Virtualization Technologies in Information Systems Education

Dale L. Lunsford
School of Accountancy and Information Systems
The University of Southern Mississippi
730 East Beach Blvd.
Long Beach, MS 39560
Dale.Lunsford@usm.edu

ABSTRACT

Information systems educators must balance the need to protect the stability, availability, and security of computer laboratories with the learning objectives of various courses. In advanced courses where students need to install, configure, and otherwise manipulate application and operating system settings, this is especially problematic as these activities threaten the stability of workstations and security of networks. Virtualization platforms offer the capability to integrate advanced topics into courses in a way that gives students control so that they can perform hands-on activities that would be infeasible on shared physical computers. This paper introduces virtualization technologies, discusses the use of desktop virtualization in a business information systems security course, outlines some challenges and limitations of virtualization, and enumerates additional opportunities and benefits of virtual technologies.

Keywords: Virtualization, Computer laboratory, Education, Security, VMWare, Parallels

1. INTRODUCTION

Information systems educators often encounter control and management issues with regard to shared computers in university laboratories; when students use computers in laboratories, they are using equipment that must be available and operational for the next student (Hu, Cordel, and Meinel, 2004). In many cases, the transition time between users is short as is the case between class sessions. As a result, there is a need to regulate the use of these computers to ensure availability. Often, the solution is to lock the computer down so that students are unable to make changes to settings or the computer rolls back to a stable state after a reboot; for example, products such as Faronics Deep Freeze (http://www.faronics.com) prevent permanent changes to desktop configurations. At the same time, problems arise when the restrictions placed on the use of a computer in a laboratory interfere with the instructional objectives of the course.

Information systems curriculums address a wide range of topics. Students work with personal productivity applications such as word processors, spreadsheets, presentation graphics, and database management systems. These applications generally do not pose a threat to availability of shared computers. Students taking more advanced information systems courses often need access to sophisticated tools as well as the capability to install and configure applications. For example, to understand fully the issues associated with information assurance and the implementation of appropriate security controls, students need to work with tools that may pose a threat to the stability of systems. In some settings, students, especially upper-level students, need exposure to information access controls, password-auditing tools, firewalls, encryption, and similar tools, as well as the tools used by attackers to compromise the security of systems and information. Students may also need to work with system settings and otherwise manipulate their computers. This is something network administrators work hard to prevent.

Kroeker (2009) describes uses of virtualization by hardware and software vendors, including as a tool for distributing software, enabling cloud computing, and enhancing security. Virtualization technologies offer similar benefits to IS educators and students. Using virtualization technologies, students may work with systems in ways that would otherwise be undesirable because of the threat to the stability and availability of computers in shared laboratories. Additionally, virtualization enables a student's changes to remain persistent between sessions so that the student can engage in extended projects and projects that build on one another. This allows faculty to extend the range of topics covered in information systems courses, as well as integrate more risky, hands-on activities. At the same time, since the student is working in a virtual environment, the host computer remains unaffected.

This paper describes the use of virtualization in a business-oriented information systems security course focusing on the formulation and implementation of policies for information assurance, desktop security, and the examination of security measures. This paper consists of four major sections. The first section is an overview of virtualization and virtualization technologies. The second section reports on the use of virtualization in an information

systems security course. The third section discusses potential limitations and challenges when using virtualization in the classroom. The fourth section describes additional applications of virtual technologies in educational settings.

2. VIRTUALIZATION TECHNOLOGIES

Organizations are adopting virtualization, in a variety of forms, to address challenges in computing (Brandel, 2005). Drews defines virtualization as follows:

> In a nutshell, virtualization means abstracting a computer's physical resources into virtual ones with the help of specialized software. Abstraction layers allow for the creation of multiple VMs [virtual machines] on a single physical machine. Each VM can run its own OS. (Drews, 2006, ES 5)

Essentially, virtualization enables one to encapsulate the processing capabilities of a computing resource into a virtual machine and execute the virtual machine in an isolated environment on a host computer. This enables one to run one or more virtual machines on the same host computer, run a virtual machine on a host computer with a different operating system, run a virtual machine in a "sandbox" where the virtual machine's action cannot modify the host computer, to name just a few applications. Common applications range from virtual machines supporting different operating systems running on the same high-power server platform to virtual machines supporting different applications running on the same desktop computer. Figure 1 shows a Microsoft Windows XP virtual machine running under Microsoft Windows Vista. Figure 2 is a Fedora Linux virtual machine running under Microsoft Windows Vista. Given adequate resources on a host computer, one may run multiple virtual machines simultaneously. Additional combinations of guest and host computers are possible, depending on the virtualization software used. For example, using VMWare, Parallels, and other products, one may run Microsoft Windows or Linux virtual machines on Apple Mac computers.

2.1 Virtualization Environments

There are two main types of virtualization environment: hosted virtualization environment and bare-metal virtualization environment. Figure 3 and Figure 4 illustrate the components in each environment. Regardless of the virtualization environment used, there are some common components.

The host hardware is the hardware on the physical computer (host computer) running the virtual machine. The host hardware determines the maximum level of hardware support available to virtual machines. For example, a dual-core host may support dual-core virtual machines, but a a single-core host cannot support a dual-core virtual machine. In a hosted environment, the host computer has an operating system. Virtualization platforms often enable the execution of various operating systems in virtual machines regardless of the host operating system. In a bare-metal environment, the host computer does not utilize a host operating system; this configuration is most common when running virtual machines on servers.

