Broadening E-Commerce Information Security Education Using Virtual Computing Technologies

Abdullah Konak
Penn State Berks
Reading, PA 19610
konak@psu.edu

Michael Bartolacci
Penn State Berks
Reading, PA 19610
mrb24@psu.edu

Abstract

Information security is a growing concern for e-commerce transactions. However, higher education institutions generally do not provide much "hands-on" exposure to information security concepts due to costs, internal information security concerns, and a lack of worthwhile exercises that cater to students. This paper presents innovative ways to use a virtual computing technology to enhance student learning in computer networking and information security courses. The paper also demonstrates how pedagogical approaches, such as active learning, problem-based learning, and collaborative learning can be implemented inside and outside of classroom using virtual computers based on a Collaborative Virtual Computer Laboratory (CVCLAB) model. The CVCLAB model integrates well-tested virtual machine technology and proven pedagogical approaches in a collaborative leaning model to address the challenges in information security education.

1. Introduction

While the demand for information security professionals is increasing according to the Bureau of Labor Statistics 2008-2018 projections, student interest in information technology (IT) disciplines has been steadily declining since 2000 [1] and enrollments in IT-specific academic programs have continued to decline sharply [2]. As our society depends greatly on information systems, it is critical for organizations to have access to a talented pool of individuals who are skilled in confronting threats to information security, responding to emergencies, protecting vital IT assets, and helping to create policies that ensure the privacy of individuals. Information security is a dynamic field as security threats are becoming more complex and originating from very diverse sources. Therefore, the information security-related fields, particularly ones related to e-commerce and homeland security, can benefit from a diverse workforce. However, recent studies assert that minorities, and particularly women, constitute a very small percentage of IT security workforce.

Higher education institutions are also facing new challenges that need to be addressed. Particularly, in small campuses and community colleges, a majority of students are commuters who can only spend a limited amount of time on campus. Therefore, their access to campus computing resources, especially to specialized computing facilities and software, is limited. In addition, the increasing number of nontraditional students is changing classroom demographics in higher education [3]. Non-traditional students are highly motivated and generally prefer more active approaches to learning [1]. However, these students are disadvantaged in IT-related fields due to lack of basic computing skills. New solutions are needed to serve the needs of nontraditional and commuter students who have commitments away from campus. Another challenge in IT and security education is the rapidly increasing use of e-learning. While an e-learning model may not be appropriate for some courses that require large amounts of hands-on learning, still innovative solutions are needed to deliver some hands-on learning experiences in the e-learning education model as well.

To address the challenges summarized above, we have created a collaborative virtual computer laboratory (CVCLAB) that seeks to leverage a large group of virtual computers together with specially designed laboratory exercises in order to create a learning environment for computer networking and information security. The CVCLAB has been effectively used in several networking and information security courses at Penn State University's Berks Campus. A virtual computer laboratory (VCL) consists of several virtual machines (VMs). A VM is a software emulation of a computer that runs exactly like a real computer. Using this technology, a single computer can host multiple VMs with different operating systems which are isolated from each other and share the resources of the host computer. VMs can also be connected through virtual networks within the host computer. Using VMs, students can test advanced skills and perform complex tasks which are not usually allowed on campus lab computers and networks. For example, students can study the vulnerabilities of different operating systems, attempt to compromise the security of various computer systems, and take measures to defend against

attacks without any concern that their actions may affect other physical computers, production systems, or students. Furthermore, being software emulations, VMs are literarily unbreakable. Students can experiment with complex and high risk operations without any hesitation because the original state of a VM can be restored at anytime.

2. Virtualization Models

Virtualization is an approach for decoupling the underlying physical resources from the operating systems, applications, and users. The concept of virtualization is very broad, and ranges from servers and operating systems to applications, networks, and even devices such as mobile phones. In a traditional server environment, one physical server is host to one instance of an operating system supporting one or more applications. With virtualization, the server, storage, and network become a logical representation of these items. These resources are controlled through software and can be shared between multiple virtual computers. In a virtualized environment, a single physical computer or "host" may be running many virtual computers or "guests" each with different operating systems, network connections, storage, and applications.

