Virtualization Environment for Computer Labs to Maintain Security, Stability and Availability

Abdalla Alameen
Department of Computer Science, College of Arts and Science,
Prince Sattam Bin Abdulaziz University,
Wadi ad Dawaser 11990, Kingdom of Saudi Arabia

ABSTRACT
Academic organizations are supposed to seek certain balance between the concerns of security, stability and availability of shared computer labs to achieve the course learning objectives. Some academic activities in computer science courses require students to control and configure some laboratory devices. Students in advanced courses may use some risky applications for some learning activities. It may affect the stability, availability and security of the working nature in the shared lab and networks. Virtualization Platform has the ability to overcome these concerns to achieve learning objectives. Virtualization technologies allow students to access and control the computer settings as well as the working environment in advanced applications without affecting the operational availability of computer labs throughout the college day. Virtualization enables computer security teachers to train their students on many hands-on activities without exposing or causing damages to computer labs.

This paper presents the usage of virtualization technology in such environment, the opportunities and benefits of using this technology in computer security oriented courses. The paper also discusses the use of the VMware workstation pro as a sandbox for risky lab activities in computer security courses. Here the Desktop Virtualization offers great opportunities to teach advanced skills in computer security courses. Also, this paper outlines the challenges and limitations of virtualization along with some recommendations to address these limitations.

Keywords
Virtualization, virtual machine, Desktop virtualization, hypervisor, hands-on activities, computer security.

1. INTRODUCTION
These days, controlling and managing the shared computer laboratories is one of the challenging issues that educational institutions are facing. These laboratories must be sufficient and operationally available to all students throughout college day. Quite often the transition periods between different students in colleges are short or completely nonexistent. As a result, there is an urgent need to manage these labs and ensure their availability and readiness. Computer science curriculum covers a series of technical issues like programing languages, systems design and analysis, web technology, etc. Students work on cumulative applications such as email services, graphic software, SQL databases and java etc. Such programs do not pose much threat to the availability of laboratories. In advanced courses, students often need to configure and install some applications or to access some complex tools. For instance, to implement activities related to computer security courses, students need to work on applications and activities that may jeopardize laboratory devices, software and network. Sometimes students need to be trained in encryption, decryption, firewalls, intrusion, applications access control, and other security-related topics. These activities force students to change computer settings and configurations, control devices, access some websites that pose security risks to laboratories. Such risky activities are avoided by laboratory managers and technical support teams at universities.

Faculties may use some methods to secure computers through keeping computers in a stable state so that the students cannot make any permanent changes in computers configurations and settings. For example, some teachers use Deep freeze software that prevents permanent modifications in computer configurations except by an authorized person. However imposing such restrictions on shared computer laboratories may hinder many learning objectives in the computer science curriculum.

There should be some balance between concerns of security, stability and availability of shared computer labs to achieve course learning objectives. With the emergence of cloud computing and virtualization, many educational institutions have begun to migrate from traditional to virtual platforms. However availability of these services in modern form requires a lot more efforts and proper preparation in order to get the best results, and ensure sustainability.

Some researchers [1, 2, 3, 4] have suggested that the use of virtualization technologies for hardware and software may enhance managing and controlling computer labs. Virtualization technology also offers many benefits for students, teachers and technical support teams in computer science fields. Virtualization technology allows students to control computers setting and work in advanced applications without affecting the stability, availability and security of labs. Virtualization enables students to make permanent configurations on hardware settings that need not be removed between students' different sessions, enables students to work on long-term projects and helps students to develop activities based on cumulative work from the beginning to the end of the course. Students can practice on host computers in virtual environments and control these computers without affecting their configuration by setting and use some advanced applications without exposing or causing damage to the network. Virtualization offers the faculties a great opportunity to teach advanced topics in computer security courses.

This paper throws a light on virtualization technology, the opportunities and benefits of using this technology in security related courses. The paper discusses the use of the VMware workstation pro for virtual machines in computer security lab. The paper shows that Desktop Virtualization offers great opportunities to teach advanced skills in computer security courses and allow students to control computer without exposing or causing damages to computer labs. The paper

outlines the challenges and limitations of Desktop Virtualization along with some recommendations to address these limitations.