The hypervisor is the system that enables virtual machines to operate (CNet Networks, Inc., 2008). The hypervisor is a key component of a virtualization

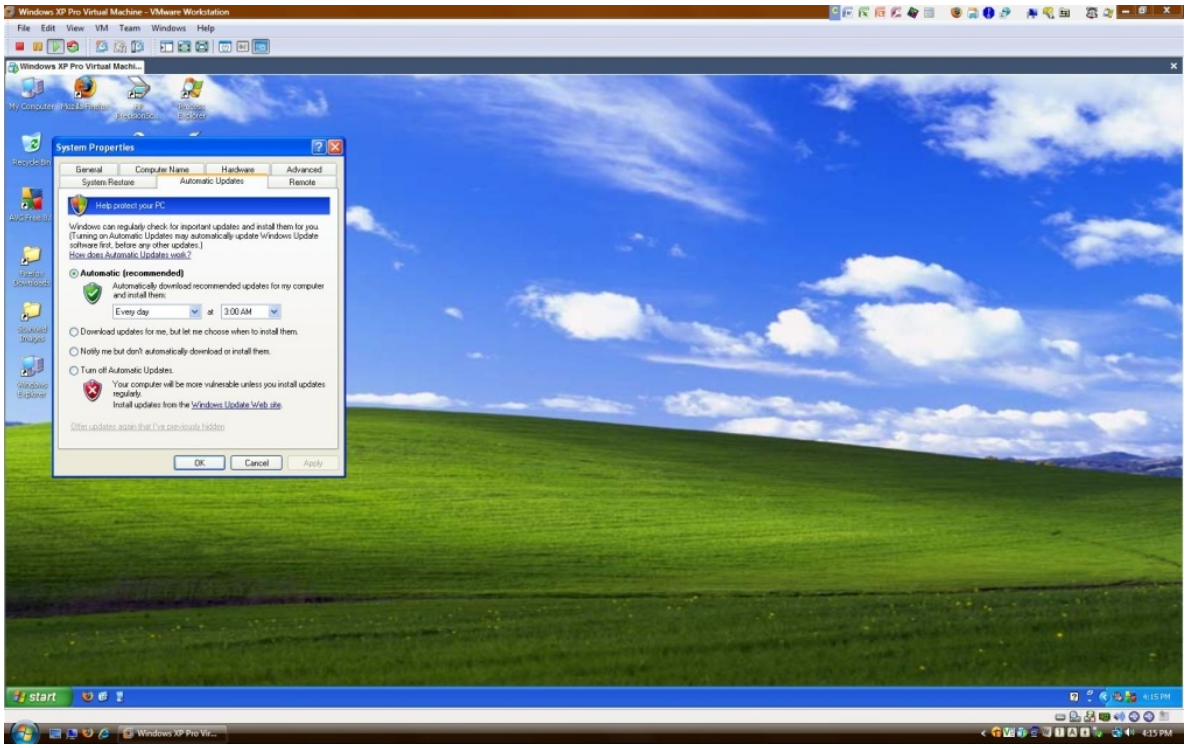

Figure 1. Windows XP Virtual Machine on a Windows Vista Host

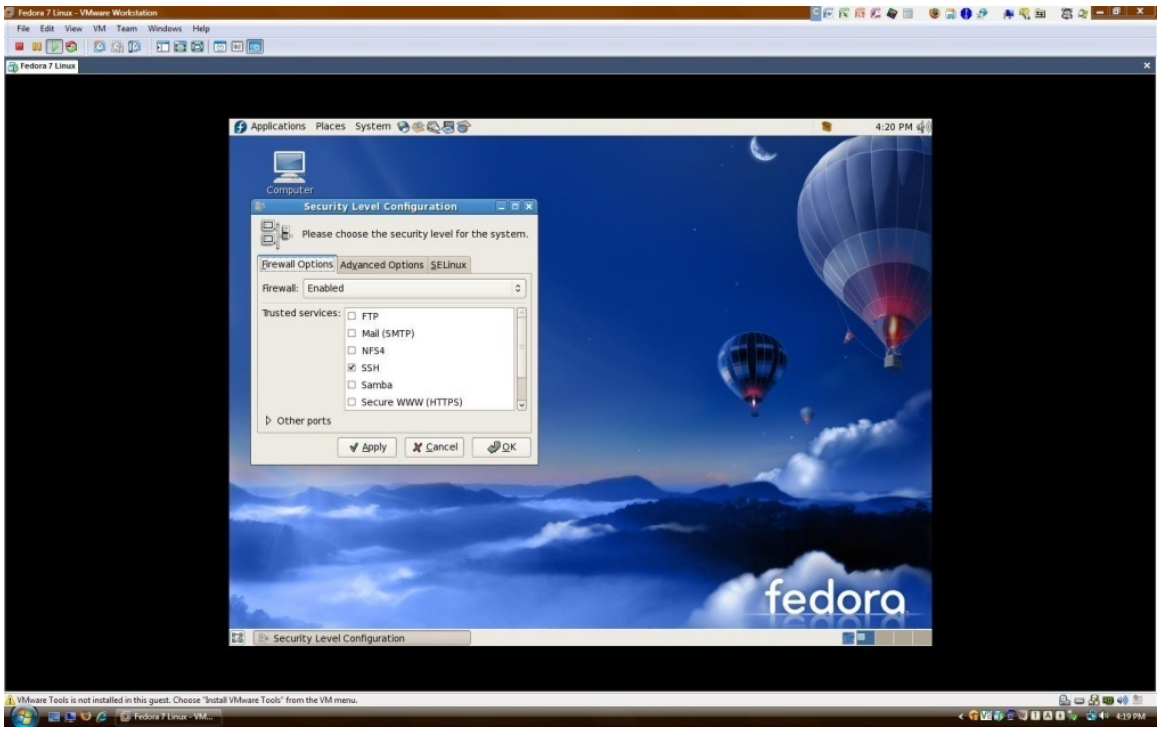

Figure 2. Fedora Linux Virtual Machine on a Windows Vista Host

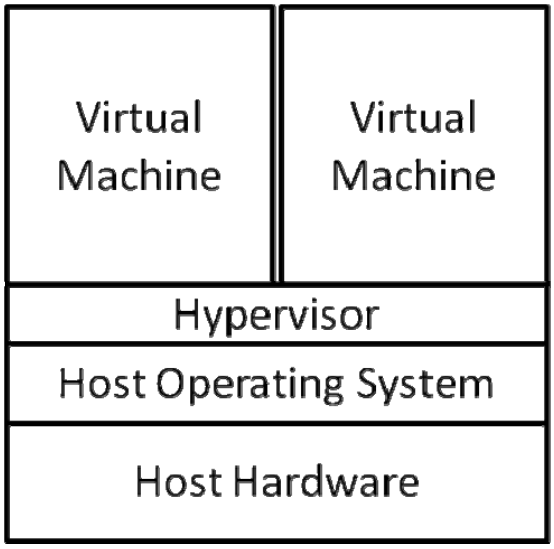

Figure 3. Hosted Virtualization Environment

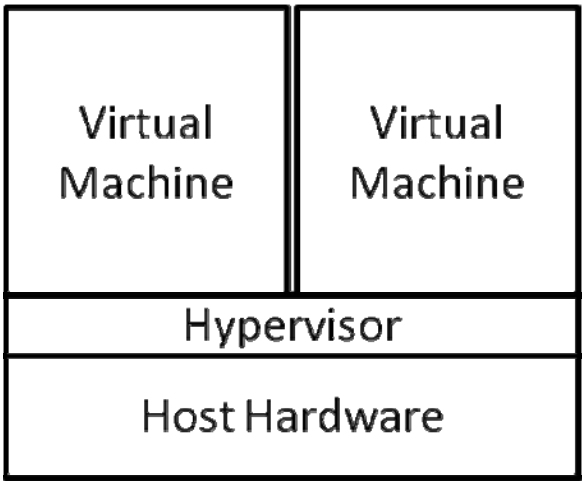

Figure 4. Bare-Metal Virtualization Environment

platform, along with tools for creating and managing virtual machines. In a bare-metal environment, a type 1 hypervisor manages the operations of the virtual machines and interfaces directly with the host hardware (IBM Corp., 2005). In a hosted environment, a type 2 hypervisor manages the virtual machines and interfaces with the host operating system to access resources (IBM Corp., 2005). Some virtualization platforms refer to a type 2 hypervisor as a lightweight hypervisor (Parallels Software International, Inc., 2007). The hypervisor determines the types of virtual resources available to the virtual machine.

2.2 Types of Virtualization

The type of the virtual machine varies across virtualization platforms. Two common forms of virtualization are hardware virtualization and operating system virtualization. A rapidly emerging form of virtualization is application virtualization.

With hardware virtualization (Figure 5), the hypervisor provides a virtual hardware layer that the guest operating system sees as its hardware. The guest operating system interacts with the virtual hardware, which behaves like physical hardware. This is the type of virtual machine supported by default in VMWare Workstation 6 and

Parallels Workstation 2.2. In a hardware virtualization setting, the guest OS is the operating system installed in a virtual machine. The guest OS is a complete instance of the operating system. The virtualization product used determines the supported guest operating systems; for example, VMWare Workstation 6 and Parallels Workstation 2.2 support various versions of Microsoft Windows, Microsoft DOS (MS-DOS), various distributions of Linux, Sun Solaris, as well as other operating systems. Once installed, the guest OS runs in the virtual machine as if on a stand-alone computer. The user may install and run applications in the guest OS the same as the user would on a physical computer.

