REAL SECURITY IN VIRTUAL SYSTEMS: A PROPOSED MODEL FOR A COMPREHENSIVE APPROACH TO SECURING VIRTUALIZED ENVIRONMENTS

Manal M. Yunis, myunis@broncs.utpa.edu
Jerald Hughes, jhughes1@utpa.edu
Joseph Roge', jroge@utpa.edu

ABSTRACT

Corporate adoption of new server virtualization technologies offered by VMWare, Microsoft, the open source community (Xen) and others raises both new opportunities and new risks for system security. Security issues of virtualization have received some attention in trade periodicals and journals, but a comprehensive and authoritative understanding of virtualized system security under current models of information security has yet to be developed. Such an understanding requires that some fundamental questions be asked: What is the place of virtualized system components in security models as they are currently understood? How should the implementation of virtualization be expected to affect security planning under such models? Our paper presents a first attempt to address these questions. We present an integrated model of system security highlighting the effects of virtualization. We then use this model to analyze security impacts of virtualization within the overall system security context, and present suggestions for further research to formalize security in systems incorporating virtualization.

Keywords: Virtualization, Information Security, Hypervisor, Security Management, Security Models

INTRODUCTION

In an era where the availability of information and information communication channels has become essential for the continuous operations and survival of organizations, corporations are deploying virtualization technology as a means of enhancing performance and reducing costs. However, while virtualization technologies may demonstrate productivity gains in terms of better information technology (IT) capacity planning, cost reduction, and flexibility, it is also true that they introduce platforms whose impact on security risks is poorly understood. That problem, information systems security, is drawing increasing attention in the business world. In a survey conducted by EDUCAUSE, 'Security and Identity Management' has been among the top three issues ranked currently important by IT managers in small, medium, and large organizations [6]. The significance of the issue has remarkably increased among IT and other managers since the year 2002, becoming the number one issue in the year 2006, and expected to be ranked the first again in 2008. Moreover, in 2002, the average security budgets of firms amounted to about $1.1 million and have been increasing since then [23].

It is therefore critical to systematically assess new technologies in terms of their impact on information security. However, an examination of literature on the security impacts of virtualization technologies clearly reveals a major problem that needs to be addressed: there is a gap between the adoption and use of virtualization technology and the understanding of its security impact, as is often the case with new IT [27]. A poll conducted by InformationWeek (Table 1 and Table 2) shows that 70% of the responding organizations have at least one virtualization server running in place, while only 12% have a security strategy that aligns with the virtual machines (VMs) they have [21].

Table 1 - Security Strategy Implementation (%)

% of Organizations	*Security Strategy Implementation*
12 %	have VM tailored strategy in place
23 %	are getting prepared to have an IT security strategy
29 %	have VM servers comply with the same security strategy related to conventional servers
36 %	have no IT security in place for virtual servers

Source: InformationWeek Poll, 2007

Table 2 - Server Virtualization Adoption Rate (%)

Percentage of Companies	*Percentage of Server Virtualization*
30 %	0 % server virtualization
48 %	1 - 25% server virtualization
10 %	51 - 75% server virtualization
9 %	26 - 50% server virtualization
2 %	76 - 99% server virtualization
1 %	100% server virtualization

Another finding of this study shows that 21% of those organizations *which have no current security plan actually perceive VMs as "more prone to risk as conventional servers*", while 36% have no formal security plan for their virtualized servers [21]. Moreover, according to a survey conducted by Network World [36], 36% of respondents said they realize virtualization has increased security risk; about 56% had deployed traditional countermeasures, like anti-spam, anti-malware, and anti-virus filters, for example; another 56% had installed virtual LANs to check unauthorized access to their virtualized systems with their intrusion detection sensors; 34% were aware of the vulnerability of their virtualization platform layer and thus wanted to push vendors to enhance the security of their products. Finally, others had not implemented any integral security measures for their virtual systems at all. This suggests that many enterprises are not applying basic security policies necessary for protecting their virtualized servers. It seems that there is a lack of understanding in some organizations regarding the nature of security needed for virtualization systems. Some of them wrongly assume that the approach for securing virtual machines is not different from that for securing physical servers. This likely would not be sufficient for optimal protection for virtualized machines. As a result, while organizations can focus on the rapid implementation of virtualization in order to realize consolidation benefits, they may fail to deploy best practices, tools, and technologies to address security issues. It has been predicted that until 2009, 60% of virtual machines will be less secure than the physical servers [17].

