Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

DESIGNING A VIRTUAL LAB FOR COMPUTER FORENSICS

Wen Yao, Chao-Hsien Chu, Bing Liu and Zang Li, *The Pennsylvania State University, University Park*

Abstract – The fast growing demand on information security education, both in terms of the numbers of courses and students, presents a major challenge to developing and maintaining a laboratory facility that reinforces concepts and skills taught in class with hands-on experiences. In this paper, we present an approach for designing a Virtual Security Lab (VSL) that allows students to access the lab resources through Internet. The feedback from students enrolled in computer forensics class showed the positive results of using VSL for this course. Our experience provides valuable lessons for security education.

Index terms – Information security curriculum, Computer forensics, Virtual security lab, Education

I. INTRODUCTION

Education in information security and assurance is better served by a laboratory component that reinforces principles and theoretical analysis learned in the classroom [1]. However, a security laboratory is difficult to build and maintain, as it needs to be dedicated and isolated, and cannot be part of a general purpose campus lab. Traditionally, hands-on labs are conducted in an isolated computer lab, so that security problems that may occur will not affect other computers in the same network. As the number of security courses and students enrolled in these programs increase, the physical space for hands-on exercises remains a finite resource. As a result, it is difficult to provide isolated lab space with sufficient computer resources to meet the schedule requirements for a variety of security classes. In addition, with the development of online education programs, we faced the challenge of developing a new mechanism to provide hands-on exercises to commuter and distance-learning students, which could not be handled by physical lab space.

W. Yao, B. Liu, and Z. Li are with the RFID Lab, College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA 16802, USA (e-mail: wxy119@psu.edu; bzl124@psu.edu ; zul110@psu.edu).

C. H. Chu is the founding director of the Center for Information Assurance, College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA 16802, USA (corresponding author, phone: 814-865-4446; fax: 814-865-6426; e-mail: chc4@psu.edu).

One alternative to solve the abovementioned challenges is to develop a virtual environment by using a virtual network and virtual machines. The virtual network can simulate the physical environment without affecting the user's experience. In this paper, we present an approach to develop a Virtual Security Lab (VSL) to meet the increasing demand for security education. With a VSL, students are able to experiment with security software, without worrying that their exercises may impact other computer systems or other students. They are able to evaluate the security issues of different operating systems, attempt to compromise the security of other computer systems, and install additional security mechanisms without concerning that their actions may affect other computers or violate the university's security policies.

We aim to achieve the following goals:

- Increase advanced hands-on learning in networking and security courses and make these computing resources available to commuter students 24 hours a day and 7 days per week.
- Provide hands-on learning experiences in a distance learning model
- Reduce lab hardware, software, and maintenance costs and the need for specialized computer labs
- Provide an agile and secure computer environment for information assurance (IA) education

II. DESIGN APPROACH

This section describes our approach for designing the VSL for a computer forensics course. We first briefly introduce this course, and then illustrate the development process and design principles. Related work is also discussed to compare our work with that of others.

A. Course Description

The course "Computer and Cyber Forensics" is one of the required IA courses in the undergraduate and online professional master programs at the College of Information Sciences and Technology at Penn State. This course allows students to learn different aspects of computer and cyber crime, and ways to uncover, protect, and document digital evidence. Students are exposed to different types of tools, techniques, and procedures, and

ISBN 1-933510-99-4 ©2010 CISSE

are able to use them to perform rudimentary forensic investigations.

Hands-on exercises are a major component of this course, covering a large range of tools and techniques, such as data imaging, forensic analysis, malware analysis, network forensics, e-mail tracing, data hiding, and steganography. Popular computer forensic tools including Forensic Took Kit (FTK), EnCase, and ProDiscover are used to help students understand the course materials better. Since our physical lab space is no longer large enough to meet the requirements for the increasing number of students (more than 100 students each year) and it is not available for students enrolled in distance learning, we designed and implemented a VSL for this course (and other IA courses as well).

