Hands-On Discovery Learning in Computer Security and Forensics

David A. Dampier[1], Rayford B. Vaughn[2]

[1,2]Department of Computer Science And Engineering, Mississippi State University, USA

dampier@cse.msstate.edu[1], vaughn@cse.msstate.edu[2]

Abstract

At Mississippi State University, we have taken the teaching of computer security and forensics seriously. These topics are best learned through experience and hands-on instruction. The computer security and computer forensics courses have developed an extensive set of hands-on experiences that enable students to discover the fields through first-hand experience in addition to lectures, and not just through lectures alone. This paper describes these discovery learning techniques and the success that has been experienced as a result.

1. Introduction

Computer security instruction began to take root in the United States during the late 1990°¶s with the recognition by the Department of Defense and the Federal government that these programs were necessary. An increase in funding provided by the federal government fueled this growth.. This funding came as support for both research and instruction, and the intention was to support the development of computer security professionals that would come to work for the federal government and relieve a growing shortage. This was done primarily through the support of infrastructure growth in the universities that showed the most potential to provide these students as well as the direct funding of scholarships to produce the graduates with specific skills that would support the varied needs of the federal government.

The Department of Defense developed a program to recognize these universities with both existing capability of a computer security research and education program and those with potential for having the capability. This program was called the Centers of Academic Excellence program, and it was originally only for Information Assurance Education, but in 2008, it was expanded to include centers with a capacity for Information Assurance Research. Mississippi State University was designated a Center of Academic Excellence in Information Assurance Education in 2001, and a Center of Academic Excellence in Information Assurance Research in 2008. Since the primary purpose of information assurance education at the undergraduate and graduate levels is to prepare students for careers in IA, Mississippi State University decided that it wanted to produce graduates that actually know how to do information assurance. The discovery learning approach is one way to do this, and it can be a very effective way. Mississippi State University has a tradition of using innovative hands-on instruction. [3,4,5,6] This paper describes how the authors at Mississippi State University have introduced Discovery Learning into their computer security and computer forensics classes.

Discovery learning is a teaching method that has been promoted in educational literature since the early 1960°¶s. It puts students in problem solving situations where they must use their experience and knowledge in their environment by exploring and manipulating objects, wrestling with questions and controversies, or performing experiments [8]. Bruner [1] suggests that students retain more of what they discover on their own.

2. Courses and Content

Mississippi State University has maintained an information assurance course focus since 1998, at the BS, MS, and PhD levels. More than 700 students have completed coursework at the undergraduate level and more than 200 at the graduate level. We have produced ten IA PhD's and have twelve PhD candidates actively engaged in research efforts. To facilitate discovery learning in our students and to motivate research, we constructed four laboratories for student use. Lastly, to motivate discovery learning, we developed several individual and team exercises that we require of our students (information assurance labs, capture the flag competition, digital forensics search and seizure in a mock vil-

lage, and a real courtroom experience for teaching expert witness skills). Our curriculum weaves IA topics throughout our ABET accredited computer science and software engineering degree programs to provide students with the necessary framework on which they can build when they take more advanced upper level IA specific courses. At the senior level (for undergraduates) or at the beginning level for graduate students, we offer three specific classes which are very focused on IA topics. The IA focus courses offered are:

- **CSE 4243/6243 Information and Computer Security:** This course is an introductory course to Information Assurance and is mapped to CNSS 4011. It covers the principles of IA, government processes, the DIACAP, Common Criteria, network security, data base security, operating systems security, and more. There is a lab requirement associated with this class.
- **CSE 4273/6273 Introduction to Computer Forensics:** This course explores computer crime and the study of evidence for solving such crimes. MOST importantly, we allow students from three colleges to take this class (students from Engineering, Arts and Sciences, and Business). We attract students from all three colleges to this popular class and we involve faculty from our Criminal Justice program (Dept of Sociology) in some of the lectures. There is a lab requirement with this course.
- **CSE 4383/6383 Cryptography and Network Security:** This class covers the workings of off-the-shelf cryptography, cryptosystems, algorithms, PKI, symmetric/asymmetric systems, and key management. It also covers network defense and network attack. A strong emphasis in placed on network protocol vulnerabilities. The course is open to all computer science and engineering students.
- **BIS 4113/6113: Business Information Systems Security Management:** This course is offered in the College of Business and open to Business students as well as Engineering students. Concepts, skills, tools and techniques involved in management of computer security as it applies to today's business environment are taught. This class has a security lab associated with it. The discovery learning aspects of our program are described in the paragraphs that follow. The reader should keep in mind that each of the discovery experiences comes only after (or in conjunction with) lectures by the instructor. The end result we are after is to provide the student with enough motivation and conceptual knowledge that they can then combine with their natural curiosity, and move to a higher level of learning.