There are two types of server virtualization and both approaches abstract the guest operating systems from the physical hardware. Type-1 virtualization uses a microkernel or a stripped down and very specific operating system with the single purpose of managing and presenting a virtualized environment to guest operating systems. A Type-1 installation might be of VMWare ESX directly on the hardware. Type-2 virtualization is essentially a process in an operating system, and is an application on top of an existing operating system. A Type-2 installation might be of VMWare Workstation or Microsoft Virtual PC installed onto an OS. Both types can be installed on servers, desktops, and laptops, but typically a Type-1 virtualization will only be found on a server.

3. Conceptual Structure of the CVCLAB and Virtual Computer Labs

The CVCLAB was designed based on the VMware ESX Server virtualization system. The logical architecture of the CVCLAB is shown in Figure 1. Currently, the CVCLAB includes several specialized computer laboratories hosted over three servers as they are briefly introduced below. The main purpose of many VCLs used in higher education is to allow students to access software resources of physical campus computers. On the other hand, the CVCLAB aims to provide students with an open learning environment in which they can experiment with complex and high risk operations without any concern. Specific implementation features of the CVCLAB are as follows:

- Students access VMs via a web browser or a client interface from anywhere with an Internet connection.
- VMs and related learning materials are available from a web page.
- VMs are connected in various configurations to support different instructional needs.
- Students can easily switch between these configurations to test different scenarios.
- Students are granted full administrative rights on VMs
- VMs have non-persistent storage (i.e., all configuration changes during a lab session are automatically deleted when students log-off)
- VMs are confined in the virtual environment and independent from the campus network. Therefore, they are not security threat to the campus network
- The system is centrally administrated, and new VM additions, software updates, or configuration changes to the system can be done anytime without interrupting the system operations.

Basic Networking and Security Virtual Labs (BNSVL): A BNSVL lab includes VMs of three types: client VM (C-VM), server VM (S-VM), and target VM (T-VM) as shown in Figure 1. Students are granted full administrative privileges on C-VMs. Each C-VM are loaded with network and security software tools such as network scanning and enumeration, system security audit, packet sniffing, intrusion detection, footprinting, cryptography, firewall, anti-virus, malware detection and removal packages. S-VMs and T-VMs are for the use of instructors. S-VMs provide network services such as DHCP, DNS, file server, routing etc. T-VMs are used by the instructors to simulate real-life scenarios. For example, instructors may set up T-VMs to simulate numerous operating system vulnerabilities and ask students to detect them using security tools available in C-VMs. VMs area equally divided between the three host servers for better user experience through load balancing. BNSVL is primarily intended to be used in introductory computer networking and security courses. To ensure the maximum security, C-VMs were configured with non-persistent hard drives and confined in the virtual environment without an outside network access. However, students are able to temporarily install and test software packages, which are made available through a shared storage.

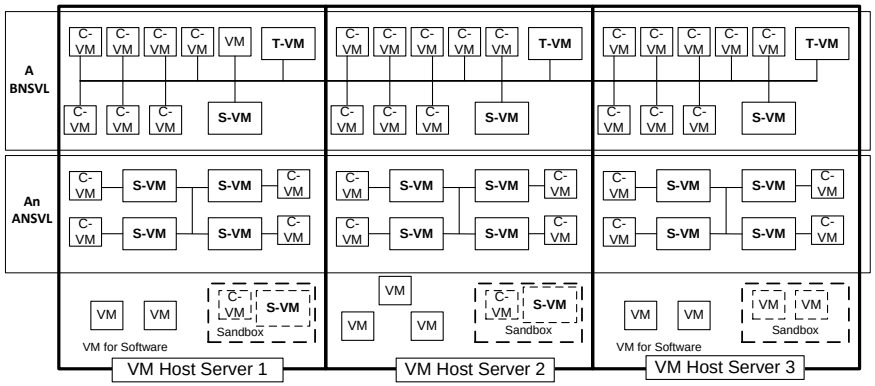


Figure 1. The logical architecture of the CVCLAB and virtual computer labs.

