Winter 12-15-2012

Dynamic Security of Virtualized Systems: An Analysis of Time-based Impact

Jerald Hughes
University of Texas-Pan American

Manal M. Yunis
University of Texas - Pan American, yunism@utpa.edu

Joseph Roge'
University of Texas-Pan American

Dynamic Security of Virtualized Systems: An Analysis of Time-based Impact

Jerald Hughes
Department of Computer Information Systems and Quantitative Methods
University of Texas-Pan American
Edinburg, Texas, USA

Manal M. Yunis[1]
Department of Computer Information Systems and Quantitative Methods
University of Texas-Pan American
Edinburg, Texas, USA

Joseph Roge'
Department of Computer Information Systems and Quantitative Methods
University of Texas-Pan American
Edinburg, Texas, USA

ABSTRACT

Virtualization technologies pose time-sensitive security challenges that need to be addressed from a dynamic security perspective. Adopting a dynamic security approach can help organizations manage the security risks inherent in virutalized environments. This paper conceptually examines current thought on best practices in information security systems which explains the dynamic nature of virtualized systems and paves the way for an information security model into which virtualization can be incorporated. We suggest that a proper analysis of time-based impact of security threats would help mitigate virtualization security risks, allowing IT security professionals and users to efficiently coordinate security objectives with the larger goals of the organization.

Keywords: Virtualization, Dynamic Security, Time-based Impact, Virtualization Security Features, Information Security, Security-Technology Fit.

[1] Corresponding author. yunism@utpa.edu +1 956 292 9263

INTRODUCTION

As virtualized systems are being adopted by more and more organizations (Marko 2012), many are discovering that they can become susceptible to new security risks (Mutch and Anderson 2011). Thus it is prudent to examine security strategies that organizations formulate and implement to accompany the deployment of their virtualized systems. Some experts contend that virtualization by itself is not inherently insecure. The problem, however, lies in the insecure deployment of virtualized systems (MacDonald 2012).

To avoid the potential security vulnerabilities of such systems, some argue that adopting proper security measures for virtual machines must precede their deployment and even precede the selection of vendors and products (Mutch and Anderson 2011; Scarfone et al. 2010). 'Security measures' here refers to not only security technologies (Kayworth and Whitten 2012), but also the integration of technology, people, and well-managed processes (Oppliger 2007). A critical problem with traditional information security models is lack of dynamism, relying on fixed sets of rules and procedures. As virtualization technologies produce dynamically changing systems, it becomes prudent for organizations' management and IT security professionals to implement security processes which address these dynamic elements as well.

Previous research has discussed virtualization technology, performance, and features (Fabian et al. 2006; Friedman 2006; Scarfone et al. 2011; Hoesing 2009; Zhang and Dong 2008) as well as business value (Cummings 2008; Fabian et al. 2006). Investigators have also discussed security challenges introduced by virtualization (for example, Garfinkel and Rosenblum 2005; Hernick 2007b; Radcliff 2007, Skapinetz 2007; Vijayan 2007). Few attempts, however, have been made to study security risks of virtualization in a systematic way, and only one has incorporated them into an IT security framework (Yunis et al. 2008). While this step is

necessary, it is nevertheless insufficient. The time-based effect of virtualization information security remains to be addressed. Accordingly, we will attempt to address the following research question:

RQ: What approaches to information security are needed to address the time-related impacts of security threats introduced by virtualized systems?

This paper provides a conceptual analysis of information security practices which account for the dynamic nature of virtualized systems and thus pave the way for an information security model which is robust to virtualization. The intended result is a positive impact on the security of virtualized systems. This paper will discuss current security practices, identify and assess time-based gaps in these practices, and highlight the need for dynamic responses appropriate for virtualized systems. The rest of this paper is organized as follows: the next section will be a review of the literature pertinent to virtualized systems, threats specific to such systems, and information security practices guidelines. After that, a sample analysis taking time scales into account will be presented. This will be followed by discussion of the analysis, and, finally, a presentation of the study conclusions, implications, and limitations.

LITERATURE REVIEW

This section will present a review of the literature pertinent to virtualization technology, its adoption by organizations, information security models extant in the literature, and the gaps in these models as identified by experts.

