IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 3 (Sep. - Oct. 2013), PP 50-54
www.iosrjournals.org

Security in a Virtualised Computing

E.Geetha Rani#[1], Dr.M.V.L.N.Raja Rao *[2], M.BalaTripuraSundary#[3], B.RakeshChandra *[4], CH. Ravi Kiran#[5]

*#1,*2,#3 ,*4& #5 Information Technology, Gudlavalleru Engineering College, Gudlavalleru JNTUK, INDIA.*

Abstract: *Do the security challenges posed by virtualisation make it a non-starter for your sensitive business applications? There is much debate about cloud computing, which promises to deliver utility-based virtual computing to the front door of every company. Some are dismissing it as marketing hype – but if it delivers the benefits it claims, it has the potential to transform enterprise computing. So what are the challenges – and what are the opportunities posed by this development?*

"We should assume that cloud computing and virtualized computing paradigms are not just a reality but a part of our future. So what can you do to make yourself safe and secure in the virtual world?"

Cynics might well say that cloud computing is just hype. It is, after all, based on today's rather than tomorrow's technology, all the technical ingredients are well established. In fact, in a sense it could be argued that it is yesterday's technology reborn. Utility-based computing has been a familiar concept since the 1960s, when it was born as the 'computer bureau'. However, there has been a shift. Many recent internet innovations are based on the cloud proposition. In the future, we'll see the joining up of these services to provide ubiquitous computing. On top of that, as organisations look torationalise their own internal computing, they are considering a virtualised model. Traditional computing on complex networks ties up capacity – underutilized in one place or over-utilised in another. The flatter and homogenized nature of a virtualised architecture allows processing and storage resources to be allocated on demand and used more efficiently and effectively. In-house computing can be rationalised and there's the option of commercial, outsourcedservices. This approach also brings a shift away from bespoke business applications to online, ready-to-use business application libraries. We should assume that cloud computing and virtualised computing paradigms are not just a reality but a part of our future. So what can you do to makeyourself safe and secure in the virtual world? Here we first explore and demystify this technology, then look at the security challenges and couple with this discussion of some of the positive opportunities and advantages it presents to overcome those challenges.

Keywords: *Cloud computing, Virtual Machine, Security Issues, Service Management, IDS/IPS.*

I. Introduction

Orientation: Before going further, we need to establish some definitions.

Hypersor:This is what makes virtualization possible. It provides the abstraction layer between the real and virtual computers. It is basically a form of specialized operating system software that can map the virtual processor, memory, storage, input/output (eg, network) of a virtual computer to the real processor, memory, storage and input/output of a real computer.

Cloud Computig: In technology terms, cloud computing can be described as an organised mass of hypervisor-enabled virtual computing spread over one or more domains, including datacentersand territories.

Virtulisation, Virtual Machine (VM):Virtualisation is the process of abstracting computer applications, services and operating systems from the hardware on which they run.

Guest Operating System:This is the operating system installed and running on a VM.

Virtual Machine Image (VMI):This is a pre-built copy of the memory and storage contents of a particular machine. It contains the guest operating system and, optionally, everything needed to run a business application in terms of software and data.

Security Layer:Here we're using this term to describe security functions embedded within the hypervisor layers that provide common services to all VMs on the hardware platform. They are also logically isolated from the guest operating systems. This conforms to the Jericho Forum Collaboration Oriented Architecture (COA) in that each distributed processing element has its own dedicated security functions.

Security as A Service:A utility-based security service that links to all security layers of a cloud and is served by one or more operations centres attached to the cloud. So what are the main security challenges to the whole-scale adoption of virtualised technology?

II. Security Architecture

How, in an essentially homogenous, structure less and transient processing environment, would you replicate the sort of protection you would get from traditional N-tier security architectures? These incorporated firewalls, intrusion detection/prevention systems, anti-virus, encryption, patch management and other services, authentication, authorization and access controls. Therein lies both the challenge and the opportunity.

