Indian Journal of Science and Technology, *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/80104, December 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Efficient Strategy to Provide Secure Authentication on using TPM

E. Padma* and S. Rajalakshmi

[1]SCSVMV University, Enathur - 631561, Tamil Nadu, India; mailtopadma@kanchiuniv.ac.in
[2]SJCAC, SCSVMV University, Enathur - 631561, Tamil Nadu, India; rajalakshmi.s@kanchiuniv.ac.in

Abstract

The major objective of the paper is to implement cost effective TPM based software, which reduces the TPM chip as it is implemented in hardware. Also to improve security among computers and to authenticate the users by using secured software based TPM. To improve the authentication of various client devices that are connected to private network. The research has to be exposed to all possible threats involved in TPM based on 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. The methodology involved in this paper must protect the compromised client and enable network administrator from causing disrupt to the available network. The systems with TPM must store sensitive data in a secure location instead on separate piece of chip. The major statistical survey of this paper deals with the primary machine, which will be allocated to each individual user by accepting their necessary details like device information. The collected information will be kept as a private connected network in a local server. If new user wants to access the locally connected machine, then his information will be collected separately and username and password will be sent to him through mobile. The temporary users' information will be kept in the secondary machine for future use. In this way, the system will get improve secure feature and avoid unauthenticated user to access the machine. The proposed system performs well to safeguard the information and it is experimentally verified in various organizations. In banking information system, each employee's information is verified and stored in the background server. This will protect the information more secure between the clients and the server. As an improvement, the research work will be carried out for business intelligence in Internet of Things using Mobile Application.

Keywords: Authenticated User, Connected Network, Information Retrieval, Password based Authentication, Trusted Platform Module

1. Introduction

The Trusted Computing Group (TCG) as a core provides number of cryptographic capabilities for TPM which helps to protect the computer and user sensitive information from threats. TPM provides specification for microcontroller provided by Trusted Computing Group (TCG). As a state of microcontroller TPM contains Keys, passwords and digital certificates. Also as a hardware initiative TCG states TPM as the heart to design many applications to provide higher level of root of trust.

TPM Stores sensitive information as a space for protected key operations under safe environment. TPM also performs security for critical tasks to report integrity measurement. In order to enhance platform security, a specifically designed capabilities of software keys, software information and software based attacks has been demonstrated.

To protect against potential damage caused by various number of attacks and threats, a TPM has been designed. A large number of vulnerabilities which are known and unknown to the clients can change the practices of industrial software unwontedly. The most kind of threats affect the system through networks and servers, as users do not keep all the patches up to date, because it is time consuming. The most valuable information has been offered by

*Author for correspondence

networks and servers for the attackers which can give better protection than the clients. The users can access information on a compromised client by the supported TPM which can prevent attackers. The network administrator enables TPM to actively work in order to prevent compromised client.

The server and the client are protected by TPM from sensitive information and also on networks they may connect to. Instead of attempting to reduce the vulnerabilities' rate in software, the client is compromised to protect sensitive information and limits the damage by seeking the detection of TPM. If the TPM detects correctly, the attacker cannot access the sensitive information. Each shared client protects sensitive information with the help of TPM by allowing multiple users. By implementing such permissions one client cannot have access to other client's secret information.

The TPM is a low cost security module that delivers the basis of a safe computing environment. Trusted computing allows users to assess the trustworthiness of computers with which they interact and create a foundation of trust for software processes. The Trusted Computing Group (TCG) defines trusted computing as "a device which behaves in a particular manner for a specific purpose". The purpose of the Trusted Platform Module (TPM) is to provide this assurance to the client and the users interacting with the client. A trusted platform should provide at least three basic features:

- **Protected Capabilities**: A set of commands with exclusive authorization to access protected locations such as memory and registers.
- **Integrity Measurement**: The process of obtaining metrics of platform characteristics that affect the trustworthiness/integrity of a platform.
- **Storage and Reporting**: The process of storing those metrics and summarizing/presenting their results. The preliminary point of measurement is called the root of Trust.

Thus, the TPM is good for:

- Machine Authentication.
- Machine Attestation.
- Data Protection.

The TPM provides an entire suite of tools used for secure authentication. The application implementing TPM are based on moving security onto hardware. Existing security systems have an inherent flaw, in that they run on top of the unknown hardware. Systems with TPM store sensitive data on a separate piece of hardware, instead on a secure location. The TPM chip uniquely identifies the hardware and does not allow sensitive data like keys to leave the TPM. The sensitive data cannot be directly accessed outside of TPM.