2.1. Information and Computer Security

In the Information and Computer Security class, in addition to a full suite of weekly lab exercises that students have to complete in the lab, a full week is devoted to a Capture the Flag contest with the vast majority of the activity conducted voluntarily and outside normal class periods. Students are formed into 4 to 5 person teams with one student per team designated as a team leader. Prior to the exercise, they are taught a framework used for attacking a system (reconnaissance, footprinting, enumeration, probing, and penetration); given lectures on specific tools useful for penetration testing; and, given experience in using tools in the laboratory. They are given the general network architecture that they will be penetrating and specific information on the tokens they will be looking for. The exercise is started one week prior to the actual live fire penetration so that the teams can organize, plan, and practice together. They are also allowed to use any form of social engineering that they can come up with to gain any advantage. No restrictions are placed on the students in this regard. Teams are awarded points for retrieving tokens during the full period of the exercise °V plus they are awarded some initial points based on a grading of their written plan of attack.
The most interesting side effect of this exercise is the intensity seen in the students during the exercise. They prepare hard for this exercise and, judging from the comments we receive on end of course evaluations, they find it instructive and fun. In preparation for the exercise, students are given brief instruction on a number of tools. We intentionally make the instruction brief so that students will necessarily need to work hard on their own to master the tools. With the motivation already established to win the contest °V students tend to not only master the tools we teach, but also discover others on their own that they later share. Specifically we provide instruction on the following [2]:

- **Reconnaissance tools:** We present a number of tools here that can help the student discover information about a targeted system. By exposing the student to these tools, the student can better understand how to defend against them. Tools included are p0f for OS fingerprinting; Network Stumbler for discovering wireless network characteristics; Google for search directives and cache information; and Netcraft for webserver information.

- **Enumeration tools:** Enumeration helps the attacker know more specifics about the operating environment to be exploited. For this lecture, two important tools are covered - NMAP and Nikto. NMAP provides a host of services to include OS fingerprinting, port scans, and other services. Nikto is a web scanner and assists an attacker in finding vulnerable web services.
- **Exploitation tools:** To actually exploit a system, tool support is very useful. Students are introduced to the Metasploit framework, one of the most powerful penetration tools available (essentially a point and click penetration tool); TCPreplay to replay packets on the network; hping2 to craft packets and OS fingerprinting; NetDude for packet crafting; and Cain and Able for wireless sniffing, VoIP recording, and password recovery.
- **Analysis tools:** As a security engineer, the ability to analyze network activity and diagnose problems is essential. Students are shown Microsoft Sysinternal tools [9]; ntop for analysis of network IP traffic; and VisualRoute to visualize network path data.
- **Hardening tools:** There are many automated tools available to lock down systems and make them more resistant to attack. Our students are shown a sampling of these to include Bastille as a tool to harden Linux, HP-UX, Mac OS X and other OS; IPtables as a host based static firewall; and Truecrypt as a freeware product to encrypt laptops.

2.2. Introduction to Computer Forensics

In the Introduction to Computer Forensics course, we offer a semester long set of discovery learning exercises. During the semester, students are exposed to an active computer forensics laboratory in every lecture, and each lecture involves hands-on exercises in computer media acquisition, authentication, and analysis. Also, an out-of-class exercise involves the class members being formed into teams and working on a semester long investigation and analysis project. In this project, students are formed into teams and each team is given a crime with a victim and a primary suspect. The first phase of the project lasts approximately five weeks and in this phase, the teams create a body of evidence, both physical and digital representing evidence that would be collected in a real investigation. This phase culminates with a trip to a mock city at a nearby law enforcement training facility where the evidence is planted in a mock crime scene..In an effort to instill good forensically sound search and seizure practices as well as sound investigative practices, the students are then required to plan a raid and take down a crime scene, collecting evidence prepared by another team. Students are then taken on a weekend to the mock village used by a Counter-drug training academy facility about 90 miles from the University. Volunteer police are used to assist in the exercise along with teaching assistants from the University. Students spend the day raiding the crime scene and arresting criminals (University staff members), seizing evidence, recording/logging evidence, imaging hard drives, and preserving evidence for courtroom presentation. As a result of the professional preparation and the seriousness presented by the instructors, the students take the exercise quite seriously.

