Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

Form Follows Function:
Information Assurance Network Design for Problem Based Learning

Sean V. Coyne
svc113@psu.edu

Scott J. Roberts
sjr16@psu.edu

School of Information Science and Technology, Pennsylvania State University

ABSTRACT

In developing a new set of courses in Information Assurance at Penn State University's School of Information Science and Technology, a group of upperclassmen with previous Information Assurance experience were recruited by professors to develop a series of educational lab assignments. These labs were developed using Problem Based Learning concepts encouraging student understanding and exploration as opposed to a more step-by-step and purely methodical approach. In conjunction these students were responsible for creating a network environment as a platform for these labs that would also be capable of supporting undergraduate research of Information Security issues. This paper will discuss the advantages of highly interactive lab assignments that engage students as opposed to rigidly structured labs with limited room for exploration. Further this paper will detail the evolution of an undergraduate teaching and research laboratory environment capable of simulating real world network architectures and supporting exercises that maximize understanding.

I. Introduction: Student Driven Initiatives in Information Assurance Education

In developing the information assurance program at Pennsylvania State University a major hurdle became the development of lab assignments to bolster the course work of the classes.

In the fall of 2004 a group of upper classmen who were familiar with issues in information assurance was recruited to develop a series of labs that would give students insights into the nature of today's relevant computer security threats. These students were each told to select an underground open source tool that was commonly used by malicious attackers and to develop a lab around it. The purpose of this was to give students taking the course a better insight into how to defend computer networks by understanding what it was that they would be defending against. The unintended result was that the students developing the labs bucked the standard technical format of the existing labs and developed a less rigidly structured far more dynamic and interactive design that included more information about how the tools worked and the ways in which they could be used.

This new more interactive format was largely embraced by students in the class as being more stimulating and educational. The purpose of this paper is to demonstrate the superiority of this less structured interactive lab design over the more rigid technical labs that are often used in Information Technology (IT) courses.

II. Class format

During the class lecture time, a period of time is given to in-class discussion. Students in the class engage in peer-learning while discussing problems posed at the end of each lecture. These in-class problems provide a way for the instructor and the students to actively engage in problem solving together, while also developing students' communication and presentation skills, forcing them to think while acquiring knowledge. During this time the students, working in small groups of four to five, develop and propose answers while the instructor acts as a guide, questioning them in-depth and helping each group to develop correct reasoning. Teacher must be effective facilitators using themes and concepts to introduce problem-solving and critical thinking skills to their students.[1]

The classroom dynamic was designed to give special attention to fostering interpersonal skills essential for students to perform in today's workplace. It was with the same ideas in mind that the educational lab assignments for the class were designed in a way to develop creative problem solving skills and foster more in-depth learning. The main purpose of the course content should be to foster a foundation which encourages continual learning.[2]

ISBN 1-933510-99-4/05/$15.00

A. Need for labs in education

Today it is well known that there is a major shortage of capable computer security professionals in the workforce. To effectively address this shortage requires Information Assurance (IA) education that provides more than descriptions of theory and security concepts. Consequently, "hands-on" lab activities are critical in an IA curriculum.[3]

While the school had been using technical lab exercises that it had received with equipment that had been donated by corporate sponsors, these technical labs lacked any real insight into the concepts behind them or the nature of the security threats they were teaching to defend against. The major problem with them was that the step-by-step format these labs followed lacked any real educational value aside from proving the student could follow specific instructions. The way these labs had been designed allowed students to carry out actions without really thinking about them. Simply having the experience of "going through the motions" does not constitute learning, but active problem solving does.

As we all know a computer program is just a tool and cannot think for the user. The key to accomplishing a goal or solving a problem with a program is to know how the tool works and how it can be used. Thusly, the dynamic labs were designed to develop creativity, critical thinking, and creative problem solving skills in the student. As stated by Colvin, "Often the course outline and learning model are dominated by concern for a common body of knowledge. The result: a design that ignores student interaction and the development of critical thinking and communication skills."[2] The TA's assistance on the dynamic labs is minimal, offering only general advice and direction while leaving the process of finding the resolution to the student. These types of lab assignments allowed students to work under the less structured circumstances that they will no doubt encounter after they graduate.