The TPM hardware is designed to protect sensitive information from physically stolen. The data stolen from the client system is more valuable than the designed hardware. The physical tampering is not required to protect the information while using TPM.

Also, Network security is one of the essential things in our modern life. In many areas, the secret information is hacked by unwanted person without any authorization from the server. This can be avoided through various mechanisms such as encryption, decryption and so on. But some unauthorized users can brilliantly hack the information instead of our security methods. To avoid this kind of actions, we propose a methodology with new authentication techniques which can help to provide security between server and client. Only, the authorized client can access the information from the server. Others can be restricted from access.

By considering all these things, we propose a methodology to provide the secure authentication for the system in a much better way by using TPM. The algorithm in this paper, performs well to demonstrate how the TPM provides security against the unwanted access and the performance evaluation is also given in the experimental results section.

2. Literature Survey

Marwan Ibrahim et al.[1], states the Trusted Computing Group (TCG) has introduced the Trusted Platform Module (TPM) as a solution to the 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 it protects computers against unwanted user's access. TPM is designed to prevent software attacks with minimal consideration towards physical attacks. Therefore, TPM focuses 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 codes then collect confidential information and store it or send it to attackers via the network. However, most of these solutions do not provide sufficient level of protection to TPM. In their study, the authors introduced 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.

Holger et al.[2] discussed that security should be integrated into future networks from the beginning, not as an extension. Secure identities and authentication schemes are an important step to fulfill this quest. They described the concept of home networks as a universal point of reference for authentication, trust and access control, and show that their scheme can be applied to any next generation network. As home networks are no safe place, they applied Trusted Computing technology to prevent the abuse of identities, i.e., identity theft.

Klenk et al.[3] states 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.

Xiao[4], 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 authorized to use the TPM. Mechanisms for authentication and identification are still fairly rudimentary.

Peng and Han[5] 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.

Ron Kim[6] described that Trusted Computing is an initiative to provide an enhanced level of security through a combination of software and a specialized hardware device. TPM is a microcontroller that provides protected storage of sensitive data and a way for remote attestation to third parties. With its promoters including big name players such as Microsoft, Intel Corporation, AMD and IBM, the technology is making sure of their steps towards the mass market. The paper examines that the TPM and its potential merits and limitations in upholding users' privacy. George[7] stated that TCG did not take into account security from the users' perspective; instead, the model is directed and focused on the platform.

Camenisch[8] discussed that The Trusted Computing Group (TCG) specified two protocols that allow a trusted hardware device to remotely convince a communication partner that is indeed a trusted hardware device. In turn, this enables two communication partners to establish a secure computing platform and hence it is safe for exchange of data. Both these remote identification protocols provide some degree of privacy to users of the platforms. That is, the communication partners can only establish trusted hardware device. The first protocol achieves this property by involving trusted third party called Privacy CA in each transaction. This party must be fully trusted by all other parties. In practice, however, this is a strong requirement that is hard to fulfill. Therefore, TCG proposed a second protocol called direct anonymous attestation that overcomes this drawback using techniques known from group signature schemes. However, it offers less privacy than the one involving the Privacy CA. The reason for this is that the protocol needs to allow the verifier to detect rogue hardware devices while this detection was done before by the Privacy CA. In this paper they showed how to extend the direct anonymous attestation protocols such that it offers the same degree of privacy as the first solution but still allows the verifier to rogue devices.

Lampson[9] described that most computers today are insecure because security is costly in terms of user inconvenience and foregone features, and people are unwilling to pay the price. Real-world security depends more on punishment than on locks, but it's hard to even find network attackers, much less punish them. The basic elements of security are authentication, authorization, and auditing: the gold standard. The idea of one principal speaking for another is the key to do these uniformly across the Internet.

Arbaugh[10] stated that the Trusted Computing Platform Alliance (TCPA) specification is a new computing platform for the next century that will provide for improved trust in the PC platform. Improving information security is an important and timely goal, but not at the cost of further weakening fair use of doctrine, encouraging anticompetitive behavior, or eliminating privacy. Unfortunately, the current specification does not meet this standard.