The seizure of evidence at the mock crime scene then kicks off the second phase of the semester long project, where student teams analyze evidence seized and prepare a case against the primary suspect. Tools and techniques taught in class as well as tools discovered by student teams on their own time are used to produce a detailed analysis and report of facts that is to be used at trial. The culmination of the second phase is the submission of a complete forensically sound report of the evidence to the prosecution team.

The third phase of the exercise comes in a mock courtroom experience. The students are given approximately ten days to prepare themselves to testify in court before real defense and prosecuting attorneys, as well as a real judge. They are given limited instruction in the classroom on courtroom procedure and an actual digital crime investigator is brought in to talk to the students and answer questions on courtroom experience. The key here is that the students must lead the discussion to obtain the information they need to prepare themselves °V it is not lectured to them. In preparation for the moot court experience, we partner with the law school at the University of Mississippi and they provide defense and prosecution attorney°¶s to argue the digital crime cases that the students prepared. We work with the local government officials and reserve the county courtroom for our use. A retired judge is obtained to sit on the bench and hear the cases. A jury is obtained by using the digital forensics class from Jackson State University. Staff members °ßarrested°® during the mock village exercise are used as defendants and have a defense attorney to argue their innocence. The students °ßcorrect°® testimony and legal evidence admission is paramount to obtaining a guilty verdict and for the eventual satisfaction of having accomplished a successful prosecution. During this exercise stu-

dents learn the difficulty of communicating technical information in a non-technical environment and they are taught the value of and need for strong communication skills in additional to technical expertise. Additionally, students are taught the value of ethical behavior throughout the semester, and especially in the court room, as they are challenged to provide truthful testimony under stress.

3. Conclusions

The purpose of this paper has been to demonstrate that students, when given the proper motivations and facilities to work with will, in many cases, learn more by doing than by listening and will actually contribute to the learning experience for the instructor and other students. Students tend to be more energetic toward learning, thrive on the challenge of discovery, and appear to respond to motivations provided by active participation in the learning process.
The authors do not claim that this method is °ßbetter°® or more effective than others that are being used. It is reported as empirical evidence of an approach that works and produces results. It appears to the authors that a discovery learning approach is one that works and excites the students to learn and to contribute. We find that students exposed to this approach value the learning experience and report such on their end of the semester evaluations. The authors are prepared to share any of the material discussed in this paper to include specifics on lab exercises.

References

01. Bruner, J. S. (1961). “The act of discovery”. Harvard Educational Review 31 (1): 21°V32.
02. Bonwell, C. & Eison, J. (1991). Active Learning: Creating Excitement in the Classroom AEHE-ERIC Higher Education Report No.1. Washington, D.C.: Jossey-Bass. ISBN 1-87838-00-87.
03. Dampier, D., “Integrating Practical Problem-Solving into Software Engineering Education,” Proceedings of the UM-Dearborn Conference on Integrating Practice into Engineering Education, Dearborn, MI, October 3-5, 2004.
04. Dampier, D., “Building an Education Program for Engineers in Digital Forensics,” Proceedings of the 2008 ASEE Conference, Pittsburgh, PA, June 22-25, 2008.
05. Dampier, D. and J. Cohoon, “Educating Tomorrow’s Digital Forensics Examiners”, Innovations 2008, INEER, July 2008, pp. 273-282.
06. Vaughn, R., D. Dampier, and M. Warkentin, “Building an Information Security Education Program,” Proceedings of The 2004 Information Security Curriculum Development Conference, Kennesaw, Georgia, September 17- 18, 2004.
07. Vaughn, R. and D. Dampier, “A Hands-On Approach to Computer Security Instruction,” Proceedings of the 2008 ASEE-SE Conference, Memphis, TN, April 6-8, 2008.
08. Vaughn, R. and D. Dampier, “A Discovery Learning Approach to Information Assurance Education”, Proceedings of the 2009 Hawaii International Conference on the System Sciences, Minitrack on Digital Forensics, Waikoloa, Hawaii, January 5-9, 2009.
09. See http://www.microsoft.com/technet/sysinternals/, May 7, 2009.