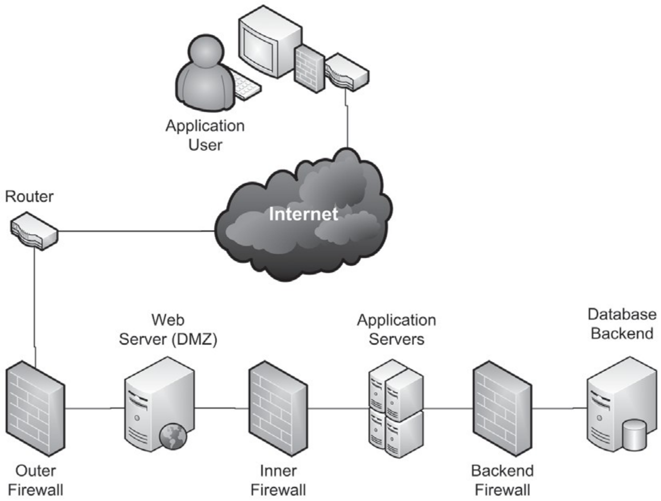

FIG 1: N-TIER SECURITY ARCHITECTURE

Firewalls: In cloud computing, the firewall is most likely to be be delivered as a VMI, running in its own processing compartment. There may also be room for a traditional hardware firewall at the base of each datacentre cabinet to regulate flowinto and out of that cabinet, and also at the outer boundaries of each cloud. These firewalls become linked in a grid with a dedicated 'out of band' firewall management channel. These are co-ordinated and allow virtual compartments for customerdistributed-processing services with per customer traffic segregation. This is essentially the Jericho COA model adapted to the cloud architecture: each processing stack becomes a repeatable unit of the architecture – the security layer – managed at security operating centres to deliver Security as a Service.This approach also makes personal firewalls which run in the context of the guest operating systems and which cannot survive once their host is compromised all but redundant.

III. Intrusion Detection/Prevention Systems (Ids/Ips)

It is also possible to build software IDS/IPS probes into the security layer with full traffic analysis, attack detection and response control capability. This is also an improvement upon Host Intrusion Detection agents, which can be compromised just as personal firewallscan. The virtualised environment offers some unique possibilities for prevention responses, for instance, it might be possible to clone an attacked VM three ways:

1. The original minus the attack traffic, which allows business to continue.
2. A forensic image to allow the attack tobe investigated.
3. A honeypot to retain and divert the interest of the attacker in which fake data is substituted for real.

Anti-Virus (A/V):One of the existing issues with A/V is that it has always run in the context of the computer, so why is it a surprise that the latest infections can disable A/V protection and makeit impossible to disinfect without a full rebuild? In the virtual age it should be possible to hide the A/V in its own VM in which it can 'scan on access' storage traffic and 'scan on demand' by backgroundscanning of the memory space of one or more local VMs. It would be unreachable and undetectable to a virus or hacker that managed to breach a business application running on a VM.

Encryption:Recently, the problem of providing affordable protection for private encryption keys was solved by adding a Trusted Platform Module (TPM) to the PC architecture. This made possible ubiquitous, end-to-end data protection in PC networks by the use of Asymmetric Key Cryptography and Public Key Infrastructures. The cloud cannot break the paradigm to require transport of private keys around the network. However, in the Jericho COA trust model, the TPM is deliberately used to provide trust connections fromconnection to connection. So this can be adopted in the cloud model to allow establishment of virtual private networks to protect customer data on the move. A similar approach can be adopted to add layers of encryption to sensitive data objects at rest.

Patch Management:With the homogenous nature of cloud computing, it's possible to simplify the problem of patch management. Many platform-level patches can be applied to all running images, but by including a patch management service within the management or security layers, it is possible to automate roll-out. It is also possible to clone individual customer environments first and test the patch before it goes live (without the extravagant costs of a dedicated test environment).