Virtualized Systems

While many definitions of "virtualization" exist within IT, this paper deals with virtualization as a technology whereby an additional layer of abstraction – a hypervisor – is inserted above the hardware level. It rules out other virtualization platforms such as storage

virtualization, application virtualization, and so on. This layer is referred to as a virtual monitoring machine (VMM), allowing multiple operating systems- or multiple instances of an operating system- to run on one physical server (Fabian et al. 2006; Miller and Pegah 2007). Enterprises deploying virtualization may thus more efficiently use computing resources (Ashford 2012; Vijayan 2007).

Important functions provided by virtualization which enhance the performance of an organization's computing resources include server consolidation, dynamic system migration, and security testing (Zhang and Dong 2008). Several benefits of virtualization technology have been discussed by researchers, trade specialists, and technical analysts. These advantages include cost savings and efficiency in an organization's computing infrastructure and resources (Fernando 2005), interoperability and mobility with legacy software (Singh 2004), and reliability and security of applications (Rosenblum and Garfinkel 2005). These features have all contributed to make virtualization systems an attractive technology for organizations.

Challenges of Virtualized Environments

According to Gartner research, server virtualization is reaching adoption rates of roughly 50% (Bittman 2012). As the technology continues to promise cost-saving benefits for small companies, server virtualization will grow even more popular (Bittman 2012). Similarly, IT professionals have on average virtualized 52% of the x86 servers operating in enterprise environments, with an expectation that the number may grow to 75% by 2014 (Holland 2012). But is the increasing adoption rate accompanied by corresponding adoption of virtualization-oriented security measures? In a survey by Prism Microsystems 85% of respondents reported that their organizations had adopted virtualization to some extent. Of these, 58% reported

deploying traditional information security measures as opposed to 20% using solutions tailored specifically to virtualized environments (Prince 2010).

This means that organizations are slow-moving when it comes to protecting virtualized environments (Prince 2010). Also, according to Gartner Research, most virtualized systems are less secure than the physical machines that they replace (MacDonald 2011). Accordingly, there is an underestimation of virtualization risks posed by virtualized environments (Ashford 2012; Skapinetz 2007). The reported findings indicate that while the adoption rate of virtualization is increasing, implementation of security measures needed for protecting their information resources lags behind.

Information Security Approaches

McDaniel (1994) defined information security as the techniques, concepts, and technical and administrative measures deployed by an organization in order to protect its information resources. According to Microsoft, IT security refers to the protection of information resources through the use of procedures, technology, and people skills (Hoesing 2009). A number of models supporting security in computer systems exist (e.g. Anderson et al. 2004; Olivier 2001; Saunders 2003).

Most IT security models suggest security processes that are static rather than dynamic. Today's advanced and sophisticated types of threats and attacks have rendered such traditional models of computer security obsolete (Grandison et al. 2007). To demonstrate the global state of information security thinking, the 2013 Global State of Information Security Survey carried out by PricewaterhouseCoopers (PWC) revealed some important results regarding information security practices. The survey of more than 9,300 IT security and business executives examined how they viewed the effectiveness and scope of their security technologies, policies, and

strategies (PWC 2012). 45% expected an increase in IT security spending over the coming year, and 48% reported that information security was involved at project inception or during the analysis and design phases. However, while IT security spending is on the increase, and while about 68% of respondents have high or moderate levels of confidence in the effectiveness of information security behaviors instilled in their organizational culture, security risks are not the major driver behind IT security spending. Instead, spending is driven by economic conditions (45.7%) and regulatory or internal policy compliance (56%), among other factors (PWC 2012). The result in such organizations would be a compliance culture, which emphasizes conformance with organizational standards and policies, rather than improving security itself (Tan et al. 2010). An earlier survey report contends that IT security tools such as intrusion detection, encryption, and identity management software (Nash 2008), are proving to be insufficient in the current dynamic security environment (Tan et al. 2010). As a result, risk analysts, statisticians, and business intelligence systems that analyze data derived from network logs and monitoring systems are needed (Nash 2008). In fact, to achieve dynamic information security, effective processes and procedures need to be put in place so as to provide for monitoring and timely response (Samy et al. 2010; Von Solms 2000).