The rest of the paper is arranged as follows. Section 2 presents virtualization concepts and Environments. Section 3 is about Literature Review. Section 4 states our methodology along with virtualization setting for computer security lab, limitations and recommendations to address these limitations. Finally, Section 5 concludes the paper highlighting findings and limitations of the research.

2. VIRTUALIZATION CONCEPTS & ENVIRONMENTS

Information Technology (IT) industry benefits from constant buzzwords and changing terms to define it is new approaches. The concept of green computing or x86 are some of these terms. In recent years, the term virtualization has become a buzzword [5]. Here a question arises, what is virtualization? The traditional answer that comes to the mind of most technicians is; the ability to run one or more guest operating systems on a host computer [6], but If we go deeper into this definition, more details will be revealed to us; we can find a large number of devices, services, software and applications that can be "virtualized". This section illustrates the differences between traditional and virtual computing environments and takes a look at virtualization concepts and environments.

In a traditional physical structure, all computer components are installed on the same machine as shown in Figure 1.a, all computer hardware and software are mostly constant and visible only for a given computing device. In such computing environment, the processes of adding new capabilities to a computer requires new configurations in hardware or software or both, that are a waste of effort, computer physical components are logically independent and isolated, thus gaining greater abilities to create, update, delete and configure computer components.

The concept of virtualization began in the 1960s when it was defined as the possibility of installing different operating systems on the same computer [7]. Since then, Virtualization concept excessively has been expanded in today's computers; including many types and methods. There are many definitions of virtualization; Virtualization technology can be considered as a set of software tools that divide server into Virtual Machines to reduce costs, expand the allocation of computing resources such as storages, processing power and others [8]. By using virtualization, applications running under a particular operating system can run independently as shown in Figure 1.b.

In nutshell, Virtualization can be described as a technology that enables the abstraction of operating systems, software and hardware [4]. Virtualization describes the process of creating a software-based representation of something rather than a physical one [3]. Virtualization technology can be applied to networks, servers, storages, applications, processing powers or even operating systems [9]. Virtualization is generally accomplished by dividing all the capabilities of a single piece of hardware or software faithfully into independent environment [3]. Virtualization technology makes computing environments independent of physical infrastructure. Commonly, virtualization enables turning of one or more virtual machines on the same device, running different operating system through virtual machines on one computer and operating a virtual machine in a "sandbox" without modifying the configurations of the host computer [1].

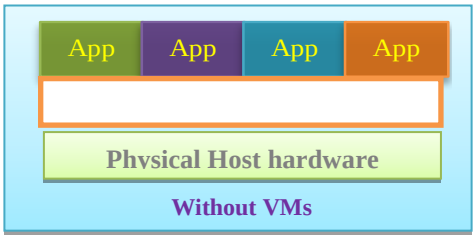

Figure 1.a Single operating system owns all hardware resources.

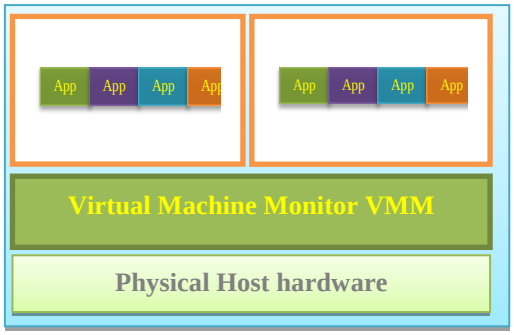

Figure 1.b Multiple operating systems share hardware resources

In virtualization environments, there is a thin software-based layer that separates the host machine from virtual machine called a hypervisor [10]. Hypervisor allocates the sufficient processing units and memories to each virtual machine [2]. Essentially, virtualization environments come in two forms: hosted virtualization form (Figure 2.a) and bare-metal also called native virtualization (Figure 2.b) [11]. In Bare-metal hypervisor, there is no need to install a server operating system first, so the hypervisor has direct access to hardware resources [10]. Bare-metal virtualization hypervisor has enhanced scalability, performance and stability [12]. Microsoft Hyper-V, VMware ESXi are some examples of bare-metal hypervisors. In hosted virtualization, the software is built completely on the top of a host operating system [12]. Unlike native hypervisor, the hosted hypervisor is like applications that install on a guest operating system. The hosted hypervisor manages the virtual machines, communicates and interacts with operating system of the host machine to access its resources [11]. Parallel Desktop, Microsoft Virtual PC and VMware Workstation pro are the most common hosted hypervisors.