B. VSL and Design Principles

A virtual machine (VM) is a software emulation of a fully functional operating system, such as Windows XP, Windows Server 2003, and Linux. Thus, multiple virtual machines can be held on a host PC and a distinct IP address can be assigned to each virtual machine. From the user's perspective, a virtual machine can be treated as any regular machine on the network. The advantage is that the destruction of a virtual machine does not result in any adverse effects on the underlying host system. The virtual network can be considered as an isolated and secure environment, which is desirable for hands-on security labs.

A virtual security lab can be designed to provide a remotely accessible environment to conduct experimental work and research in information and computer security via the Internet using a browser interface or virtual client. The virtual lab allows an instructor to create virtual networks and virtual machines so students can access them through a secure connection over the Internet. The virtual network and the hosts can be configured according to the needs of a security course. Our VSL design is based on the course requirements of "Computer and Cyber Forensics" using the principles of the characteristics proposed by [1], such as accessibility, configurability, maintainability, realistic, and insulated.

C. The Development Process

Before starting the development process, we established a task force, consisting of members from administrators, instructional design, faculty, students, and IT support, to gain a broad-base understanding, examine alternatives, formulate our vision and develop a plan. After the plan for developing virtual labs was approved by the college, a development team consists of: a faculty member, a teaching assistant, an instructional design person, and a technical staff, who were assigned to start the development. We established several VSL course development teams, one team for each course. The IT group is responsible for purchasing, implementing, and maintaining the VSL infrastructure that is designed by the VSL development team. We are primarily responsible for designing and configuring the virtual environment for the labs that were originally conducted in the physical space.

The design implementation took about six months, which consisted of the following five phases (see Figure 1): (1) determination of the software and hardware requirements, (2) design of logical virtual infrastructure, (3) design of physical virtual infrastructure, (4) installation of software tools in client machine and virtual servers, and (5) testing and maintenance. The feedback in the testing stage was analyzed and used to improve the previous four activities. The first and most important step is to determine the hands-on requirements for the course. The objectives, scope, hardware, software, and process of each lab had to be carefully identified and planned in advance. Based on those requirements, a logical and physical framework was then specified and designed, followed by software installation and network configuration. After completion of this iterative process, we tested to insure that all hands-on labs could be conducted and completed successfully in the virtual environment. All the above installations were initially conducted in the master image, which was duplicated on the client machines. Finally, students were given their own accounts and lab instructions to conduct hands-on exercises.

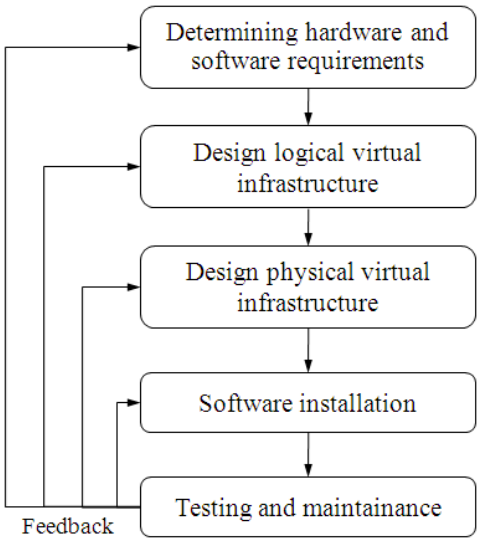

Figure 1. VSL Design Iteration

D. Related Work

Hands-on exercises are a critical and integrated component for any effective information security

education and training program. Recent years have seen an increased awareness of the importance of a laboratory component in security education. For example, the Georgia Tech Information Security Center has developed an isolated laboratory network to teach defensive and offensive security experimentation [2].

With the increasing need for such laboratory environment, a virtual laboratory concept was proposed and applied in IT security education [3]. Their work proves that virtual laboratories are helpful to eliminate geographical and financial limitations in traditional IT security education. At Polytechnic University, NY, a virtual laboratory has been designed to allow multiple institutions to share one physical laboratory for information assurance education and research [4]. They also identified the key characteristics that a well designed virtual laboratory must be able to demonstrate. A list of exercises was given that could be run on the proposed design. Most of the existing exercises focused on computer, network, or cyber security.