THEORY DEVELOPMENT

Our approach draws upon previous IT security models and is theoretically based on the task-technology fit model (Goodhue and Thompson 1995). According to this model, for a technology to have positive performance impact, it must be a good fit with the tasks it intends to support (Goodhue and Thomson 1995). This choice stems from the fact that different technologies require security strategies with differing timing requirements. Based on this reasoning, our analysis approach emphasizes the importance of security strategy - technology fit.

At the heart of this approach is the assertion that different technologies, systems, and applications have different security requirements (Jeloka et al. 2012; EWH IEEE 2005). Moreover, it takes into consideration the security challenges which are the result of the features of the technology itself, and will be discussed in the following section.

Virtualization: Security Challenges

Fluidity of the Virtual Machine Environment: Fluidity refers to the possibility of easily building virtual machines anytime and on the fly. In fact, it has been suggested that mobility and security are at odds with each other (Luo et al. 2011). To address this issue, a company with a static security infrastructure may be forced to isolate applications to their own physical servers in order to avoid migration attacks. This suppresses one of the benefits of virtualization, namely server consolidation.

Virtual Server Replication: This is one of the main advantages of virtualization. Replicating virtual servers to meet IT computational demands can be done quickly. Nevertheless, this feature presents serious security hazards, including data theft, interruption of services, and denial of service (Greene 2008) while the VMs are moving around without having the required security functions replicated to the new location (Hietala 2009). Moreover, replication may result in VM sprawl, with many VMs not being well managed, patched, tested, or protected (Higgins 2007). In addition, unencrypted migration of a virtual machine from one physical server to another makes the VM potentially vulnerable to attacks. Here, a "man-in-the-middle" can attack through methods like spoofing or IP hijacking (Greene 2008). As a result, the VM will migrate to the attackers' machine, granting them full access and allowing them to perpetrate various kinds of exploits.

Logging: This is a critical element for enabling a useful security audit. However, logging systems currently used are not mature enough to help in an appropriate intrusion analysis in a virtualized computing environment (PCI 2011). This consequently leads to two security challenges: security logging and lack of forensic trail (Ritter 2009) since the traffic between the VMs cannot be properly logged, since the tools for virtual systems may not provide an adequate level of monitoring or insight (PCI 2011). Consequently, malicious or threatening traffic flows may go undetected.

Isolation for Malware Analysis: Today, antivirus companies might simply be unable to keep up with the volume of malware samples submitted to them daily (Sanders 2011). Hence, according to the author, it is prudent for organizations to be capable of conducting their own malware analysis. Secure isolation of virtual machines in a way that any action performed inside it – such as testing applications for malware – does not interfere with the hosting system is one of the major security advantages of virtualized environments. However, this isolation is not complete (Stelte et al, 2010; Fabian 2006), which means that the virtualized environment might turn out to be a hostile one used to execute untrusted code or process untrusted data. Such security threats might subject a VMM to compromise or termination. These challenges call for security solutions that are designed specifically for a virtualized computing environment, such as splitting the hypervisor into smaller elements (Pan et al. 2012), or replacing 'rigid security walls' with 'flexible security shields' that can move with the portable virtual machines which they are designed to protect (Nelson 2007).

These challenges make it critical to design a security spectrum that takes into consideration the type as well as the timing of the various security requirements needed for

virtualized systems. The spectrum is depicted in Figure 1 and will be discussed in the following section.

Theory: A time-based virtualization security spectrum

A dynamic security system should address the dynamic features of the computing environment as well as the frequent changing patterns of threats. This makes it prudent to highlight the importance of these two factors:

- First, security solutions should be provided at the right time to attain the desired security level. For example, research has shown that timing related to patch deployment matters, because 'mis-timing' may exacerbate the costs incurred by the company (Ioannidis et al. 2012).
- Second, the security strategy and solutions should be updated, and should always reflect state-of-the-art technology and strategic thinking. This also involves continuously updating people's skills and core competencies (Hoesing 2009), as well as continuous changes in processes, to reflect the changing security requirements of the virtualized environment.