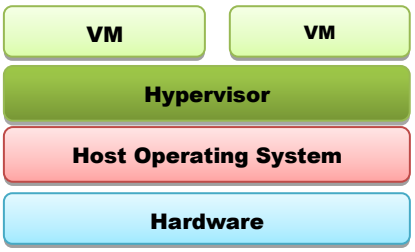

Figure 2.a: Hosted Virtualization

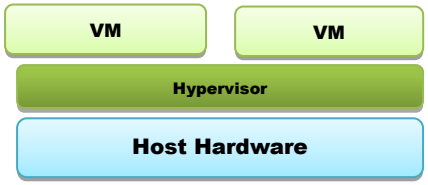

Figure 2.b: Bare-Metal Virtualization

3. LITERATURE REVIEW

Academic institutions usually maintain their IT solutions and allocate new budgets for developing innovative IT solutions to maximize the benefits in learning process. The high cost of computers, software licenses and complex network configurations have led universities to rethink carefully about using the existing IT infrastructures [13].Many educational institutions have begun to migrate from traditional to virtual forms to take their benefits and addressed many problems they were facing. Educational institutions use virtualization for the reasonable cost, ease of management and control [14].

Nowadays, many universities have used virtualization in teaching some courses, especially practical courses [13]. The successful experience of virtualization in some academic institutions has forced others to plan and implement virtualization to increase learning outcomes [15]. Many researches discuss the use of different types of virtualization in teaching technical courses. Virtualization provides a lot of flexibility in education and increase productivity [14].

Many researchers have investigated the use of virtualization in universities all over the world. For example, Nasereddin et al. [16] described different virtualization technologies that educational institutions have used to build virtual academic environments.

Dale (17) presented virtual computer laboratory. The paper investigated the use of hosted virtual machines in business-oriented information system security course. He focused on implementation and formulation of rules for business-oriented information system security course. He discussed some challenges and limitations of virtual machines in labs. Dale outlined some recommendations for using virtualization in education.

Rajeshwari et al [18] discussed the use of virtualization at the University of California. They highlighted the potential financial benefits that can be offered to the universities and other educational institutions, noting that the main benefits of virtualization are the reasonable cost and low power consumption. They clarified the required computer infrastructure for implementing this innovative technology without any obstacles. The paper explained a useful platform of virtualization in education. Citrix, VMware, and Microsoft have possible virtualization solutions and have shown that for maximum benefits, educational institutions must plan to implement the appropriate virtualization technology according to their size and structure [18].

García, Rajeshwari, Prasad [19, 18, 13] discussed about the deployment and implementation of innovative unique virtual infrastructure for educational purposes. They showed how to allow the students to remotely access some applications and systems using web browsers. They also discussed the use of hypervisor, which isolates virtual machines for each server in order to protect the virtual machines from each other.

Bell et al [15] discussed how teachers use virtual network laboratories in IT courses. They addressed the effective use of virtualization in different contexts to deliver the desired learning outcomes after completion of certain courses. They showed the high success rates in virtualized academic courses as compared to those in traditional training courses. Mahdi et al [Mahdi] introduced a collaborative computer lab; they discussed best policies to foster their student teaching information security utilizing virtual Labs. Mahdi used substantial class activities to master security course content. The paper introduced a solution based on Kolb's Experiential Learning Cycle to design hands-on activities for virtualized computer lab.

To summarize, the existing researches have discussed the basic benefits of adopting virtualization technology in academic environments, including the choices of different virtualization deployments and characteristics (e.g. compatibility with current IT infrastructure, cost, etc.). Some existing work provides a framework for testing the impact of using these technologies on student's performance. However, to this end, it is noticed that no existing researches discuss the use of virtualization in managing and controlling shared laboratories for computer security courses that may threaten the stability, availability and security of labs.

