Mobile Trust Monitoring System (mTMS) for Securing Mobile Cloud Computing Environment

Mr. Pramod
Associate Professor CSE Department,
EPCET Bangalore, India

Dr. B. R. Prasad Babu
Professor & Head of Department, CSE
Department, EPCET, Bangalore, India

***Abstract*—: Security is a main concern in cloud enabled Smartphone. There are many ways to enhance security for Smartphone which are connected to cloud; one feasible sloution is to adopt hardware security in smartphone through TPM. TPM (Trusted Platform Module), is industry standard coordinated by Trusted computing Group (TCG) which facilitate to build trust cloud computing environment.TPM is a Cryotoprocessor which is designed to enhance security to devices such as Personal computer, laptop and smart phone. To reach a greater degree of security in cloud computing, TPM is used. The mTPM (mobile Trust Platform Module) which provides portable and secure cloud computing environment for portable devices connected to cloud.**

Keywords— Trusted Platform Module, Trusted Computing Group, Trusted Services, Cloud Computing, Mobile Computing

I. INTRODUCTION

Cloud computing is one of the hot topics today; it can the possibly change large parts of the IT industry [1]. More number of smartphone growing exponentially with technology, huge number of smart phones replacing personal computer to access cloud services because portability and compactness. Various application of the Smartphone's such as for web browsing; gaming etc.The major issues related to smartphones are battery life and computation overhead. One way to overcome this issue is to offloading computation to cloud environment [2]. The TPM chip is an industry standard specifcation [5], which provides hardware security to portable devices such as laptop and smartphones. It provides features such hardware encryption, secure key storage, machine authtication and attestation.

The TPM chip is invented to provide hardware security to portable devices such as laptop and smartphone which is conneted to cloud.

Many of current sytems in cloud makes use of authrorization protocals such as pass word authroication protocals PAKE and Kerberos and password authenticaion protocal (PAP).

The protocals mentioned above which require the system need to specify credentials such as password and user name and which require certain Cryptographic key to authorize. One major issue with these protacals is that it verfiy only the machine identifaction but no where verfication of state of machine is not done.

Portable devices such as laptop and smrtphone which need to connect to cloud which are need to protect from viruses.These devices corruped because of the software stack and viruses. Malicious programs on these machines can corrupt funcational behavior, even though credentials in the network are maintained. When these devices which try to connect to cloud, what mechanism are used to verify, to check whether the device which are connected to cloud are corrupted or not Table [3] below shows the top 10 obstacle and opportunity for development of cloud computing.

Obstacle	**Opportunity**
Availability/Business Continuity	Usage of Multiple Cloud Providers
Data Lock-In	Standardize APIs; compatible Software to enable Surge or Hybrid Cloud Computing
Data Confidentiality and Audit ability	Deploy Encryption, VLANs, Firewalls
Data Transfer Bottlenecks	Improved VM Support; Flash Memory; Gang Schedule VMs
Scalable Storage	Invent Scalable Store
Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs
Scaling Quickly	Invent Auto-Scalar that relies on ML; snapshots for Conservation

Reputation Fate Sharing	Offer reputation-guarding services like those for email
Software Licensing	Pay-for-use licenses

To verify the state of machine, TPM solution is used, which in turn measure the system integrity and uses protocals to authorize, before access the services of cloud.

To track the software changes, trust computing is used. Portable devices such as laptop or smartphone have built in TPM chip on their mother board. The TPM which is mainly used to facilitate the data storage in secure way, and also measuring in a secured way the software components and at device booting the configration of hardware. To addition to this key migration, data encryption and decryption and for key attestion and signing measurements

II RELATED WORK

TPM Components

The components of TPM chip comprises of cryptographic processor, persistent memory and versatile memory. Figure 1 below show the various components inside the TPM