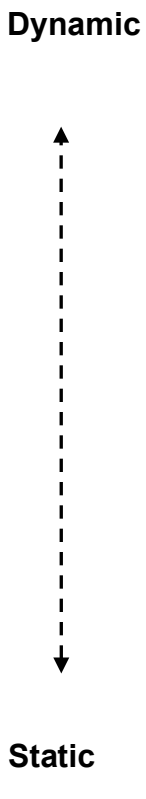
In Table 1, the security methods and steps considered important in virtualized environments, as well as how frequently they should be addressed, are depicted in a security solution spectrum. We separate these security tasks by the time frame in which they should occur, ranging from long-time scale activities (the final row) all the way up to ongoing time-based activities. This, we hold, should be considered pivotal to achieve security task–technology fit, efficiency in security strategy implementation, timely response to threats, optimal combination of static and dynamic security solutions, and systematic monitoring and controlling for performance.

Discussion: Time Factors of Information Security

In the material which follows, we look at the various components of the security spectrum. We begin with the most static elements; those dealt with on the longest time scale, and proceed through shorter and shorter time scales to the most dynamic elements of security.

Table 1. Timing Spectrum of Security Practices

Security Activity	Time Scale	Specific to Virtualization	Security needs increased by virtualization
Tracking information across multiple virtualization platforms	Continuous	✓	
Following up cloned templates and tracking changes	Continuous	✓	
Updating patches, fixes	Hourly		✓
Up-to-date security tools	Weekly		✓
Integrity checks	Monthly		✓
Threat analysis	Monthly		✓
Updated employee training	Quarterly		✓
Applying forensic tools	Quarterly		✓
Assessing security posture	Quarterly		✓
Information security infrastructure	Semi-annually		✓
Security considerations during system development lifecycle	Annually		✓
Compliance with information security regulation	3-5 years		



3 to 5 Years

Regulatory and legal compliance requirements such as HIPAA, Sarbanes - Oxley regulations, and privacy laws have to be taken into consideration (Tamizkan et al. 2012). Since such requirements do not change frequently, they are placed at the static end of the spectrum, estimating changes every 3 to 5 years-or as regulatory changes warrant, with major technology

developments and organizational strategies addressing emerging security issues through policy. Other candidate entries here (not shown) might be information security personnel, certification or re-certification, or information security department restructuring.

Annual

Next, the security strategy should be a part of the virtualized system development life cycle (Higgins 2007). This ensures that addressing security issues posed by the technology will be proactively handled. Assuming that an organization introduces new technology systems or technology updates every year, this element is recommended to take place yearly.

Semi-annual

Security infrastructure in a virtualized computing environment is harder to manage (Cummings 2008). The problem is that while in certain cases, security tools for virtualized servers are embedded within the virtualized systems (Randell 2008), others may be tied to the physical servers- a case that will not provide protection to the virtual systems running on it (Bradley 2012). This means that security tools may have a static association even when servers are virtualized. A proactive and automated monitoring system is suggested, which would validate security tools and the patching used, and ensure that the network is not exposed to new threats. Moreover, the authors recommend that vulnerability scanning be a part of the infrastructure, to ensure meeting the minimum security requirements in the organization's computing environment. With this in mind, the IT infrastructure is recommended to be updated semi-annually.

Quarterly

In addition to this, the need for a strong security policy to be established and well enforced stems from the very nature of the virtualization computing environment, where new servers that don't adhere to security standards could be easily created (Greenemeier 2007). Another feature requiring strong security policy is the fact that while many users have their servers connected to a private network that is not accessed by the public, they use the VM to browse the web, thus possibly exposing the server to public access and misuse. Assessing security posture is thus required and should involve a review of the security policy and strategy in place. This is recommended to be done on a quarterly basis.

Moreover, the effectiveness and success of any security solution depends on how well it is implemented. This highlights the importance of having well trained employees (Alto 2008; Bulgurcu and Cavusoglu 2010), who are very much aware of the security hazards inherent in virtualization technology for better performance and higher security levels.