Other Services

There are many more potential security services that could be added to the security layer and be delivered as Security as a Service. Some of these can offload functionality and complexity from the business applications. Others can provide a common Application Programming Interface (API) to allow functions to be accessed by business applications. Examples include proxy services, content and spam filtering, web caches, user registration, authentication, authorisation, password management and secure single sign-on. These will also have the benefit of a common management interface.

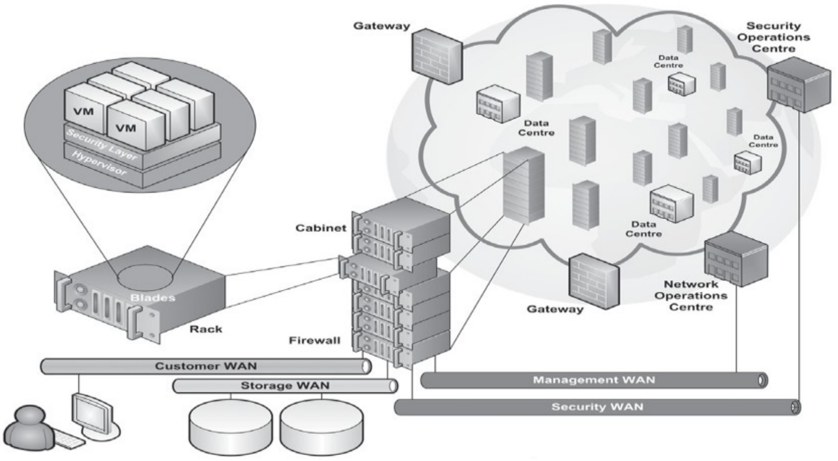

Fig 2: Cloud Computing Security Architecture

IV. Building Blocks

These are the building blocks. It is possible now to envisage a full cloud computing architecture constructed using these blocks as illustrated in Figure 2. Notice the differences between this and the traditional approach given in Figure 1.

Technical Assurance:Within cloud computing there are significant trust interfaces at hypervisor, security layer and security management network levels. The hypervisor is becoming a slim component, and therefore ripe for detailed assurance work. The security layer should also aim for similar characteristics, although it will in part overlap with the hypervisor (interspersed between storage and peripheral channelling) but can benefit from off the shelf security components installed in their own VMI. The security management network can be conventionally assured as an effectively dedicated infrastructure management network. With any luck, recent initiatives started by the Cloud Security Alliance will bear fruit. It may be possible to create a scheme similar to the PaymentCard Industries Data Security Standards (PCI DSS) to provide an assurance framework based on the newly published Security Guidance for Cloud Computing. This is a holistic approach covering 15security domains, allowing organizations to identify appropriate controls to be put into place for secure cloud computing. It applies to organisations that wish to operate their own private cloud, procure the services of public clouds, outsource to a managed service provision or adopt anyother hybrid approach.

"With such a wide surface to attack, it is likely that any fault in any common component could lead to widespread compromise within a cloud"

Vulnerability Management:Cloud computing provides an homogenous computing environment involving racks of equipment of very similar configuration. However, it also loses the distinction of customer-owned boundaries, especially if there is a need to provide instant scale-up and scale-down of capacity. This poses challenges for vulnerability management, which is a large part of technical assurance in the operational environment. With such a wide surface to attack, it is likely that any fault in any common component could lead to widespread compromise within a cloud andthe customer systems itcontains. The opportunity is that Security as a Service can provide independent oversight of the security status across the cloud. It is also possible to envisage virtual test points for each customer interface. This would provide a bandwidth-limited point to allowtraditional penetration testing of the customer's virtual network with minimal risk to the resources of other cloud users.

V. Data Location And Privacy

The challenge with data privacy is ensuring that personally identifiable information is protected against compromises to confidentiality, integrity and availability – and that its handling complies with data protection legislation relevant to the local jurisdiction. How do customersput constraints on the locations where data is stored and processed, and to limit or prohibit any additional uses? Undoubtedly, many of the answers depend on the degree to which data canbe controlled, and this is an area that needs to be covered in the contract with the service provider.However, there are technology considerations too, and it is possible to foresee that cloud computing could allow for ubiquitous, fine-grained access control to customer data using processing constraints. These will ensure that data stays within virtual 'sub-clouds' that can be mapped to physical jurisdictions.