Industry experts have often discussed virtualization technology and its performance features, but few have tackled the issue of potential security risks associated with virtualization technology. Moreover, among those who did, none have specifically addressed virtualization within a security framework. Discussions of virtualization security questions have been taking place so far within the context of cost-benefit analysis [17] or within the context of technical security mechanisms and budget limits [11], but a broader perspective than these is needed. Although important security issues pertinent to contemporary virtualized systems have been addressed by many researchers from the perspective of finding the right technologies, hardware, and software that would mitigate or eliminate the security risks or threats enhanced by such environments (example, [25, 34]), there is a serious risk that these efforts will not be sufficient. This is the point of view taken by Gartner research, which argues that the process of establishing security measures for virtual machines must precede their deployment, and even better, before vendors or products are selected [17]. This way, the product selection process takes the security measures into consideration rather than tailoring security measures to the products' characteristics.

Security is never a one-dimensional situation, where any hole can be filled or covered with a technology product. Rather, security is a process [14, 3, 27, 24, 45] entailing interdependent elements that function together in order to achieve an optimal level of security in the organization, thus resulting in the prevention or mitigation of possible information security threats – whether they are natural or man-made threats. A framework which incorporates virtualization explicitly can help in viewing the security problems arising from virtualization technology characteristics from the perspective of their relationships to antecedents and outcomes, facilitating the comprehension of causes and promoting the generation of good solutions.

The objective of this paper is to develop a framework to incorporate virtualization technology into a security model for the comprehensive analysis of information security risk. The purpose of such a framework is to help in better assessing the opportunities as well as the risks presented by this technology. The context referred to is the hypervisor-based server virtualization, with the hypervisor being the virtual machine monitor (VMM), which runs directly above the hardware and enables instances of operating systems to run. This can be viewed as a three-layer model, with the hardware at the base, the operating system at the top, and the hypervisor being the middle layer [48].The remainder of the paper is organized as follows. In section 2 we conduct a review of extant literature on virtualization technology, as well as on general IT security frameworks. In section 3 a virtualization security framework is developed, in which a strength-weakness analysis (SWA) of virtualization technology is depicted and discussed. Section 4 will present conclusions and suggestions for future research.

OVERVIEW AND LITERATURE

Simply put, virtualization technology allows multiple operation systems to run and handle several applications on a single physical resource, such as a server or a storage array [29]. The recent new offerings of this basic technology have affected the way IT managers manage their IT systems and applications [40]. But virtualization itself is not new; its roots extend back to the 1960s [41]. It was then devised to provide a means for partitioning large IBM mainframes into several virtual machines [20]. The Java RunTime Environment is a more current example of a virtual machine with widespread adoption. For the purposes of this paper, "virtualization" and "virtualized" systems refer to a collection of related technologies which insert an additional layer of abstraction, the 'hypervisor', above the hardware level, to allow the implementation of multiple guest operating systems which themselves do not have direct access to hardware.

Today, virtualization is a highly discussed topic in trade as well as academic papers, for at least two reasons. First, the adoption rate of the technology seems to be increasing. A survey conducted by Forrester Research shows a remarkable increase in the adoption of server virtualization in North America since 2005, with 51% of enterprises now using or testing the technology. A similar growing interest in server virtualization is observed worldwide, with the highest being in Asia Pacific [16]. Moreover, IDC expects the rate to increase in the future, and forecasts the number of virtual servers will increase at a compound annual growth rate of 40.6 percent by 2010 [26]. Second, the technology provides several advantages, but also presents challenges. Wlodarz [47] has pointed out that the technology could be considered a double-edged sword. We now turn first to the advantages which are largely driving the adoption of virtualization.

Advantages of Virtualization Technologies

Several advantages of virtualization technology have been identified by researchers, vendors and technical analysts. These may be grouped into major categories, including: cost savings and efficiency in an organization's computing infrastructure and resources [9, 40, 13], interoperability and mobility with legacy software [41, 40, 46], and reliability and security of applications [40, 37].

The cost efficiency advantage is derived from the server consolidation feature of virtualization [47, 10]. It is estimated that modern servers typically use 5-10% of capacity at one time [48]. With its parallel execution feature, virtual server utilization may approach 100% [13]. A virtualized server can replace several underutilized servers [41], thus enhancing IT efficiency. According to IBM, such a "resource optimization strategy" through server consolidation can both support an organization's strategic goals and achieve a lower total cost of ownership. IBM reports levels of savings that could be achieved with server consolidation based on data gathered in 2006: hardware costs, 33% to 70%; maintenance costs, 50%; support costs, 33%; and floor space and facility costs, 33% to 50% [8]. Bielski [4] concurs that virtualization technology provides organizations with the ability to "call up" idle servers, thus avoiding inefficiencies and wasted resources.

Moreover, legacy applications are well supported through virtualization technology [48]. For example, older software can be enabled to run on modern hardware/software. The advantage here lies in extending the life cycle of legacy software at minimal cost and lower risk [40, 37]. Cost efficiency is also manifested in the number of software licenses the organization has to buy to maintain redundant and conforming infrastructure. Consequently, based on operating system independence, instead of buying many versions of any software, only one version, which operates at the virtualized level, would be installed and supported [37].