Monthly / Weekly

As a major input for IT security (in this case, virtualization) strategy development, threat analysis and risk assessment are suggested to be done on a monthly basis. This puts the organization in a proactive position to anticipate threats, assess their impact on the organization's information assets, update their security strategy, and choose a proper security solution that would prevent the threat from taking place, or at least mitigate its effect if totally preventing it could not be achieved. The National Institute of Science and Technology (NIST) has emphasized the importance of monitoring and analyzing hypervisor logs on an ongoing basis (Scarfone et al. 2011; Cavallaro 2008). Integrity checking systems and continuously monitored audit logs that are not located on the same host or hypervisor as the components generating the audit logs (PCI

Security Standards Council 2011) can help in this regard. These, in addition to applying measures for accessing and using the VMs and the host applications, can allow for building a forensic trail to trace the transactions related to accessing and moving VMs. Applying forensic tools to follow such trails is recommended quarterly or monthly depending on the new forensic tool innovations and methods introduced in the market. At the same time, integrity checking systems generally should be updated monthly and security tools generally should be updated weekly in order to maintain the main security features of the technology used.

Hourly

The need for immediate patching is acute. The purpose here is to block incoming attacks before a threat reaches the server. If patches are not up-to-date, a possible remedy would be virtual shields. These sit between the hypervisor and the VMs (Higgins 2007), and are designed to prevent malware from reaching VMs that are not properly patched. In other words, they play the role of "zone defense" mechanisms (Greenemeier 2007) that buy the system some time until proper patches are installed. Patching updates should take place hourly, or at least be supplemented by shields until they get updated. NIST recommends centralized patch management solutions to administer patch updates (Scarfone et al. 2011).

Continuous

The above mentioned security tools or solutions are generally applied to any computing technology environment. The time element was set based on the security challenges introduced by virtualization technologies. Yet, two new security tools were introduced to the spectrum, and these are pertinent only to virtualization computing environments. These are: following up cloned templates and tracking changes, and tracking information across heterogeneous virtualization platforms. Since VMs can be cloned very easily and on the fly (Hoesing 2009),

controlling the number and the purpose for which cloning is taking place can significantly reduce this threat. Also, today's data centers may include a variety of platforms, where VMs can be installed. Such hybrid environments pose the challenge of bridging the gap amongst these different platforms and tracking VM performance in all of them. Both security items should be enforced around the clock. This could be done by dynamic monitoring, scanning, and auditing systems.

It should be apparent that as we move from static to dynamic, more time-based actions and security implementations are necessary.

Discussion: Time Factors of Information Security

As in any other computing environment, the aim here is to achieve efficiency and effectiveness in the security practices being applied. From this perspective, the technology features would require different kinds of security measures that would flow in a continuum ranging from static to dynamic, or from less dynamic to more dynamic.

Based on this, a grid of four cells is presented below to show a descriptive status of the possible responses in security procedures for each practice-need cell. The grid is shown in Figure 1, with two dimensions: security practices (static-dynamic) and need for time-based response to threats (high-low).

When the need is low and the security practices are static, then the security procedures are the standard normal or traditional procedures commonly used to combat security threats. The opposite situation will emerge when the need is high and thus matched with dynamic practices. This cell reveals on-going time-based procedures that are effective in being adaptive to changes in security threats patterns and technology features and properties. In this sense, the security procedures are effective since they are fit with the technology environment, and are achieving

the desired security objectives. Problems in efficiency or performance will take place in the remaining two situations. If the need for time-based response to threats is low and the security practices are dynamic, sophisticated, and rather expensive in what they require to be implemented, then the security procedures would be more than what the situation needs (flooding) and would thus be inefficient.

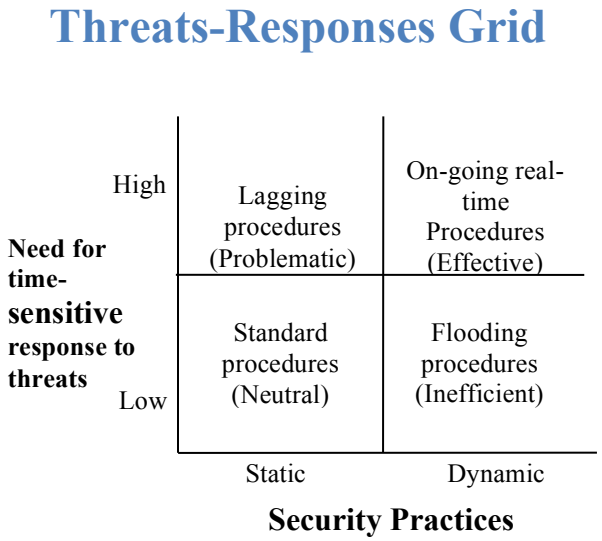


Figure 1. Time-Based Threats – Responses

Finally, another problem will ensue if the need is high while the security practices are static. This implies that deployed security practices lag behind the requirements of a vulnerable computing environment for time-based measures to combat probable security threats and attacks.