Following this stream of security education, we designed and developed virtual labs for our computer forensics course. Compared to other studies, we focused on the entire iterative process of developing a VSL and typical problems encountered during this process. The details of the transition from a physical lab to a virtual lab are discussed. We also collected the feedback from students who took this class and their comments are helpful in evaluating the practicability of our VSL design. Our approach provides valuable resources for other practitioners in this field to develop virtual labs in similar disciplines.

III. Design of a VSL for Computer Forensics

This section describes the details of the five steps used in designing a VSL for the computer forensics course and examples of labs.

A. Requirement Analysis and Problems Encountered

Originally the hands-on exercises were conducted by using two isolated small local-area networks; each with two PCs running Windows operating system and one machine running Linux OS. We used eight hands-on labs for the "Computer and Cyber Forensics" course:

- Lab 1: Data Imaging Using Windows Tools
- Lab 2: Forensics Analysis
- Lab 3: Investigating Windows Systems
- Lab 4: Data Hiding and Steganography
- Lab 5: E-mail Tracing
- Lab 6: Worm and Virus Analysis
- Lab 7: Network Forensics
- Lab 8: Mobile Forensics

Table 1 summarizes the software and hardware that were originally used in the physical labs. Due to the limited space here, we only present the major requirements and omit the others.

Then we examined and decided for which lab, software and hardware can be virtualized. For some labs, their hardware cannot be virtualized because of hardware protection such as a USB dongle (e.g., lab 1). Another example is lab 8, which needed a PDA device. To solve these issues, we either use emulators to simulate the functionality of the hardware or dropped that portion of the lab. Table 2 provides the solutions for the problem encountered in the conversion process. This can be a useful guide to solve similar problems that may be encountered.

Table 1. Software and Hardware Requirements

	Lab 1	**Lab 2**	**Lab 3**	**Lab 4**	**Lab 6**	**Lab 7**	**Lab 8**
Software:							
FTK Imager			y				
Jphs05				y			
XVI32				y			
Stegdetect				y			
Camouflage				y			
Anna Kournikova virus					y		
Argosoft mail server					y		
Microsoft outlook					y		
Nmap						y	
Wireshark						y	
Snort(Linux)						y	
Microsoft Active Sync							y
ProDiscover		y	y				
Hardware:							
Switch						y	
PDA							y
EnCase	y	y					
Forensic Toolkit	y	y	y				
Power brick	y						
Write Blockers	y						

B. Logical Virtual Infrastructure

The proposed virtual lab framework is presented in Figure 2. The network contains a virtual server running on Window 2003 server OS, and several pairs of virtual client machines. This virtual server and client machines

have been carefully configured so that students can explore and investigate different security problems and scenarios. The virtual server has DNS and file server installed. Additional services can be added thereafter. The virtual server and clients are connected together within a local area network (LAN) by a secure gateway.

Table 2: Problem Encountered and Solutions

Lab	Problems	Solutions/Remarks
Lab 1: Imaging Process	Hardware write blocker	Use software write blocker
	Need external suspect drive	Use internal suspect drive
	Software write blocker cannot be used in virtual environment	Practice the write protection outside the virtual environment
	Disk to Disk Imaging	Add a Linux Imaging Lab
	Dongle is needed for full function on EnCase	Use ProDiscover
	Dongle is needed for full function FTK	Use ProDiscover
Lab 2: Linux Forensics	Dcfldd tool not built in Linux	Store the tool in File server for access
	Live CD distribution may not work	Need to verify
Lab 3: Forensics Analysis	Dongle is needed for full function on EnCase	Use smaller file Use ProDiscover
Lab 4: Windows Forensics	Dongle is needed for full function on Registry Viewer	Use freeware Registry Editor
	The virtual keyboard is not functioned properly	Need to resolve the problem!
Lab 5: E-mail Tracing	No formal Internet connection	Practice the skills outside the virtual environment
Lab 7: Network Forensics	Software installation for Linux is very complication due to the lack of Internet connection	Emulate the connection outside virtual network and then start the configuration process
Lab 8: Mobile Forensics	Hardware PDA/Cell Phone needed	Use PDA emulator
	Device Seizure software is outdated	Use trial version