Virtualization also presents potential benefits for reliability and security. Many virtualization systems have been developed for the purpose of testing and debugging purposes, especially in the process of system development [47]. This allows new or

upgraded systems testing to be run without disrupting ongoing operations. It also eliminates the need for duplicate non-virtual environments [40] normally required in such processes. Since virtualization technologies provide isolation based on the concept of process abstraction [47], they may provide secure environments with minimum risk levels, especially for sensitive data and information. In fact, virtual machines are thought by some researchers as being capable of providing "secure, isolated sandboxes for running untrusted applications" [41]. Such an execution environment could be created on the spot as the user downloads something from the Internet and runs it. Finally, virtualization technologies are recommended for data protection, continuity of operations, and rapid data recovery [28].

Despite the advantages enumerated above, it cannot be said that virtualization is a technology without challenges. We next examine the issues which are the focus of this paper, those related to security.

Security and Virtualization Technologies

According to Gartner research, while virtualization offers organizations many benefits related to cost reduction and IT productivity increases, if it is adopted without having specific IT security measures in place then its effects on the company can be problematic. This stems from the fact that virtualization is based on a "privileged layer of software", which places all the virtualized tasks at risk in the event that that layer is compromised [17]. Although virtualized systems' mobility and transparency can enhance network monitoring, security checking, and security information sharing, they also bring negative issues to the picture. For example, while VMs make isolation possible, experience shows that this isolation is not complete, potentially allowing VM cross-interference which negatively affects their behavior [10]. Another point is the simplicity and speed with which VMs can be set up. Sometimes, such processes are done without the control of the IT department, thus increasing the risk of having VMs created, moved, or removed anytime by any source [45]. Some IT analysts have noted that virtualized servers face the same risks as traditional ones, implying that if a virtualized server is at risk, all associated VMs and applications related to them may also be vulnerable [45].

In addition, some researchers highlight security problems resulting from implementation flaws in virtualization software. Ormandy [31] points out that virtualization packages may include security flaws which allow a potential attacker to escape reliably from a virtual machine assumed to be well secured and protected into the hosting layer beneath. Ormandy also classifies the threat levels to which virtualization machines may be exposed as *total compromise* (in which arbitrary code may be run on the victim's machine by the attacker), *partial compromise* (in which sensitive information about the host is leaked), and *abnormal termination* (in which the hypervisor stops unexpectedly or prevents the administrator from interacting with the virtual machine with his original rights).

Experts have listed methods to deal with the negative security aspects of virtualization - for example, intrusion detection systems, integrity checking, and forensic analysis [34]. But this struggle is a defensive one, since the methods applied are static rather than dynamic [42]. Unfortunately, static security methods in virtualized IT are considered by some to be ineffective [47]. Security measures should be both dynamic and flexible to deal with the portable and flexible features of virtualized servers; however, this makes such IT environments more prone to security hazards [1]. Oppliger [32] also argues that security risks cannot be faced with products and services only, since security issues are problems of engineering and management – not technology alone.

Security Frameworks

Computer security – whether in traditional computing or virtualized environments – should be viewed as a core process and looked at from a holistic perspective rather than from a specific technology or a cost perspective. Baskerville and Siponen [3] and Trim [44] emphasize the need for security management standards, and for having security issues placed within the management decision-making framework. With this approach, commitment to security policy is enhanced at the employee, department, and organization levels.

Moreover, managers should know both the impact that an attack can have and its probability of occurrence [12]. This is important in order to select appropriate measures of prevention or mitigation. The need for such knowledge stems from the fact that organizations are increasingly being exposed to the risks of attacks and their resulting damage. Thus, choosing the appropriate safeguards requires that security issues be considered from a security framework perspective, viewing information security as a process which starts with an assessment and understanding of the possible threats and vulnerabilities, and ends with the selection of appropriate control, measures [12]. These will help IT managers deal with threats and mitigate their effect on the company's information resources. We now consider several models from the literature dealing the IS security issues.

A basic model for information security includes the notions of information assets, threats (e.g., data theft), threat agents (such as a hacker), vulnerabilities (such as an unchecked buffer), exploits (e.g., malware), and the risk of attack [7]. Using a certain intrusion technique (physical, personal, hardware, software, or procedural), a threat agent (authorized user, unauthorized user, or an environmental factor) may attack the information assets of a company. The consequences of such attacks may include destruction of information, information corruption, theft/loss of information, disclosure of information, or interruption of services [12]. Fundamental security measures to deal with threats include:

- Authentication - the identity of the party requesting access is verified;
- Access Control - unauthorized use of resources is prevented;
- Data Confidentiality - meaning that information privacy is preserved;
- Data Integrity - the prevention of unauthorized alteration or destruction of data;
- Non-repudiation - audit records and logs should be maintained and archived in order to prevent denial of communication.