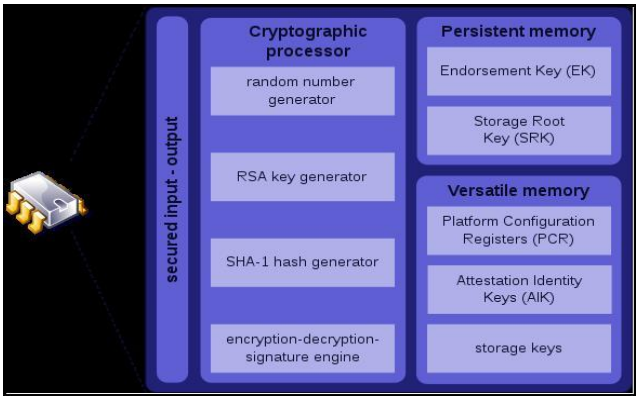

Figure 1: TPM Chip

TPM takes care of Confidentiality, Authentication and Integrity.

Confidentiality, Integrity and Authentication are taken care by the TPM.

Confidentiality: The TPM which provides the Hardware enabled cryptography, which can protect the information against software attacks and data can need to flow through the proper authorization channel.

Authentication: The TPM provides secure channel for keys ,certificates and Password within the enterprise network for smart phones users .Hence it eliminate the need of special token.

Platform Integrity: In TPM, various reports and measuures to check integrity of platform which includes disk, BIOS, Operting system ,MBR(Master boot record) and various application software which ensure that no changes unauthorizly have occurred.

To faciliate the harware based apporoach to manage the access to cloud and authentication of users a secure cryptographic enabled TPM chip is used.

Authentication and Authorization of Data in TCG TPM

TPM stores sensitive information and keys related to cryptogrphic within its sheiled memory. The keys within TPM are stored in hirecharial manner; with its root is storage rootkey. Every key has authdata and password to authorize the data. A malicious user who had authdata can forgery all the TPM storage capabilities. The protocal such as OSAP and OIAP which can provide only integrity of message but fail to achive the confidentiality. SKAP [6] which promises to provide solution to both integrity and confidentility issues.

The TPM offers commands, to create storage Root Key (SRK) for TPM Ownership, and to create child key for already existing key, TPM_CreateWrapkey. The TPM_Loadkey2 is used for loading purpose. The TPM_CertifyKey (represents the key to be certified).These commands which provides authentication mechanisms.

Data Security of Cloud Storage by TPM

The big conern in cloud computing is security. During data storage in cloud these security threats are inevitable and also during data in transit and seperation between the consumers. To overcome these issues Trust computing platform (TCP) along with TPM concentrate on security issues in cloud computing. Which in turn more focus on CIA, Confidentiality, Integrity and Authentication?

Mobile Clouds

Mobile Trust Platform Module which provides a solution for secure and portable cloud environment.In smartphone , TPM is bounded to VM, and these specification defined by Trust Computing Group(TCG).The main aim of TPM is to comibing smartphone and TPM[7].

With mTPM enabled smartphone, it provides mobile Core Root of Trust (mCRT), which is in turn encrypted with virtual machine, Symetric key and mTPM[8].

The mCRT is able access the Host TPM VM and mTPM, which makes it imposible to any disclosure of data when mTPM is lost. To monitor the status of security, mTMS (Mobile trust monitoring system) is used. mTMS which reocrds PCR values and Identification of user group. TPM has benefit of sharing digital form between the smartphone devices

III ADVANTAGES OF TPM

TPM having many features to protect the privacy of users. Many of the IC vendors have manufactred TPM Chip, which

have TPM on board of smartphone and laptop. The main advantage of TPM which offers cryptographic functionality, which also includes the Encryption, key generation, hashing and digital signature. It securly stores the root of trust passwords and keys. TPM also includes unique RSA public key which 2048 bit private key pair. The key creation happens during time of manufacting.

IV PROPOSED SOLUTION

Intially smartphone booted with software stack, which is need to measure and later placed in the PCR(Platform configurable Register). The Fig 2 show below, cloud server keeps track of all only PCR valid values and compares them with measurements which it reads from the smartphone.