Advanced Networking and Security Virtual Labs (ANSVL): This virtual lab provides students with resources to practice advanced skills for Windows or Linux based server administration. Each S-VM has pre-installed services such as web, email, DNS, certification, authentication, authorization, remote access, etc. Therefore, students can practice numerous advanced server administration tasks. For example, they can activate web services on S-VMs, and then learn to implement specific web server configurations that are necessary to defend against network attacks such as denial of service. Depending upon scenarios, C-VMs serve as clients to test the services provided by S-VMs, as well as malicious computers where attacks are initiated. ANSVL are primarily used in advanced networking and security courses. ANSVL are also used in the delivery of online credit or non-credit programs on server administration and security.

Sandboxes: A Sandbox is a group of VMs dedicated to the exclusive use of a student or a team of students for inquiry based learning and undergraduate research activities over extended time periods. Within a sandbox, students are allowed to create, configure and network VMs without prior configuration or restriction. In addition, students are able to install and use a wide range of software packages which are available through a software library. A typical use of sandboxes is student semester projects or undergraduate research activities. For example, a sandbox could be created for a student team project and could be maintained by the team during the course of the project. Therefore, sandbox VMs have persistent storage so that students can build up on their work. Sandboxes are an unconventional idea that could make a high impact on student learning through problem-based [4-5] and collaborative learning [6-7]. Particularly, a sandbox is a great way to create a collaborative learning environment in which a group of students engage in a common task.

Virtual Software Labs (VSL): A VSL consists of independent VM machines that will be used to provide students, particularly commuter students, with an access to special software that is available on campus computers. A VSL can be used for many general purposes. For example, AutoCAD software can be installed on a VM so that commuter engineering students can access it from home.

4. Hands-On Learning Materials

The CVCLAB can address many of the financial, physical, administrative, and security related obstacles to providing hands-on education in IT and e-commerce security, but it is alone not sufficient to enhance student learning without guidance. Therefore, many hands-on learning materials have been developed to utilize full potential of the CVCLAB. Table 1 summarizes the list of hands-on activities that have been developed for the CVCLAB and their specific virtual computer labs. Some of these activities were previously used in the related courses. However, these activities were not easily transferable between the institutions because of the differences in hardware and software resources. In this sense, the CVCLAB has provided standardized platforms in which learning materials can be collaboratively developed and freely exchanged between different institutions and instructors. In addition, instructors and students are encouraged to design new activities and share them with others through the CVCLAB wiki. The CVCLAB currently has following type of learning materials.

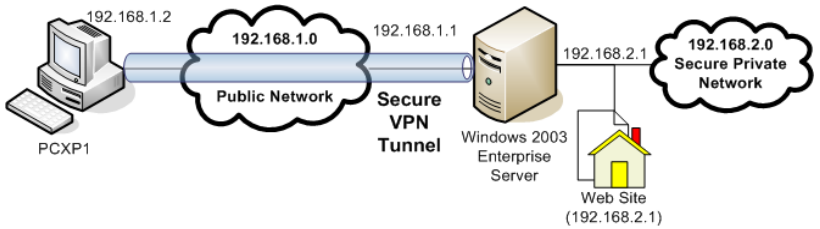
Short Class Activities (10-15 minutes): Short class activities aim to promote active learning [8-9] in class. A typical example for a short class activity is as follows. Students are grouped in teams of two such that each student controls a VM as shown in Figure 3. Teams are asked to configure their computers IP address settings according to the different scenarios given by the instructor and to test connectivity between their computers. During the activity, students are expected to figure out why two computers can communicate for some IP address settings and cannot for the others. This short activity is an effective way of teaching IP addressing.