CONCLUSIONS, IMPLICATIONS, LIMITATIONS, AND RECOMMENDATIONS

A traditional security approach that depends on static rules and techniques as countermeasures for analyzing and assessing a computing environment with dynamic features cannot be adequate. The paper presented a conceptual analysis of virtualization security characteristics and practices, using a time-based spectrum. This is intended to pave the way for

the development of a dynamic time-sensitive model for hypervisor-based virtualization security. Dynamic security is of pivotal importance if the organization is to address the specific security vulnerabilities that virtualization might introduce. Stressing the importance of security solution-technology fit, our approach emphasizes that a successful IT security process takes two fundamental measures into consideration: time factors of threats and time factors of security practice responses.

Organizations should set their information security plans, policies, and standards through strategy-in-action, which entails the setting of a detailed action plan encompassing the use of goal-setting and critical success factors along with performance appraisal in order to facilitate an effective strategy implementation process (Reed and Buckley 1988). This approach is expected to continuously align people and tools to desired security goals, continuously get the security strategy updated, and continuously work on improving the security performance outcomes. Such an approach can help in understanding adversaries and the way they work, which can provide a better chance of choosing optimal countermeasures and applying them at the right time and place (Potts 2012).

Finally, while the adoption rate of virtualization technologies is on the increase, a security strategy - incorporating people, process, technology, and compliance regulations - that takes the importance of flexibility, timeliness, and continuous improvement into consideration would be of paramount importance to the effective deployment and utilization of virtualization the key for virtualization success. It is only through such dynamic strategies that benefits could be realized in a challenging technology environment such as that introduced by virtualization.

REFERENCES

Alto, P. 2008. "Power of Virtualization Largely Untapped despite Massive Adoption", HP News Advisory, September 2, (available online at: www.hp.com/go/virtualizationresearch08).

Anderson, D.F., Cappelli, D.M., Gonzalez, J.J., Mojtahedzadeh, M., Moore, A.P., Rich, E., Sarriegui, J.M., Shimeall, T.J., Stanton, J.M., Weaver, E., and Zagonel, A. 2004. "Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem," in *Proceedings of the 22nd International Conference of the System Dynamics Society*, Oxford, England, July 25-29.

Ashford, W. 2012. "Race to virtualization leaves critical business environments vulnerable," *ComputerWeekly* (July), p. 6.

Bradley, T. 2012. "Virtualization: McAfee Updates MOVE AV with Agentless Deployment," *PCWorld* (April 4), (available online at:

http://www.pcworld.com/article/253189/mcafee_updates_move_av_with_agentless_deployment.html).

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), pp. 523–548.

Cavallaro,L. Saxena, P. and Sekar, R. 2008. "On the limits of information flow techniques for malware analysis and containment," in *Proceedings of Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*.

Cummings, J. 2008. "Virtualization at every layer", *Network World*, pp. 64-67.

EWH IEEE 2005. "Security Risk Assessment Methodology Using IntelliGrid Environments," IEEE P1649 Draft ver 1, (available online at: http://www.ewh.ieee.org/soc/pes/pscc/Security_subcommittee/Security_Risk_Methodology_Paper.pdf).

Fabian, P., Palmer, J., Richardson, J., Bowman, M., Brett, P., Knauerhase, R., Sedayao, J., Vicente, J., Koh, C., and Rungta, S. 2006. "Virtualization in the Enterprise," *Intel Technology Journal* (10: 3), pp. 227-242.

Fernando, G. 2005. "To V or Not To V: A Practical Guide to Virtualization," BMC Software, Inc., (available online at: http://regions.cmg.org/regions/mcmg/m032206_files/To_V_or_not_To_V_submitted.pdf).

