Goals, Models, and Progress towards Establishing a Virtual Information Security Laboratory in Maine

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 - *Information security education remains a critical topic in today's information driven societies. Educational institutions have been called to action to help raise information security awareness, knowledge and skills in those they serve. Cyber defense competitions are an attractive option to help raise awareness and interest in information security. Effective information security educational activities and cyber defense competitions most often require significant technical resource requirements including an information security laboratory infrastructure. Universities and other organizations have made progress to date in defining and demonstrating practical information security laboratory infrastructures. The purpose of this paper is to identify the goals associated with establishing an information security laboratory that will support information security education and outreach efforts within Maine, identify models that have been successfully demonstrated to date, and report on progress made in the design and implementation of this laboratory in Maine.*

Keywords: Cybersecurity competition, information security education, security lab, virtual machine

1 Introduction

Information security remains a critical topic in today's information driven societies. Driving much of this increased attention is the increased severity of damage that has resulted from failed efforts to secure information systems, the prolonged dearth of information security practitioners, and the low level of information security awareness in our general population.

Educational institutions have been called to action to help raise information security awareness [1]. In 2009, President Obama ordered a 60-day, comprehensive, *clean-slate* review to assess U.S. policies and structures for cybersecurity. Specific recommendations contained in the resulting report included a call to initiate a K-12 cybersecurity education program for digital safety, ethics, and security as well as expanded university curricula [12].

Universities are ideally positioned to orchestrate such competitions for the betterment of current and future students and to contribute to the best preparation of future information workers and leaders.

Cyber defense competitions are an attractive and effective option for raising awareness and interest in information security while simultaneously educating for prevention and addressing the private and government sector needs, but they require significant technical resource requirements [2, 5]. Chief among these is an information security laboratory that can be used to help prepare participants and avail them an environment in which to compete.

The intended audience and instructional delivery modalities that must be supported are two considerations that must be made when establishing an information security lab in support of higher education initiatives, including outreach efforts. Our context requires provisioning for secure access to lab facilities by students enrolled in our distance education programs and potentially by those participating in the Maine Cyber Defense Competition (MECDC).

The educational potential of virtual computer labs, including those in support of information security instruction in different contexts has been reported by many researchers [4, 13, 14, 18, 19]. Such experiences have contributed greatly to the evolution of goals and models used to inform subsequent designs.

A virtual information security laboratory does not yet exist in Maine and this is believed to be the first effort of its kind in the state.

2 Common Information Security Lab Goals

The goals for the Maine virtual information security lab were established following a review of the goals, outcomes, benefits, and recommendations stemming from similar efforts to date. For example, goals were defined to ensure realization of the instructional advantages identified as being associated with delivering a rich learning experience made possible through virtualization.

Desirable characteristics of a virtual lab include accessibility, observability of host and network events, ability to simulate realistic scenarios and devices, separability of virtual networks, remote configurability, and the ability to share resources efficiently [14]. In this context, a virtual lab is defined as a facility that provides a remotely accessible environment to conduct hands-on experimental work and research in information security. An additional primary characteristic should be the ability to isolate the virtual lab systems from the campus network [11].

Virtualization has been reported to provide benefits including giving each student control over configuration, providing unique IP addresses to each server, and the ability to demonstrate centralized logging [16]. Additional benefits include the provisioning of an appropriate platform in support of different areas of IA instruction, support for rapid prototyping of computer and network configuration, increased availability of lab environment, providing a uniform experience across students, and simplified and cost effective course administration [13]. All of the benefits can be viewed as supporting constructivist approaches to instruction.

The instructional advantages of a constructivist approach to instruction are well established [3, 9, 15]. Problem solving in authentic environments is an example of an effective constructivist learning technique [19]. 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.

Virtualization, when coupled with online synchronous instruction software (e.g., Elluminate, GoToMeeting), has been reported to provide opportunities for dealing with heterogeneous groups, facilitating instructional design possibilities for a diverse audience, enhancing student-teacher interactions, and assisting students in acquiring complicated technical skills with greater ease and more interest [13]. Inclusion of online synchronous instruction software should therefore be considered an essential component of a well designed virtual information security lab that supports distance education.