Table 1. A list of sample hands-on learning materials

Topic	Hand-on Educational Material Topics	Virtual Computer Lab
Foundations of Computer Networking	Configuring TCP/IP (Windows and LINUX), Network Addressing (IP, Ports, MAC, ARP) , Network management and diagnostic tools, Network applications (FTP & TELNET);	BNSVL
Advanced Networking	Packet Sniffing and Analyzing; Firewall Configuration; Routing; Packet Filtering; Remote Access; DCHP and DNS Management;	BNSVL ANSVL
Server Administration	User Administration and Policies; Web Server Administration; Email Server Administration;	ANSVL Sandbox
Applied Cryptography in Ecommerce	Symmetric and Asymmetric Ciphers; Cryptanalysis; Public Key Infrastructure; Pretty Good Privacy; Hashing and Digital Signatures; Digital Certificates; Authorization and Authentication using Encryption.	BNSVL
Prevention & Protection Mechanisms	Antivirus software; Trojan Horses; Hardening Operating Systems; Firewall Configuration; Vulnerability Scanning; DMZ; Proxy Servers; Securing Networks with IPSec; Virtual Private Networks (VPNs); Secure Socket Layer (SSL)	ANSVL Sandbox
Detection Mechanisms	Intrusion Detection (SNORT); Logging and Auditing; Denial of Service Attacks;	BNSVL
Recovery & Forensics	Computer Investigations; Working with File Systems; Extraction Exercises; Data reconstruction;	Sandbox

Problem Based Lab Exercises & Assignments: (30-90 minutes): These activities aim enhancing student's problem solving and critical thinking skills, as well as technical skills. Each activity starts with a problem scenario and build on the concepts taught in class, and encourage students to make generalizations through review questions and class discussions. Figure 2 illustrates a sample exercise from IST 402 Web and E-Commerce Security class that is performed in ANSVL. Since students will be able to access VMs outside of campus, parts of the exercises can be assigned as homework. This enables more time for discussions and group work during class.

Problem & Scenario: Assume that network 192.168.1.0 is an unsecured public network and network 192.168.2.0 is a secured private network in the following network diagram. You have a few employees who work from home (denoted by PCXP1) and they have to have access resources available on private network 192.168.2.0. For example, they must access the web/application server (192.168.2.1) on this network. The problem is that your telecommuter employees must use the public network 192.168.1.0 to access private network 192.168.2.0. You are expected to create a secure communication over the public network in order to protect sensitive company data. Discuss solutions to achieve this goal and implement them.



Expected Tasks: (*i*) Creating a user group for remote access; (*ii*) Configuring a VPN connection on the server; (*iii*) Creating a remote user access policy; (*iv*) Configuring an employee computer for VPN; (*v*) Testing connections and analyzing VPN traffic.
Sample Review: (*i*) Discuss possible security risks due to allowing remote access through VPN in this scenario. (*ii*) Compare alternative technologies to achieve the same goals.

Figure 2. A Sample Problem-Based Lab Exercise used in Web and E-Commerce Security Course.

Class Projects: Almost every IT related courses have a project that typically is integrated with real world issues and practices. The sandbox concept of CVCLAB is used in such projects.

5. Distance Learning Model in the CVCLAB

Distance learning is the fastest growing segment of the U.S. higher education system. Distance learning promises to be an important opportunity to broaden information security education and deliver it to a larger population of students. However, distance learning has been criticized for lacking certain elements such as teamwork and hands-on learning; both of which are very important for information security education as security threats are becoming very complex and diverse. The CVCLAB promises unique opportunities for hands-on learning in a distance learning model.