Sundeep[11] described that the objective of the Trusted Computing Platform Alliance (TCPA) is to complement existing capabilities, including the X.509 standard for digital certificates, IPSEC (Internet Protocol Security Protocol), IKE (Internet Key Exchange), VPN (Virtual Private Network), PKI (Public Key Infrastructure), PC/SC Specification for smart cards, biometrics, S/MIME (Secure Multi-purpose Internet Mail Extensions), SSL, SET (Secure Electronic Transaction), IEEE 802.11 WEP, IEEE 802.1x, etc. The TCPA provides a platform for root of trust, which uniquely identifies a particular platform and provides various crypto capabilities including hardware-protected storage. The Trusted Platform Module (TPM) is defined as a hardware instantiation of the TCPA specification. The current revision of the TCPA main specification is version 1.1a. The above document provides a discussion about the various requirements for a TCPA-enabled mobile PC platform.

3. Proposed Methodology

3.1 Proposed Method

The constant growth of computer users and the interconnection between computer systems has increased the need for protection from attacks. To address these needs the TCG developed a set of specification to create a computer system with enhanced security named Trusted Platform. A trusted platform is based on two key components: protected capabilities and shielded memory locations. This trusted platform is shortly termed as TPM which means Trusted Platform Module. This TPM has been most commonly implemented in a chip-level and so it is hardware based. While implemented TPM as hardware-based, it becomes costlier and it is difficult to implement. To avoid this kind of difficulty, we propose to implement TPM as software based.

The aim of our paper is to propose a methodology to improve security among computers and to authenticate the users by using TPM. The proposed methodology provides the authentication to the system through a set of mechanisms which are as discussed below:

3.1.1 Collect the Basic Information of the user System

We develop a service, which is necessary to implement this TPM into our work. This service runs at background, between the connected client and the server. When the user first enters into the system, this service automatically collects all the basic information about the system which is required to authenticate the client's system. This basic information contains the information such as

- Login ID of the Machine
- Drives available in the machine
- Size of the RAM
- IP Address of the machine
- MAC Address of the machine
- Type of Processor used by the machine

3.1.2 Fix the Size for the Information

For each information, we have to allocate the size to store the information. Upon getting the information, we have to verify the size of the information to check if it matches the allocated size. If so, then the information is stored normally. Otherwise, the remaining space of the information can be filled with dummy values or special characters.

η (number of characters in the given information) = η (allocated size of the information)

If true, information → information

Else, N=size – number of characters in the information

information → information + N(dummy)

Where, dummy can be any characters or special characters such as */&/^/$/@/...

The sample original data filled with dummy value as per the allocated size is given below:

3.1.3 Encrypt the Information

Upon collecting the information, the next step is to encrypt the information using encryption techniques such as substitution or transposition. The values are encrypted and stored in a separate variable. This has to be carried out in order to prevent the original values to be visible to others. That is, hiding the original values by substituting duplicate one.

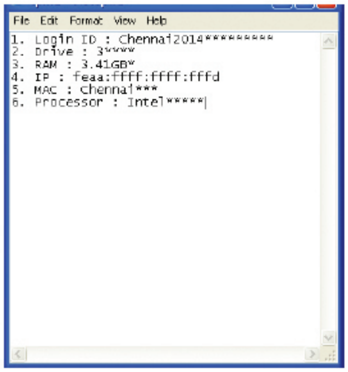
The sample file containing encrypted information in below given Figure.

3.1.4 Send the Information to the Server

The encrypted information is all gathered by the service and is sent to the server. The server receives and stores all the information along with the client's unique username and password. This unique username and password is allocated by the server based on the client information. Only by providing this username and password, the client can enter into the system to access the server.

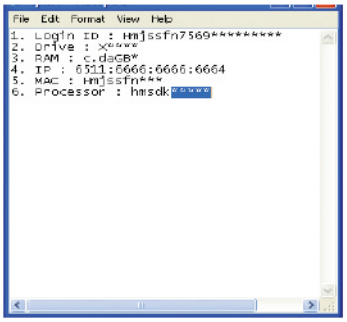
Thus, when the client enters into the system, they must be validated with the username and password. Upon matching these details, the service which runs at the background obtain the basic information about the system, encrypts that information, and sends to the server for authentication. Only when all these details satisfy the validation process, the client is allowed to access the server further. Hence, the client can only access the server with that same allocated machine (i.e.,) the security is purely based on Machine.