While it is well know that experience is a part of learning, having an experience does not necessarily mean the participant has learned anything. Kolb's experiential learning model defines learning as "The process whereby knowledge is created through the transformation of experience." Knowledge then, "results from the combination of grasping experience and transforming it."[4] This is why the dynamic, student developed labs are believed to be superior to the more technical structured labs, because they provided students with a deeper, richer experience. Experiential learning may be simply defined as active participation in the learning process, it involves students in an activity closely related to course material and forcing them to think about the experience. [5]

B. Sample Labs

Lab Group A (dynamic / interactive)
Lab1: Password Cracking
Lab2: Metasploit Framework

Lab Group B (structured / technical)
Lab3: PIX Firewall Configuration
Lab4: Syslog Output From Firewall

The lab assignments themselves were divided into two groups for the purpose of this informal study. Lab group "A" consisted of two of the more dynamic interactive labs, while lab group "B" consisted of two of the highly structured technical labs. Each lab followed a lecture on the relevant topics and course work. The lectures review the concepts and theories that are used in the technical labs the students will be performing. Prior to the lab assignment each student receives a printout of the lab exercise to be preformed by their group that week. The printouts for both types of labs contain the necessary steps to follow as well as follow-up questions to be completed and handed in by students. There are however, differences between the printouts of lab group A and lab group B. Lab group A's printouts included additional content besides the raw technical steps which a student needed to take to complete the assignment. This content included descriptions of the processes at work and details about other concepts behind each lab. The most important difference between lab groups A and B was that labs of group A could not be fully complete by simply following the steps on the printout. It was necessary to repeat several steps in different ways and view problems from multiple angles before a student could complete a group A lab. The result being that there was no one way for group A labs to be done. Post lab exercises that were to be completed and handed in later provided the students with an opportunity to reflect on their working experience and to look into each topic more deeply. The labs from group B however, could be easily completed on the first try by following each step exactly. While this did give students the experience of working with a piece of equipment like a firewall, it did not propagate true learning and students were found to be unlikely to be able to recall much of how to do the lab without the instructions.

ISBN 1-933510-99-4/05/$15.00

Several weeks into the semester students had completed a number of both groups of labs. A survey of the class was taken and students discussed their feelings on the lab assignments they had worked on. The students appear to identify more personally with the group A labs. They had a greater interest in their work and assumed more personal ownership of their experience and the methods they had used to complete the assignments. Students regarded the group B labs as generally less interesting and unimagined, groups were less inclined to work together and in the end there was very little each student could take away from the experience.

In the survey students were asked questions and answered by rating the labs on a scale of 1 to 5:
1 = Not at All
3 = Somewhat
5 = Very Much

Here we see the student's answers as a percentage of the class:

1) How educational/intellectually stimulating did you find Lab Group A to be?

1	*2*	*3*	*4*	*5*
0%	*0%*	*12.50%*	*37.50%*	*50.00%*

2) How educational/intellectually stimulating did you find Lab Group B to be?

1	*2*	*3*	*4*	*5*
12.50%	*12.50%*	*43.75%*	*18.75%*	*12.50%*

3) Did you find the knowledge and skills learned in Lab Group A to be practical or useful?

1	*2*	*3*	*4*	*5*
0%	*18.75%*	*6.25%*	*43.75%*	*31.25%*

4) Did you find the knowledge and skills learned in Lab Group B to be practical or useful?

1	*2*	*3*	*4*	*5*
12.50%	*12.50%*	*18.75%*	*50.00%*	*6.25%*

Students were also asked to talk about which lab assignments they preferred, or was the better learning experience and which lab they enjoyed least, or was the least valuable experience.

1. Students' answers on what they preferred.

"I preferred group A because you learned more from it, especially since the lab handouts contained more informative information on what was actually being done and why."

"These (A) labs even showed how the exploits work that we are defending against instead of keeping them as abstract ideas."

"Lab Group A because it was more than just typing in a bunch of commands that were given to us. We actually had to think a little bit about what we were doing."

"I preferred the Lab Group A because I felt the labs demonstrated something that I didn't know, versus the other lab that just took you through the motions of configuring and stuff- which is somewhat self explanatory."

"I preferred Group A because it was something that I haven't seen covered in any other class. I'd like to see more labs like these rather than simply following instructions to configure a firewall. I didn't feel like I learned very much with the firewall labs, since it was simply copying commands out of the lab description. I didn't get a good feel for what was going on. But for Group A, this was something new and it very effectively demonstrated how easy it is to breach security. I think that if the firewall had been paired with something like this, it would have been a more effective set of labs."

"Lab group A: because there was actually some thinking required, and everyone in the groups was more involved. Everyone from our group worked on helping to figure out Lab 1, which was a great way to start off the labs. It is also something most people don't get to have experience with at this point in their education… at least not legally. I pretty much knew how a firewall worked, at least in principal, although I'm sure I'll learn something along the way. But I never really had a good understanding on what it took to launch exploits or crack passwords, and both of the Lab Group A labs helped to expose me to a whole new tree of knowledge."