Each team was assigned to access a pair of virtual client machines, running Win XP and Linux operating systems respectively. All the virtual machines had the same configuration, with all forensics software installed. These software tools could be used to conduct investigations on the victim machine inside the virtual network. Students also had administrative privileges to install other software in their virtual client machines. We didn't need to worry about the crashing of client machines since they would go back to their original state after being rebooted, and any change by students would disappear after logoff. Additional software tools were available for downloading from the file server. We also provided documents for each lab to describe available software with their configuration and other data.

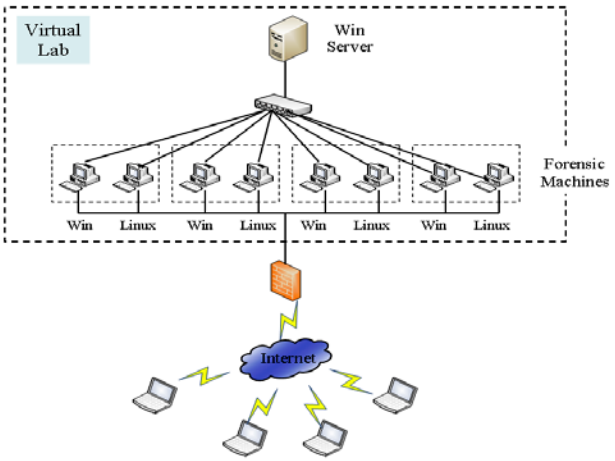

Figure 2. The Logical Virtual Infrastructure

C. Physical Virtual Infrastructure

Figure 3 presents the physical infrastructure used for the computer forensics labs, which are the foundation for students to log into the client machines and use software applications. The detailed specifications are discussed below.

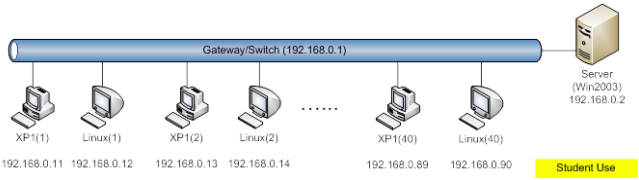

Figure 3. Physical Infrastructure for IST454 Lab

1. We need to have three master images: XP1, Linux and Win2003. Win2003 was used as the server. Each student team was assigned a pair of XP1 and Linux client machines.
2. The class had 40 students and each student needed one XP1 image and one Linux image. So we need to make 40 images of XP1 and 40 images of Linux.

Based on those considerations, we would have 80 virtual machines, all of which would be on the same LAN.

3. For each virtual machine, an account was needed to log into the operating systems. Students may have wanted to install or delete software in their virtual machines. Instructor and the teaching assistant needed the ability to view and monitor student machines.

According to the above specification, the IT group of our college helped to construct the infrastructure and the master images, on which we could do the installation and configuration. Due to a limitation in computational resources, we ended up with 20 set of client machines. That meant two students as a team shared a pair of virtual client machines.

D. Software Installation

We installed and configured the required software (see Table 3) for the hands-on exercises on the master image. For most labs, we use freeware if possible to avoid any license issue. For example, on the windows machine, we installed Argosoft mail server and Registry viewer, both of which are free. All software for Linux machine is open source and thus free of charge. For those software tools that need licenses, we use the evaluation version so the license would not be a concern. For example, FTK, EnCase, and ProDiscover were installed on the master image and reproduced to client machines. After expiration, we would reinstall the software. For those light weight tools with evaluation periods and only used once, we put them on the file server and asked students to download and install as necessary. In this way, they learned how to access the server and install software on the virtual machine. After rebooting, the installed software would disappear and the virtual machine goes back to the original state. Software licensing is a complicate issue to deal with; we are exploring converting the imaging lab to one using Linux Live CD, which would also eliminate the need of using write blocker.