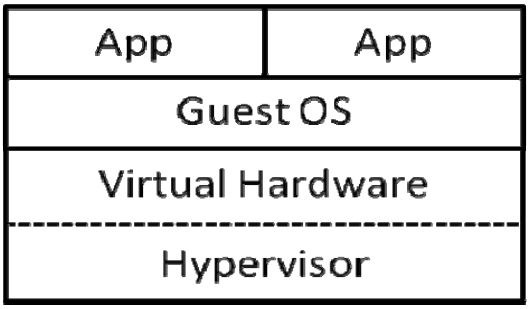

Figure 5. Hardware Virtualization

With operating system virtualization (Figure 6), the virtualization platform creates containers that utilize the host hardware via the hypervisor and host operating system (Introduction to Virtualization, 2007; Parallels Software International, Inc., 2008a). The OS container is not a full instance of the operating system. The hypervisor is responsible for managing the host system resources required by the containers. Parallels Virtuozzo provides this type of virtual machine. This type of virtualization is most useful in settings where an organization desires to partition a number of server applications that use the same type of operating system in their own virtual machines to isolate failures and maintain security.

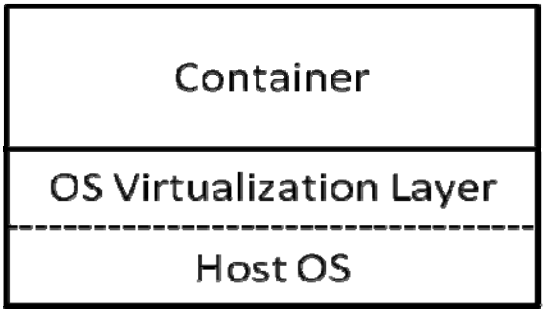

Figure 6. Operating System Virtualization

Application virtualization (Figure 7) encapsulates an application into a container along with the set of system files specifically associated with the application (Application Virtualization Simplified, 2008; van Dijk, 2008; VMWare, Inc., 2007). This form of virtualization provides for portability of applications across computers and isolates the system settings of one application from the system settings of another application. VMWare, Parallels, and Microsoft, as well as others provide application virtualization platforms.

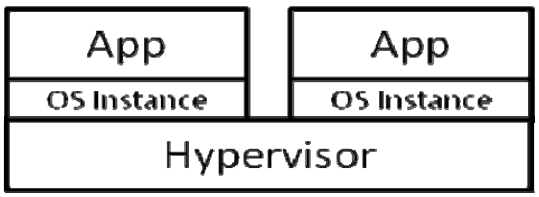

Figure 7. Application Virtualization

2.3 Platforms Virtualized

In addition to the virtualization environment and type of virtual machine, a third issue is the type of "computer" virtualized. Early efforts with virtualization focused on creating virtual machines that encapsulate a fully functional server; server virtualization has become common over the past few years. Today, organizations are exploring virtualization of desktop computers to reduce total cost of ownership, simplify management of desktop computers, and make desktop environments available virtually anywhere at any time.