Nugent and Raisinghani [30] add threat analysis and system availability and reliability as important elements. Parker [33] mentions that information security comprises six important elements, including: authenticity, confidentiality, integrity, possession, availability, and utility. Moreover, many researchers have emphasized the importance of considering information security an information risk management process. For example, Blakely [5]states that an effective process starts with policies that are first defined and then enforced. This, according to the author, can be done through a mix of procedures and technical measures, including:

- Protection measures to prevent threats or their adverse consequences from taking place;
- Detection measures to warn the company when harmful events occur;
- Response measures to deal with threats and facilitate continuity and recovery;
- Assurance measures to assess and validate the effectiveness of the above-mentioned measures.

By talking about processes and not confining the discussion to security technology only, Blakely includes an important additional dimension in information security management. Similarly, [22] suggested an integrated systems model for information security management based on information policy theory, risk management theory, control and edit theory, management system theory, and contingency theory. This integration was based on the idea that data security and integrity can be achieved by combining systems, internal controls, and operations [22]. In fact, the concept of having a comprehensive system development generally that is well aligned and integrated with the IT security approach is an important one [2].

In an attempt to overcome the limitations of static analysis and modeling Saunders [39] introduced a dynamic risk model for information technology security. The model included three dimensions for security counter measures to possible threats. These are:

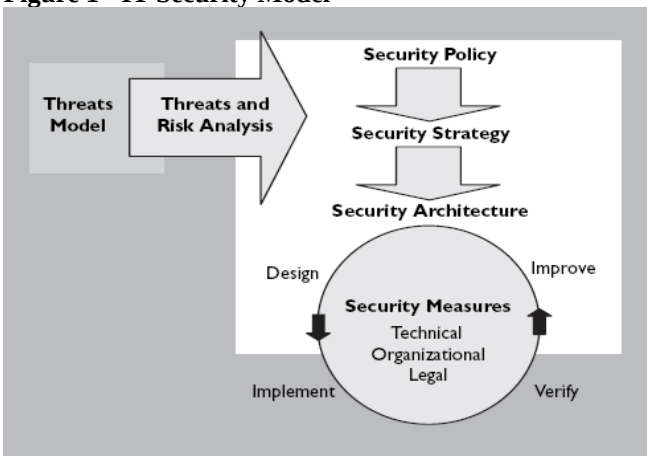
- People counter-measures, such as security administrator competence;
- Process control measures, such as intrusion detection and access control;
- Technology counter-measures, such as firewall technology.

Along the same lines, Vijayan [45] refers to the importance of tackling security hazards from a people, process, and technology perspective. His point is that while it is useful to have tools that can instantly detect virtual machines once they are installed on a server, it is equally, if not more, important to have well enforced policies in place in order to control and better manage the virtualization environment. The significance of these policies is seen when the possibility of creating new servers that don't adhere to security policies in a virtualization environment is considered [18]. Moreover, a framework for managing such information security risks has been created to help organizations identify, assess, and handle threats through a risk management strategy that includes coordination, credibility, effectiveness, and transparency [24].

Finally, an IT security model (Figure 1) has been suggested in which security problems would be approached within the context of a comprehensive IT security process that takes into consideration strategic, political, architectural, and legal measures [32]. The result would be a security architecture that is developed and enforced in alignment with all requirements of the corporation and its environment.

This security architecture includes technical, organizational, and legal measures that are subjected to a complete process of design, implementation, verification, and continued improvement. According to the author, the security process should start with a threat model and a risk analysis that would identify threats and assess their impact on the organization. It also should include a security policy that would govern the security measures to be adopted and deployed. Another important point to be considered is that these security measures must be periodically improved [32]. Because of the comprehensive nature of this particular model, we have made it the foundation for our virtualization security framework which appears in the following section.

