ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

Affording User Security Assurances in Public Infrastructure Clouds

G.Ranjitha[1], Dr.V.Ravikumar[2]
[1] Master of engineering student,[2]Head of the Department,
[1,2]Department of Computer Science & Engineering, Maha Barathi Engineering College, Chinnasalem, Tamilnadu, India
ranjithamanirathinam@gmail.com

Abstract: *The infrastructure cloud (IaaS) service model offers improved resource flexibility and availability, where tenants – insulated from the minutiae of hardware maintenance – rent computing resources to deploy and operate complex systems. Large-scale services running on IaaS platforms demonstrate the viability of this model; nevertheless, many organizations operating on sensitive data avoid migrating operations to IaaS platforms due to security concerns. In this paper, we describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. We continue with an extensive theoretical analysis with proofs about protocol resistance against attacks in the defined threat model. The protocols allow trust to be established by remotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality of data in remote storage, with encryption keys maintained outside of the IaaS domain. Presented experimental results demonstrate the validity and efficiency of the proposed protocols. The framework prototype was implemented on a test bed operating a public electronic health record system, showing that the proposed protocols can be integrated into existing cloud environments.*

Keywords: *Infrastructure cloud, Trusted launch of virtual machines, Domain-based storage protection, Large-scale services, protocols.*

I. Introduction

Cloud computing has progressed from a bold vision to massive deployments in various application domains. However, the complexity of technology underlying cloud computing introduces novel security risks and challenges. Threats and mitigation techniques for the IaaS model have been under intensive scrutiny in recent years. While providers may offer security enhancements such as protection of data at rest, end-users have limited or no control over such mechanisms. There is a clear need for usable and cost-effective cloud platform security mechanisms suitable for organizations that rely on cloud infrastructure[1].

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation[2.] Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

There are two major improvement vectors regarding these implementations. First, details of such proprietary solutions are not disclosed and can thus not be implemented and improved by other cloud platforms. Second, to the best of our knowledge, none of the solutions provides cloud tenants a proof regarding the integrity of compute hosts supporting their slice of the cloud infrastructure. To address this, we propose a set of protocols for trusted launch of virtual machines (VM) in IaaS, which provide tenants with a proof that the requested VM instances were launched on a host with an expected software stack[3,4].We focus on the Infrastructure-as-a-Service model – in a simplified form, it exposes to its tenants a coherent platform supported by compute hosts which operate VM guests that communicate through a virtual network. The system model chosen for this paper is based on requirements identified while migrating a currently deployed, distributed electronic health record (EHR) system to an IaaS platform [5].

II. Existing System

One such mechanism is platform integrity verification for compute hosts that support the virtualized cloud infrastructure. Several large cloud vendors have signaled practical implementations of this mechanism, primarily to protect the cloud infrastructure from insider threats and advanced persistent threats.

We see two major improvement vectors regarding these implementations. First, details of such proprietary solutions are not disclosed and can thus not be implemented and improved by other cloud platforms. Second, to the best of our knowledge, none of the solutions provides cloud tenants a proof regarding the integrity of compute hosts supporting their slice of the cloud infrastructure.

To address this, we propose a set of protocols for trusted launch of virtual machines (VM) in IaaS, which provide tenants with a proof that the requested VM instances were launched on a host with an expected software stack .

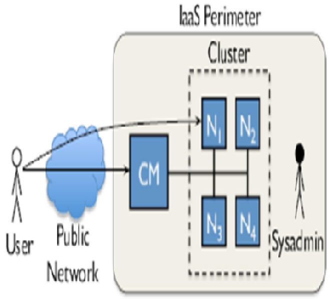
III. Proposed System

In this proposed system a “Trusted Cloud Compute Platform”(TCCP) to ensure VMs are running on a trusted hardware and software stack on a remote and initially untrusted host. To enable this, a trusted coordinator stores the list of attested hosts that run a “trusted virtual machine monitor” which can securely run the client’s VM.

Trusted hosts maintain in memory an individual trusted key use for identification each time a client launches a VM. The paper presents a good initial set of ideas for trusted VM launch and migration, in particular the use of a trusted coordinator. A limitation of this solution is that the trusted coordinator maintains information about all hosts deployed on the IaaS platform, making it a valuable target to an adversary who attempts to expose the public IaaS provider to privacy attacks host, beyond the initial launch arguments.

A decentralized approach to integrity attestation is adopted by Schiffmanetal. To address the limited transparency of IaaS platforms and scalability limits imposed by third party integrity attestation mechanisms. The authors describe a trusted architecture where tenants verify the integrity of IaaS hosts through a trusted cloud verifier proxy placed in the cloud provider domain. Tenants evaluate the cloud verifier integrity, which in turn attests the hosts. Once the VM image has been verified by the host and countersigned by the cloud verifier, the tenant can allow the launch.

IV. System Architecture



Advantages of the system:

- A domain-based storage protection protocol to allow domain managers store encrypted data volumes partitioned according to administrative domains.
- A list of attacks applicable to IaaS environments and use them to develop protocols with desired security properties, perform their security analysis and prove their resistance against the attacks.
- The implementation of the proposed protocols on an open-source cloud platform and present extensive experimental results that demonstrate their practicality and efficiency.