Incident Management:Incidents may be external to the cloud (eg, hacking), originate on customer premises (eg, a user uploading malware) or be the result of malpractice by a cloud administrator.One challenge is that logs may span many customers, and that firewall logs are specific to the infrastructure rather than virtual components. The customer may be limited to diagnosing incidents and relying on whatever incident management services are given by the provider. This is another area where contractual arrangements are required, but it is also an area where independent Security as a Service comes into its own. A security operations centre should be set up that is distinct from the service management and which has the tools to provide percustomer views of incident data.

"Customers must be able to undertake 'no notice' physical inspections and audits of service provider facilities to ensure full compliance with the relevant
regulations and standards"

Compliance: Many regulation regimes (including PCI DSS and Sarbanes-Oxley) require a very hands-on approach to information security controls. Customers must be able to undertake 'nonotice' physical inspections and audits of service provider facilities toensure full compliance with the relevant regulations and standards. However, in a virtual environment, where the datacentres usedtoday may be different from those used tomorrow, how could this apply? It is possible to build either private clouds or managed environments in which virtualised technology is used, allowing the inspection to take place. But there are other opportunities: we can expect future standards that will cover public cloud service provision. With the independent oversight of a regime similar to ISO27001 certification of datacentres, it may be possible to develop qualifications that apply to providers joining regulated public cloud services. This will help engender confidence that there is adequate oversight within such a cloud. Independent Security as Service offerings may also come with an auditservice as a subscription option.

Service Management:An inevitable issue with any outsourcing or public subscription arrangement is how in control of the administration of the service are the providers? There are several aspects to this:

a) From where are the services being administered (eg, via a global 'follow the sun' arrangement)?
b) How much can you trust the service administrators, and how competent are they?
c) What controls are in place to manage privileges and enable accounting of administrator actions?

These are key points to research during the procurement phase. Regardless of the business requirements, there should be some form of technical trust and privilege management in place. This issue is accentuated in virtualised environments: administrators will have the ability to allocate storage and processing resources, including the ability to remove barriers and cause data leakage between compartments. It's essential to provide a set of rules for the segregation of duties amongadministration domains: administrators should be limited in what they can do --eg, they may be limited to a group of customer assets, or a distinct datacenter zone. And there must be full accounting and audit of their actions – eg, every administrative action should be recorded and traceable to the administrator responsible. Again, with Security as a Service, a separate security operations centre could independently oversee and audit service management operations.

VI. Summary

The age of cloud and virtual computing is presenting new challenges and the re-emergence of old challenges in new guises. The message is twofold: potential customers need to do their homework and select the right solution for their requirements; and many of the technology issues posed by cloud computing and virtualisation can be solved by adapting traditional approaches so that they work with the diffused nature of cloud architectures. Assuming that industry delivers on the promise of cloud computing, there is no reason to think that it is something that should be avoided on security grounds. It is instead a significant opportunity for the safe and secure computing of tomorrow. An essential enabler will be the development of a future standard against which this model can be secured – an equivalent to PCI DSS, and something that will doubtless emerge out of the emerging work of the Cloud Security Alliance.

References

[1] D. Patterson, "The trouble with multi-core," *IEEE Spectrum*, vol. 47, no. 7, pp. 28–53, 2010.

[2] J. V. Neumann, "Theory of natural and artificial automata," in *Papers of John Von Neuman on Computers and ComputerTheory*, W. Aspray and A. W. Burks, Eds., vol. 12 of *Charles Babbage Institute Reprint, Series for the History of Computing*,pp. 408–474, The MIT Press, Cambridge, Mass, USA, 1986.

