International Approaches to Security and Virtualisation

BIC Discussion Paper **22-JUN-2011**

Syed Naqvi [1]

1 Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC), Belgium

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

Virtualization infrastructures present promising features to address the ever-increasing demands of information society. The concept of virtualization is not new in the field of ICT. It dates back to the inception of programming language compilers that virtualize the object code[1], and to the virtualisation of specific physical resources such as memory. However, the general concept of virtualization infrastructures, where physical resources are dynamically mapped to address the spontaneous business needs, is relatively new. Moreover, the scale and scope of this concept brings several challenges for its deployment including a lot of uncertainty as to how and where to implement security [2]]. Classical security solutions and practices are getting obsolete in the face of the peculiar security requirements of virtualization infrastructures. Therefore, security and dependability issues of virtualization infrastructures are emerging as gauging factor for measuring the success of this Endeavour.

The inherent nature of virtualization requires totally different security provisioning approach than the classical one developed decades ago. Classical IT security solutions and practices require precise information of the underlying infrastructure for their deployment and functional validation. They cannot be applied to these virtual infrastructures due to the intrinsic characteristic of virtualisation that provides abstraction to the underlying resources and infrastructures. This section examines two major security challenges of virtualization infrastructures – security audit and digital investigations. Finally, a quick glance of a federated Cloud security experiment funded by the European Commission is given before drawing some perspectives of international cooperation in the area of virtualisation security.

Security Audit of Virtualisation Infrastructures

Security audit assess the security of a networked system's physical configuration and environment, software, information handling processes, and user practices. Various security audit standards such as Payment Card Industry Data Security Standard (PCI-DSS) require audit of the physical controls [3]. The virtualisation infrastructures provide an abstraction layer to the underlying lower-level details. This situation raises several security concerns such as multi-tenancy; lack of security tools [4]; and disparity with the classical IT security audit practices. Another important issue in this regard is the data export control that requires operators and providers to ensure that particular kind of data should only be stored and processed in some specific location. Audit inspectors need to certify compliance to these regulations for the issuance of the operating licenses to infrastructure and service providers. Check-pointing mechanisms including monitoring tools are indispensable for auditors (both internal and external) to verify that operators and providers are respecting the corresponding regulations.

There exist a number of generic monitoring tools such as hardware monitoring (e.g. HP Insight Manager, Dell Open Manage, VMWare Virtual Center, etc.), performance monitoring (e.g. VizionCore, Veeam Monitor, Vmtree, Nagios, etc.), machine state monitoring (e.g. Virtualshield, Logcheck, etc.), and security monitoring (e.g. intrusion detection, honeypots, etc.). However, these tools may not be suitable for security audit controls of virtualization infrastructures as physical controls can be distributed that will require onsite checks by the local controllers. There is a strong need of a new set of matrices for measuring security strength. With more reliable matrices, new check-pointing models need to be developed. Besides these technical requirements for carrying out security audit of the virtualisation infrastructures, there is also a need of new regulations/legislations for the cross-border deployment of resources used in virtualisation infrastructures.

Digital Investigations of Virtualisation Infrastructures

While virtualization infrastructures are poised to drive cybercrimes in the near future [5], these virtualisation infrastructures (such as Clouds) have no 'forensic friendly' design characteristics. Therefore, classical investigation techniques (such as confiscation of computing resource, copying and analysing digital contents) is not feasible as unplugging of a Cloud is not the option its stakeholder are willing to choose! Moreover, a Cloud is required to copy the contents of the Cloud under investigation. Furthermore, another Cloud is required to have computational capacity to analyse the contents of the Cloud being analysed. The current practice of carrying out digital investigations of Clouds involves analysis of individual computers connected to a Cloud. These investigations include recovery of connection details, logins, and data exchange to establish the sequence of actions carried out on the Clouds and to eventually demarcate the responsibilities. The Cloud operations are therefore not affected by these investigations of individual PCs. However, this paradigm is not sustainable in the advent of shrinking features on the client side of Clouds. Complete externalisation of software artefacts (from the operating systems to the applications) will not provide any meaningful information to the investigators. This paradigm is already realised in 'Cloud PCs' (e.g. Wyse technology's X00m Cloud PC [6]). Dell's takeover of Wyse technology to expand their enterprise business heralds a widespread use of Cloud PCs in the very

near future. Cloud PC X00m has only 2GB RAM with no storage or optical device connected to it. Digital forensics analysis could not be performed on these Cloud PCs without including Cloud infrastructure in the investigations. This paradigm will give birth to a number of serious security challenges including operational challenges (such business continuity assurances for the customers) as well as legal challenges (notably acceptability of the proofs originating from a 'virtual' world).