Figure 1 - IT Security Model

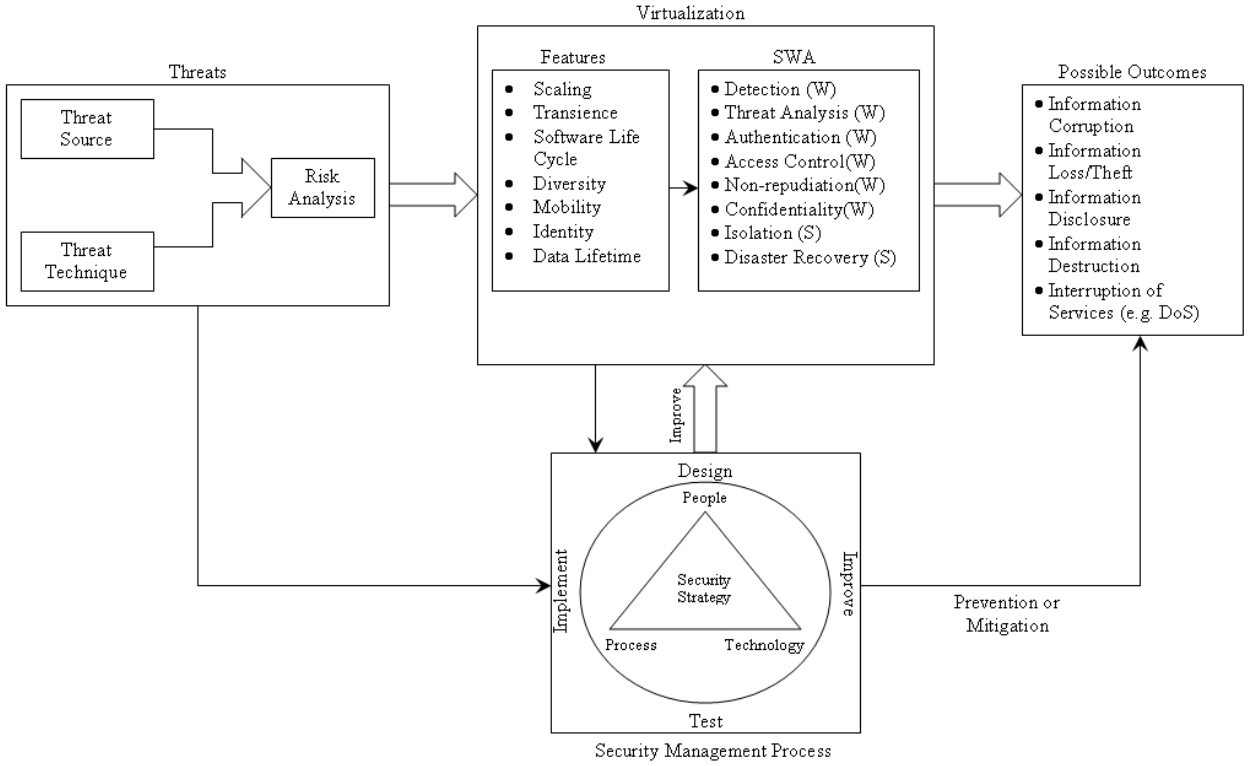


Source: Oppliger [32]

3. A Virtualization-Security Framework

The proposed model (Figure 2) in this study is an attempt to incorporate virtualization into a security framework. It builds upon several information security models: Ciampa's [7] threat model, Saunder's [39] risk analysis model, and Oppliger's [32] IT security model. It also builds on our review of virtualization literature in order to analyze the security features of this technology in terms of both strengths and weaknesses. Following is a description of the model components.

Figure 2 - Virtualization-IT Security Framework



3.1 Model Components and Description

The model starts with a threat and risk assessment and analysis. On the left side, threats to information assets are created by a **threat source** (threat agents and their resources), and realized by a specific **threat technique** (exploits and methods of attack). A threat analysis based on these first two components will identify the quantity and nature of potential threats, whereas **risk analysis** will assess the risk level of these threats in terms of their impact on the organizational information assets and resources. Of course, these are relative to the computing environment available in the organization. In a virtualized environment, these threats may have diverse effects on IT corporate security, which may be weakened or enhanced through the features of the virtualization technology.

Consequently, a virtualization security strategy should take into consideration the nature of this corporate computing environment, as well as the results of the threat and risk analysis stage. Based on this, identifying the features of hypervisor-based virtualization technologies can make the process of designing, developing, implementing, and enforcing a security policy and strategy more systematic, feasible, and effective.

Those features of the **virtualization** (our center-top) component of the corporate information environment which can be regarded as security problems are derived from Garfinkel and Rosenblum [15], and are herein summarized:

- Scaling – The number of VMs in an organization can increase at a rapid sometimes unpredictable rate. This might weaken the control and management process of the virtualization environment.
- Transience – VMs may appear and disappear from a network environment irregularly. If a VM gets infected, it can infect other machines and disappear before being detected.
- Software Lifecycle – In VMs, a machine lifecycle does not progress forward monotonically. Instead, the machine can be rolled back to previous states, with the potential to reload older flawed software versions.
- Diversity – VMs allow diverse software versions, current and old, to run. While this promotes efficiency, it can create problems because of the need to maintain and protect a wide range of operating systems.
- Mobility – VMs can be copied, shared and carried on portable media, which introduces a range of vulnerabilities. Also, a VM may run on several hosts, so if it gets infected it may be difficult to determine accountability, since activity logs may be lacking.
- Identity – a VM can be used by several users, making identity establishment problematic. Identifying who did what and where the problem originated may be a difficult task.
- Data Lifetime – The period of time in during which data remains in the system might not be minimized in a VM. As a result confidential data might be accessed by unauthorized users, destroyed, or compromised [15].