[3] S. Balasubramaniam, K. Leibnitz, P. Lio, D. Botvich, and M. Murata, "Biological principles for future Internet architecturedesign," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 44–52, 2011.

[4] R. Mikkilineni, "Is the Network-centric Computing Paradigm for Multicore, the Next Big Thing?" Convergence of Distributed Clouds, Grids and Their Management,2010,http://www.computingclouds.wordpress.com/.

[5] G. Morana and R. Mikkilineni, "Scaling and self-repair of Linux based services using a novel distributed computingmodel exploiting parallelism," in *Proceedings of the 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '11)*, pp. 98–103, June 2011.

[6] R. Mikkilineni and I. Seyler, "Parallax—a new operating system for scalable, distributed, and parallel computing,"in *Proceedings of the IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum(IPDPSW '11)*, pp. 976–983, 2011.

[7] R. Mikkilineni and I. Seyler, "Parallax—a new operating system prototype demonstrating service scaling and serviceself-repair in multi-core servers," in *Proceedings of the 20th IEEE InternationalWorkshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '11)*, pp. 104– 109, 2011.

[8] R. Mikkilineni, *Designing a New Class of Distributed Systems*, Springer, New York, NY, USA, 2011.

[9] R. Buyya, T. Cortes, and H. Jin, "Single system image," *International Journal of High Performance Computing Applications*,vol. 15, no. 2, pp. 124–135, 2001.

[10] http://www.seamicro.com/.

[11] J. V. Neumann, "Theory of natural and artificial automata,"in*Papers of John Von Neuman on Computers and ComputerTheory*, W. Aspray and A. W. Burks, Eds., vol. 12 of *Charles Babbage Institute Reprint, Series for the History of Computing*,p. 454, The MIT Press, Cambridge, Mass, USA, 1986.

[12] P. Stanier and G. Moore, "Embryos, genes and birth defects," in *The Relationship Between Genotype and Phenotype: SomeBasic Concepts*, P. Ferretti, A. Copp, C. Tickle, and G. Moore, Eds., p. 5, JohnWiley& Sons, London, UK, 2nd edition, 2006.

[13] F. Tusa, A. Celesti, and R. Mikkilineni, "AAA in a cloud-based virtual DIME network architecture (DNA)," in *Proceedings of the 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.*

[14] R. Buyya and R. Ranjan, "Special section: federated resource management in grid and cloud computing systems," *FutureGeneration Computer Systems*, vol. 26, no. 8, pp. 1189–1191, 2010.

[15] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype,and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.

[16] M. M. Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos*, Simon and Schuster, New York, NY, USA,1992.

[17] M. Mohamed, S. Yangui, S. Moalla, and S. Tata, "Web service micro-container for service-based applications in cloud environments," in *Proceedings of the 20th IEEE InternationalWorkshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '11)*, pp. 61–66, IEEE Computer Society, 2011.

[18] J. Von Neumann, "The General and Logical Theory of Automata," in *Cerebral Mechanisms in Behavior, The HixonSymposium, Edited by L. A. Jeffress*, W. Asprey and A. Burks, Eds., Reprinted in Papers of John von Neumann onComputers and Computing Theory, pp. 456–457, The MIT Press, Cambridge, Mass, USA, 1987.

[19] S. B. Carroll, *The New Science of EvoDevo—Endless Forms Most Beautiful*, W. W. Norton & Company, New York, NY,USA, 2005.

[20]. Jericho Forum: 'Position Paper –Collaboration Oriented Architectures',Version 2.0, November 2008, 10 July 2009 http://www.opengroup.org/jericho/COA_v2.0.pdf

[18]. http://www.cloudsecurityalliance.org

[19]. Cloud Security Alliance: 'Security Guidance – Critical Areas of Focus in Cloud Computing', April 2009,10 July 2009 http://www.cloudsecurityalliance. org/guidance/csaguide. Pdf

[20]. J.M.Kaplan. How SaaS is Overcoming Common Customer Objections. Cutter Consortium: Sourcing and Vendor Relationships.