4. METHODOLOGY

The methodology of this work starts with explaining the experience of virtualization technologies in computers security course (CS 350). This course, which is taught within the curriculum of department of Computer Science at college of Arts and Sciences at Prince Sattam bin Abdul Aziz University - located in Wadi Al-Dawaser city in Saudi Arabia. The department teaches CS 350 to level seven students in bachelor of computer science. During six semesters before registering for CS 350, students have completed many courses in computer science. The course is divided into theoretical and hands-on activities as shown in Figure 6. The course contains many practical exercises, readings and applications to provide students with a comprehensive understanding of the security topics. Like most other courses in computer science, CS 350 is taught in 15 weeks at a rate of 3 hours per week for lectures and two hours for hands-on activities, so CS 350 has 75 contact hours. The main objectives of this course are to provide students an understanding of basic computer security issues and concepts. The course introduce computer threats, risks and systems vulnerabilities .The course develops students' ability to recognize, analyses, evaluate and mitigate security threats. CS350 enhances students' understanding issues they may face in their careers after graduation.

The college faces a biggest challenge during teaching this course. The hands-on activities has a potential to compromise the security of shared computer labs. Firstly, the College thought about establishing a specialized computer security lab to teach this risky course. The proposed lab would be equipped with the necessary technologies and computer security applications. It was not possible to establish this dedicated lab due to the difficulty of having the necessary budget in due time. More specifically, the university did not want to spend more money in building new facilities in the current compound because the new buildings were near completion. The college rethought to implement that course in the current laboratories without endangering labs hardware and software. The department of computer science agreed to use virtualization technologies in a shared laboratory to teach security course.

We developed our methodology through desktop virtualization for its several advantages over the other virtualization types. First, desktop virtualization can reduce pressures on network and server bandwidth. As a result, hands-on activities will not be blocked by network speed. Second, virtualized desktop isolates security activities to local network because it does not require Internet connection. Consequently, it prevents the threats of the hands-on activities results on the network. Third, virtualized desktops are portable. As there is a hypervisors on each operating system and virtualized desktop is implemented as files in specific folder, students could copy, distribute and download this folder a long with the activities on any storage device to another computer in the labs or outside the college. In addition, virtual desktop is easy to maintain during any software modifications, the virtualized desktop can be easily transferred to other computer. Moreover, desktop virtualization is flexible since it can be implemented on lab desktops, students portable devices, with only hypervisor installed. Lastly, desktop virtualization is cost effective because hypervisors mostly are free for educational purposes.

Computer Security Course CS 350

Hands-on Activities

- User Account Management
- Footprinting
- Network Sniffing
- Evaluating Security
- Using Encrypting File System
- Using TrueCrypt
- Vulnerability Scanning
- Setting up pgp accounts
- Password Cracking
- Social Engineering
- Penetration teams
- Firewalls
- Recovery Agent with Encrypting File System

Figure 6: CS 350 Hands-on Activities

4.1 Virtualization setting

Implementation of virtualization in CS 350 was to allow students conduct hands-on activities in computer security in a shared computer lab without exposing these devices and network to any threats. So the college chose Desktop virtualization technology using a virtual desktop infrastructure as shown in Figure 7.

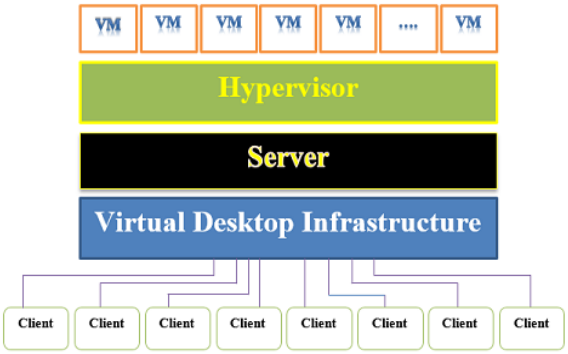

Figure 7: Desktop Virtualization using a virtual Desktop Infrastructure

Desktops in Lab6 were new and fulfilled desktop virtualization requirements. The Lab contained 28 desktop computers for students and one for the trainer. Each desktop computer had 2 Core i7 AMD Opteron processor, memory of 64GB of RAM, 1 Terabyte SCSI hard disk, 3 Network Cards, 17" flat-panel screen and CD/DVD writer. All desktop were connected to a Local Area Network (LAN) .The trainer's computer was connected to the Internet through the University Intranet. For the above mentions reasons, the department of computer science chose Lab 6 to virtualize some desktops for computer security courses.