According to Roberts and Yacono (2003), in 2003 85% of information-technology solution providers were already or planned to recommend server virtualization to their customers. Server virtualization (Figure 8) provides the capability to consolidate multiple servers on newer, high-powered server technologies (Hassell, 2007; Roberts and Yacono, 2003). By doing this, organizations can reduce the number of physical servers operating in corporate back ends, thus reducing space needs and power consumption. At the same time, by using server virtualization, the hypervisor isolates each server virtual machine, preventing the virtual machines from tampering with one another's configurations, processes, or other characteristics. VMWare, Parallels, Microsoft, as well as others, provide server virtualization platforms.

While similar to server virtualization, desktop virtualization enables virtualization of desktop operating systems. The two major variations of desktop virtualization are desktop virtualization on the workstation similar to server virtualization (Figure 9) and desktop virtualization using a Virtual Desktop Infrastructure (Figure 10). With desktop virtualization, the virtualization platform enables the execution of one or more virtual machines on a workstation. The virtual machine may access workstation resources via the hypervisor. One may implement desktop virtualization on the workstation using various desktop virtualization platforms, including VMWare Workstation, Parallel Workstations, Microsoft Virtual PC, as well as others. Desktop virtualization using a VDI executes the virtual machine on a server, while the user may employ a fat client or thin client (Parallels Software International, Inc., 2008b). In this scenario, a server may host a number of desktop virtual machines. The user may access the virtual machine from any location with sufficient bandwidth to support the necessary communications between the client and server. Common virtualization platforms include VMWare Virtual Desktop Infrastructure and Parallels Virtuozzo Containers, as well as others.

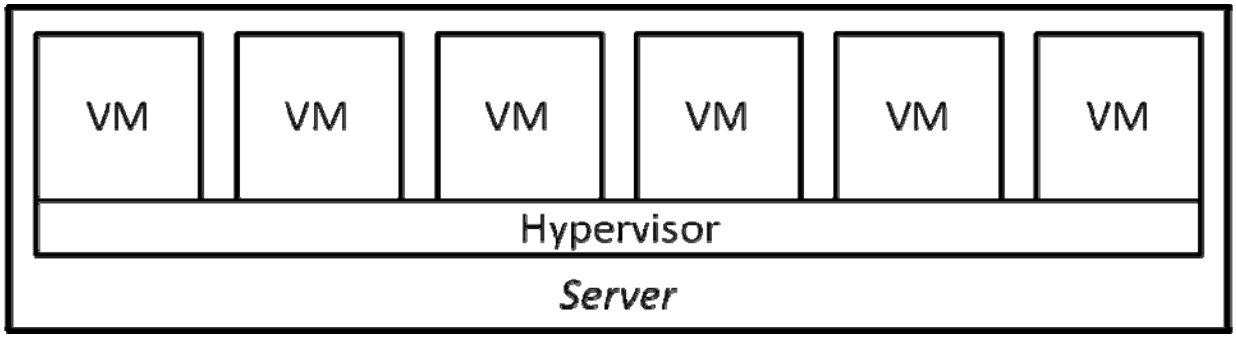

Figure 8. Server Virtualization

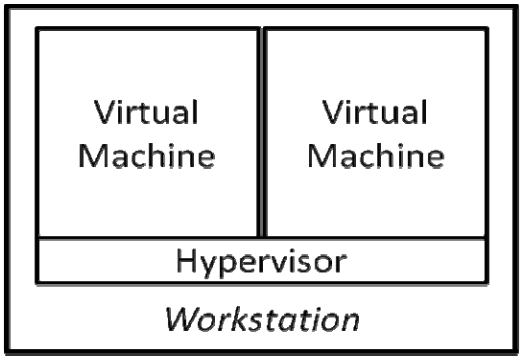

Figure 9. Desktop Virtualization on Workstation

3. EXPERIENCES IN AN INFORMATION SYSTEMS SECURITY COURSE

This paper focuses on the use of virtualization technologies in a business-oriented information systems security course covering security policies. The primary objective of this course was to introduce students to the business and technical issues associated with the formulation and implementation of security policies. To enhance student learning, this IS educator established the goal of integrating significant hands-on activities complementing the topics of the course. The challenge this IS educator faced was that the hands-on activities presented the potential to compromise system and network security in a heavily used computer lab. Initially, this IS educator planned to use a dedicated computer laboratory with computers isolated from the campus networks; however, the dedicated computer laboratory was not available due to construction delays. As a result, this IS educator decided to test the use of virtualization technologies in this course.

3.1 Prior Use of Virtualization in Educational Settings

In computer science and computer engineering, educators have employed virtual machines to address challenges associated with a range of technical instruction areas. United States Military Academy at West Point educators developed the Virtual Information Assurance Network (VIAN) to provide advanced instruction in information warfare (Ragsdale, Lathrop, and Dodge, 2003). The VIAN provides students with access to multiple virtual machines running various operating systems; this enables students to engage in attack and defense activities. Hu, Cordel, and Meinel (2004) described the development of a Linux based security system employing virtual machines for remote connection online. This enables students to engage in various activities either by working through the host computer or a web-based interface. Abler, et al. (2006) used virtual machines running on a single computer to create a small virtual network to simulate the structure of the Internet. Azadegan, et al. (2006) used virtual machines to provide students with access to multiple operating systems and virtual networks as part of a wide range of operating systems, programming, networking, and computer security courses.

3.2 The Information Systems Security Course

This IS educator employed virtualization technologies in an information systems security course to enable coverage of high-risk computer security topics. The course selected, ISP 350, is a junior-level course in an Information Security and Privacy (ISP) major at a small liberal arts institution. The major is interdisciplinary but housed in the Department of Information Systems. Students in the ISP major complete a variety of courses in information systems security and privacy, criminal justice, political science, computer science, information systems, as well as other university core courses. The target students for this course are second-semester juniors who have completed most university-core courses. Prior to taking ISP 350, students complete an introduction to information systems security course (ISP 205) that covers a variety of topics, including threats to systems and information security, tools for safeguarding resources, and risk management. Students also complete an introductory database course (MIS 231) before taking this course.