We also implement a technique to override this Machine-based environment, which can be discussed below. In case, when the username and password matches, but the basic information doesn't match with the server information, we undergo for the second kind of authentication. When this situation arises, a prompt is displayed containing the information. "This is not your Allocated Machine. Enter your mobile number to send a temporary password". Thus, by providing the mobile number, the client receives a temporary password for accessing the new system. This information can also be stored in the server. That is, the client now has permissible rights to access two systems. Thus, a client can have 1 Primary Machine and N number of Secondary Machines with limited access.



```
1. Login ID : Chennai2014*********
2. Drive : 3****
3. RAM : 3.41GB*
4. IP : feaa:ffff:ffff:fffd
5. MAC : chennai***
6. Processor : Intel*****
```

Figure 1. Sample data filled with Dummy Value.



```
1. Login ID : Hmjssfn7569*********
2. Drive : x****
3. RAM : c.daGB*
4. IP : 6511:6666:6666:6664
5. MAC : Hmjssfn***
6. Processor : hmsdk*****
```

Figure 2. Sample File containing Encrypted Information.

The summary of the TPM authentication can be carried out as follows:

- When the user login into the system, we have to check the server for the Username and Password. If the username and password found in the server, then the user is identified to as existing one. Otherwise, the basic information is collected and creates a new record for the user.
- In case of existing user, the username and password can be validated by the server.
- If both of them match, then validate the basic information of the system.
- If the validation gets success, then the user is considered to be as an Authenticated and Valid User, accessing the Primary Machine.
- If the username and password match, but the basic information does not match, then the user is considered to be as an Authenticated but accessing unallocated machine.

Table 1. Sample dataset for size

Information Type	Size
Login ID	20
Drive	5
RAM	7
IP	19
MAC	10
Processor	10

Table 2. Server database

Username	Password	Login ID	Drive	RAM	IP	MAC	Processor
…	…	…	…	…	…	…	…

- Then the user is required to provide the mobile number to receive the temporary password.
- By providing the temporary password, the user can access the Secondary Machine.
- Locate the user entry and get the value from it.
- The values are then decrypted and compared to the information collected.
- If the comparison gets true, then the user is considered as an Authenticated and Valid User. Else the user is considered as an Invalid User.
- Only the valid user has the permission to access the system. The invalid user has to be prohibited.

Thus, only the trusted client can access the server. These are all carried out within the server’s IP Permissible area. That is, within the office or building. While accessing the server within the permissible area, the client can access the server at any number of times, within being provided with the password. This is because; the service runs at the background, which will authenticate the client at each and every process.

In case of accessing the server apart from the permissible area, (i.e.,) Browsing Center, they can access the server by providing the password at each and every process, with only limited access since there is no services running between the client and the server.

Thus our proposed methodology provides authentication to secure the information on the system. Also, the TPM is not Machine-Based. Our paper also proposes an algorithm which implements the methodology.

3.2 Algorithm

```
Begin
Step-1: Gather the Basic Information of the user through the service
        I={LogID, Drive, RAM, IP, MAC, Processor}
Step-2: Verify the user information (un,pwd) with the Server
        Database
        Server={Username, Password, {I}}
If un exists Server.Username then
     If (Server.Username = un and Server.Password =Pwd) then
        Collect the information Server.I of (un) and decrypt it, Server.I’
        Compare Server.I’ = I
        If true then
             Service allows the user (un) to access the Server [Primary Machine]
             Else
                 Prompt “This is not your allocated machine. Please Enter your mobile number to get temporary password”
                 Get the Mobile Number from the User
                 Send the Temporary Password
                 Allows accessing the server using Temporary Password [Secondary Machine]
                 Store the details in Server
                 Goto Step-7
             Goto Step-8
           Else
              Message “Invalid User”
        Else
        Goto Step-3
End If
Step-3: Fix the Size for the Information
I.Size = {LogID.Size, Drive.Size, RAM.Size,
        IP.Size, MAC.Size, Processor.Size}
Step-4: Process the Information with respect to I.Size
For m=0 to 5
        If I.Value[m].Size = I.Size[m] then
          I[m].Value = I[m].Value
        Else
          Balance = I.Size[m]-I.Value.Size[m]
           Append the dummy variable in the balance location of the variable
            I[m].Value = I[m].Value + dummy variable
        End If
        m++
        Next
End
Step-5: Encrypt the Information
Step-6: Service send the Encrypted Information to server
Step-7: Add the new user entry into the Server
Step-8: Check the Server IP which the client access
        If Server.IP found
Allow the client to access further without any interruption
Else
```

```
    Allow the client to have limited access by providing password at each and every refreshing
End If
End
```

3.2.1 *Algorithm Explanation*

The proposed algorithm thus validates the user through their basic information on the machine. The algorithm is explained in this section.