In addition, we incorporate in the expanded **virtualization** component of our model a strength-weakness analysis (SWA) of hypervisor-based virtualization technology, based on the security dimensions proposed by various researchers. A list of these dimensions, with description and assessment, appears in Table 3 below.

Table 3 – IT Security Measures in a Virtualization Technology Context

Security Measure	Description	Reference	Strong or Weak
Detection	VM can be detected by cutting-edge malware, like a rootkit. The malware modifies its behavior, gets unidentified by security analysts, leaving the computer systems highly vulnerable	Saydjari, 2007 Wlodarz, 2007 Potter, 2006	**W**
Threat Analysis	Monitoring the host OS and virtual network is limited if architecture is poorly designed. This means finding vulnerabilities and assessing correct configuration may not be reliable.	DeCarlo, 2007 Gold, 2007	**W**
Authentication	In some cases, if an unauthorized user accesses a VM, he/she may modify the authorization application so that it does not check for authentication correctly and allows compromised code to execute. In another case, the application may be totally compromised by the attacker, and the authentication step may be skipped.	Shimizu et al, 2007 Haifeng et al, 2007	**W**

Access Control	Unless there is a hypervisor-based mandatory access control (MAC) that provides proper distributed workload isolation, the hypervisor-based platforms cannot currently enforce restrictions on the sharing of resources between multiple VMs.	Valdez et al, 2007 Payne et al, 2007	**W**
Non - repudiation	Can be achieved only through secure communication and cryptography	Smith et al, 2006	**W**
Confidentiality	A buffer overflow attack can allow for the extraction of useful information from a VMM	Haifeng et al, 2007	**W**
Isolation	Malware, new security software, susceptible programs, and new web sites, for example, can be examined in a sandboxed VM without the fear of adversely harming other VMs.	Skapinetz, 2007 Rosenblum, 2004	**S**
Disaster Recovery	Virtualization helps in making the IT environment more portable. Also, since the operating systems are run on the same server, the operations can not be all down when malware targets a VM.	Greenemeier, 2007	**S**

On the top right of our model, the effect on information resources can be any of the '**possible outcomes**' component in the model. These outcomes are adopted from Farahmand et al [12].

To mitigate the effect of these adversarial outcomes or prevent them from taking place, a **security management process** – based on Oppliger [32] - should be in place. With this process, a security policy or strategy should be designed, implemented, and periodically tested through a combination of elements that work as an integrated system, namely the organization's people, technology, and operations processes. This policy or strategy should be continuously improved and updated, since there will always be changes and/or advancements in technology, expertise, and process reengineering outcomes. The synergic effects of all the elements mentioned in the security management process can allow for a dynamic rather than a static approach to be followed in dealing with virtualization security challenges.

Conclusion, Limitations, and Implications for Future Research

The authors believe that incorporating virtualization security hazards into a comprehensive information security framework can help organizational and IT managers systematically plan and enforce security policies. These policies should include people, procedures, and technology dimensions in order to make use of the benefits of this technology and to eliminate or mitigate its security hazards. Our proposed model of virtualization security supports this goal by viewing information security from a holistic perspective rather than a technology-based perspective. Another implication is for hardware, hypervisor, and security vendors to work together to include ample security mechanisms that are optimal to the client organization's security strategy and objectives. Finally, academicians may find in this model new ways to look at virtualization security challenges and find new avenues for virtualization security related research.

Since the current generation of hypervisor-based virtualization products is so new, of primary interest at this stage is observing and understanding outcomes in the field, particularly any best practices which have arisen as the result of ad hoc analysis and trial-and-error. As the purely technical features and weaknesses of their implementation become better known and catalogued, it should become possible to observe patterns of interactions among assets, threats, and technology which can give rise to rigorous theoretical description. Also not yet explored is the nature and impact of human interactions with this technology. For example: how do users make decisions about virtualized legacy software; how does the use of virtualized systems affect trust among users, security awareness and vigilance among system administrators, and IT strategic decision-making among upper management; how does the use of virtualized systems affect attackers' decision-making in the selection of targets and methods; is the perception of virtualized systems' security among IT professional aligned or mis-aligned with actual observed outcomes in deployed technology? A strong and systematic security assurance approach, such as the one recommended by our model, can benefit from the answers to all of these user-interaction questions.

The major implications of this research can be summarized in the following points:

- Virtualization security is an integrated process. Moreover, it is a continuous process that should

always be verified and improved; it is not a one-point-of-time solution to a certain threat or problem.
- Virtualization security policy and strategy should be aligned to the environment where it is implemented.
- Finally, the virtualization security process is a socio-technical process, requiring behavioral as well as technological factors to achieve desired security objectives. This is important as it will provide a dynamic rather than a static solution to security issues.

