides users with a security environment which can confirm safety and security of information and software application that the user might have or use. Despite the tremendous support that the TPM provides for the end users, TPM itself found to have and suffer a number of issues. To solve the problem associated with the TPM security and safety, in depth analysis for the structure and the technologies compound within TPM had been conducted, the result of the analysis reveals the main weakness that confronts TPM performance, which might affect the TPM work and TPM's acceptance by the end users.

The main problem occurs to TPM due to direct interactions between unauthorized users and TPM. Hence, to enhance the security of TPM, we have to isolate TPM from direct interaction with random users. Where the risk can be explained as, TPM works with users who have privilege, an owner of TPM has to prove himself in order to use TPM. Thus, when a user tends to use TPM, the user has to provide the Owner password. TPM will open its registrars to collect and confirm the users' password. This is considered as risk toward the TPM, as an attacker might try to interact with the TPM, and in this case a serious damage can occur to the TPM as discussed in the Evil Maid attack method by [11] and (Schneier 2009).

On the other hand, TPM relies on password authentication in order to authenticate users. A number of drawbacks within password authentication techniques were discussed and password-based authentication was found not to be the optimal authentication technique to secure and protect TPM, and that other available authentication techniques can be more reliable to secure TPM. A number researches adopt different methods to provide better authentication mechanisms to confirm user identity, where they try to use advanced methods such as the case to store authentication credentials into smart cards or USB tokens or to authenticates users through mobile devices and tokens [2], [3], [4] and [5].

2.1 The Trusted Platform Module User Authentication Model (TPM-UAM)

Trusted Platform Module User Authentication Model (TPM-UAM) was proposed and explained in [6] as shown in Figure 1. TPM-UAM model, benefits from virtualisation concepts to create multiple platforms on the same 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 the 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.

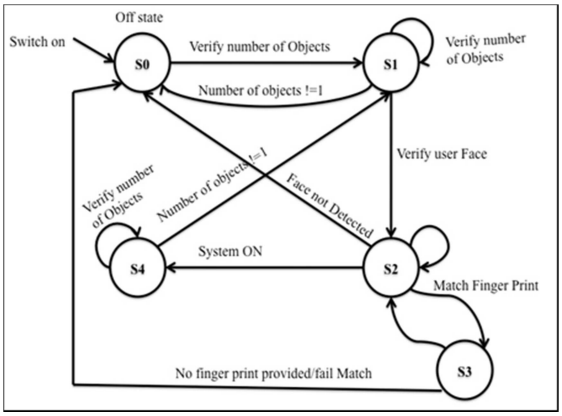

Figure 1: TPM-User Authentication Model [6]

The model had been evaluated using focus group to confirm the model efficiency. The results of the focus group was in line with the assumption of this research, as the respondents by the experts for the various focus group interview questions have confirmed the advantages and the importance of TPM use and implementation protecting and securing computer systems and user's confidential information, as well as confirming some drawbacks with TPM mainly the drawbacks of this research concerns and the needs to overcome these drawbacks.

Journal of Theoretical and Applied Information Technology
20th November 2015. Vol.81. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2 The Design and Implementation a System Prototype Based on TPM-UAM

In order to confirm the usability and abilities of TPM-UAM model, [7] introduced the design and implementation of a system prototype based on TPM-UAM model. To implement the system, the open source image processing library from the *openCV* was used to ease the development of the face recognition and fingerprint process through the use of available and free libraries. The *Xen* hypervisor was installed on top of the *Fedora 18* to support the virtualization and to create the desired multiple number of platforms.

The implementation process has shown that the use of the virtualization concept to was useful to create multiple platforms on the same machine. The first platform was used as authorization platform, which serve to authorize users before they can use TPM in a secure platform. The second platform is to run the TPM securely. The protection of user privacy and confidentiality is granted by monitoring the presence of the authorized user all the time using motion detection, based on the face detection process from openCV library. Biometric authentication techniques were used to authenticate users in terms of identity and authority to use the TPM.