For students to fully comprehend and benefit from lab activities, it is also essential to ensure they first have the necessary background knowledge [17]. Well crafted lab activities that are remotely accessible can well serve this need. “Web labs” in particular, have been constructed at a high level of abstraction and used to introduce, demonstrate, reinforce, and encourage experimentation with complex security concepts. Lab activities such as these should also be considered an essential component of a well designed virtual information security lab.

Efforts such as the University of Maine Cybersecurity Education Guide [10] to collect, categorize, and improve the searchability and accessibility of all forms of information security educational materials are greatly valued for their potential to aid a much larger audience of educators. The addition of appropriate search metatags and corresponding data to form true digital libraries of such resources represents a significant contribution. Access to the fruits of these efforts should be considered an essential component of a well designed virtual information security lab.

3 Maine Virtual Information Security Lab Design Goals

The goals established for the virtual Maine Information Security Lab (MEISLab) are based predominantly on the need to establish an information security laboratory in support of information security outreach and educational efforts within Maine. They are also based on the aforementioned goals, outcomes, benefits, and recommendations. Finally, the goals are based in part on the design considerations for constructing a virtual computer lab environment appropriate to small campus environments. These design considerations include particular sensitivity to the often very limited financial, space, machine, time, and staffing resources available at many schools [7].

The aim is to design an instructional laboratory environment that:

- Harnesses the instructional benefits of virtualization;
- Provides remote access in support of online education modalities including the option for synchronous instruction; and
- Supports 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.

4 Virtual Information Security Lab Models

There are several predominant virtualization solution models including, Apache Virtual Computing Lab (AVCL), Microsoft HyperV (MHV), VMLogix LabManager, and Xen. Each model exhibits its own benefits and challenges.

For example, benefits reported being associated with an information security lab model combining VMware Lab Manager, Virtual Center, and ESX include:

- increased accessibility for students to laboratory resources;
- fewer hardware components resulting in decreased administrative overhead; and
- support for complex laboratory exercises [4].

Challenges, as reported for this same example, include:

- Training requirements to prepare instructors and students to correctly navigate and complete the process of selecting and deploying a virtual machine;
- Limited cataloging and organizing features for virtual machine images, thereby making searching and selection more challenging;
- Limited browser support; and
- Significant demands on underlying server resources (especially disk space) and their management [4].

Similar reports are available that provide an account of the benefits and challenges of each of the other models. In the end, a model should be selected based on the particular needs and resources of the organization.

5 Progress

This report is as much an outline of the process used to identify the design goals of the MEISLab as it is an account of progress toward implementation and experience gained to date. Nevertheless, several final product comparisons have been made and this has led to the selection and installation of several key hardware and software components.

As this is a small scale pilot operation, the server that has been selected is a Dell PowerEdge R610 configured with Dual Xeon E5620 2.4 GHz processors each with 12MB cache, 24GB RAM, 146GB RAID configured storage spanning 6 physical disks and a quad port Gigabit Ethernet NIC. The virtualization solution that was selected is a "bare metal" VMware vSphere Hypervisor (ESXi) and VMware vCenter Lab Manager 4.0. As of this writing, the Lab Manager product is being deprecated and replaced by VMware vCloud Director that will require evaluation in the year ahead.

The department has also registered with the VMware Academic Program that provides free or reduced cost access to many VMware products in non-production, instructional settings. The selection of VMware was made in part due to it being the closest to being an "out-of-box" solution [4]. The combination of low/no cost and feature maturity of the commercial product line made it the best candidate for this particular application. Having access to VMware's products will avail students the opportunity to quickly access and deploy "stock" course-oriented virtual machine images enabling them to take the assignments further with additional exploration and experimentation. The Lab Manager product will be used to control access by both local and distance situated students.

The Citrix GoToMeeting service was purchased for use in synchronous instruction as needed to support distance education students. The service provides for impromptu or scheduled presentations and live demos to individual students or groups that can be used to fill instructional gaps. It can also be used to provide the instructor the ability to remotely observe and control a student's computer. This can be very useful when a simple demonstration or technique correction within the student's actual computer is called for. Training of key personnel has also been completed.

Progress has begun on the establishing a collection of useful VM images in support of laboratory exercises. This effort is expected to continue and include the preparation of images in support of the cyber defense competition.