Table 3. Software Installed on XP Client Machine

• EnCase v6.7	• Wireshark
• Forensic Toolkit	• ProDiscover Basic
• FTK Imager	• PDF Reader 9
• Registry viewer	• Windows Mobile 6 Localized Emulator
• Jphs05	
• XVI32	• Microsoft Device Emulator 3.0
• Stegdetect	
• Camouflage	• Microsoft Active Sync
• Argosoft mail server	• Microsoft outlook/word/excel
• Nmap-4.11	

We also installed DNS Server and File Server on the Win2003 server. The DNS Server is used to convert domain name to IP address. We created a "public" folder for data and information sharing so students could remotely access the server by using their own accounts. We created a "Submissions" folder for students to upload their temporary data files. Each student could only access their own folder on the server.

E. Testing and Maintenance

Testing was an essential stage of the VSL development process. Before the master image was cloned to the virtual client machines, we thoroughly tested the software and configuration for each lab to identify potential problems and resolve them. This course had two teaching assistants (TA); one designed and maintained the virtual environment and labs. The other would independently test and verify the lab procedures and environment worked correctly. First, the TA for designing the virtual labs went through the lab procedure and then the other TA tested the lab again. Potential problems were identified, listed, and solved. After that, the instructional designer for our college, with less technical background, conducted the lab to see if the lab instructions were easy to follow. She gave suggestions and helped to revise lab instructions. After three rounds of independent testing and revision, we ensured that our configuration was ready to implement. We asked the IT group to clone the virtual clients and create ID, password, and IP for each virtual machine. We also developed a brief user guide to describe how to use the virtual lab.

We needed to maintain the virtual environment during the semester. Students would encounter occasional problems with the virtual machines, e.g., server crash and password not working. Most of these problems would be solved by the TA. For example, a lab needed an additional piece of software; the TA usually put it in the file server so students could download easily. Other technical problems that could not be solved by the TA were passed to the IT group (e.g., exception in network failure) for resolution.

F. Example Labs

We provide two example labs in computer forensics to demonstrate the use of the VSL.

Lab 1 – Windows Imaging

This lab deals with the creation of several images of the media as evidences (i.e. forensic copies) so that the digital contents can be investigated and analyzed without altering the originals. In this lab, students will use forensic tools including EnCase and FTK to conduct the imaging process, which consist of four steps:

- Forensically wipe the storage hard drive: Before the image of a suspect drive is written to a hard drive in the forensic computer, the drive has to be forensically wiped clean of all prior data.
- Write-protect the original data source: The suspect drive should be write-protected using a hardware or software write blocker to prevent altering during the imaging process.
- Data acquisition: This is a bit-by-bit copying of every bit of the data on a suspect drive, including the file slack and unallocated file space that often contain deleted files and e-mail messages. Residual data is also captured by this process, this is the data that has been deleted but not erased.
- Verify the accuracy of the image: A drive image can be fingerprinted with a hash value, which insures the integrity of the file. Whenever there is any modification of the data, it can be detected.

We have installed the forensic tools EnCase and FTK on the virtual Windows XP machines. Three virtual disk drives are available for conducting the experiment. Drive C is the regular drive used to store all forensic tools and data. Drive D is a suspect drive, which we assume it was removed from a suspect machine. Drive E is a drive to be used to store images acquired from the suspect drive. Once students use their own accounts to log on to the virtual machines, they can follow the lab instruction to conduct the lab.