The mechanism that the implementation of the TPM-UAM model shows is, the ability to secure the platform containing the TPM by forcing users to pass the authentication process at the authentication platform. Only confirmed and verified identities can proceed to the secure platform, which contains the TPM. Two main facts have been used to assess whether the model works perfectly. Firstly, the nature of the TPM which supports only a single owner, which in this case is brought to the virtual platform; and secondly, the Xen hypervisor modifies the kernel of the OS, which will be detected by the TPM. Since the TPM will not work on a modified kernel, thus it can be brought to work only on the virtual platform.

Finally, a functional testing of the model has approved the system's functionality, where the prototype could respond to various situations and tasks as planned.

3. EVALUATION PROCESS

The system evaluation process consists of three main sections. The first section evaluates the system performance according to the TPM-UAM model and confirms the system functionality as proposed by the model. The second section is '*can you break it?*' test to confirm the system robustness and confirm the systems validity to protect a secure platform The third session is usability heuristic evaluation, to test the system usability and design as security tool, heuristic evaluation use a set of heuristic for user authentication system.

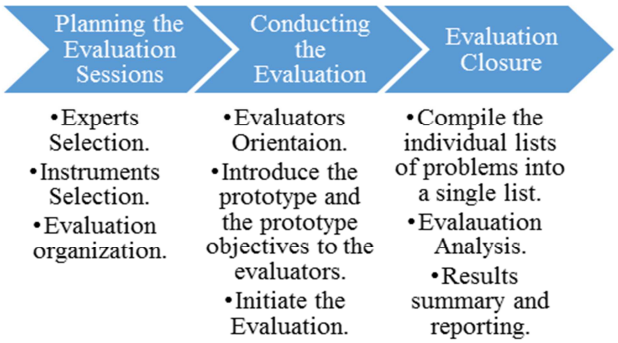

Figure 2: Expert Evaluation Process.

3.1 Planning Evaluation Session

The first stage of the evaluation approach is to plan the evaluation session. The planning session undertaken the various activities to be carried out in consideration, and draw the main lines to prepare the required materials to ease and facilitate the conduction of the evaluation and obtain the desired results, the activities involved in this phase are as follow:

i. Experts Selection.

Previous studies recommended two or three judges or experts to evaluate the systems design and functionality according to cases or scenarios provided by the developer [12] and [13]. As this research focuses on the security concept of TPM, three experts were invited to evaluate the system prototype and confirm the usability and correctness of the prototype securing the TPM according to the proposed TPM-UAM model. All experts are required to have the expertise in TPM and TPM security and information security in general.

ii. Instruments Selection.

The instruments to be used for the purpose of the evaluation need to fit in a zone where the result of using these instruments shall prove the system correctness and robustness responding to the problem statement of this research study. To achieve the objectives of this evaluation three main instruments are to be used by the expert to evaluate the system, which are (1) the functional evaluation and testing, where experts needs to carry out a functional evaluation to confirm the system abilities

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and correctness in protecting the TPM in trusted computing environment; (2) the 'can you break it?' test, which is required to prove the systems robustness and ability to prevent intruders from getting access to protected region; and (3) heuristic evaluation, which is a specific designed and domain-based set of heuristics that are widely recommended to suit the nature of the system application and to provide more reliable results which should convey the needs and the use of the system [14]; [15]. The heuristic list used in this evaluation is based on HCI-S list adopted from [16] which are as shown in Table 1.

Table 1: Human Computer Interface- Security (HCI-S) Criteria.

Criteria	Description
Convey features	The interface needs to convey the available security features to the user.
Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
Learnability	The interface needs to be as non-threatening and easy to learn as possible.
Aesthetic and minimalist design	Only relevant security information should be displayed.
Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?
Does the interface lead to trust being developed?	
Trust	It is essential for the user to trust the system. This is particularly important in a security environment.

iii. Evaluation Organization.

The organization of the heuristic evaluation should take place to prepare the required facilities to conduct the evaluation [9].

iv. Select the Heuristic Evaluation Approach.