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

2. Students' answers on which labs they found least valuable.

"I looked forward to group B the most but I liked it the least. They were rather simple labs to complete, however, the hand outs were not very explanatory in providing information about what was being done and why."

"Lab group B because all we really did was type in commands given to us and other than reading the instructions we didn't get a chance to do much else with the lab programs."

"Lab group B, because it was not very stimulating or difficult. I was not overly challenging and did not require the students to really learn anything besides what commands to type."

"I disliked Group B because I feel that it was completely useless in adding educational value to the course. After completing the lab, I'm still not very familiar with the types of firewalls used or with the instructions on how to configure them. Instead of learning something, I pretty much watched one of my group members type commands into the command prompt from a piece of paper, and no one was really sure what those commands meant. There is no possible way that this lab will help me in the future. Instead, I might have liked to learn something about the firewalls we configured or maybe had to figure out the commands myself using a manual or something so that I would understand what I was doing and remember how I did it."

"I would say the PIX configuration it gave us no room to think, just to follow simple directions where no real information will be retained."

"B is definitely useful in the real world but all it is entering commands in a terminal…boring."

"Configuring a firewall isn't all that complicated or hard provided you read the manual. I think we should have more labs like group A. Focusing on how to break things provides better ideas about how to defend them. Students should be challenged to think more rather than just read out of the CISCO manuals."

"Lab Group B – mostly because both labs were just following along on paper without having to even think about the lab, nothing to figure out. Also, Lab 4 seemed incredibly short and simple. The TA wasn't there for it, but I doubt that would have changed anything. I feel like it was pretty much a waste of time… "Configuring output"? It seems like it could have just been tacked onto the last firewall lab, or the next one."

III. Designing a Network for Problem Based Learning.

While lab design is certainly the most vital part of the creation of hands-on exercises for teaching information assurance, the question quickly turns to where to implement these labs. The answer is nearly universal: a dedicated Information Security Lab. This provides a safe and controlled environment where students can experiment with tools that may cause harm in the real world.

In designing this lab a wide variety of criteria must be met to satisfy many different parties. First and foremost the lab must facilitate students' ability to perform the required labs, but that is simply a start. To most effectively do this job an information security teaching network must be able to simulate a production environment, or ideally be able to simulate multiple production environments. It must also provide structure to students while allowing them to explore and experiment with tools they are using. In accordance with the methods of the School of Information Science and Technology, problem based learning encourages students to not simply understand what a piece of technology does, but how and why it does it. Students need the opportunity to explore, hypothesize, and test their hypothesis.

A. Organizational Needs.

1. Professors

Professors' needs must also be met. Of the many, reusability and flexibility are most note worthy. As indicated from student feedback, labs are one of the best methods of teaching students so that they don't just know concepts, but understand and can make use of technologies in practical situations. In developing Information Security programs lab resources are limited; therefore it must be easy for a professor or TA to construct a lab that can be used by multiple teams back to back with limited reset effort and time. Efforts should be made to create the ability to build once, run as needed. Labs also need to provide professors the ability to make labs covering a wide range of topics. With security threats expanding daily the scope of Information Security continues to grow.

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

What was once simply about keeping out hackers has moved to cover diverse areas ranging from virus protection and firewalls to spam reductions and spyware. Professors, to effectively teach the many aspects facing IA professionals now and in the future, need to be able to give labs covering all those subjects and thus need an environment to support that.

2. The School

The needs of the school administration must also be met. In many cases teaching information assurance is a double edged sword, and skills that are necessary for protecting information and defending networks can often be used to steal and attack. Safeguards must be put in place to protect the school networks and computer resources from accidental and involuntary damage, as well as from malicious attacks. While this can only be handled to a certain degree by the lab staff those small contributions none the less play a vital part in keeping the campus safe and the lab in operation. [6]