Lab 7 – PDA Forensics

Handheld devices such as PDA provide highly mobile data storage in addition to computational and networking capabilities. As they are becoming more affordable and commonplace in the workplace, more and more handheld devices are involved in crimes and incidents. This lab equips students with the techniques to properly acquire, retrieve, and examine information present on the mobile devices for digital forensics. The architecture for the concept of PDA forensic analysis is presented in Figure 3.

We configure the virtual forensic computer as follows:

- A PDA emulator will be used as the suspect handheld device.
- Microsoft Active Sync will be used to synchronize data between the virtual PDA and the forensic computer. This tool has been properly installed on the virtual forensic computer.
- An evaluation version of a PDA forensics tool will be used to conduct the investigation. Students need to follow the instruction and download the tool from virtual server and install it.
- Four testing files in different formats have been created and stored in the virtual machine for use in this lab. These files are used for learning and practice.

Although we use a PDA simulator which is essentially a piece of software instead of a real PDA in the VSL, student can still learn the process of synchronizing data between a handheld device and an investigating computer, without much difference as experimenting in the real scenario. With a VSL, we can avoid the hardware costs of PDA's by using a virtual PDA without losing its functionality.

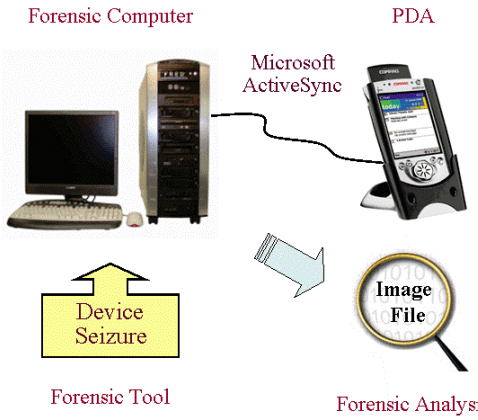

Figure 3. Physical lab scenario for PDA forensic analysis

IV. Student Experiences, Benefits and Lessons Learned

Our VSL for computer forensics course has been used for more than two semesters. When asked the different experiences in using physical and virtual labs, students in the class provided feedback as follows:

- "I appreciated the convenience of the virtual lab environment. It allowed me to access the lab anytime of the day." "It was nice that each time I accessed the virtual lab it was in a pure state. It had not been altered by the students before me. It was also forgiving of mistakes I would make in the learning process. If I made a mistake that altered the virtual machines configuration all I needed to do was log out and log back in again. Also the virtual environment allowed me to use programs that otherwise would have been expensive or difficult to install on my own machine."
- "I preferred the virtual lab because the equipment always functioned correctly. The physical labs that I have used in the past where plagued by connectivity and configuration issues that disrupted the learning processes. Also physical labs lack the resources to allow individuals to have their own equipment to experiment with. The times that physical labs are available for students to access also make them less than ideal learning environments." "Overall the virtual lab learning environment was far better than a

physical lab. I feel I was able to learn more and understand the material better."

From the above comments, we see that compared to using physical labs, students prefer to use the virtual machines, because they have flexible time to conduct exercises without the need of physically attending labs on campus. Students also have more privileges on the virtual machines, such as installation of new software because the virtual machine will recover to the original state after rebooting. Students were able to experiment with security software without concern that their experiment would impact other computer systems or violate the university's policy. Moreover, students could evaluate the potential security issues of different operating systems, attempt to compromise the security of computer systems, and install additional security mechanisms.

Overall the instructors, teaching assistants and technical support staff all liked the VSL better than the physical lab. Here are some of key benefits:

First, the operations and maintenance of the virtual lab is easier and straightforward. In the physical lab, since the lab was shared by several different classes, technical supports and TAs always need to spend a lot of time to fix hardware failure and debug software configuration change before each new exercise was given. With the virtual lab, since the client machines for each class are configured separately and given in a separate directory, if there are problems in one class, technical support can fix the problems at the master image and then cone the client machines in a short period of time.

Second, the college also saved significant money avoiding maintenance and upgrades to the lab machines every other years. Moreover, technical support saved time in monitoring possible security leakage from the physical lab. With the virtual lab, these types of cost can be eliminated completely or reduced significantly.