According to [9] a number of approaches such as System Scenarios, System Goals, Specific User Interface (UI) Review and Methods Combination that can be used for the heuristic evaluation process. Each approach decide the form and the way of the evaluation to be carried out with.

Based on the nature of this research and to ensure the evaluation of the main objectives of the system, the System Goals approach is used to assist in performing the heuristic evaluation. Two main categories are used, first category is to evaluate the success and satisfactory level of using the system in a normal flow, the second category is to evaluate the system resistance against false inputs and justify the ability of the system to perform the main tasks that the system intended to perform in satisfactory manner.

3.2 Conducting the Evaluation

The process of conducting the evaluation has been undertaken into three main stages which are as follow:

i. Evaluators Orientation.

For the experts to get a clear view of the system and the purpose of developing it, an introduction about the objectives of the system will help the experts to have a whole view of the purpose of the system, also to provide them with an introduction about the system and how it works

ii. Introduce the Prototype and the Prototype Objectives to the Evaluators.

In this stage, the evaluators are briefed about the system and the objectives behind the system. The pre prepaid materials to introduce the system and the objective of the system is handed and discussed with the evaluators.

iii. Initiating the Evaluation.

The evaluator is clear with the objectives of the prototype and the prototype itself, and the process of the evaluation is started. Once the evaluator has finished evaluating the system the forms and materials are collected and recorded.

3.3 Evaluation Closure.

After the evaluation process is done, prototype is checked by the experts and the evaluation materials are collected. The final stage in the prototype

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

evaluation process is to analyze the respondent by the experts, obtain and report the final result. The evaluation closure includes the following process:

i. Compiling the individual lists of problems into a single list.

The opinions and feedback from the experts about the different tasks of the system are collected and combine in one list, where the new combined list shows how each expert rates each particular task. The severity rate of a problem with a certain task decides the required action to be taken as well as the quality of the system. To decide on the severity, experts were asked to rate each problem's severity.

ii. Evaluation Analysis

For a small group of interviewees, it is recommended for the interviewer to analyze the data using his/ her own skills in writing a summary, paraphrasing, and quotation to document accurately what have been discussed by the experts during the evaluation and in respondent to the questions [17] and [18].

For the heuristic evaluation the analysis is carried out by listing and categorizing the problems found by the experts. These problems form the primary data from individual expert review [9]. The categories of problems are Type of the Problem, Location in the UI, Scope of the problem, Severity rating and Estimated effort to fix the problem. Results Summary and Reporting.

The final report from individual expert review describes the problems found by the experts and their comments over the different parts of the system.

4. THE PROTOTYPE EVALUATION

The individual expert review is performed by implementing three main tests by each expert individually to evaluate, how the system implements the concepts presented by the model as discussed (6), to evaluate the prototype's ability to perform the tasks that it was intended to perform, and to evaluate the prototype's implementation correctness by using usability evaluation.

The process of evaluation was started by presenting the proposed model of this research. Then, the functionality of the prototype and the scenarios for using the system to perform the different tasks were described.

4.1 Context

During the evaluation, three tests were implemented to answer a number of questions regarding the prototype's correctness and ability to protect the trusted computing environment with TPM. The questions are as follow:

1. Does the prototype convey the features presented in the TPM-UAM model correctly
2. Is the prototype capable of protecting trusted environment protected by TPM, and how solid it is against attacks?
3. Does the design and implementation of the prototype convey the required features of a security tool?

The feedback collected from each test helps in answering each question, and helps to enhance the prototype according to the comments from the experts in the usability evaluation.

4.2 Participants

As mentioned before, three experts in the field of information security and usability testing were involved in the evaluation process. The participants were academicians in the field of information security and have experience with the usability evaluation. The responsibilities for evaluators are to attempt the performance of certain task scenarios which reflect the functionality of the prototype, and then, to provide feedback about each task according to the nature of the scenario and the required type of evaluation.