We decided to install VMware Workstation Pro software for desktop virtualization for many reasons. First, VMware Workstation Pro is a standard virtualization platform that enables running multiple operating systems such as Windows and Linux as virtual machines on the same computer. Second, VMware Workstation Pro can run more than one virtual system at the same time without having to restart the computer. Third, Workstation provides a secure and isolated environment for evaluating applications and systems without affecting the host machine's configurations and it does not expose itself to any risks. Forth, Workstation is compatible with the famous Web browsers. Fifth, VMware Workstation Pro Isolates virtual machines from BIOS setting and disables BIOS editing. Finally, VMware Workstation accesses to USB ports. University of Prince Sattam Bin Abdul Aziz provides free copies of Microsoft Windows 8 for each staff or student, so we decided to install Windows 8 on the virtual machines.

4.2 Students' Experiments and Results

During the course, we covered topics related to the basic concepts of computer security such as: Cryptography, computer threats, security application, services, Countermeasures, security protocols and issues in network security. We covered discussions and hands-on activities in computer security. Each hands-on activity takes 60 minutes. We explain the basic ideas in the first 20 minutes; students take approximately 20 minutes to practice in groups or individually. At the end of each session, students explain their results and experiences.

Students trained themselves using VMware Workstation and its interfaces. Students installed VMware Workstation Pro for virtualization and Windows 8 on the virtual machine. Students gained good skills with VMware Workstation management through Admin accounts to control their virtual machines without posing any threats to the physical computers and network.

Day after day, students implemented many security activities based on each other. Students created virtual sandbox for risky hands-on activities, for example, students encrypted some applications, cracked passwords, detected and scanned viruses and more in isolated virtual environment. Virtualization offers students more opportunities to access some products not available on their physical computers. Students recorded their notes, observations, problems encountered during the exercises, solutions they have reached and learned lessons from all hands-on activities. At the end of the course, students gained a number of applications and documentation related to computer security.

Students expressed their satisfaction with CS 350 course and the hands-on activities they practiced through virtualization. All students developed their technical skills on VMware and became more confident in using the new security applications. Students satisfied with virtualization technology in education. Some students decided to take use of virtualization as a

method and to dig deeper into this technology after graduation. In general, it is possible to say that the experiments of students in CS 350 were positive and successful.

4.3 Limitations & Recommendations

Desktop Virtualization is still an emerging technology despite virtualization has been harnessed in all computing environments and has become an integral part of many educational institutions as previously mentioned in section 3. During installation and using virtualization in CS 350 course, we have come across many issues that affected the course contents and its learning objectives; we have addressed these limitations during the sessions. These issues include: students lack of experience in virtualization, the inability to control and monitor students' virtual machines, incompatibility of many hardware and applications with the virtual environment, the inability to backup and restore files from virtual machines.

The students had no prior practical experience with virtualization. Of course, some of the other courses that the students have studied before this course contain topics related to virtualization, such as Internet Technology and selected topics 1, however the students studied it theoretically and they did not practice them. As a result, students needed more time to master this technology, even though it was not a primary goal of the course but was a means to facilitate hands-on activities on certain security issues that could hurt or expose labs to risky.

When students installed a virtual machine on their computer, they had full control over the virtual machine. This is desirable and helps students achieve many tasks; however that made it difficult to control student activities or help them in solving some problems. Based on our experience, the teacher may install virtual machines for all the students with predefined Administrator accounts to facilitate teacher access to activities that do not require student control over the virtual machine. For activities that require students control on virtual machines, each student can create another Admin account on his virtual machine.

Some physical components were not compatible with virtualization platforms such as external storage devices and USB ports, so we couldn't use some required devices during some activities. Some applications were compatible only with Windows environments but not compatible with virtual environments, although the workstation has a good compatibility with many modern applications and systems. Therefore, we recommend computer security teachers to determine the hardware and software required for the course carefully and be sure that they are compatible with the virtual environment.

During the middle weeks of the course, we encountered difficulties in using backup and restore applications where some backup and file recovery programs only work on physical computers and on normal operating systems but are not compatible with virtual environments and this confirms our previous recommendation regarding pre-test of software and hardware compatibility with the appropriate virtualization platform.