BonFIRE Security Experiment

European Future Internet experimental facility and experimentally driven research project BonFIRE [7] is executing a security monitoring experiment that aims to examine the implications of security on the virtualisation infrastructures – i.e. federated Cloud infrastructures. This experiment – ExSec: Experimenting Scalability of Continuous Security Monitoring – aims to develop a mean of quantifying the impact on security functions under various operating conditions and parameters of federated Cloud deployments. The results of this experimental study will help businesses to identify the best security architecture that will fit their Cloud architectures and performance requirements.

The main objectives of the ExSec experiment is to study and quantify the impact on the quality of protection of Future Internet based virtualisation infrastructures that will be highly scalable in nature and use heterogeneous underlying technologies. These experimental evaluations will be useful to determine the stretching limit of Cloud security functions; and eventually, workout some remedial solutions especially to explore the possibility of making use of abundance of Cloud resources to compensate the performance degradation.

Perspectives of International Cooperation

Virtualization infrastructures envision a number of promising benefits for global businesses such as resource management, service provisioning and cost effectiveness. However, the scope of these infrastructures requires them to be dependable and secure, as markets will depend on them, as much as governments, to function properly. Globalisation of computing and storage resources require security solutions at the global scale, otherwise it will be impossible to achieve concrete security assurances for these infrastructures. International collaboration is crucial for ensuring security of the emerging networked society's core architecture whether it is security audit framework for virtual infrastructures or their digital investigations.

Recent economic meltdown has shown the degree of dependence at the global scale in general and among the emerging and developed economies in particular. This situation obliges us to take some international dimension for virtualisation security. It is understood that bringing different societies and cultures to a common understanding of security requirements is not trivial. Even member states of politico-economic blocs such as European Union maintain conflicting views of IT security [8]. Still, we need to involve all the stakeholders in a constructive cooperation to workout a common vision for securing virtual infrastructures. Significant breakthrough could be made if some business dimensions are added by bringing commercial stakeholders on-board. For example, best practices proposed by payment card industries (such as VISA & MASTER) are adopted and followed by all the players irrespective of their political and societal affiliations. Without some effective international cooperation, there will be a number of Achilles' heels that malicious entities will use to attack the critical information infrastructures from their safe havens with complete impunity.

Acknowledgements

This work is partially funded by the European Union's seventh framework programme (FP7 2007-2013) Project BonFIRE under grant agreement number 257386.

References

[1] Jason Bloomberg, Building Security into a Service-Oriented Architecture, ZapThink Whitepaper, ZapThink LLC Publisher, May 2003

[2] Richard Adhikari, The Virtualization Challenge, Part 5: Virtualization and Security, TechNewsWorld, March 2008

[3] Payment Card Industry Data Security Standard (PCI-DSS) https://www.pcisecuritystandards.org/

[4] Edward L. Haletky, Virtualization Security - Security and Compliance within the Virtual Environment, DABCC online article 08 April 2009 http://www.dabcc.com/channel.aspx?id=279

[5] Trend Micro Report: The Future of threats and Threat Technologies – How the Landscape is Changing, December 2009 – http://affinitypartner.trendmicro.com/media/34716/trend_micro_2010_future_threat_report_final.pdf

[6] DELL Wyse Cloud PCs – http://www.wyse.com/products/cloud-clients/cloud-pcs

[7] European 7th Framework project BonFIRE: Building Service Testbeds on FIRE (Future Internet Research Experimentation) – http://www.bonfire-project.eu

[8] F. Calderoni, The European legal framework on cybercrime: striving for an effective implementation, Crime, Law and Social Change 2010, Vol. 54, 339-357