4.3 Procedure

The evaluation was conducted in a discussion room in the university. Each evaluator was equipped with a computer system with the installed prototype as well as the required virtual machine and platform. The facilitators were available during the time when the evaluators interact with the prototype, and briefed the evaluators about the prototype and the procedures of doing the evaluation. The facilitators then provided the evaluators with the evaluation forms and commenced the evaluation session.

The evaluation forms contain the necessary description for each task and evaluation to guide the evaluator while doing the testing on each task. After the evaluator have finished each section of the evaluation, the facilitator discussed with the evaluator on the general findings and comments about the evaluation section and notes were taken to confirm clear understanding of the finished section.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.4 Roles

For the prototype evaluation there are two main roles which are the facilitator and the evaluators. The responsibilities of both the facilitator and evaluators are briefly described below:

Facilitator

- Provide overview of the study to the evaluators.
- Explain the purpose of the evaluation.
- Respond to the evaluators' requests for assistance.

Evaluators

- Perform the required tests over the prototype according to the defined scenarios and descriptions of the tests.
- Fill the evaluation form with the results obtained from each test.
- Comment and suggest any required changes or enhancement for the prototype.

5. FUNCTIONALITY EVALUATION

The purpose of this evaluation is to confirm on the system's ability to perform the tasks that it was intended to do as described and discussed by the proposed TPM-UAM model.

Experts used the prototype to perform the different tasks that the system should do, then they individually evaluated and confirmed each function's ability to perform and work as it was designed for on the evaluation form as shown in Table 2.

Table 2: Prototype's Functionality Evaluation.

Function No	Function Description	Expected Behaviour	Result P	Result F
F1	Unauthorized user Starts the Secure Platform. **Procedure:** Expert tries to access to secure platform before enrolling to the system.	The system should ask the user to present finger print and stand in front of the camera. If user is not a registered user, the system should reject the request and inform user that he is not authorized.	□	□
F2	Authorized user Starts the Secure Platform. **Procedure:** Expert tries to access the secure platform using his /her registered biometrics as registered user.	The system should ask user to present finger print and stand in front of the camera, The system notifies success authentication and opens secure platform.	□	□
F3	Confirm the presence of single user **Procedure:** Expert holds his place in front of the camera while secure platform is running.	Secure platform is accessible as long as user is present in front of the camera.	□	□
F4	System's response to the absence of authorized user. **Procedure:** Expert changes position and moves away from the PC.	The system should hide and pause secure platform whenever the authorized user is absence.	□	□
F5	System's response to the return of authorized user. **Procedure:** The expert moves back to the front of the PC.	System should recognize the returning of the user and then asks for finger print to open the system again.	□	□
F6	System's response to the presence of a second user **Procedure:** Second user comes along next to the expert making the number of users in front of the system more than one.	The system should hide and pause secure platform.	□	□

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

F7	System's response to the return of unauthorized user **Procedure:** Expert will move away from PC, another user will be present alone in front of PC.	System should require user to scan his thumb to the finger print scanner, system keeps secure platform paused and locked	□	□

5.1 Results of the Functionality Evaluation

There were three evaluators performed the evaluation, and each evaluation session lasted two hours. Each task required the evaluator to follow certain scenario to fulfil that task. The task is recorded as completed if the evaluator decides that the task goal is achieved or not (Pass (P) or Fail (F)).

The observation from all experts' evaluation confirms on the experts' satisfaction with the general functionality of the prototype in terms of prototype correctness and the reflection of the model of this study. The evaluation results show that all functions perform and behave as expected and designed for. The experts' responses for the different tasks and scenarios are shown in Table 3.

Table 3: Respondents' Results on the Functional Evaluation.

Evaluator	F1	F2	F3	F4	F5	F6	F7
1	Pass	Pass	Pass	Pass	Pass	Pass	Pass
2	Pass	Pass	Pass	Pass	Pass	Pass	Pass
3	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Success Rate	100%	100%	100%	100%	100%	100%	100%

Table 4: 'Can you break it' test's Form and Scenarios.

