Trusted Platform Module for Security in Cloud Computing

Ms. Poojashree.
B.E. Student Department of IS&E,
BMS Institute of Technology & Management
Yelahanka,Bangalore -560064, Karnataka.

H. S Ms. Navitha Kumar
B.E. Student Department of IS&E
BMS Institute of Technology & Management,
Yelahanka,Bangalore -560064, Karnataka,

Mrs. Swetha M.S[3]
Assistant Professor, Department of IS&E
BMS Institute of Technology & Management
Yelahanka,Bangalore -560064, Karnataka.

Mr. Muneshwara M.S[4]
Assistant Professor, Department of CS&E,
BMS Institute of Technology & Management,
Yelahanka,Bangalore -560064, Karnataka.

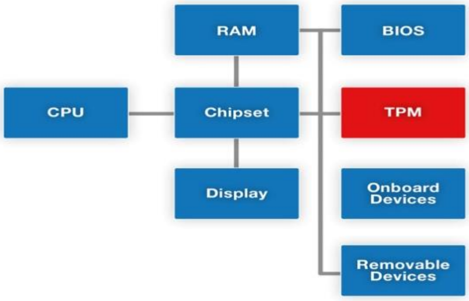
***Abstract*:- This paper studies the possibility of using TCG (Trusted Computing Group) specifications to establish trust in Cloud Computing, especially between the provider of Cloud Computing infrastructures and his customers. The first part describes the context and the motivations that led to TCG specifications. The second part describes the architecture, the functions and the properties of TPM (Trusted Platform Module) which is the root of trust in TCG. The last part analyses several approaches to adapt TPM in order to build trust in Cloud computing.**

***Keywords: Cloud Computing, Virtualized Networks, Security, Trusted Computing, Trusted Platform Module*.**

1. INTRODUCTION

Cloud Computing brings new security paradigms and challenges, since physical platforms are shared by several entities.The physical platform owner is responsible for the isolation of the services and applications hosted by the physical platform.A Cloud customer may need some assurance or trust on the state and configuration of the physical platform before installing his services on it. The trust of the physical platform may be measured by some indicators that should be available at any time. The measurements must be reliable and trustworthy. The physical platform provider may also need to measure the trust of the applications he hosts. All trust indicators are provided by the physical platform. The integrity and the trust on these indicators cannot be guaranteed without the help of a trusted hardware component (tamper-resistant). A common intuitive assumption states that ”software alone could never be completely secure if it is not assisted with hardware”.

This is the reason why Trusted Computing Group (TCG) has specified the Trusted Platform Module (TPM). Currently, theTPM is the only standardized physical device to measure trust indicators in open platforms such as PCs. This paper analyzes the state of the art regarding Cloud Computing security based on Trusted Computing Group concepts. We describe the objectives, principles and concepts of the Trusted Computing Group (TCG). The third part of the document describes theTrusted Platform Module (TPM) which is a hardware tamperresistant component that makes TCG concepts feasible. In the last part, we analyze research approaches aiming to virtualize the TPM in order to bring a new security enabler in Cloud Computing environments.



2. THE TRUSTED COMPUTING GROUP

The Trusted Computing Group (TCG) is a consortium of semiconductor manufacturers and computer actors which exists since 2000 under the name of Trusted Computing Platform Alliance (TCPA). This consortium is composed of three member categories: Promoters, Contributors and Adaptors. Promoters are mainly industrials and manufacturers. TheTCG first main goal was to specify a hardware component,the Trusted Platform Module (TPM) to, essentially, handledigital rights management (DRM). The scope of TCG has been extended, progressively, to many fields such as:

- Mobile phone;
- Authentication;
- Infrastructure;
- PC security;

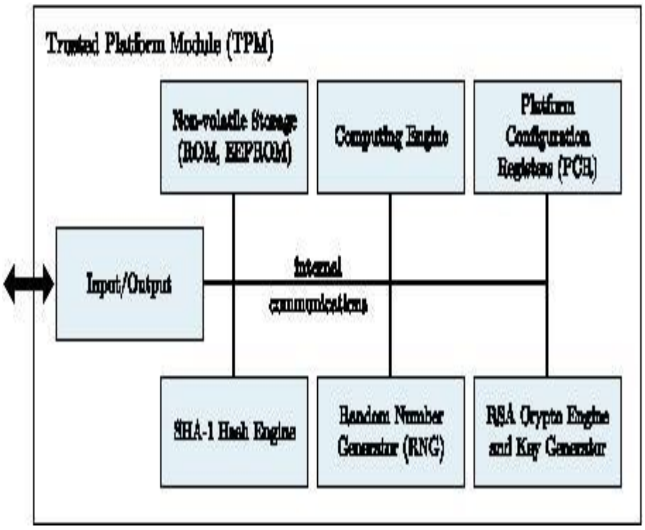
- Storage;
- Trust of the nodes within a network.