This is preliminary research. Our model was based on both the literature and on professionals' testimony related to models of information security and to virtualization technologies. The model presented is not directly validated by empirical evidence. With this in mind, future research may empirically assess the validity of the model, introduce a quantitative approach whereby the model can be tested using real or simulation data, and consider the behavioral elements that would influence the success of the process.

In conclusion, vulnerabilities are certainly present. However, they can not be managed with limited testing and technology products and services. A security management process, including technology, business processes, and people dimensions should be systematically designed, implemented, and periodically updated. Also, security policies that are well articulated and enforced should be in place. We believe this will help organizations reap the ultimate benefits of virtualization technologies. It will also help in building a new approach to deal with technology security hazards, an approach that is more proactive than reactive, more dynamic than static, and more preventive than defensive.

REFERENCES

1. Antonopoulos, A., Virtual Servers: more or less secure, *Network World*, July 23, 2007, retrieved from: www.networkworld.com.
2. Baskerville, R., Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computing Surveys*, Vol. 25, No. 4, December 1993, PP. 375-414.
3. Baskerville, R. and Siponen, M., An information security meta-policy for emergent organizations, *Logistics Information Management*, Vol. 15, No. 5/6, 2002, pp. 337-346.
4. Bielski, L., Have server, will "virtualize", *ABA Banking Journal*, Vol. 95, No. 12, 2003, p. 45.
5. Blakely, B., McDermott, E., and Geer D., Information Security is Information Risk Management, *Proceedings of the 2001 workshop on New security paradigms*, ACM, 2002, pp. 97–104.
6. Camp, J., and Deblois, P., Current Issues Survey Report, 2007, *EDUCAUSE Quarterly*, Vol. 30, No. 2, 2007.
7. Ciampa, M. (2005). Security+ Guide to Network Security Fundamentals, 2nd edition, Boston: Thomson Course Technology.
8. CMP, Improving TCO with Server Consolidation and Allocation, 2007, retrieved from: http://www.businessinnovation.cmp.com/ebook1.jhtml.
9. Crosby, S. and Brown, D., The Virtualization Reality, *ACM Queue*, December/January 2006-2007, pp. 34-41.
10. Fabian, P., Palmer, J., Richardson, J., Bowman, M., Brett, P., Knauerhase, R., Sedayao, J., Vicente, J., Koh, C., And Rungta, S., Virtualization in the Enterprise, *Intel Technology Journal*, Vol. 10, No. 3, 2006.
11. Faisst U. and Prokein, O., An Optimization Model for the Management of Security Risks in Banking Companies, *Proceedings of the Seventh IEEE International Conference on E-Commerce Technology*, IEEE, 2005.
12. Farahmand, F., Navathe, S.B., Enslow, P.H., and Sharp G.P., Managing vulnerabilities of information systems to security incidents, *Proceedings of the 5th international conference on Electronic commerce*, ACM, 2003, pp. 348-354.
13. Fernando, G., To V or Not To V: A Practical Guide to Virtualization, *BMC Software, Inc*, 2005, retrieved from: http://regions.cmg.org/regions/mcmg/m032206_files/To_V_or_not_To_V_submitted.pdf.
14. Fisher, R., Information Systems Security, *Prentice-Hall*, New Jersey, 1984.
15. Garfinkel, T. and Rosenblum, M., When virtual is harder than real: security challenges in virtual machine based computing environments, *Proceedings of the 10th conference on Hot Topics in Operating Systems*, Volume 10, *ACM*, 2005.
16. Gillett, F. E., Server Virtualization Accelerates in North America, February 2007, retrieved from: http://www.forrester.com/Research/Document/Excerpt/0,7211,42868,00.html.
17. Gold, S., Time to face virtualized realities, *Infosecurity*, May/June, 2007, pp. 35-38.
18. Greenemeier, L., Virtualization's Next Frontier: Security, *InformationWeek*, March 17, 2007.