Attempt ID	Test	Breaking Test Scenario	Result of Break Attempt	
			Fail	Success
A1	Unregistered user Logs on to the system.	• Expert tries to access the system before enrolment. Exposing different finger prints to the scanner and posing in various positions in front of the camera.		
A2	Unregistered user attempts to use secure platform	• An authorized user logs on to the system and then moves away from the system. • Then the expert tries to break the system to reach the secure platform.		
A3	Multiple users' presence in front of PC.	• Authorized user logs in to the system and starts use the secure platform. • Expert moves next to the authorized user trying to have visual access to the contents of secure platform violating the authorized user privacy.		

One of the evaluators suggests that the ability of implementing the 3D face recognition mechanism instead of the 2D as enhancement for the prototype is to increase the security level.

6. 'CAN YOU BREAK IT?' TEST

This test aims to evaluate the prototype's resistance against possible attacks. The evaluators referred to the possible attack scenarios provided by the facilitators as shown in Table 4. Additionally, evaluators were also requested to perform or suggest any other attempt that they feel might help detect any flaw within the prototype. However, evaluators were satisfied with the suggested scenarios to cover the possible threats and attacks to the system.

6.1 'Can you break it' Test Results

The result of the test shows the prototype's resistance against possible attack attempts where the evaluator failed to bypass the prototype to reach the protected platform. The break attempts is designed according to specific scenarios which can emulate all possible breakings into the system and the system stands for all the possible attempts and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

prevents the unauthorized access. The results of the attacking attempts are shown in Table 5. Here, the evaluators confirm on the failure attempts to break the prototype and the prototype functions exactly the way what it was designed for.

Table 5: Can you break it test result feedback.

Evaluator	A1	A2	A3
1	Fail	Fail	Fail
2	Fail	Fail	Fail
3	Fail	Fail	Fail
Attempts to attack's Failure Rate.	100 %	100 %	100 %

7. USABILITY EVALUATION

According to [19] the evaluation process focuses on gathering the data to examine a product by a certain type of users for an activity within certain environment.

Usability evaluation methods can be categorized into two main sets which are usability inspection methods also known as the analytical methods and end-user evaluation methods also known as empirical testing [20] and [21]. The usability inspection methods which are well known as the heuristic evaluations, can be described as, "a group of experts evaluate the instrument on the basis of a set of heuristics or evaluation criteria". There is no special requirement required for the usability inspection, and expert can define a wide range of drawbacks if they exists within a short time [20].

Empirical methods for usability testing are relatively costly and time consuming compared to the analytical inspection methods. Further, in the usability inspection methods, we rely on the experts to analyse the system rather than the actual users which shall cut the cost and the required time to perform the inspection [22]. Several approaches to usability inspection have been proposed, mainly, the heuristic evaluation, cognitive walkthrough, pluralistic walkthrough, and formal inspections.

Nielson and Molich [23] first introduced the heuristic evaluation as a method to evaluate user interface. This method works by having small group of experts to evaluate the interface using some guidelines and to take note of problem if detected. Also [22] confirmed on the necessity of experts to perform heuristic evaluation to achieve accurate results and also to compete with other evaluation methods in terms of cost and time efficiency.

7.1 Heuristics Evaluation

In this method, evaluator looks into user interface and provides opinion about what's good and what's bad about it. For better resolution well planned set of rules or checklist is highly recommended to provide more accurate results and capture more usability problems.

Johnston, Eloff and Labuschagne (2003) [16] discussed the HCI development and evaluation criteria in [24] and suggested that the set of heuristics to be selected for the purpose of any system evaluation has to be decided according to the nature of the system being evaluated. Therefore, they proposed a set of heuristics to be considered when evaluating systems that are relevant in information security environment [16] .

However, the selected criteria are concentrated in and limited to those criteria's which are relevant to the security environments, and then modified as needed to provide more suitable ground for the security HCI design as shown in Table 1.