Friedman, M. 2006. "The Reality of Virtualization for Windows Servers," in *Proceedings of the 32nd International Computer Measurement Group Conference*, December 3-6, Reno, Nevada, pp. 907-918.

Garfinkel, T. and Rosenblum, M. 2005. When virtual is harder than real: security challenges in virtual machine based computing environments, in *Proceedings of the 10th conference on Hot Topics in Operating Systems*, ACM (10), p. 20.

Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M., Schunter, M., Wespi, A., and Zunic, N. 2007. Elevating the Discussion on Security Management: The Data Centric Paradigm, *in 2nd IEEE/IFIP International Workshop on Business-Driven IT Management*, IEEE Xplore, pp. 84-93.

Greene, T. 2008. "Replicating virtual servers vulnerable to attack", Network World, (available online at: http://www.networkworld.com/news/2008/021508-replicating-virtual-servers.html?fsrc=netflash-rss).

Greenemeier, L. 2007. "Virtualization's Next Frontier: Security", *InformationWeek*, March 17, (available online at: http://www.findwhitepapers.com/whitepaper1283/).

Hernick, J. 2007. "New Rules for Security," *InformationWeek* (December), p. AB2.

Hernick(b), J. 2007. "Virtualization Security Heats Up", *InformationWeek* (September), (available online at: http://www.informationweek.com/news/security/app-security/showArticle.jhtml?articleID=201803212).

Hietala, J.D. 2009. "Top Virtualization Security Mistakes (and How to Avoid Them)," SANS Analyst Program (August), (available online at:

http://www.sans.org/reading_room/analysts_program/McAfee_Catbird_Virtualization_Jul09.pdf).

Higgins, K. J. 2007. "New Tool: Virtual Tip of the Iceberg," Secure Virtualization Playbook, (available online at: http://www.findwhitepapers.com/whitepaper1283/).

Hoesing, M. T. 2009. "Virtualization Security Assessment," *Information Security Journal: A Global Perspective* (18:3), pp. 124-130.

Ioannidis, C., Pym, D. and Williams, J. 2012. "Information security trade-offs and optimal patching policies," *European Journal of Operational Research* (216: 2), pp. 434-444.

Jeloka, S., Gosselin, D., and Smith, R. 2012. *Oracle Database Security Guide -10g Release 2 (10.2)*, CA: Oracle America, Inc.

Kayworth, T. and Whitten, D. 2012. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive* (9:3), pp. 163-175.

Luo, S., Lin, Z., Chen, X., Yang, Z., and Chen, J. 2011. "Virtualization security for cloud computing service," in *International Conference on Cloud and Service Computing*, IEEE, 2011, pp. 174-179.

MacDonald, N. 2012. "Five Myths and Realities of Virtualization Security", Gartner, (available online at: http://blogs.gartner.com/neil_macdonald/2012/09/06/five-myths-and-realities-of-virtualization-security/).

MacDonald, N. 2011. "Securing the Virtualized Data Center: From Private Cloud to Public Cloud," Gartner, Oct. 25, (available online at: https://jmc.juniper.net/FileExplorer/Partners/Data%20Center/Data%20Center/English/Americas/How%20to%20Secure%20Your%20Virtualized%20Data%20Center.pdf).

Marko, K. 2012. "State of the Data Center," *InformationWeek*, (available online at: http://reports.informationweek.com/abstract/6/8845/data-center/research-2012-state-of-the-data-center.html).

McDaniel, G. 1994. *IBM Dictionary of computing* (Mcdaniel, G.,ed.). New York: McGraw-Hill, Inc.

Miller, K. and Pegah, M. 2007. "Virtualization: virtually at the desktop," in *Proceedings of the 35th annual ACM SIGUCCS fall conference*, ACM, pp. 255-260.

Mutch, J.and Anderson, B. 2011. "Protecting Virtual Environments from Hypervisor Sabotage" in *Preventing Good People from Doing Bad Things*, New York: Springer-Verlag, Inc.

Nelson, F. 2007. "Securing Your Virtualized Data Center," Secure Virtualization Playbook (August 17), (available online at: http://www.findwhitepapers.com/whitepaper1283/).

Olivier, M. 2007. "Towards a Configurable Security Architecture," *Data Engineering* (38:2), pp. 121-145.