TCG has created, in 2010, a new working group Trusted Multi-Tenant Infrastructure to develop security standards, based on the existing TCG specifications, to meet Cloud Computing security needs. TCG work addresses security of open platforms such as personal PCs. It does not address security of closed systems such as SIM cards. TCG definition of trust in computer environment is ”An entity can be trusted if it always behaves in the expected manner for the intended purpose.”

This definition does not mean that a trusted computer has a good or honest behavior. It means that the trusted computer will not change its behavior over the time. The first approach TPM 1.1 - February 2002 was criticized for privacy issues since it links users to their specific platforms even if they use pseudonymous machine credentials. In response to criticisms, TCG specifications evolved to TPM 1.2 2007 which uses a zero-knowledge mechanism to prevent linking pseudonymous machine credentials to the physical platform. While it is possible to ensure privacy when needed, this latter approach prevents usage of rogue TPMs. TCG specifications are freely available and have been adopted as standards by the ISO/IEC Personalization of TPM is similar to smart card personalization; each TPM is provided with its own specific keys. If one TPM is compromised, other existing TPMs will not be compromised. It will not be possible to create other trustable TPMs except by producing several copies of the compromised TPM. This threat is not considered as critical.

3. THE TRUSTED PLATFORM MODULE :

The TPM is a hardware component which becomes part of professional PC motherboard. TPM may be compared to smart cards since it securely stores sensitive cryptographic keys. Some of these keys never leave the TPM. It is also able to compute some cryptographic primitives such as digital signatures and session keys, etc. The TPM is a slave; it does not initiate any action. It is not possible to upload any software in it. Like smart cards, it responds to specific commands. However, a smart card protects only its internal environment against the external world without providing any means to secure external data. In contrast, TPM does both aspects. It protects its internal environment and provides functions to secure external data.


Trusted Platform Module (TPM)
Non-volatile Storage (ROM, EEPROM)
Computing Engine
Platform Configuration Registers (PCR)
Input/Output
internal communications
SHA-1 Hash Engine
Random Number Generator (RNG)
RSA Crypto Engine and Key Generator

1.Assumptions on the root of trust

Some components of the architecture described in figure 1 have to be trustworthy. Misbehaviour of one of them is difficult to detect. In a PC environment, TCG assumes that the following components are trusted: • TPM, • CRTM, Core Root of Trust Module. It is a relatively small code that is executed first when the platform is powered on. It may be a part of BIOS. This code measures the hardware configuration and the integrity of the BIOS,

- CPU since it is the element that executes the CRTM code,
- The BUSes (data and address),
- The controllers (Northbridge and Southbridge),
- RAM,
- The keyboard.

Let us recall that, as mentioned earlier, breaking one platform by succeeding to access to keys stored in its TPM does not corrupt other platforms since these keys are personalized. It is though possible to duplicate a corrupted platform.

2.TPM Internal Architecture:

The I/O block is the interface to LPC bus that connects the TPM to external world. The logic of access control is enforced in this block. The cryptographic co-processor computes at least RSA encryption/decryption, SHA-1 hash algorithm, key generation, and random number generation. RSA may be used for both encryption and digital signature for key sizes 512 to 2024 bits. Symmetric encryption is also supported to provide confidentiality for data stored outside TPM and transport sessions. Other traditional cryptographic functions are supported such as RSA key generation and HMAC computation.

1)The Power Detection function: Monitors the power supply changes. In fact some attacks are based on changing the voltage and/or states of the power.The Opt-In mechanism allows the TPM to be enabled/disabled. The Non-Volatile Memory stores cryptographic keys and states used by the TPM to ensure its security.

2) Attestation: Attestation provided by an entity is a proof of specific data knowledge by that entity. It is usually associated with a digital signature. TCG uses this functionality to prove to a remote entity (e.g. service provider) that a platform wishing to access to the service meets specific integrity requirements. The attestation may be related to hardware or software integrity.

