# Implementation Progress, Student Perceptions, and Refinement of a Virtual Information Security Laboratory

**C. Cavanagh**[1] **and R. Albert**[2]
[1]University of Maine at Fort Kent, Fort Kent, ME, USA
[2]Professional Management Division, University of Maine at Fort Kent, Fort Kent, ME, USA

**Abstract -** *Effective information security laboratory exercises are increasingly being viewed as an essential element of information security educational offerings. Such offerings are, in turn, considered by most to be the primary means of raising student awareness and interest in information security and ultimately preparing a much needed, knowledgeable, and skilled information security workforce. Virtual laboratory exercises exist in a variety of formats, each better suited to a particular educational purpose, but all compatible with a distance education delivery modality. The design of a remotely accessible virtual laboratory and the exercises themselves must also provision for a secure environment that encourages experimentation while minimizing the risk of introducing a security incident. The purpose of this paper is to report on progress made in the implementation of a virtual information security laboratory, student experience with and perceptions of the laboratory, and refinement of the laboratories design based on reported advancements in the design and implementation of virtual information security labs and corresponding curricular elements in higher education settings.*

**Keywords:** Cybersecurity, information security, online education, virtual lab

## 1 Introduction

Information security remains a critical topic in society, government, and education today. Educational institutions have been called upon to help raise information security awareness through, among several approaches, expanding university curricula [6]. Professional organizations, in response to this and other related needs expressed by various constituencies, have responded in part, by being more explicit in their curricular recommendations to educational organizations. The Association of Computing Machinery (ACM) for example, has evolved its curriculum recommendations for Computer Science to include “information security” as a core topic in several of the fundamental knowledge areas [1].

Effective information security laboratory exercises are increasingly being viewed as an essential element of information security educational offerings [5, 7, 8]. Practical skills oriented laboratory exercises are an attractive means of raising student awareness and interest in information security and ultimately preparing a much needed, knowledgeable, and skilled information security workforce.

The need to expand appropriate information security learning activities as essential elements of information security instruction, especially hands-on laboratory exercises, should become even more pronounced as university curricula continue to evolve. Similarly, the need to extend access to such laboratory exercises to distance situated students should increase in response to increased utilization of distance education delivery modalities.

The context in which the Maine Information Security Lab (MEISLab) operates requires provisioning for secure access to virtual lab resources by students enrolled in our distance education programs (e.g., online Associate of Science in Information Security). This context also requires making available a variety of exercise formats in addition to virtual labs (e.g., Web labs) that are better suited to a particular educational purpose.

Above all, the laboratory environment and exercises must encourage students to engage in active experimentation that enables attainment of learning objectives while simultaneously minimizing the risk of a student introduced security incident. Hence, the ability to isolate the virtual computer lab was one of the key goals targeted in the design of the MEISLab [3].

## 2 MEISLab Goals

The goals for MEISLab were established following a review of the goals, outcomes, benefits, and recommendations stemming from similar efforts that have been reported [3]. The predominant aim of establishing the MEISLab was to ensure realization of the instructional advantages identified as being associated with delivering a rich learning experience made possible through virtualization.

The specific goals that have driven the design of the MEISLab reflect the following desirable characteristics:

- Accessibility (remote access)
- Observability of host and network events
- Ability to simulate realistic scenarios and various client/server configurations

- Separability of virtual networks including the ability to isolate the virtual lab systems from the campus network

- Remote configurability

- Ability to share resources efficiently

- Provisioning of an appropriate platform in support of different areas of information security instruction

- Support for rapid prototyping of computer and network configurations

- Provisioning of a uniform experience across students

- Simple and cost effective course administration

All of these characteristics support constructivist approaches to instruction [3]. Using virtualization to support lab activities that reinforce problem-solving skills in authentic environments should be considered an essential component of a well-designed virtual information security lab.

To these ends, the lab was designed and implemented to:

- Harness the instructional benefits of virtualization;

- Provide remote access in support of online education modalities including the option for synchronous instruction; and

- Support learning activities that:

    - Ensure students have sufficient background knowledge to maximize comprehension

    - Promote students' appreciation of the ethical dimensions associated with engaging in information security activities

    - Promote students' compliance with all information security and technology use policies

    - Ensure students meet the student learning outcomes and related curricular requirements defined for the information security degree programs.

# 3 Implementation Progress

The virtualization solution that was selected is a "bare metal" VMware vSphere Hypervisor (ESXi) and VMware vCenter Lab Manager 4.0. The Lab Manager product provides access control over local and distance situated students. Local and distance situated students involved in this study participated in an information security course designed to support a hybrid delivery approach and offered during the spring semester of 2012. Online synchronous meeting software/services (e.g., GotoMeeting) was utilized in support of distance situated students on as needed basis. Some have argued the use of synchronous meeting software/services as an essential element of online instruction will become the standard for conducting information assurance instruction going into the future [7].