The System Goals approach is used to assist in performing the heuristic evaluation. The defined goals for evaluators is categorized into two main objectives. The first objective is to evaluate the success and satisfactory level of using the system in a normal flow, while the second objective is to evaluate the system's resistance against false inputs and justify on the ability of the system to perform the main tasks that the system intended to perform in satisfactory manner. The system's goals and description are shown in Table 6 below.

Table 6: Heuristic Evaluation System's Goals' Description.

Category	Goal	Description
Normal Flow	Create user account and declare authority over the system.	Expert is to enroll him /her self to the system using the face and the fingerprint.
	Login to the secure platform using the registered biometrics.	Expert will intend to run the secure platform and the prototype will start to work asking for user to prove identity by presenting clear image of the face in front of the camera

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

		and placing his / her thumb to the fingerprint scanner.
	Confirm on the TPM running session protection.	Expert will move away from the camera to cause secure platform to stop working.
False Input	Evaluate the system's resistance against penetration by unauthorized user.	Expert will attempt to access the system before he / she is enrolled.
	Evaluate the system's response to the absence of the authorized user and protection of the running TPM session.	Expert will move away from the camera and come back, and wait for the system to recognize him / her before giving back the authority to resume with security platform.

Experts used the list of goals to guide them in the process of prototype evaluation, and then to evaluate in accordance to the HCI-S heuristic list and record the problems as they find them or mark the heuristic as passed. The severity of each problem is also recorded as soon as a problem is defined.

7.2 Usability Test Results

The evaluators carried out the heuristic evaluation using six heuristics with number of checklist items. The number of checklist items included in each high-level heuristic is presented in Table 7. The results obtained from all experts are as shown in Table 8. The results generally show the examiners acceptance and satisfaction over the checklist of the examined heuristics.

Table 7: The Number of Checklist Items.

Number	Heuristic	Checklist Items	Numbering Order
1	Convey features	3	1.1 – 1.3
2	Visibility of system status	6	2.1 – 2.6
3	Learnability	5	3.1 – 3.5
4	Aesthetic and minimalist design	5	4.1 – 4.5
5	Errors	6	5.1 – 5.6
6	Satisfaction	3	6.1 – 6.3

Table 8: Respondents' Feedback on Usability Evaluation

	Evaluator 1				Evaluator 2				Evaluator 3			
No	**Yes**	**No**	**NA**	**Severity 0-4**	**Yes**	**No**	**NA**	**Severity 0-4**	**Yes**	**No**	**NA**	**Severity 0-4**
1.1	✓			0	✓			0	✓			0
1.2	✓			0	✓			0	✓			0
1.3	✓			1		✓		2	✓			1
2.1	✓			0	✓			0	✓			0
2.2	✓			0	✓			0	✓			0
2.3			✓	0			✓	0			✓	0
2.4	✓			0	✓			0	✓			0
2.5	✓			0	✓			0	✓			0
2.6	✓			0	✓			0	✓			0
3.1	✓			0	✓			0	✓			0
3.2	✓			0		✓		1	✓			0
3.3	✓			0	✓			0	✓			0
3.4	✓			0	✓			0	✓			0
3.5	✓			0	✓			0	✓			0
4.1	✓			0	✓			0	✓			0
4.2	✓			0	✓			0	✓			0
4.3	✓			0	✓			0	✓			0

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.4	✓		0	✓		0	✓			0
4.5	✓		0		✓	2	✓			0
5.1	✓		0	✓		0	✓			0
5.2		✓	0		✓	0			✓	0
5.3		✓	0		✓	0			✓	0
5.4	✓		0	✓		0	✓			0
5.5	✓		0	✓		0	✓			0
5.6	✓		1	✓		0	✓			1
6.1	✓		0	✓		0	✓			0
6.2	✓		0	✓		0	✓			0
6.3	✓		0	✓		0	✓			0

The evaluators have confirmed on that the prototype have met the security heuristics requirements for security tools. The experts have also reviewed the checklist of heuristics and approved the design of the prototype. Their comments for the items in the checklist are as follows:

- Checklist number 1.3. Evaluator number 1 and 3 expressed satisfaction over the item and appointed severity rate of 1. Meanwhile, the second evaluator commented that the item needed more information to be given upon request to users to understand any security capability of the prototype with severity rate of 2. Overall, the item passed the evaluation and only small fixes were only required but they were not critical.