3) Measurements, Logging and Reporting: The measurement is the process of computing a state indicator of hardware and/or software. It may be a hash for a software code. If the measurement is reliable, it gives information on the integrity of the measured entity. The measuring entity must be trustable in order to obtain reliable measurements. TCG defines a module called CRTM (Core Root of Trust for Measurement) which is assumed to be trustable. It is executed when the platform is powered on. Some of the measurement results may be stored in PCRs. Other measurement results may be logged outside the TPM in order to interpret them later. TCG defines reporting as a process of attesting the values stored in PCRs.

A measure, related to an entity, stored in a PCR does not mean that the corresponding entity is an entity of integrity. An outside process should take the decision on the integrity and the opportunity to launch adequate actions when receiving PCR content. It may be done at application level. This approach is compatible with applications managing DRMs. It is also suitable for an open platform composed of different software, provided by independent entities, which need to be updated. The entity wishing to verify the integrity of an application binary code requests the value of a corresponding PCR and compares it to the MAC (Message Authentication Value) of the expected version application code.

3.Chain of Trust of a Platform Containing a TPM:

Five types of credentials were defined by TCG to establish some kind of chain of trust. It is up to the verifier to check the content of these credentials and to decide if they meet his security requirements.

1) Validation Credential: This credential will provide a digital signature related to some sensitive platform components. It may be computed by the component manufacturer or a trusted third party. It points to measurable components including hardware and software such as disk storage adapters, memory controllers, processor, keyboard driver etc. The Validation Credential may be common to same models of components. It is not privacy sensitive. The Validation Credential will provide information such as: component type, manufacturer, model, version, digest, Validation Entity and the signature of the Validation Entity. Each sensitive component is provided with its own Validation Component

2) Endorsement Credential: The Endorsement Credential is related to the platform TPM. It is normally signed by the TPM manufacturer when generating Endorsement Key (EK key pair). This credential includes: the identifier of TPM manufacturer, TPM version and serial number and the public key pair of EK. It is digitally signed by the TPM manufacturer or by the entity generating the EK. The public part of EK is privacy sensitive since it would be possible to track platform transactions if the cryptographic keys used by that platform are linked to EK.

3) Conformance Credential: A Conformance Credential is related to its critical elements such as TPM, processors, display adapter and keyboard driver. Other elements may require being included in Conformance Credential depending on the applications. This Credential is linked to a set of platforms of the same model and make; it is not privacy sensitive. It is possible to establish separate Conformance Credential for each sensitive element of the platform. The Conformance Credential is issued and digitally signed by a skilled entity that is able to evaluate platform adapted to TPM. Information contained in the Conformance Credential may include platform model, the manufacturer name, TPM model, TPM manufacturer, processor model, the evaluator name etc.

4) Platform Credential: The platform credential aims at providing the possibility to verify the platform integrity. It contains information related to the manufacturer, the platform model, the endorsement credential (TPM with EK key pair) and the Conformance Credentials. In opposition to Conformance Credential which is shared among a set of platforms, the Platform Credential is unique to a single platform. It is then privacy sensitive.

5) Attestation Identity Credential: The Attestation Identity Credential is a kind of a certificate binding Attestation Identity Key pair (AIK) to a specific platform containing an authentic TPM. AIK is used by the TPM to sign PCR content. It is issued by a trusted third party that is able to verify all or some credentials described above. Attestation Identity Credential is privacy sensitive; the issuer should take care of not linking AIK to EK. By signing Attestation Identity Credential, the trusted third party guarantees that:

- The TPM is authentic;
- AIK is stored in the TPM;
- The platform and TPM are valid.

4. TYPES OF SECURE MESSAGES EXCHANGEABLE WITH TPM:

The world outside the platform can communicate with the platform's TPM using messages that cannot be altered, without detection, by any entity including the platform where the TPM resides. Four message types were defined by TCG:

• Binding this message type uses a TPM public key related to a non-migratable private key stored in TPM. It gives the assurance to the sender that the message will be disclosed by the targeted TPM only. The platform containing TPM will not be able to decrypt it.

• Signing signing messages in TCG environment are equivalent to those of traditional cryptography. Some keys managed by TPM are unambiguously reserved for signing. They cannot be misused for encryption.