As noted earlier, one of the key objectives for the MEISLab design was the ability to separate virtual machine traffic from the campus network. This separation is intended to enable students to freely modify the network and virtual machine configurations without risk of introducing potentially malicious traffic or actions on the campus network. In order to achieve this objective we used a creative technical workaround in order to accommodate the VMware Lab Manager installation requirements and ensure proper isolation of network traffic.

When performing the initial installation of Lab Manager the setup wizard requires specification of a physical network that will be designated the default network for Lab Manager [9, 10]. In many common networking configurations, Lab Manager will use this default network to obtain external IP addresses for the virtual machines in order to allow users to remotely access the virtual machines even if the virtual machines are configured to use private IP addresses [9]. As we did not want to make the campus network the default physical network for Lab Manager we utilized a residential-class router to simulate a physical network. This router was configured as a DHCP server that would assign addresses in a private address range. This router was then plugged directly into the physical ESXi server in order to simulate a physical network in Lab Manager. With this router in place, we were successfully able to complete the Lab Manager installation process.

With this configuration implemented, we were able to isolate traffic between the campus and virtual machines in one of two methods. The first method involved attaching the virtual machine's network adapters to a virtual network that had no connection to the Internet [10]. The second method involves connecting the virtual machine's network adapters to a physical network but enabling the block in/out network fencing setting [10]. By specifying the block in/out option the virtual machines are essentially partitioned off from connecting to the physical network and Lab Manager ensures that traffic does not escape [10].

Efforts to build a library of "stock" course-oriented virtual machine images in support of specific instructional lab activities are continuing. Additional effort has been made to ensure the proper training necessary for the synchronous instruction support system and to ensure the availability to students of "Web labs" for the purpose of ensuring students will be better able to fully comprehend and benefit from lab activities by having the prerequisite conceptual knowledge.

## 4 Student Experience and Perceptions

In order to establish how effective the virtual lab implementation was in meeting the goals we had outlined, student feedback was solicited and analyzed. As eight out of 16 of our stated goals dealt with administrative and infrastructure concerns (e.g., centralized logging within the lab and isolation of virtual machine traffic), the students were asked to provide responses to questions focusing on the remaining eight goals.

A web survey consisting of 17 questions was created to gauge how well our implementation met our goals concerning virtual lab accessibility, the ability to simulate realistic scenarios and devices, the separability of virtual networks, remote configurability of virtual machines, the ability to share lab resources efficiently, rapid prototyping of computer/network configurations, problem solving in authentic environments, and quick access to course-oriented virtual machine images. The first section of the survey focused on the accessibility of the virtual lab to students and so we were interested in determining the types of Internet connections used to access the lab. The survey found almost half of the students were accessing the lab from on-campus and the other half from off-campus. The majority of on-campus students were utilizing a wired Internet connection with all off-campus students utilizing a high-speed Internet connection. The most popular type of connection by off-campus students was digital subscriber line (DSL) followed by cable and then satellite. Students found the performance of the lab to be suitable with the majority rating the performance as “acceptable”.

The next section of the survey was dedicated to determining if the students believed that the labs they had completed were models of real-world scenarios. Configuration of virtual private network (VPN) services and a password cracking activity are two examples of lab exercises the students completed. An overwhelming majority of students agreed that the labs did indeed represent real-world scenarios and the majority also agreeing that the configurations of the virtual machines represented real client/server configurations. Furthermore, the majority of students felt that the particular labs they had completed were realistic.

Separation of the virtual networks from one another was an important concern of ours and the next section in the survey was written with that topic in mind. Students were asked if they experienced any odd network behavior while completing their labs and an even spread of responses was recorded. However, the majority of students stated that they did not encounter any odd network behavior while completing their labs. The survey then asked those who did experience odd network behavior if the behavior prevented them from successfully completing the labs. An equal amount of students stated that they were prevented from completing their labs, were not prevented from completing the labs, and were unsure if the behavior prevented them from completing the labs.

Remote configurability of the virtual machines and virtual networks was a very important goal to us, as we want to offer students the freedom to explore new machine configurations and network designs to facilitate their own personal research interests and curiosities. Students were asked if they felt they could configure the virtual machines as they desired and the majority of students answered “yes” for this question. The survey then asked students if they encountered issues with the virtual machines or their configuration and the majority of students responded that they did not encounter issues with the virtual machines. Those users who did encounter issues with the virtual machines stated that their issues were stemming from attempting to use the VMware web browser plug-in. The final question in this section asked students if they felt that they could reconfigure their virtual machines, as they desired with the majority stating “yes” that they could.

We were interested in determining if there were specific times of the day when heavy lab usage could affect performance such as in the late afternoon or on the weekends. Students were asked if they experienced performance issues when accessing the lab during specific parts of the day and the majority of students responded that they did not encounter poor performance during specific times.