5. CONCLUSION

This paper presents some knowledge about virtualization technologies, the opportunities and benefits of using this technology in educational institutions. The paper discusses the use of the VMware workstation pro in virtual machines for computer security lab. The challenges and limitations of virtualization technology are also outlined here. Virtualization is an effective means that helps students to implement many lab activities, and to achieve the course objectives. Desktop Virtualization offers faculties a great opportunity to teach advanced skills in computer security related courses and enables them to train the students on many hands-on activities that may expose or cause damage to computer labs. However, desktop virtualization is still an emerging technology and it has some limitations over security related issues. Computer security teachers may choose and test the appropriate virtualization platform that compatible with the applications and devices required during their courses.

6. REFERENCES

[1] Abdalla Alameen, "Cloud Computing Data Breach". International Journal of Computer Trends and Technology (IJCTT) V47(1):42-49, May 2017.

[2] Düpmeier, C., Stucky, K.U., Mikut, R. and Hagenmeyer, V., 2015, November. A concept for the control, monitoring and visualization center in Energy Lab 2.0. In DA-CH Conference on Energy Informatics (pp. 83-94). Springer International Publishing.

[3] Fernandes, S., 2017. Principles of Performance Evaluation of Computer Networks. In Performance Evaluation for Network Services, Systems and Protocols (pp. 1-43). Springer International Publishing.

[4] Knodel, O., Genssler, P.R. and Spallek, R.G., 2017. Migration of long-running Tasks between Reconfigurable Resources using Virtualization. ACM SIGARCH Computer Architecture News, 44(4), pp.56-61.

[5] Klement, M., 2017. Models of integration of virtualization in education: Virtualization technology and possibilities of its use in education. Computers & Education, 105, pp.31-43.

[6] Batalla, J.M., Mastorakis, G., 2016. On cohabitating networking technologies with common wireless access for home automation system purposes. IEEE Wireless Communications, 23(5), pp.76-83.

[7] Xu, M., Tian, W. and Buyya, R., 2016. A Survey on Load Balancing Algorithms for VM Placement in Cloud Computing. arXiv preprint arXiv:1607.06269.

[8] Jararweh, Y., Al-Ayyoub, M., 2016. Software defined cloud: Survey, system and evaluation. Future Generation Computer Systems, 58, pp.56-74.

[9] Hawilo, H., Shami, A., Mirahmadi, M. and Asal, R., 2014. NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC). IEEE Network, 28(6), pp.18-26.

[10] Liang, W.E. and Shen, C.A., 2017, January. A high performance media server and QoS routing for SVC streaming based on Software-Defined Networking. In Computing, Networking and Communications (ICNC), 2017 International Conference on (pp. 556-560). IEEE.

[11] Bugnion, E., Nieh, J. and Tsafrir, D., 2017. Hardware and Software Support for Virtualization. Synthesis Lectures on Computer Architecture, 12(1), pp.1-206.

[12] Tuminauskas, R., Ambraziene, D., Miseviciene, R. and Pazereckas, N., 2012. Educational infrastructure using virtualization technologies: Experience at kaunas university of technology. Informatics in Education-An International Journal, (Vol11_2), pp.227-240.

[13] Prasad, S.K., Banicescu, I., 2017. Keeping up with technology: Teaching parallel, Distributed and High-Performance Computing.

[14] Pankowska, M.B., 2017. MOOCs as Supplement of Informal Education. International Journal of E-Adoption (IJEA), 9(1), pp.10-25.

[15] Bell, S., Lane, A., Collins, K., Berardi, A. and Slater, R., 2017. Teaching Environmental Management Competencies Online: Towards" Authentic" Collaboration? European Journal of Open, Distance and E-learning, 20(1).

[16] Nasereddin, M., Clark, T.K. and Konak, A., 2014, March. Using virtual machines in a K-12 Outreach program to increase interest in information security fields. In Integrated STEM Education Conference (ISEC), 2014 IEEE (pp. 1-5). IEEE.

[17] Lunsford, D.L., 2009. Virtualization technologies in information systems education. Journal of Information Systems Education, 20(3), p.339.

[18] Rajeshwari, B.S. and Dakshayini, M., 2014. Comprehensive Study on Load Balancing Techniques in Cloud. Compusoft, 3(6), p.900.

[19] García-Valls, M. and Basanta-Val, P., 2017. Analyzing point-to-point DDS communication over desktop virtualization software. Computer Standards & Interfaces, 49, pp.11-21.