• Sealed-Binding this message type is used by an external entity to send some sensitive information to the platform through TPM. TPM will disclose this information to the platform if the platform is under some configurations. The external entity uses a non-migratable public key of the TPM to send an encrypted message containing sealed information and the expected values of some PCRs. If the platform configuration meets PCR values indicated by the sender, TPM decrypts the information and transmits it to the platform. The information type is in general a session symmetric key that the platform uses to decrypt protected contents. Here is an example of how Sealed-Binding may be used: a user downloads an encrypted content from a server. The service provider sends, to the TPM of the user, a message containing some requirements regarding the platform configuration as well as the symmetric key needed to decrypt the downloaded content. TPM compares PCR values stored inside its memory to those required by the service provider. If they match, TPM decrypts and transmits the symmetric key to the user platform. This principle will guarantee to the service provider that its contents are accessed only by platforms meeting some security requirements.

• Sealed-Signing this message type allows an external entity to request the TPM to provide the configuration state of some platform elements during the signature process. Configuration measurements are executed and the results are encrypted, signed and sent by the TPM to the requesting entity. The signature is based on a TPM non-migratable asymmetric key. The difference between Sealed-Binding and Sealed-Signing resides in the freshness of the configuration measurements and the decision point element. The Sealed-Binding takes into account the values of PCRs as they are stored in the TPM and the decision point is the TPM. The Sealed-Signing mandates new measurements at the time of signing. The decision point is the entity that requests the Sealed-Signature.

5. KEY MANAGEMENT:

Seven key types were defined by TCG. These keys may be classified into four categories:

• Keys that are non-migratable and should never leave internal TPM memory. Endorsement Key and Storage Root Key are the two key types of this group.

• Keys that are non-migratable but may be stored in encrypted format outside TPM memory. Keys used for Binding and/or Sealing are included in this group.

• Keys which are migratable from one platform to another platform. Signing and Storing keys are among those keys. Legacy keys are always migratable.

• Keys that may be migratable or non-migratable from one platform to another platform. Signing keys and Storage keys form this group.

Since TPM operates as a slave, the platform needs to include a software interface to manage storage of keys outside TPM. TCG calls this interface Key Cache Manager. The keys stored outside TPM are encrypted and constitute a hierarchy of keys; the Storage Root Key (SRK) is stored in the TPM. All key types may be stored outside TPM except Endorsement Key and Storage Root Key. Confusion among migratable keys and keys stored outside TPM should not be made. For example an AIK (an Attestation Identity Key) may be stored outside the TPM but it never migrates from one platform to another platform.

IV. VIRTUALIZATION OF THE TPM FUNCTIONALITIES

The complexity of TPM virtualization is related to the fact that a platform contains a single TPM and that a TPM has a single owner. In a virtualized environment, each virtual machine may need its own TPM. Moreover, the associated platform components described in section III also need to be virtualized securely like the CRTM, display controller, etc. The TPM security-sensitive functionalities and information that need to be studied carefully in virtualized environment are those residing in TPM hardware. The sensitive functionalities include cryptographic primitives and the sensitive data stored in TPM are Endorsement Keys and Storage Root Key. Some other sensitive data may be stored outside TPM in encrypted format. In what follows, we analyse some significant existing approaches. IBM researchers proposed TPM virtualization as shown in figure 3. This approach is based on certificate chain linking virtual TPMs (vTPMs) to the physical TPM. vTPMs are located in a specific layer over the hypervisor. A vTPM instance is created per a virtual machine by vTPM Manager. The vTPM Manager is built in a specific VM (Virtual Machine) that multiplexes communications between VM and vTPMsA virtual machine may invoke its own vTPM through the hypervisor. New communication protocol is defined between VMs and vTPMs. OSs, installed over VM, should be aware of the presence of this protocol. This is a drawback of this solution since vTPM concept is not transparent to OSs and applications running in VMs. The feasibility of vTPM was verified on Xen machine .Many research activities on virtualization security using virtual TPM refer to the IBM approach.

In authors proposed trust architecture based on virtualization. The trust is based on a third party that certifies the integrity of the software installed in a platform A. Time stamped attestation is delivered to platform A in order to prove that it is trustworthy without revealing any information on the software running on it. Virtualization is used to isolate different applications running on the same physical platform. A set of applications is provided with its own virtual TPM (vTPM). The authors argue that this approach is less complex than TCG approach. While TPM provides measurements for all components of the platform, vTPM measures only application software of VM. Two types of VM were defined, open VM and Trusted VM with a vTPM. Surprisingly, the Management VM which is responsible for creating VMs, is not provided with a vTPM. All vTPMs are bound to the physical TPM. The virtualization architecture is a traditional one where the hypervisor Trusted Virtual Machine Monitor (TVMM) is assumed to be trustworthy. TVMM supports necessary interface functions for secure binding vTPMs to physical TPM. It provides also attestation regarding the state of underlying hardware and software. This approach does not provide means to verify the configuration of the VM operation system (OS) since vTPM will provide only measurements of applications installed over a trusted VM. If OS of the trusted VM is corrupted, the associated vTPM will not help to detect VM misbehavior.