ISP 350 makes significant use of readings and hands-on activities to provide students with a thorough understanding of security topics. ISP 350 occurs during the spring semester of the academic year. The semester consists of 15 weeks plus one final examination session yielding 48 hours of in-class, contact time. During the semester covered in this paper, the course met three days per week for 50 minutes. The first three weeks consisted of a review of information systems security topics covered in ISP 205 and an introduction to the creation and documentation of security policies using supplemental readings and exercises. The remainder of the semester focused on hands-activities and discussion of the security topics covered in the course. Students worked on a series of hands-on activities (Figure 11) throughout the semester; see the appendix for a sample activity description.

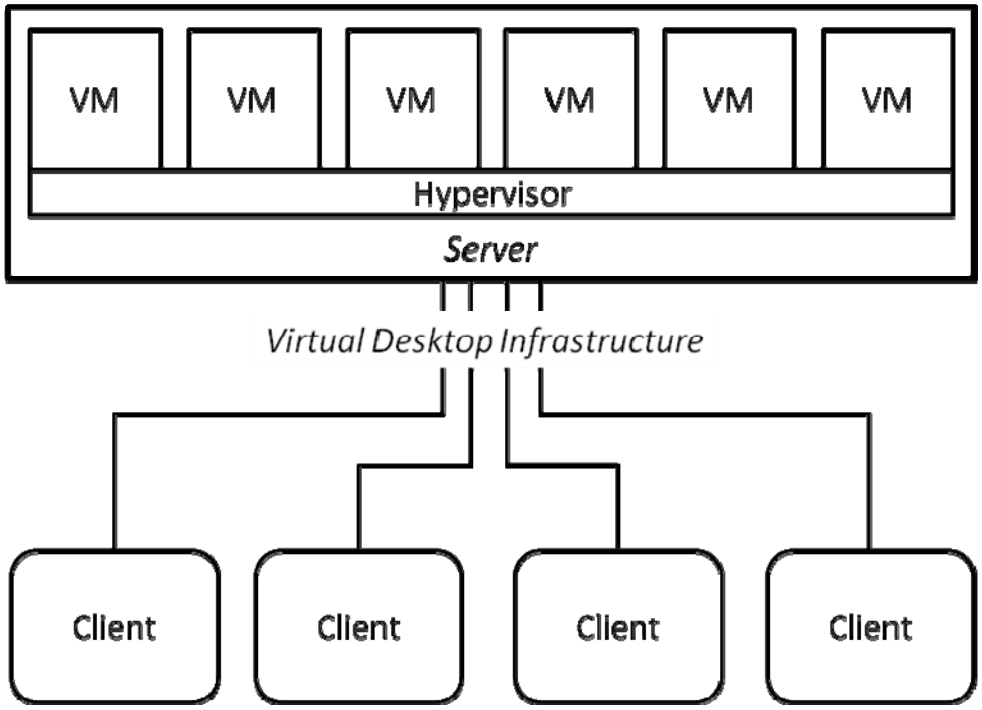

Figure 10. Desktop Virtualization using a Virtual Desktop Infrastructure

During most class sessions, the students worked on the hands-on activities for approximately 45 minutes and discussed their experiences during the last five minutes of the class. In total, students spent 30 class sessions engaged in hands-on activities. Four students completed the course; two of the students were second-semester juniors and two were graduating seniors.

3.3 Computer Laboratory and Virtualization Setting

The computer laboratory used for this course consisted of student workstations and an IS educator's workstation connected to the campus network. Students used the computer laboratory heavily throughout the day and for evening classes. Most classes made full use of the computer laboratory with all available computers taken. As a result, it was not possible to dedicate some computers to the security class. Fortunately, the computers had sufficient resources to run VMWare Workstation 6. Each computer consisted of an Intel dual-core processor (2.13 GHz) with 1 GB RAM, an 80 GB hard drive, CD/DVD writer, 17" flat-panel display, and an Internet connection via a local area network. Using VMWare Workstation 6, each student worked in a hosted virtualization environment, employing hardware virtualization to enable desktop virtualization.

This IS educator selected VMWare Workstation 6 as the virtualization platform for several reasons. First, VMWare provides a range of virtualization products, including server and desktop virtualization. Second, VMWare Workstation 6 supports a range of hardware, including universal serial bus (USB) 2.0 storage devices natively, while other virtualization products require the user to setup a shared folder with the host operating system to access these devices. Third, VMWare Workstation 6 supports a wide range of guest operating systems, including most versions of Microsoft Windows, Linux distributions, and several other operating systems. Fourth, VMWare has an active user community providing an assortment of virtual appliances, which are pre-configured virtual machines for various applications. Finally, VMWare operates an academic program (http://www.vmware.com/partners/academic/) that makes select VMWare products available to the academic community free of charge for instructional purposes.

Installing Windows XP Professional
User Account Management
Cracking Passwords
Securing Folders and Files
Creating and Securing Shares
Evaluating Baseline Security
Patching Windows
Managing Processes and Startup Items
Installing and Configuring a Personal Firewall
Installing and Configuring a Virus Scanner
Using Encrypting File System
Using a Recovery Agent with Encrypting File System
Using TrueCrypt
Working with Secure E-mail
Poking Around on a System
Using a Packet Sniffer

Figure 11. Hands-on Activities

3.4 Daily Hands-on Activities

In ISP 350, each student created a virtual machine and installed Microsoft Windows XP Service Pack 1 on the virtual machine. This IS educator provided each student with a copy of Windows XP on CD for the duration of the course. Windows XP Service Pack 1 served as the starting point so

that the students could work with Windows XP at various levels of maturity.