The CVCLAB has been successfully used in two asynchronous online courses, IST 451-Network Security and IST 402 -Web and E-commerce Security, to provide students with hands-on learning experiences as follows. The course content and hands-on learning materials are made available through a course web page. A group of VMs are dedicated for the sole use of each enrolled student throughout the semester so that students do not interfere with one another other while performing hands-on exercises. Students are expected to independently complete a series of activities such as the ones given in Table 1. The course content includes step-by-step detailed instructions and video clips of these activities. Upon completion of an activity, students are expected to submit a report summarizing their learning. Because the CVCLAB can be accessed at anytime and from anywhere, these courses can be delivered asynchronously to geographically distributed students. In addition, students don't have to come to the campus to use the CVCLAB.

Table 2 summarizes the feedback from students about their overall satisfaction with the CVCLAB in online IST 451 and IST 402 courses and how much the CVCLAB have contributed to their learning in this course. Students were highly satisfied with their learning experiences in the CVCLAB, and they felt that the CVCLAB significantly contributed to their learning. Close to 80% of the students stated that these online courses provided as much hands-on learning experiences as a traditional course. When student were asked about what they liked most about the CVCLAB, they indicated the ability of working at their own pace and learning materials outside of class time.

Students also commented the CVCLAB about the variety of the activities that they can practice. One of the challenges in hands-on learning is the variation in skill levels of students. This is particularly an issue for commuter campuses and community colleges where the student population is very diverse in terms of students' age and background. The CVCLAB makes computing resources available to students for 24/7. Students can use VMs any time to improve their skills or learn new skills to be ready for the workplace. The CVCLAB has also structured this process by providing roadmaps that guide students through series of self-paced activities and assessment tools to excel their skills in various information security areas. During the semester, many online students used these self-paced activities to improve their skills although some of these activities were not required by the course.

Table 2. Sample results from the CVCLAB satisfaction survey in online IST 451 (Spring 2012) and IST 402 classes (Fall 2011)

Overall, are you satisfied with the virtual computer lab (CVCLAB), neither satisfied nor dissatisfied it, or dissatisfied with it?						
Extremely satisfied	Moderately satisfied	Slightly satisfied	Neither satisfied nor dissatisfied	Slightly dissatisfied	Moderately dissatisfied	Extremely dissatisfied
31.8%	63.6%	4.5%	0.0%	0.0%	0.0%	0.0%
Overall, how much did hands-on exercises in CVCLAB contribute to your learning in this course?						
Extremely contributed	Very much contributed	Moderately contributed	Slightly contributed	Little contributed	Very little contributed	Not contributed at all
45.5%	31.8%	22.7%	0.0%	0.0%	0.0%	0.0%
Please state how much you agree with the statement: "this course has provided as much hands-on learning experiences as a traditional course"						
Strongly agree	Moderately agree	Slightly agree	Neither agree or disagree	Slightly disagree	Moderately disagree	Strongly disagree
50.0%	27.3%	18.2%	0.0%	4.5%	0.0%	0.0%

6. Groupwork in the CVCLAB

Research suggests that collaborative and cooperative learning environments have positive impacts on student learning. In the context of face-to-face education, several studies have shown that students who work in groups learn more and retain their learning longer than those who work alone [10-12]. Unfortunately, most virtual computer lab architectures for information security training do not support groupwork. The architecture of the CVCLAB was designed to maximize collaborative learning opportunities for students.

The CVCLAB has many associated groupwork exercises that provide students with the opportunity to use the knowledge being acquired to complete context-relevant problems or tasks. A successful completion of a groupwork exercise requires collaboration between two or more students. A groupwork

exercise is designed in a way that each student depends on and is accountable to one another other for a successful completion of the exercise. Although guidance is provided in terms of learning objectives, expected outcomes, and general step-by-step instructions, students have to make several decisions. For example, in an IPSec exercise to secure the traffic between two hosts, two students must choose the same encryption algorithm set and the same pre-shared secret key and implement the same IP filter action making this type of exercise challenging outside the classroom. However, based-on our classroom experiences, learning outcomes are well justified.