- Checklist number 3.2. Evaluator number 1 and 3 accepted the item as the visual behaviour and usage instruction displayed for the user. Meanwhile, evaluator number 2 suggested providing the running state description text to explain the current state of which security item is being used.

- Checklist number 4.5. Evaluator number 1 and 3 accepted the checklist item as the displayed information describing the general security concept for the user or the system in general. Meanwhile, evaluator number 2 suggested providing more specific description message directed to the user if it particularly concern the user with severity rating of 2.

8. SUMMARY OF THE RESULTS

The functionality test is used by the expert to confirm each task's functionality of the prototype and the prototype's correctness in terms of design to reflect the proposed model of this research study. The result of the evaluation shows that the prototype reflects the functionality and the perspectives discussed in the proposed model of this study. The evaluation also leads to the confirmation on the functionality and performance of all tasks of the prototype as they were intended for.

Can you break it? Test was used by the evaluators to test the system robustness against possible attacks to prove the prototype's efficiency in responding to the problem statement of this research study. The result of this test comes in line with the expectation since the evaluators had failed to break into the system in all attempts and scenarios.

Meanwhile, usability evaluation was used by the evaluators to evaluate the prototype's compliance with the HCI-S design. The result of the evaluation generally proves the design's correctness and compliance according to the selected set of heuristics. However, three minor problems were detected by the evaluators and the severity rate for them ranged between 1 and 2, which means that they were only non- critical errors that may not significantly affect the capability of the prototype.

Based on the results, the prototype system passed the evaluation and the prototype was successful in protecting the platform with TPM on it. The prototype's successes reflects the proposed model's capabilities and functionality. It solved the problem of platform by isolating TPM from unauthorised user's interaction. Specifically, the prototype successfully supports the weak authentication of TPM by forcing the user to authenticate their self, using the biometrics features before they can use the TPM.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

9. CONCLUSION

The individual expert review method was used to evaluate the system. In particular, the evaluators used three evaluation instruments to evaluate the prototype. The aims of the evaluation were, firstly, to confirm the prototype's correctness in terms of design to reflect the proposed model of this research study and then confirm the functionality of each task, secondly, to test the prototype's robustness against attacks which shall prove the model's efficiency responding to the problem of TPM vulnerability to physical attack, and finally, to evaluate the correctness of the design of the prototype as a security tool using the usability evaluation.

The evaluation was conducted as planed and the results were recorded and analysed accordingly, and then reported independently. Further, the final results' summary describes the overall results of the prototype evaluation.

The prototype passed the functional evaluation and this proves the prototype's functionality, and reflects the proposed model as well as the correctness of all tasks performance and success to fulfil the purpose of their existence. Meanwhile, the second section proves the system's robustness against possible attacks attempting to break into the system and reach protected areas. This was proven when all evaluators had failed in their attempts to break into the prototype or certain function to access the protected area. Further, the results of the usability evaluation on the prototype had met the heuristic standards with only 3 minor errors, which are considered not severe, and thus, the prototype can generally be implemented securely.

REFERENCES

[1]. Pearson, S. Trusted computing platforms, the next security solution. HP Labs; 2002.

[2]. George P. User authentication with smart cards in trusted computing architecture. Proceedings of the International Conference on Security and Management, SAM'04; 2004. p. 25–31.