During the first activity, the students familiarized themselves with the basic VMWare Workstation 6 interface, created a virtual machine, and installed Windows XP. Only one student had previous experience using VMWare or other virtualization products; however, all students quickly developed an understanding of the basics of VMWare Workstation 6. Once the students installed Windows XP in the virtual machine, the students served as the administrators of their own virtual machines; this enabled the students to do things on the virtual machines that they could not do on the host computers. Subsequent activities built on the previous activities; by the end of the semester, the students' virtual machines included all updates to Windows XP, user accounts, user directories, various security applications, and customized system settings. As the students completed each activity, they recorded notes in laboratory notebooks; students were to record in their laboratory notebooks information about problems encountered and the solutions, answers to questions in the activity handout, lessons learned, and a list of sources used during the activity.

3.5 Student Experiences

The students expressed satisfaction with the course and the use of virtual machines. In addition to developing technical skills, the students demonstrated an increased level of confidence in working with advanced features of Windows XP and other applications over the course of the semester. One student commented that the student felt using the virtual machine helped the student become more comfortable and confident with existing and new skills. Students commented that they would like to have had a course of this type before because the use of hands-on activities helped them to understand better the material presented in lectures; students especially commented about this after performing the password cracking and encryption activities. While the experiences in this course were generally positive, the use of virtual machines in an instructional setting introduces some challenges and limitations over the use of dedicated computers.

4. CHALLENGES AND LIMITATIONS OF VIRTUAL TECHNOLOGIES

During the process of preparing for and using virtual machines in this security course, this IS educator had to address several issues that affect the course structure and learning objectives. These issues include the students' lack of experience using virtual machines, educator control over the students' virtual machines, hardware and software compatibility with the virtualization platform, disk space and machine requirements, and the ability to make regular backups of virtual machines.

Although virtualization technologies have penetrated the corporate IT infrastructure in many settings, desktop virtualization is still a novelty. Many students do not have hands on experience with these technologies; as a result, students need to become comfortable with the technology so that it is not the focus of the student's attention during class. In the pilot use here, it took most students a couple class sessions to stop thinking about the virtual machine as the focus and start interacting with the virtual machine as if it were an ordinary desktop computer.

When students work in a virtual machine of their own creation, they have complete control over the virtual machine. This is desirable in settings where the student is acting as a system administrator; however, this can also make it difficult for the IS educator to monitor the students' activities or assist students in solving some problems. In settings where the student does not require administrator control over the virtual machine, the IS educator may choose to distribute a virtual machine with a pre-defined student account with the appropriate level of access. In settings where the student does need greater levels of control, the IS educator may ask the student to create a second administrator account with a designated password. This also provides a fallback in case the student forgets their virtual machine password. In this course, students created two administrator accounts; the students assigned their own passwords for the first account and all students used the same password for the second account.

Not all hardware and software work with all virtualization platforms. In the case of this pilot use of virtualization, this IS educator attempted to use Microsoft Virtual PC but Virtual PC did not support native USB storage devices; VMWare Workstation 6 did. Additionally, some hardware designed specifically for Microsoft Windows, such as internal Winmodems, will not work in many virtualization products. Because of this, it is important to identify any special hardware requirements before selecting a virtualization platform. During course development, a difficulty with file recovery software arose. File recovery software that worked on physical computers running Windows XP would not work on a Windows XP virtual machine. Once again, it is a good practice to test software to ensure it works in the virtualization platform selected if possible. A third issue that arose was the inability to boot from a CD within a virtual machine during a restart operation. This situation comes up when one needs to boot from a CD after the initial installation of Windows to access Windows file structures or other resources via third-party applications such as password cracking programs. After the semester, this IS educator found a solution to this problem online. VMWare's BIOS (Basic Input/Output System) employs a boot process similar to that used by the physical computer; however, by default the boot process is so fast that the user does not have time to elect to boot from a CD. By introducing a delay in the boot process, the user may select operations similar to those on a physical computer, including display the boot menu, configure BIOS, and boot to safe mode. A side benefit of this is that the student sees a virtual machine that looks more like a physical computer.

Like operating systems and applications on their physical peers, operating systems and applications on virtual machines require significant disk space, especially when running Microsoft Windows and server operating systems. As an example, the virtual machine used in this security course required approximately seven gigabytes of disk space when turned off and approximately eight gigabytes when turned on. This presents several challenges in a laboratory environment. First, if multiple students use the same host computer to run their virtual machines, disk requirements

quickly grow. This is most likely to be a factor if the physical drive in the host computer has limited space; however, one must consider disk requirements for virtual machines when selecting host computers or evaluate alternatives for storing virtual machines when turned off. Second, assuming the student stores his or her virtual machine on a host computer in a laboratory, this necessitates the student having access to a specific computer to perform work. This is not an issue if students use the same computer during each class session, but it becomes a problem during open laboratory times when another student may be using the host computer. Finally, when students use virtual machines, it is a good practice to make a backup of the virtual machine periodically in case the student accidentally damages the virtual machine, the host computer fails, or another problem prevents the student from accessing the virtual machine. If a network has limited bandwidth or backup servers have limited storage space, this becomes a problem given the size of virtual machines. Given adequate resources, desktop virtualization using a Virtual Desktop Infrastructure may provide a good solution for these problems. Additionally, as storage capacities of USB storage devices increase and prices drop, it is likely one will be able to store a virtual machine on a USB storage device. Finally, as Kroeker (2009) indicates, as virtualization becomes more common in corporate information technology infrastructures, virtualization technology companies are developing tools to better manage the deployment of virtual machines; these same tools will be beneficial in educational settings as well.

5. OPPORTUNITIES AND BENEFITS OF VIRTUAL TECHNOLOGIES

Virtualization offers potential opportunities and benefits in an educational setting, including creating a virtual sandbox for risky activities, providing instruction in various applications or operating systems, using virtual appliances, using virtual teams for client/server applications, and enabling distance education via virtual desktop infrastructure.