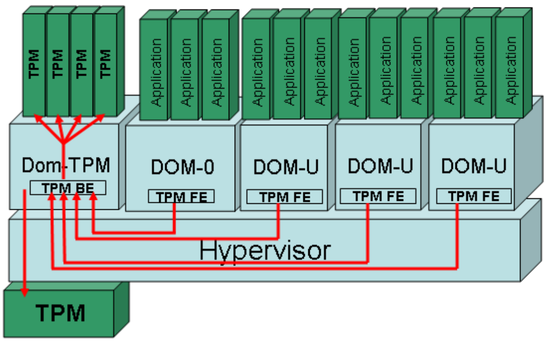
Propose to use vTPM work to secure IBM's Trusted Virtual Datacenter (TVDc). They have specified a new hypervisor sHype which is a modified Xen hypervisor that implements a software component called Access Control Module (ACM). ACM controls inter-VM communication and virtual resources shared by VMs as well as access of VMs to physical resources. A specific VM is dedicated to management (Management VM). It stores Access Control Policy related to each VM and global policy which defines the isolation principles of VMs. sHype consults this policy to decide what resources a VM can access to or to which entity it may communicate. Management VM contains also vTPMs.

proposed a security model for Cloud Computing called Private Virtual Infrastructure (PVI) for Infrastructure as a Service (IaaS). This proposal suggests sharing security responsibility between the cloud service provider and the client. It is based on some principles such as Service Level Agreement guaranteed by the service provider to establish security primitives needed to construct secure VM. Authors make the following assumptions:

- Availability of some measurements equivalent to those defined by TCG in order to verify the configuration of the physical infrastructure;

- Presence of secure provisioning interface under the responsibility of the customer;

- Availability of secure shutdown and destruction of virtual devices.



A special VM called LoBot (Local Bot) is installed first. This VM measures the trust of the Infrastructure; precisely the trust measurement is related to a platform that will host the VM. If the measurements are satisfactory, the customer installs the associated effective VM. Each VM is associated to a specific LoBot. The measurement is based on TCG specifications; it assumes that the infrastructure contains a physical TPM. LoBot includes a virtual TPM (vTPM) bound to the physical TPM. The description of this solution is a high level one; it does not provide details on how the vTPM is provisioned. Besides, management of cryptographic keys is not described. TVEM (Trusted Virtual Environment Module) to build a root of trust for a customer and the service provider. This root of trust is obtained by combining the trust from the physical platform owner and the trust from the customer. TVEM is a software appliance equivalent to vTPM where both the service provider and the customer cooperate for its creation.

As in this paper is a high level description; the authors did not mention any feasibility validation of concept related to their work. on the trust deployment in a physical node shared by several entities. This approach is derived from the Trusted Computing Group specifications, to bring trust within Virtualized Networks defined in the European project 4WARD.Chain of trust is established from the root of trust to high level applications. This solution does not provide a virtual TPM to each entity sharing the physical node.

V. CONCLUSION

Although the TPM design was at the origin, targeting DRM applications, various fields of information technology, including Cloud Computing, start to study its adaptation to their security needs. At the moment, TPM is the only tamper resistant device implemented in open physical platforms such as the PC. Original TCG specifications assume a single TPM owner who is the owner of the physical platform. Cloud computing brings new paradigm and new security challenges which are not covered by the present TCG specifications. Some additional functionality are needed. We have analyzed the literature approaches adapting TPM to virtualization and Cloud Computing. Those approaches are not mature yet. We believe that some research is still needed to make the extension of TCG specifications transparent to virtual machines. Future work may focus on the following topics:

- Transparency of the extensions of TCG specifications needed to meet Cloud Computing security requirements.

- Evaluation of emerging industrial solutions using TPM to establish trust in Cloud Computing services.

ACKNOWLEDGEMENT

The authors would like to thank the editor and reviewers for their priceless suggestions that appreciably improved the eminence of this paper.
I heartily thank to Principal, *BMS Institute of Technology &Management,Yelahanka ,Bangalore -560064, Karnataka*

and HOD Department of CSE and ISE*Management*,affiliated to *VTU,Karnataka, INDIA.*

Last but not least to all of them who helped to get a warm success in completion of this paper?