The first step of the algorithm is to gather the basic information from the user. Using the Username and password provided by the client, the service checks for validation. If the username found in the server, then match the password with that. If both of them match, then the user is treated as 'Existing User'. If the username not found in the server, then the user is considered to be as 'New User' and the record is created for that user as follows:

- Fix the size for the information.
- Get the values and alter the values with respect to size, by entering dummy values.
- Encrypt the values
- Make the entry into the server.

Thus the record can be created successfully for the new user.

When the user is found to be an existing user, then the information is obtained from the server, decrypts it and matches the resultant information with the information collected by the service. If both the information gets matched, then the user is "Valid Authenticated User and access the Allocated Primary Machine" and they are allowed to access the server.

If the information does not match, then the algorithm asks for the mobile number for the user by displaying the prompt, "This is not your allocated machine. Please Enter your mobile number to get temporary password". Then send the password to the mobile number. This temporary password is now used by the user to access the unallocated machine in an authenticated manner. Thus the user is "Valid Authenticated User and access the Secondary Machine".

If the server contains the username but the password doesn't match, then the user is treated as "Invalid User". The server blocks the invalid user to access the machine. Thus the Trusted Platform is provided to secure the information and to authenticate the user.

4. Analysis of Information

TPM is very useful to trust the valid user and to secure the information from unauthorized user and to block the information from unwanted access. Our proposed method performs well to safeguard the information and it is experimentally verified in various organizations such as IT Companies, Banking and so on. We implement our proposed algorithm in .Net by hiding the background application from unwanted access. The implementation performs well and it satisfies the aim of the paper by providing security among the information.

In Banking, each employee assigns a job and is provided with separate machine. On implementing our software, when they entering the machine for the first time, the service runs at the background of the connection between client and the server, gathers the information and it is processed as per our algorithm. The processed information can be saved into the server. On each time the employee enters into the system, the information is verified automatically and then allows them to access the system. If the verification fails, then the employee is blocked to access. Thus the sensitive information such as customer information, transaction details, Currency Details are all secured with our proposed TPM.

5. Conclusion and Future Enhancement

TPM's are a versatile tool that can be used in many industries. It can be used to secure online banking and E-commerce. The TPM can be used against hacking the information or any unwanted access on the system with or without networks. TPM's by their very nature are tools that uniquely identify the system. In addition as we have seen in this paper, TPM's by design are vulnerable to a variety of attacks and how the TPM prevent the sensitive information from unwanted access. Trusted Computing is a new technology that provides a unique approach to enhancing the security of a system. TPM provide harden security both on a local and on a network level. The TPM is one of the tools used to secure our machine and when it is implemented in an efficient way, it provides best result.

As a future enhancement MobileApp security feature can be designed and implemented to provide more security for Authenticated Trusted Platform.

6. References

1. Alshar'e MI, Sulaiman R, Mukhtar MR, Mohd Zin A. A user protection model for the trusted computing environment. Journal of Computer Science. 2014; 1692-1702.
2. Kinkelin H, Holz R, Niedermayer H, Mittelberger S, Carle G. On using TPM for secure identities in future home networks. Future Internet. 2011; 1-31.
3. Klenk A, Kinkelin H, Eunicke C, Carle G. Preventing identity theft with electronic identity cards and the trusted platform module. Proceedings of the 2nd European Workshop on System Security; 2009. p. 44-51.
4. Xiao Z, Yang Y. TPM main, Part 1, design principles, specification version 1.2, Level 2 revision 103. Trust Computing Group; 2007. p. 1-34.
5. Peng, S, Han Z. Trust of user using U-Key on trusted platform. Proceedings of the 8th International Conference on Signal Processing; 2006. p. 3023-6.
6. Kim R. Trusted platform module and privacy: promises and limitations. TCG Group; 2006. p. 1-14.
7. George P. User authentication with smart cards in trusted computing architecture. Proceedings of the International Conference on Security and Management; 2004. p. 25-31.
8. Camenisch J. Better privacy for trusted computing platforms. 2004; 3193:73-88.
9. Lampson BW. Computer security in the real world. Computer. 2004; 37(6):37-46.
10. Arbaugh B. Improving the TCPA Specification. Computer. 2002; 35(8):77-9.
11. Bajikar S. Trusted Platform Module (TPM) based Security on Notebook PCs-White Paper. TCG Publication; 2002. p. 23-36.
12. Jadhav Shital Suresh, Lee Jongkun. A TPM-based architecture to secure VANET. Indian Journal of Science and Technology. 2015; 8(15).
13. European Journal of Scientific Research. 2011; 58(1):6-10.