Third, the major advantages to the instructors are: (a) instructors can use the system in class to enhance teaching and discussion anywhere and anytime. In class, the instructor and first ask students login to the lab, try something new with different settings, and explore the results. The instructor can then explain the concepts and discuss the countermeasures in class. (b) VSL lab also gives instructors some flexibility in introducing new tools to class if needed; the instructor can upload the tools to the file server himself/herself and ask students to download and install them without waiting for technical support to install the tool in all machines. Students will also learn the skills to configure and debug new tools.

Fourth, with VSL, class and lab scheduling is also simplified significantly. In the past, scheduling IA related classes and lab hours was a major headache as (a) instructors, TA, and students all have different schedules and (b) class size is too big to fit into one lab session. Thus, most labs needed to be scheduled in the late afternoon, evening or weekend so that the TA and students can be physically present. With the VSL, TA no longer need to be physically present and students can complete lab anytime and anywhere according to their own schedule. If students have question, they can e-mail the TA to get feedback. If needed, the TA can even log into the system to work out the problem with students simultaneously.

However, in order to run the VSL smoothly, a well prepared and carefully designed instructional guide for each lab is critical. In our experience, the instructional guide should provide sufficient details on the process but at the same time should leave some rooms to motivate and trigger students thinking (instead of just following though step by step). Also, each lab should include some challenging questions or tasks for students to explore.

Currently, the VMware only supports limited virtual hardware (e.g., it did not support USB devices and portable hard drive) so it may be difficult or impossible to explore all aspects and tools of digital forensics. In this case, we suggest supplement it with videos. For instance, we tape the "write blocking" process to illustrate its importance to data acquisition.

Possible disadvantages of VSL include: (1) the virtual machines may running slow at times, especially when there are many concurrent users login. Adding more servers may resolve the problem; and (2) the network or the server maybe broken or power down, thus, no one can access the virtual machines without notice. Therefore, the virtual network should be well maintained to ensure the accessibility of the VSL. A backup plan maybe also needed.

V. CONCLUSION

Developing a virtual lab to support information security education and distance learning program is a very important but challenging task. This paper presented a formal and pragmatic approach to enhance courses and facilitate the computer and cyber forensics curricula to meet the growing number of students in this area. We have discussed the detailed process of transforming a physical lab into a virtual lab. Problems encountered in this process are also detailed and solutions are presented. Finally, the advantages of using a VSL experienced by students are discussed, benefits listed, and lessons learned are identified to improve the development process. Currently, the VSL is being used for the computer forensics course by undergraduate students and online students. We are continuing to migrate other information security related courses into virtual labs.

VI. Acknowledgement

First, we would like to express our sincere thanks to the National Security Agency and Department of Defense for providing us funds to support the development of the Virtual Security Lab at Penn State (Grant H98230-09-1-0397). Special thanks go to John Staedt, an undergraduate student in our Security and Risk Analysis major, who provides valuable feedback and suggestions to improve the lab design and this paper. Finally, we would like to acknowledge the IT group at the College of IST at Penn State for their contribution and support of the VSL implementation.

VII. References

[1] V. Ananthapadmanabhan, P. Frankl, N. Memon, and G. Naumovich, "Design of a Laboratory for Information Security Education," in *Proceedings of World Conference on Information Security Education* Monterey, CA, 2003, pp. 61-73.

[2] R. T. Abler, D. Contis, J. B. Grizzard, and H. L. Owen, "Georgia Tech Information Security Center Hands-On Network Security Laboratory," *IEEE TRANSACTIONS ON EDUCATION,* vol. 49, 2006.

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

[4] V. Padman and N. Memon, "Design of A Virtual Laboratory for Information Assurance Education and Research," in *Proceedings of the 9th Colloquium for Information Systems Security Education* Georgia Institute of Technology, Atlanta, Georgia, USA, 2005, pp. 6-9.