An example for how to conduct groupwork in the CVCLAB is given in Figure 3. The learning objective of this exercise is to describe different parts of IP address, IP address classes, and sub-/super-netting. In the group work treatment, two students are assigned to two networked C-VMs (PC A and PC B), and then they are instructed to configure their computers' TCP/IP settings according to the different scenarios and to test connectivity between them for each settings and to figure out why their computers can communicate for some settings and why not for the others. When this exercise is performed outside the classroom, students are expected work and communicate synchronously through a chat or video conferencing session. The CVCLAB also allows team members to access all VMs assigned to the team. Therefore, students can remotely help one another if needed.

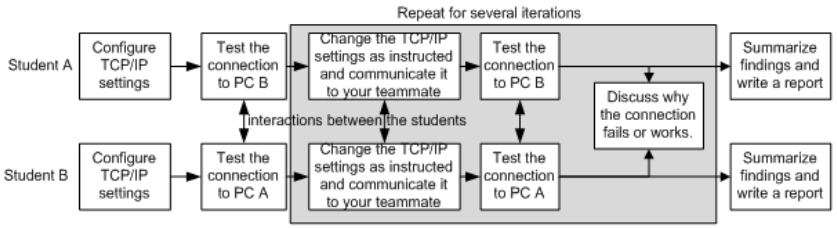


Figure 3. A Sample Groupwork Exercise.

6. Conclusions

Distance learning is one of the fastest growing segments of the US higher education. However, a lack of collaborative learning and hands-on experimentations are considered among the important weaknesses of distance learning. In this paper, the CVCLAB is presented as a solution to provide students with collaborative hands-learning experiences. A virtual computer laboratory should not only provide students with an environment in which they can test critical skills in isolation but also opportunities to collaborate and interact with other students.

Acknowledgements

This paper is based on work supported by The National Science Foundation under Award No. DUE-1044800. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] J. M. Benshoff, "Nontraditional college students: A developmental look at the needs of women and men returning to school," *Journal of Young Adulthood and Middle Age*, vol. 3, pp. 47-61, 1991.

[2] M. Granger, *et al.*, "Information Systems Enrollments: Challenges and Strategies," *Journal of Information Systems Education*, vol. 18, pp. 303-311, 2007.

[3] "Special Analysis 2002 Nontraditional Undergraduates," U.S. Department of Education Institute of Education Sciences2002.

[4] M. D. Merrill, "A Task-Centered Instructional Strategy," *Journal of Research on Technology in Education*, vol. 40, pp. 33-50, 2007

[5] M. A. Albanese and S. Mitchell, "Problem-based learning: A review of literature on its outcomes and implementation issues," *Academic Medicine*, vol. 68, pp. 52-81, 1993.

[6] M. Beckman, "Collaborative Learning: Preparation for the Workplace and Democracy," *College Teaching*, vol. 38, pp. 128-133, 1990.

[7] J. Cooper, "Cooperative Learning and College Teaching: Tips from the Trenches," *Teaching Professor*, vol. 4, pp. 1-2, 1990.

[8] A. C. Hare, "Active Learning and assessment in mathematics," *College Teaching*, vol. 42, pp. 76-77, 1997.

[9] E. J. Anderson, "Active Learning in the Lecture Hall," *Journal of College Science Teaching*, vol. 428-429., pp. 428-429, 1997.

[10] B. Heffler, "Individual learning style and the learning style inventory," *Educational Studies*, vol. 27, pp. 307-316, 2001.

[11] M. Kirk and C. Zander, "Bridging the digital divide by co-creating a collaborative computer science classroom," *Journal of Computing Sciences in Colleges*, vol. 18, pp. 117-125, 2002.

[12] P. Dillenbourg, *Collaborative Learning: Cognitive and Computational Approaches* New York, NY: Elsevier Science, 1999.