6 Conclusion

The need for better securing the information that today's societies increasingly dependent upon is expected to continue well into the foreseeable future and so to the need for more and better information security education. Educational institutions have been called to action to help raise information security awareness, knowledge and skills in those they serve and cyber defense competitions are but one attractive option.

Significant technical resource requirements including an information security laboratory infrastructure must be met to fully support information security education and outreach initiatives. Providing remote availability of these resources to a distant population is considered essential in situations in which distance education is involved.

There are many design considerations that should be taken into account and it is essential to identify the specific goals of a virtual information security Lab and select the most appropriate model that will support attainment of these. In our context, the infrastructure model that has been selected consists of a combination of VMware products.

Our progress to date in implementing this infrastructure includes the purchase of the necessary services, software and prerequisite hardware components. Efforts have begun to build a library of "stock" course-oriented virtual machine images in support of specific instructional lab activities. 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.

7 References

[1] Albert, R. (2009). “The ‘U’ in Information Security”. *Proceedings of the 2009 ASCUE Summer Conference*, pp. 23-31. Retrieved May 1, 2010 from http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/45/2f/85.pdf

[2] Albert, R. & Wallingford, J. (2010). “Cyber Defense Competitions - Educating for Prevention”, *Proceedings of the 2010 ASCUE Summer Conference*, pp. 22-30.

[3] Boghossian, P. (2006). “Behaviorism, Constructivism, and Socratic pedagogy”, Educational Philosophy and Theory, 38(6), pp. 713-722.

[4] 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*.

[5] Conklin, A. (2006). “Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course”, *Proceedings of the 39th Hawaii International Conference on System Sciences.*

[6] Elluminate. Retrieved May 1, 2011 from www.elluminate.com

[7] Gephardt, N. & Kuperman, B. A. (2010). “Design of a Virtual Computer Lab Environment for Hands-on Information Security Exercises”, Journal for Computing Sciences in Colleges, 26(1), 32-39.

[8] GoToMeeting. Retrieved May 1, 2011 from www.gotomeeting.com

[9] Kumar, M. (2006). “Constructivist epistemology in action”. Journal of Educational Thought, 40(3), pp. 247-261.

[10] Markowsky, G. & Markowsky, L. (2010). “Consumer Guide to Online Cybersecurity Resources: UMCEG”. *Proceedings of the 2010 International Conference on Security Management, SAM 2010, July 12-15, 2010, Las Vegas Nevada, USA, 2 Volumes.*

[11] Nance, K. L., Hay, B., Dodge, R., Wrubel, J., Burd, S. D. & Seazzu, A. F. (2009). “Replicating and Sharing Computer Security Laboratory Environments”, *Proceedings of the 42nd Hawaii International Conference on Systems Sciences.*

[12] National Security Council (2009). “60-day Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”. Retrieved May 1, 2010 from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[13] 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*.

[14] Padman, V. & Memon, N. (2002). “Design of A Virtual Laboratory for Information Assurance Education and Research”, *Proceedings of the IEEE Workshop on Information Assurance and Security, June 17-19, 2002, USMA, West Point, New York, USA.*

[15] Powell, K. C. & Kalina, C. J. (2009). “Cognitive and social constructivism: Developing tools for an effective classroom”, *Education*, 130(2), pp. 241-250.

[16] Powell, V. J. H., Johnson, R. S. & Turcheck, J. C. (2007). “VLABNET: The Integrated Design of Hands-on Learning in Information Security and Networking”, *Proceedings of the 2007 Information Security Curriculum Development Conference*, September 28-29, 2007, Kennesaw, Georgia, USA.

[17] Schweitzer, D. & Boleng, J. (2009). “Designing Web Labs for Teaching Security Concepts”, Journal of Computing Sciences in Colleges, 25(2), pp. 39-45.

[18] Stackpole, B., Koppe, J., Haskell, T., Guay, L. & Pan, Y. (2009). “Decentralized virtualization in systems administration education”, *Proceedings of the 9th ACM SIGITE conference on Information Technology Education*.

[19] Wu, Yu (2010). “Benefits of Virtualization in Security Lab Design”, ACM Inroads, 1(4), pp. 38-42.