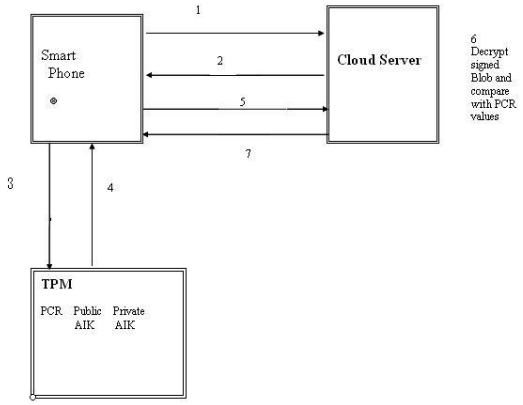

Fig 2: Cloud Server Verify the TPM enabled smart phone.

The cloud server makes sure that smartphone sending only the value of its current state and not the oldboot measurement taken at previous attempt in time. If the smartphone is sending PCR hash, then cloud server is no where detect the client is not reply its previous values.This is also referred as replay attack.

The various stpes involved between smart phone enabled TPM and Cloud Server.

Step 1: Smart phone intially contact the Cloud Server to verify its state.

Step 2: In this step, Cloud server is able to generate new nonce value and it challenges the TPM enabled smartphone with new nonce value.

Step 3: TPM embeded with smartphone on receving nonce, in turn call Tspi_TPM-Quote ( ) procedure, which will generate bit map value for select PCR. Finally it appends nonce with list of PCR values.

Step 4 : Hash is applied on all appended PCR values by means of SHA -1 and then sigend with public AIK , which is present within the TPM chip

Step 5 : In this step , TPM enalbed smartphone sends public AIK half part to cloud server and blob of bits which are signed into the cloud server thorugh secure channel.Cloud server verifies whether that AIK from
TPM which is genuine.

Step 6: In this step, Decrypttion of signed blob will occour and comparing that value with valid PCR values.

Step 7: Finally, Cloud Server do the comparision of blob of bits which are decryted with whole set of PCR values which are valid, then it checks whether it is valid message or invalid message to TPM embedded in smartphone.

V CONCLUSION AND FUTURE WORK

This paper, focus on providing hardware enabled security to portable devices with the help of TPM tamper proof chip. There are various features and real time applications of TPM chip which is enlisted by author. The major concern is security in Mobile Cloud Computing. Proposed solution along with TPM will be emerging as one of the powerful security tool for increasing security measures in mobile cloud computing..

REFERENCES

[1] http://queue.acm.org/detail.cfm?id=1721672
[2] https://www.cs.purdue.edu/homes/bb/mobile-cloud-survey.pdf
[3] http://delivery.acm.org/10.1145/1730000/1721672
[4] Trusted Computing Group.TPM specification
[5] Dimitrios Zissis and Dimitrios Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems Vol. 28, No. 3, pp. 583–592, March 2012. Version 1.2 Part 1-3 www.trustcomputinggroup.org/specs/TPM/
[6] Stephanie Delanuae, Steve Kremer school of computer science University of Birmingham ―A Formal analysis of Authentication in the TPM‖ International Journal of Soft Computing and Engineering(IJSCE)ISSN:2277 77128X, Volume 3, Issue 4,April 2013.
[7] TCG mobile phone work group. https:/www.trustedcomputinggroup.org/groups/TCG-1-0-Archicture Overview.pdf
[8] Jesus Molina,Houching Sung Lee Lee,Zhexuan Song ―A Mobile Trusted Module Architecture‖8400 Baltimore Avenue, Suite 302 College Park,Maryland 20740, USA.
[9] Safford, D., Yoder, K., Chatherman, R., Safford, D.,Van Doorn, L. A Guide to Trusted Computing. IBM Press. 2008.