[3]. Peng S, Han Z, 2006. Trust of User Using U-Key on Trusted Platform. 8th international Conference on Signal Processing. Beijing, China: IEEE;

[4]. Klenk, A., Kinkelin, H., Eunicke, C., and Carle, G. 2009 . Preventing Identity Theft With Electronic Identity Cards And The Trusted Platform Module. Proceedings of the Second European Workshop on System Security, March. 31 – 31, ACM, Nuremburg, Germany, pp: 44-51

[5]. Mannan M, Kim BH, Ganjali A, Lie D. Unicorn: Two-factor attestation for data security. Proceedings of the 18th ACM conference on Computer and communications security - CCS '11 [Internet]. New York, New York, USA: ACM Press; 2011 [cited 2014 Dec 31]. p. 17. Available from: http://dl.acm.org/citation.cfm?doid=2046707.2046712

[6]. Alshar'e MI, Sulaiman R, Mukhtar MR, MohdZin A. A User Protection Model For The Trusted Computing Environment. J Comput Sci. 2014;10(9):1692–702; 2014.

[7]. Alshar'e MI, Sulaiman R, Mukhtar MR, MohdZin A. Design And Implementation Of The Tpm User Authentication Model. J Comput Sci. 2014;10(11):2299–314; 2014.

[8]. Tsai, P. (2006). A Survey Of Empirical Usability Evaluation Methods. Retrieved on June 27, 2015, http://web.simmons.edu/~tsai/Papers/PBartley-empirical-usability-eval.pdf

[9]. Wilson C. User Interface Inspection Methods. Waltham, MA, USA: Elsevier Inc; 2014.

[10]. TCG. Black hat conference report about TPMs; 2010.http://www.trustedcomputinggroup.org/community/2010/02/black_hat_conference_report_about_tpms

[11]. Rutkowska J. Evil Maid goes after TrueCrypt!. 2009 [cited 2015 June 27]. Available from: http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

[12]. Nielsen, J. 1992. Finding usability problems through heuristic evaluation. Proceedings of the SIGCHI Conference on Human, 373–380.

[13]. Nielsen J. Usability Engineering Usability Engineering. San Francisco, CA, USA: Morgan Kaufmann; 1993.

[14]. Masip, L., Oliva, M., and Granollers, T. Common Industry Format (CIF) Report Customization for UX Heuristic Evaluation. In A. Marcus (Ed.), Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience SE - 46 (Vol. 8517, pp. 475–483). Springer International Publishing; 2014.

[15]. Bonastre L, Granollers T. A Set Of Heuristics for User Experience Evaluation in E-commerce Websites. ACHI 2014, The Seventh International Conference on Advances in Computer-Human Interactions. 2014. p. 27–34.

[16]. Johnston, J., Eloff, J. H. P., and Labuschagne, L. Security and human computer interfaces.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Computers and Security, 22(8); 2003. 675–684.

[17]. Mathers, N. J., Fox, N. J., and Hunn, A. Using interviews in a research project. NHS Executive, Trent; 1998.

[18]. Driscoll, Dana Lynn. "Introduction to primary research: Observations, surveys, and interviews." Writing Spaces: Readings on Writing 2 (2011): 153-174.

[19]. Preece J, Rogers Y, Sharp H, Benyon D, Holland S, Carey T. Human-computer interaction. Addison-Wesley Longman Ltd.; 1994.

[20]. Triacca L, Inversini A, Bolchini D. Evaluating web usability with MiLE+. Proceedings - Seventh IEEE International Symposium on Web Site Evolution, WSE. 2005. p. 22–9.

[21]. Vukovac P, Dijana, Kirinic V, Klicek B. A Comparison of Usability Evaluation Methods for e-Learning Systems. DAAAM International Scientific Book. Vienna, Austria: DAAAM International; 2010. p. 271–88.

[22]. Hollingsed T, Novick DG. Usability inspection methods after 15 years of research and practice. Proceedings of the 25th annual ACM international conference on Design of communication - SIGDOC '07. New York, New York, USA: ACM Press; 2007

[23]. Nielsen J, Molich R. Heuristic evaluation of user interfaces. Proceedings of the SIGCHI conference on Human factors in computing systems Empowering people - CHI '90. New York, New York, USA: ACM Press; 1990. p. 249–56.

[24]. Molich R, Nielsen J. Improving a human-computer dialogue. Communications of the ACM. 1990. p. 338–48.