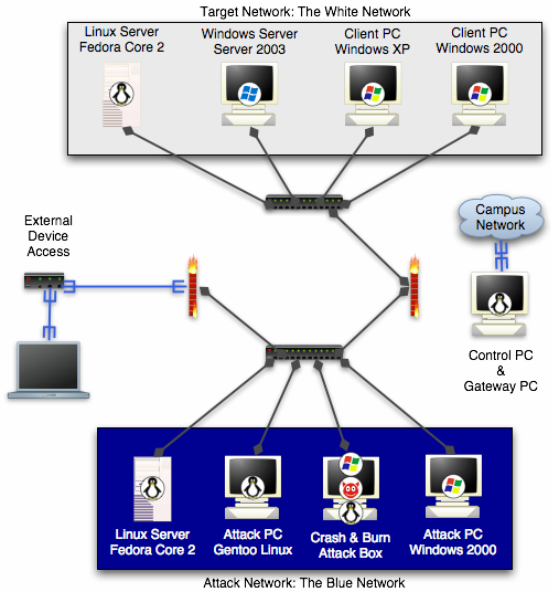

Fig 1. Current Lab Design

IV. Evolution of the Dynamic Learning Network

Our past lab environment met our criteria with little room to spare. All lab objectives could be complete after closely tailoring the labs to the environment, but left little room for exploring or side experiments. Flexibility was limited due to requirements of other labs and extremely limited equipment. Our lab currently consists of only 8 boxes. Two are dedicated target boxes running Windows 2000 server, two administrative boxes also running Windows 2000. Two are attack boxes running Windows XP, and two are development boxes running Fedora Core 3. Boxes are connected by switches as necessary for each lab. Currently we are only equipped to run three different lab scenarios, password cracking, remote buffer overflow, and Cisco labs that utilize one of the administrative boxes as a console for Cisco firewalls, routers, and an intrusion detection system. Because we want directed labs, nearly every box is setup for one specific purpose, making the system functional, but not meeting our conditions of being flexible. Teacher assistants are also required to reset lab experiments between every group, cycling servers, restarting services, re-prepping attack tools. Students wanting to do research also ran into issues with no machines to be dedicated specifically for research applications. Lab students were using machines setup for running specific tools and settings were changed, logs were deleted and other issues forcing researchers to go back and begin again.

A. Obstacles and Inspirations

After examining the situation it was determined that our biggest problem centered on our lack of hardware to allow specialized situations for labs and research. In searching for solutions we came across the United States Military Academy's iWar Range[3], while interesting reading it did not provide an adequate solution as we could not dedicate nearly the amount of hardware, nor space, to create our lab. We had to find a way to make use of the eight machines available, yet have as much flexibility as possible. While the iWar architecture was too much for us the USMA's EVIAN architecture was nearly ideal.[6] By modifying this design to match our criteria we developed the Virtual Cyber Defense Laboratory Architecture (VCDLA). Through the use of the VMWare virtual machine environment we can multiply each machine using virtual hosts, taking us from a network of six machines to a network of 36 concurrently running machines, with virtually limitless combinations restrained only by size. Students are able to run individual networks on single machines, or combine machines to create labs of larger sizes. This gives us the flexibility we need to cover the range of possible scenarios. In addition the use of images allows for repeatability, simply restarting an image back to a static build, saving considerable difficulty for Teacher Assistants during lab periods. Below is an example of how VMWare images could be used to with our past semesters lab assignments.

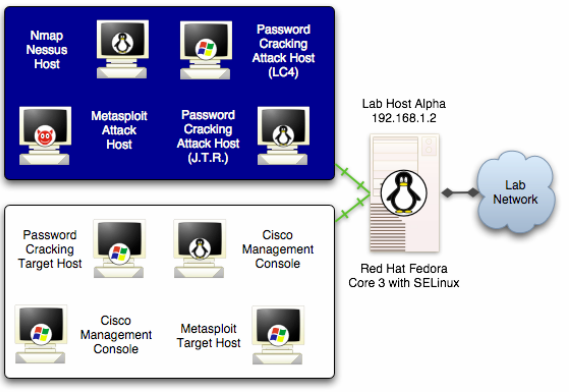

Fig 2. New Lab host configured for use in the new Cyber Defense Lab

In this lab design it is easy for the TA to preload the specially prepared for each lab. This creates an environment where the students have full access to the tool, and even control the root account on the box, but in a limited, protected manner. Each lab can be finished using the resources from only one machine, instead of requiring multiple. At the conclusion of the lab a TA needs only a few clicks to set the lab back to the original position, just in time for the next group.

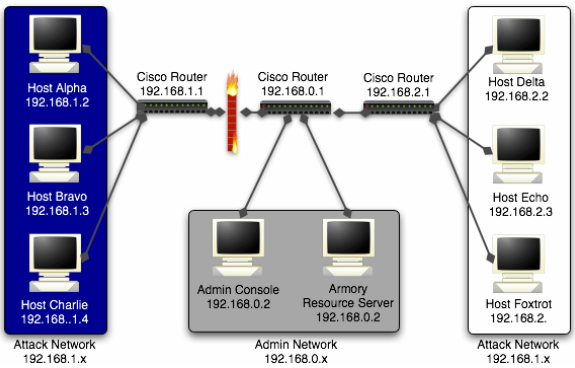

Fig 3. Full Lab Configuration for Virtual Cyber Defense Laboratory

V. Birth of a Dynamic Cyber Defense Network

When combined together the VCDL Architecture gives the flexibility of larger networks with a greater number of boxes. This architecture allows many combinations, simulating multiple networks, giving opportunities for more complicated advanced exercises involving multiple hosts and more realistic environments such as students might run into in industry. From a technical perspective each set of virtual machines runs using VMWare on top of Redhat Fedora Core 3 with the tightened SELinux Kernel. All services are disabled and students log in using restricted user accounts. Root accounts are kept strictly guarded and students are not allowed to log into their hardware as root.