19. Haifeng, x., Sihan, Q., and Huanguo, Z., XEN Virtual Machine Technology and its Security Analysis, *Wuhan University Journal of Natural Sciences*, Vol. 12, No. 1, 2007, pp. 159-162.
20. Hensbergen, E. V., The Effect of Virtualization on OS Infrastructure, April, 2007, retrieved from: http://whitepapers.zdnet.co.uk/0,1000000651,260277141p-39000684q,00.htm.
21. Hernick, J., New Rules for Security, *InformationWeek*, December, 2007, p. AB2.
22. Hong, K, Chi Y., Chao, L., and Tang J., An integrated system theory of information security management, *Information Management and Computer Security*, Vol. 11, No. 5, 2003, pp. 243-248.
23. Jaquith, A., Security Metrics: Replacing Fear, Uncertainty, and Doubt, NJ: Pearson Education, Inc., 2007.
24. Jones, A., A framework for the management of information security risks, *BT Technology Journal*, Vol. 25, No. 1, January, 2007, pp. 30-36.
25. Karger, P., Multi-Level Security Requirements for Hypervisors, *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE*, 2005.
26. LeClaire, J., IDC Report: Virtualization Cannibalizes Server Sales, March 21, 2007, retrieved from: http://www.cio-today.com/story.xhtml?story_id=021001DOJMIF.
27. Loch K., Carr, H., and Warkentin, M., Threats to Information Systems: Today's Reality, Yesterday's Understanding, *MIS Quarterly*, June 1992, pp. 173 – 186.
28. Matthews, J.N., Herne, J.J., Deshane, T.M., Jablonski, P.A., Cherian, L.R., and McCabe, M.T., Data Protection and Rapid Recovery from Attack With A Virtual Private File Server and Virtual Machine Appliances, *Proc. of the IASTED Int. Conf. on Communication, Network and Information Security*, Nov. 2005, pp.170–181.
29. Miller, K. and Pegah, M., Virtualization: Virtually at the Desktop, *Proceedings of the SIGUCCS'07, October 7-10, 2007, ACM*, 2007, pp. 255-260.
30. Nugent, J. and Rasinghani, M., The Information Technology and Telecommunications Security Imperative: Important Issues and Drivers, *Journal of Electronic Commerce Research*, Vol. 3, No. 1, 2002, pp. 1-14.
31. Ormandy, T., An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments, *CanSecWest 2007*, Vancouver BC, Apr. 18-20, 2007.
32. Oppliger, R., IT Security: In Search of the Holy Grail, *Communications of the ACM*, Vol. 50, No. 2 February 2007, pp. 96 – 98.
33. Parker, D., The Folk Art of Information Security Needs an Upgrade, *Communications of the ACM*, Vol. 47, No. 8, August, 2004, pp. 11-12.
34. Payne, B., Carbone, M., and Lee, W., Secure and Flexible Monitoring of Virtual Machines, *IEEE Computer*, 2007, pp. 385-397.
35. Payne, R., Sailer, R., Cáceres, R., Perez, R., and Lee, W., A layered approach to simplified access control in virtualized systems, *ACM SIGOPS Operating Systems Review*, Vol. 41, No. 4, July 2007.
36. Radcliff, D., Virtual System, Real Risk, *Network World*, August 20, 2007, pp. 30 – 34, retrieved from: http://www.networkworld.com/supp/2007/ndc5/082007-virtualization-security.html.
37. Rosenblum, M. and Garfinkel, T., Virtual Machine Monitors: Current Technology and Future Trends, *IEEE Computer Society*, May 2005, pp. 39-47.
38. Rosenblum, M., The Reincarnation of Virtual Machines, *ACM Queue*, July/August, 2004, pp. 34-40.
39. Saunders, J., A Dynamic Risk Model for Information Technology Security in a Critical Infrastructure Environment, *ASCE*, 2004, retrieved from: http://www.johnsaunders.com/papers/riskcip/RiskConference.htm.
40. Shiveley, R., Enhanced Virtualization on Intel Architecture-based servers, *Technology@Intel Magazine*, April, 2005.
41. Singh, A., An Introduction to Virtualization, Kernelthread.com, 2004, retrieved from: http://www.kernelthread.com/publications/virtualization/.
42. Skapinetz, K., Virtualization as a blackhat tool, *Network Security*, October 2007, pp. 4-7.
43. Smith M., Friese, T., Engel, M., and Freisleben, B., Countering security threats in service-oriented on-demand grid computing using sandboxing and trusted computing techniques, *ScienceDirect*, Vol. 16, 2006, pp. 1189 – 1204.
44. Trim, P., Managing computer security issues: preventing and limiting future threats and disasters, *Disaster Prevention and Management*, Vol. 14, Issue 4, 2005, pp. 493-505.
45. Vijayan, J., Virtualization Increases IT Security Pressures, *Computerworld*, August 27, 2007, pp. 14 – 16.

46. Waters, J., Locked down, not out, *T.H.E. Journal*, Vol. 34, No. 2, 2007, pp. 35-39, retrieved from: http://thejournal.com/articles/20160.
47. Wlodarz, J.J., Virtualization: A double-edged sword, May 19, 2007, retrieved from: http://arxiv.org/abs/0705.2786.
48. Young, E. and Thrower, M., Towards Virtualization: A New Approach in Server Management, *Ariadne*, issue 51, April, 2007, retrieved from: http://www.ariadne.ac.uk/issue51/young-thrower/.