Virtualization technologies are ideally suited for providing a sandbox for executing risky code or engaging in experiments. As already discussed, students may perform actions on the virtual machine that they should not perform on a physical machine as these actions pose a threat to the availability and stability of the physical machine. Students may engage in activities in a virtual machine that IS educators and network administrators would not want them to do on a host machine or live network. For example, students in this course cracked passwords in their virtual machines. Since the virtual machine limited the scope of this activity, real user information on the host machine and network remained secure. Students also experimented with various applications, such as firewalls, virus scanners, encryption applications, to name a few, which have the potential to weaken security if not properly implemented. Once again, the virtual machine isolates the potential weakness to the virtual machine.

Virtualization offers the opportunity for students to work with a range of applications not available on the host machine. For example, a host machine might include Microsoft Office while a virtual machine could provide students with access to OpenOffice.org and IBM Lotus Symphony without the file association entanglements often common when competing applications exist on the same machine. In more advanced courses, student might work with accounting systems, business applications, and other products. The virtual machine provides an ideal platform for this since the student can serve as a user or administrator without affecting other students. This enables the student to enter data, create reports or macros, adjust system settings, or otherwise work with the application. As it matures, application virtualization offers the potential to do many of the same things that a virtual machine does without the need for a full virtual machine; thus simplifying the deployment of this type of instructional tool.

Virtualization provides a useful tool for introducing operating systems. While a dual-boot configuration enables the introduction of multiple operating systems, virtualization offers several advantages. First, virtualization may be easier to implement and manage than dual boot configurations. Second, since the virtual machine and host operating system coexist and are accessible, the student may more easily access both resources in class. Third, students may install and configure their own operating systems, thus extending the range of topics possible. Fourth, the IS educator may distribute virtual machines to students if there is no need for the students to install their own operating systems. Finally, one may introduce several different operating systems by using a virtual machine for each operating system.

Virtualization platform developers such as VMWare and Parallels provide access to a collection of third party, preconfigured virtual appliances for a variety of purposes, including testing applications, quickly enabling security and communications systems, and providing bootstrap implementations of Linux. IS educators may take advantage of this to implement server-side applications for use in all types of courses, not just courses using student-implemented virtual machines. In this course, the need arose to have access to an e-mail server. This IS educator downloaded and configured an evaluation copy of the Kerio MailServer virtual appliance available through the VMWare virtual appliance marketplace. Additionally, rather than having each student create a virtual machine, an IS educator may elect to create a virtual machine with the necessary software and make this pre-configured virtual machine available to students. This is especially useful in settings where the focus of the course is on application software and it is impractical to install the application software on the physical computer.

Some virtualization platforms, such as VMWare Workstation 6, support virtual teams, which are a collection of virtual machines on a virtual network that one may start as a unit. In settings where students need access to a collection of computers on a network, such as when working with client-server applications, the capability to create a virtual team of virtual machines is beneficial. Rather than having to provide each student with multiple physical computers, the IS educator may implement a virtual team. For example, when developing client/server applications, the virtual team might consist of a server and client, each on their own virtual machine, interacting as if they were on separate physical computers. In another setting, one might create a more complex virtual team to explore various network and system auditing tools.

Given the proliferation of high-speed Internet connectivity, virtualization provides an opportunity for distance learning students to have access to IS educator-developed environments either via download or through a remote connection. In the first case, an IS educator may develop a virtual machine and make it available for download, either for students in a traditional setting or for distance learning students. In the second case, given the appropriate desktop virtualization using a VDI, a distance learner may connect to a university server to access a full instance of the appropriate desktop environment so that the distance learner has access to the same resources as a traditional student. This could be especially beneficial when students need access to costly software and students do not have access to discounted versions of the software. This also provides a way for the IS educator to assist the student or ensure that the student completes the necessary work as long as the IS educator has access to the student's virtual machine.

6. SUMMARY

This paper provides an introduction to virtualization technologies, discussed the use of VMWare Workstation 6 in a classroom setting, outlined some challenges and limitations of virtualization, and presented some opportunities and benefits from using virtualization. Virtualization covers a wide range of techniques, from application virtualization to server virtualization. Desktop virtualization provides an opportunity for IS educators to introduce more advanced or risky topics in information systems courses, while safeguarding the computers in laboratories. In a pilot test of this in a business information systems security course, this IS educator found virtualization to be an effective tool for giving students access to a variety of hands-on learning experiences. At the same time, IS educators choosing to use virtualization must be aware of the limitations of virtual environments and plan carefully to select the right tools for their individual needs. As virtualization platforms mature, the opportunities for using these technologies in instructional settings will grow, making it possible to introduce a wide range of topics in more realistic settings, without the need to provide multiple physical computers for each student.

7. REFERENCES

Abler, R., Contis, D., Grizzard, J., and Owen, H. (2006), "Georgia tech information security center hands-on network security laboratory," IEEE Transactions on Education, Vol. 49, No. 1, 82-87.

Anonymous. (2007), "Introduction to Virtualization," accessible at http://www.virtualization.org/ Virtualization/ Introduction_to_Virtuaization.html.

Anonymous. (2008), "Application Virtualization Simplified," accessible at http://www.serverwatch.com/ virtualization/article.php/3748966.

Azadegan, S., O'Leary, M., Wijesinha, A., and Zimand, M. (2006), "Undergraduate Computer Security Education: A Report on our Experiences & Learning," Proceedings of Seventh Workshop on Education in Computer Security (WECS 7), pp. 17-27.

Brandel, M. (2005), "Virtual Unity," ComputerWorld, Vol. 39, No. 42, October 17, 2005, p. 52.

CNet Networks, Inc. (2008), "ZDNet Definition for: Hypervisor," accessible at http://dictionary.zdnet.com/ definition/Hypervisor.html.

Drews, J. E. (2006), "Going Virtual," Network Computing, Vol. 17, No. 9, May 11, 2006, p. ES 5.

Hassell, J. (2007), "Server Virtualization: Getting Started," Computerworld, Vol. 41, No. 22, May 28, 2007, p. 31.