Images are handled very differently. For lab environments all images are "read only" and students are given full root access, allowing them to do anything they want within the images, but causing the to return to their original state when the virtual machine is shut down. This gives students full access to new and different operating systems, to explore, yet without any consequences for mistakes that may be made. As additional protection the Cyber Defense Lab is isolated from the campus network, so that even a poorly guided attack will not disrupt the school network. Research images will be similar, allowing things like saving so that progress isn't lost on shutdown.

In addition to the Lab Hosts (Named Alpha to Foxtrot) there are two additional hosts, Admin and Armory. On their own protected subnet these machines serve the general lab. Admin is responsible for control of the three Cisco routers and the Cisco firewall. This machine is locked down in case of accidental attack but is not a valid target machine and should only be used by lab personnel, teacher assistants, or professors themselves to setup scenarios, such as creating a corporate network environment or separating teams for capture the flag exercises. Armory is a storage server primarily meant to hold tools teams might use in scenarios where adaptation and creativity is expected in solutions. Armory can also be used to allow teams places to store documents or tools, and in future versions of the VCDL Armory will also house a VMWare GSX server, a central repository and control for all virtual machines, allowing further automation of lab operations.

VI. Conclusion

Student's comments repeatedly applauded the innovative design of the lab assignments and flexibility they had in finding the right solutions. The results demonstrate that university learning can often be significantly enriched when it is less structured more student driven.

The use of Lab assignments with broader goals or less specific methods allow students to take a more personal ownership of the activities in the lab and of their learning. Lab exercises designed to help students become more active learners and assume an

amount of control of learning activities; enhance learner confidence and motivation; improve group inquiry and problem-solving skills; and develop practical thinking.[7]

Classrooms that are no longer boring or mundane but active through electronic resources have become the centerpiece for the education restructuring movement. As we advance our system to meet the demands of generating a well-educated, technically skilled, and flexible individual able to compete in a global economy. [5]

A major problem that still exists in Information Assurance (IA) education and IT education in general is that dynamic and interactive lab assignments are the exception and not the norm. Schools, intent on measuring, testing, and assigning grades, are typically engaged in shallow-level learning, like note memorization and recall activities. But, such reproductive, surface-level learning severely limits persons in problem-solving and application-demanding settings. People themselves often choose to either reproduce a task shallowly or penetrate deeper into subject mastery. Unfortunately most school systems reward the former.[7] With the constantly changing environment of the IT world, there is a need to rethink how to teach at all levels. The traditional approach to teaching at the university level has been through the use of text, lecture and structured assignments. This approach lacks certain elements of the real world and so students are not fully prepared for the workforce. [8]

References

[1] O'Niel, Patrick. "Student/Teacher Satisfaction with Interactive Instructional Technologies." American Vocational Association Convention, December 1995

[2] Colvin, Scott. "Participative Learning Experiences in the Professional Studies Classroom." National Conference on Successful College Teaching, February 26th, 1994

[3] Crowley, Ed. "Experiential Learning and Security Lab Design." SIGITE'04, October 28th: pg169 – 176

[4] MR Garvin, RD Ramsier. "Experiential learning at the University Level." Education & Training. London: 2003. Vol.45, Iss.4/5; pg. 280

[5] O'Hara, Margaret, Stephens, Charlotte. "Experiential Learning in the MIS Class." International Academy for Information Management Annual Conference, December 6th, 2000

[6] L. J. Hoffman, R. Dodge, T Rosenberg and D. J. Ragsdale "Information Assurance Laboratory Innovations," 7th Colloquium for Information Systems Security Education Washington, DC, June 2-6, 2003.

[7] Eastmond, Daniel. "Learning Approaches of Adult Students." National Education Research Association Conference, October 28th 1992

[8] Kolb, D. "Experiential Learning", Prentice Hall, Englewood Cliffs, NJ, 1984.

[9] D. Ragsdale, R. Dodge, and S. Lathrop, "The Educational Virtual Information Assurance Network (EVIAN) ," Proceedings of the 4th Annual IEEE Information Assurance Workshop, West Point, NY, June 17-19, 2003.