Oppliger, R. 2007, "IT Security: In Search of the Holy Grail," *Communications of the ACM* (50:2), pp. 96 – 98.

Pan, W., Zhang, Y., Yu, M., and Jing, J. 2012. "Improving Virtualization Security by Splitting Hypervisor into Smaller Components," *Lecture Notes in Computer Science (*7371), pp. 298-313.

PCI Security Standards Council 2011. *Information Supplement: PCI DSS Virtualization Guidelines*, (available online at: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf).

Potts, M. 2012. "The state of information security," *Network Security* (July), pp. 9-11.

Prince, B. 2010. "Virtualization Security Falls Short among Enterprises, Survey Says," *eWEEK*, (available online at: http://www.eweek.com/c/a/Security/Virtualization-Security-Falling-Short-Among-Enterprises-Survey-506959/).

Radcliff, D. 2007. "Virtual System, Real Risk", *Network World* (August 20), pp. 30-34, (available online at: http://www.networkworld.com/supp/2007/ndc5/082007-virtualization-security.html).

Randel, R. 2008. "Virtualization Security and Best Practices," in *Netsecure'08: It Security and Forensics Conference and Expo*, Illinois, Chicago.

Reed, R. and Buckley, M. R. 1988. "Strategy in action – Techniques for implementing strategy," *Long Range Planning* (21:3), pp. 67-74.

Ritter, T. 2009. "Virtualization Security: Achieving Compliance for the Virtual Infrastructure," Nemertes Research, (retrieved from: http://www.gtsi.com/eblast/corporate/cn/02_25_2010/PDFs/Nemertes%20Virtualization%20Security%20Key%20Trends.pdf).

Rosenblum, M. and Garfinkel, T. 2005. "Virtual Machine Monitors: Current Technology and Future Trends", *IEEE Computer Society* (38:5), pp. 39-47.

Samy, G.N., Ahmad, R., and Ismail, Z. 2010. "A framework for integrated risk management process using survival analysis approach in information security," in *2010 Sixth International Conference on Information Assurance and Security (IAS), IEEE,* pp. 185-190.

Sanders, C. 2011. "Building a Malware Analysis Lab," (available online at: http://www.windowsecurity.com/articles/Building-Malware-Analysis-Lab.html).

Saunders, J. 2003. "A Risk Management Methodology for Information Security: The Analytic Hierarchy Process," (available online at: http://www.johnsaunders.com/papers/risk-ahp/risk-ahp.htm).

Scarfone, K., Souppaya, M., and Hoffman, P. 2011. "Guide to Security for Full Virtualization Technologies: Recommendations of the National Institute of Standards and Technology, Special Publication 800-125," National Institute of Standards and Technology (NIST) (1-35).

Singh, A. 2004. "An Introduction to Virtualization," (available online at: http://www.kernelthread.com/publications/virtualization/).

Skapinetz, K. 2007. "Virtualization as a blackhat tool", *Network Security* (October), pp. 4-7.

Stelte, B., Koch, R., and Ullmann, M. 2010. "Towards integrity measurement in virtualized environments – A hypervisor based sensory integrity measurement architecture (SIMA)," in *International Conference on Technologies for Homeland Security, IEEE*, (106-112).

Tan, T. C. C., Ruighaver, A. B. and Ahmad, A. 2010. "Information Security Governance: When Compliance Becomes More Important than Security," *IFIP Advances in Information and Communication Technology* (330), pp. 55-67.

Vijayan, J. 2007. "Virtualization Increases IT Security Pressures," *Computerworld* (August 27), pp. 14 – 16.

Von Solms, S. 2000. "Information Security - The Third Wave?", *Computers & Security* (19:7), pp. 615-620

Yunis, M., Hughes, J., and Roge' J. 2008. "Real Security in Virtualized Systems: A Proposed Model for a Comprehensive Approach to Securing Virtualized Environments", *Issues in Information Systems* (9:2), pp. 385-395

Zhang, X. and Dong, Y. 2008. "Optimizing Xen VMM Based on Intel Virtualization Technology," in *Proceedings of 2008 International Conference on Internet Computing in Science and Engineering* (ICICSE 2008), IEEE, pp. 367-374.