Hu, J., Cordel, D., and Meinel, C. (2004), "A Virtual Laboratory for IT Security Education," Proceeding of the Conference on Information Systems in E-Business and E-Government, pp. 60-71.

IBM Corp. (2005), Virtualization. IBM, Rochester.

Kroeker, K. L. (2009), "The Evolution of Virtualization," Comunications of the ACM, Vol. 52, No. 3, March, pp. 18-20.

Parallels Software International, Inc. (2008a), Parallels® Virtuozzo Containers: An Introduction to OS Virtualization and Parallels Virtuozzo Containers. Parallels, Inc., Renton.

Parallels Software International, Inc. (2008b). Parallels® Virtuozzo Containers: Virtual Desktop Infrastructure. Parallels, Inc., Renton.

Ragsdale, D., Lathrop, S., and Dodge, R. J. (2003), "A virtual environment for IA education," IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, pp. 17-23.

Roberts, J., and Yacono, J. (2003), "Server Virtualization Offers Many Opportunities," CRN, No. 1076, December 22-29, p. 34.

van Dijk, L. (2008, February 25), "Application Virtualization," accessible at http://www.anandtech.com/IT/showdoc.aspx?i=3237.

VMWare, Inc. (2007), "Thinstall Application Virtualization Platform," accessible at http://www.thinstall.com/products/it_managers.php.

AUTHOR BIOGRAPHY

Dale L. Lunsford is an Assistant Professor of Information Systems in the College of Business at the University of Southern Mississippi. He received his Ph.D. in Management Information Systems from the Ohio State University in 1996. He teaches a variety of courses, including IS ethics, computer security, programming, database development, networking, and accounting information systems. He has a broad range of research interests, including information and information systems security, privacy, disaster preparation and recovery, systems development, and ethics. Dale has published papers in *The Forensic Examiner*, *CPA Journal*, *Journal of Information Systems*, *Review of Business Information Systems*, *Teaching Business Ethics*, and *Journal of Educational Technology Systems*.

APPENDIX: SAMPLE HANDS-ON ACTIVITY – CRACKING PASSWORDS

Preparation: Read the following article for background on Windows passwords: http://www.securityfocus.com/infocus/1319
Unless specifically indicated here, use your virtual machine for all commands.

1. Experiment with Password cracking/testing tools
   a. On the host map a network drive to *file_server\course_directory*
   b. Using My Computer or Windows Explorer, create a directory on the C: drive called tools (C:\tools).
   c. Copy the following files from the network drive you mapped to your tools directory:
      - john171w.zip
      - ophcrack-win32-installer-2.4.1.exe
      - pwdump6-1.6.0.zip
      - SSTIC04-10k.zip
   d. Work with Ophcrack
      i. Extract the contents of SSTIC04-10k.zip.
      ii. Install Ophcrack. For Select Components, select the last option to install Ophcrack without tables.
      iii. Run Ophcrack
         1. Click Load and select the option to load accounts from the local SAM (Security Accounts Management Database).
         2. Click Tables and navigate to the C:\tools\SSTIC04-10k directory. Ophcrack uses pre-computed password hashes to attempt to crack passwords.
         3. Click Launch.
            Notice that Ophcrack first identifies several user accounts with no passwords. Next, Ophcrack begins cracking the passwords.
            As it cracks a portion of a password, it displays the result under either the LMpasswd1 or LMpasswd2 column, depending on which part of the password breaks first.
            After Ophcrack completely cracks a password, it displays the result under the NTpasswd column.
      iv. Eventually, Ophcrack gets to the point where it is really working to crack passwords. After Ophcrack has cracked the user1, user3, and possibly the administrator account (depending on how good of a password you selected) and runs for several minutes without generating any output, terminate Ophcrack by pressing the Stop button. Note: If you let Ophcrack run long enough, it will crack most passwords.
   e. Work with John the Ripper (JTR)
      i. Extract the contents of john171w.zip and pwdump6-1.6.0.zip.
      ii. Create a directory on the C: drive called tools (C:\john).
      iii. Copy the contents of the C:\tools\john171w\john1701\run directory to the C:\john directory.
      iv. Copy the contents of the C:\tools\pwdump6-1.6.0\PwDumpDebug directory to the C:\john directory.
      v. Open a command line window by selecting Start → Run, entering cmd, and pressing Enter.
      vi. Change directory to your john directory by typing CD \john and pressing Enter.
      vii. To capture passwords, you need the host name of the virtual machine. Type ipconfig /all and press Enter. Locate the host name and write it here:
      viii. To use JTR, you must first capture the user names and password information on the computer. To do this, type the following command and press Enter.
            pwdump –o passwords.pw *hostname*
            Substitute *hostname* with the host name you found in the previous step.
            This runs the pwdump program, which extracts the user information, and saves the information to a file called passwords.
      ix. Now, use JTR to try to crack your passwords. Type john-386 passwords.pw and press Enter. This runs the JTR program and attempts to crack any passwords in the passwords.pw file.
      x. As JTR cracks passwords, it displays them on the screen. Notice the information displayed for user1, user3, and possibly the administrator account (depending on how good of a password you selected). What is JTR displaying?
      xi. Eventually, JTR gets to the point where it is really working to crack passwords. After JTR runs for several minutes without generating any output, terminate JTR by pressing and holding the Control key (Ctrl) and pressing the C key. Note: If you let JTR run long enough, it will crack most passwords.
   f. Based on your experiments with Ophcrack and JTR, what conclusions can you make regarding the quality of passwords?
2. Explore Local Security Policies – Password and Account Lockout Policies
   a. Search the Internet for information on how to configure Windows local security policies.
   b. Access the Local Security Policies.
   c. Describe each of the six Password Policies in your own words.
   d. List the password complexity requirements.
   e. When should you use each of the Password Policies?
   f. Describe each of the three Account Lockout Policies in your own words.
   g. When should you use each of the Account Lockout Policies?
   h. Set Password and Account Lockout Policies as desired.