AUTHOR(S) PROFILE

Ms.Poojashree H S is a student of 6th sem studying in the Department of Information Science and Technology and Engineering at BMS Institute of Technology &Management, Bangalore, affiliated to VisvesvarayaTechnological University, KARNATAKA, INDIA.

Ms.Navitha Kumar is a student of 6th sem studying in the Department of Information Science and Technology and Engineering at BMS Institute of Technology &Management,Bangalore,affiliated to Visvesvaraya Technological University, KARNATAKA, INDIA.

Mr. Muneshwara M.S is an Assistant Professor in the Department of Computer Science and Engineering at BMS Institute of Technology &Management, Bangalore, affiliated to VisvesvarayaTechnological University, KARNATAKA, INDIA He has Completed M. Tech in Computer Science &Engineering Branch & B.E. Degree in Information Science & Engineering Branch from VisvesvarayaTechnological University, Belgaum, KARNATAKA, INDIA. He has around 9 years of experience in teaching.

Mrs. Swetha M.S is an Assistant Professor in the Department of Information Science and Engineering at BMS Institute of Technology & Management, Bangalore, affiliated to Visvesvaray Technological University, KARNATAKA, INDIA. She has Completed M. Tech in Computer Science & Engineering Branch Visvesvaraya Technological University, KARNATAKA. &B.E.Degree in Computer Science & Engineering Branch from Visvesvaraya Technological University, KARNATAKA and She has around 7 years of experience in teaching.

REFERENCES

[1] TCG, “TCPA Main Specification Version 1.1b,” Trusted Platform Mod-ule - Trusted Computing Group, Feb. 2002.

[2] ——, “TPM Main Specification Level 2 Version 1.2, Revision 103,”TCG Trusted Platform Module - Trusted Computing Group, Jul. 2007.

[3] ISO, “Trusted Platform Module-Part 1: Overview,” ISO/IEC 11889-1:2009 Information technology - International Organization for Stan-dardization, 2009.

[4] ——, “Trusted Platform Module-Part 2: Design principles,” ISO/IEC11889-2:2009 Information technology - International Organization for Standardization, 2009.

[5] ——, “Trusted Platform Module-Part 3: Structures,” ISO/IEC 11889-3:2009 Information technology - International Organization for Stan- dardization, 2009.

[6] ——, “Trusted Platform Module-Part 4: Commands,” ISO/IEC 11889-4:2009 Information technology - International Organization for Stan- dardization, 2009.

[7] TCG, “TCG Specification - Architecture Overview. Specification Revi-sion 1.4,” TCG Work In Progress - Trusted Computing Group, 2007.

[8] H. Krawczyk, M. Bellare, and R. Canetti, “HMAC: Keyed-Hashing forMessage Authentication,” IETF RFC. status: informational, Feb. 1997.

[9] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, and ´L. van Doorn, “vTPM: virtualizing the trusted platform module,” inProceedings of the 15th conference on USENIX Security Symposium - Volume 15. Berkeley, CA, USA: USENIX Association, 2006.

[10] F. Stumpf, M. Benz, M. Hermanowski, and C. Eckert, “An Approachto a Trustworthy System Architecture UsingVirtualization,” in 4thInternational Conference on Autonomic and Trusted Computing(ATC),2007, pp. 191–202.[11] S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, ´W. Schildhauer, and D. Srinivasan, “TVDc: managing security in thetrusted virtual datacenter,” SIGOPS Oper. Syst. Rev., vol. 42, pp. 40–47, Jan. 2008.

[12] F. J. Krautheim, “Private virtual infrastructure for cloud computing,” inProceedings of the 2009 conference on Hot topics in cloud computing,ser. HotCloud’09. Berkeley, CA, USA: USENIX Association, 2009,pp. 5–5.

[13] F. J. Krautheim, D. S. Phatak, and A. T. Sherman, “Introducing thetrusted virtual environment module: a new mechanism for rooting trust incloud computing,” in Proceedings of the 3rd international conference onTrust and trustworthy computing, ser. TRUST’10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 211–227.

[14] M. Achemlal, J.-C. Pailles, and C. Gaber, “Building trust in virtualized[9] S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, “vTPM: virtualizing the trusted platform module,” in Proceedings of the 15th conference on USENIX Security Symposium Volume 15. Berkeley, CA, USA: USENIX Association, 2006.networks,” in 2nd International Conference on Evolving Internet, Sep.2010.