V. Protocols

Trusted Platform Module (TPM): a hardware cryptographic co-processor following specifications of the Trusted Computing Group (TCG) ; we assume CH are equipped with a TPM . The tamper-evident property facilitates monitoring CH integrity and strengthens the assumption of physical security. An active TPM records the platform boot time software state and stores it as a list of hashes in platform configuration registers (PCRs). TPM has 16 PCRs reserved for static measurements (PCR0 - PCR15), cleared upon a hard reboot. Additional runtime resettable registers (PCR16-PCR23) are available for dynamic measurements. Endorsement keys are an asymmetric key pair stored inside the TPM in the trusted platform supply chain, used to create an endorsement credential signed by the TPM vendor to certify the TPM specification compliance. A message encrypted (“bound”) using a TPM’s public key is decryptable only with the private key of the same TPM. Sealing is a special case of binding –

bound messages are only decryptable in the platform state defined by PCR values. [4] discussed about a method, In vehicular ad hoc networks (VANETs), because of the nonexistence of end-to-end connections, it is essential that nodes take advantage of connection opportunities to forward messages to make end-to-end messaging possible.

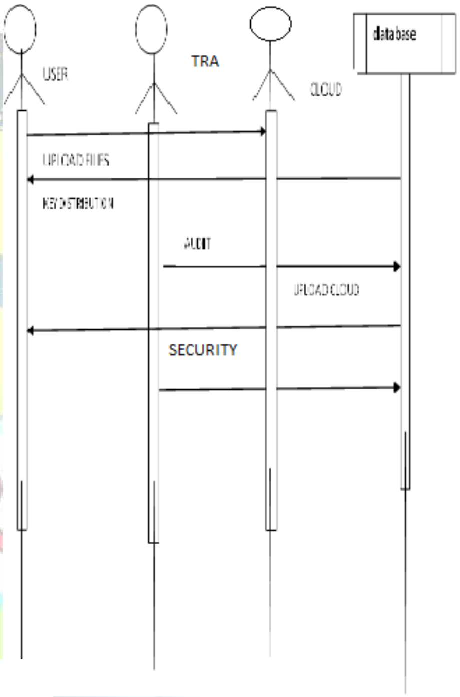
Platform attestation allows a remote party to authenticate a target platform and obtain a guarantee that it up to a certain level in the boot chain – runs software that is identical to the expected one. To do this, an attester requests accompanied by anonce the target platform to produce an attestation quote and the measurement aggregate, or Integrity Measurement List (IML).

We assume that TTP has access to an access control list (ACL) describing access and ownership relations between DM and D. Furthermore, TTP communicates with CH to exchange integrity attestation data, authentication tokens and cryptographic keys. TTP can attest platform integrity based on the integrity attestation quotes and the valid AIK certificate from a TPM, and seal data to a trusted host configuration. Finally, TTP can verify the authenticity of DM and perform necessary cryptographic operations. In this paper, we treat the TTP as a "black box" with a limited, well-defined functionality, and omit its internals. Availability of the TTP is essential in the cloud scenario, we refer the reader to the rich body of work on fault tolerance for approaches to building highly available systems.

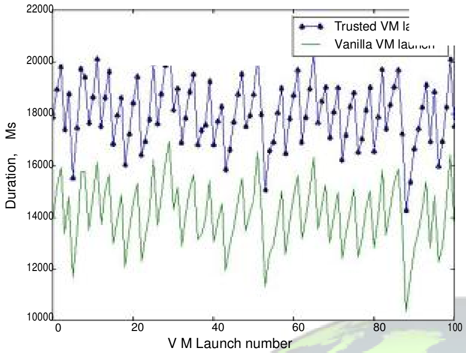
Sequence Diagram

The TPM generates the attestation quote a signed structure that includes the IML and the received nonce – and returns the quote and the IML itself. The attestation quote is signed with the TPMs,Attestation Identity Key (AIK). The exact IML contents are implementation-specific, but should contain enough data to allow the verifier to establish the target platform integrity.

Trusted Third Party (TTP): an entity trusted by the other components. TTP verifies the TPM endorsement credentials on hosts operated by the cloud provider and enrolls the respective TPMs' AIKs by issuing a signed AIK certificate.



VI. Evaluation and Result



V

Our results show that it is possible and practical to provide strong platform software integrity guarantees for tenants and efficiently isolate their data using established cryptographic tools. With reasonable engineering effort the framework can be integrated into production environments to strengthen their security properties.

VII. Conclusion

Today, cloud computing is being defined and talked about across the ICT industry under different contexts and with different definitions attached to it. The core point is that cloud computing means having a server firm that can host services for users connected to it by the ork. Technology has moved in this direction because of the advancement in computing, communication and networking technologies. Fast and reliable connectivity is a must for the existence of cloud computing.

Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control is transparency in the cloud implementation – somewhat contrary to the original promise of cloud computing in which cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches.

VIII. References

[1] Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. IEEE Security & Privacy, Vol 7, Issue 4, pp. 61-64, July-August 2009.

[2] Messmer, E. (2009). Gartner on Cloud Security: ‘Our Nightmare Scenario is Here Now.’ Network World October 21, 2009. URL: http://www.networkworld.com/news/2009/102109-gartner-cloud-security.html. (Accessed on: January 23, 2013).

[3] Pearson, S. (2009). Taking Account of Privacy when Designing Cloud Computing Services. In Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD’09), pp. 44-52, Vancouver, British Columbia, Canada, May 2009.

[4] Christo Ananth, Kavya.S., Karthika.K., Lakshmi Priya.G., Mary Varsha Peter, Priya.M., “CGT Method of Message forwarding”, International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015,pp:10-15

[5] Petry, A. (2007). Design and Implementation of a Xen-Based Execution Environment. Diploma Thesis, Technische Universitat Kaiserslautern, April 2007.