The last section of our survey concentrated on the students’ ability to quickly access course-oriented virtual machine images. We asked students if they felt they were able to easily access virtual machine configurations (the virtual labs) stored in the MEISLab library and the majority responded that they could easily access the configurations. Those who were not able to easily access the configurations stated that their issues were with the VMware web browser plug-in and being able to locate the virtual labs assigned to them within the MEISLab.

These student perspectives are similar to those reported by others [2]. Similarly, the authors’ concerns over the practical use of such facilities are similar to those expressed by others [7], especially the need for training of instructional and IT support staff to be more comfortable with the additional levels of abstraction involved with such technology. Further refinement of the design and implementation of the MEISLab is necessary to support even greater levels of effectiveness and student achievement.

## 5 Future Design Refinement

Recent studies have suggested that the choice of laboratory configuration should be based on the complexity of the concepts being taught and the student’s background

[4]. Web labs that consist of a Java-based applet requiring student access to only a web browser and typically focused on a single concept are one configuration option that was initially explored [3]. Web labs will clearly continue to play a significant role in provisioning laboratory exercises accessible to local and distance situated students.

Part of the future refinement of the laboratory exercises will therefore include categorizing the lab exercises based on complexity of the underlying concepts and student background, and then refining the MEISLab configuration to support those exercises for which student knowledge requirements are relatively high (i.e., students who more readily conceptualize a multiple computer environment).

Open source software virtualization platforms (e.g., Oracle VirtualBox) are also important to include when considering implementation options. Such options are particularly appealing for their low/zero licensing cost and for providing opportunities for end-user modification to meet local customization demands and/or environmental conditions. These will be explored further in the continuing evolution of the MEISLab.

## 6 Conclusion

As the number of information security educational offerings continue to grow as significant components of evolving program curricula targeted to address the growing demand for increased information security awareness and preparation of a knowledgeable and skilled information security workforce, so too the need for practical security laboratory exercises accessible in a variety of formats and delivery modalities.

The survey of student perceptions revealed support for MEISLab meeting its goals. In particular, a majority of student respondents rated MEISLab performance as "acceptable", lab activities as being "realistic", virtual machines as being "easily accessible" and "reconfigurable", with no unexplained erroneous behavior.

The design and implementation of the MEISLab will continue to evolve based on students perceptions, complexity of the laboratory exercises relative to achievement of learning objectives, and availability of more affordable and customizable open source virtualization platforms.

## 7 References

[1] Association of Computing Machinery (ACM) (2008). "CS2008 Curriculum Recommendations for Computer Science". Retrieved May 11, 2012 from http://www.acm.org//education/curricula/ComputerScience2008.pdf

[2] Burd, S. D., Gaillard, G., Rooney, E., & Seazzu, A. F. (2011). "Virtual Computing Laboratories Using VMware Lab Manager", *Proceedings of the 44th Hawaii International Conference on System Sciences*.

[3] Cavanagh, C. & Albert, R. (2011). "Goals, Models, and Progress towards Establishing a Virtual Information Security Laboratory in Maine". *Proceedings of the SAM '11 Conference*, pp. 496-500. Retrieved May 11, 2012 from http://cerc.wvu.edu/download/WORLDCOMP%2711/2011%20CD%20papers/SAM5057.pdf

[4] Fulton, S. & Schwietzer, D. (2011). "A Concept Focused Security Lab Environment". *Proceedings of the 15th Colloquium for Information Systems Security Education*, pp. 126-131. Retrieved May 11, 2012 from http://cisse.info/archives/15th-colloquium/papers

[5] Irvine, C. E. (1999). "Amplifying security education in the laboratory", *First World Conference in Information Security Education, pp. 139-199*. Retrieved May 11, 2012 from http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/schweitzer2009c.pdf

[6] National Security Council (2009). "60-day Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure". Retrieved May 11, 2012 from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[7] Nestler, V. & Bose, D. (2011). "Leveraging Advances in Remote Virtualization to Improve Online Instruction of Information Assurance", *Proceedings of the 44th Hawaii International Conference on System Sciences*.

[8] Schweitzer, D., Gibson, D. & Collins, M. (2009). "Active Learning in the Security Classroom", *Proceedings of the 42nd Hawaii International Conference on System Sciences, pp. 1-8*. Retrieved May 11, 2012 from http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/schweitzer2009c.pdf

[9] VMware (2011). *Lab Manager Installation and Upgrade Guide*. Retrieved May 11, 2012 from http://www.vmware.com/pdf/labmanager25_Installation_Guide.pdf

[10] VMware (2011). *Lab Manager User's Guide*. Retrieved May 11, 2012 from http://www.vmware.com/pdf/lm40_users_guide.pdf