Preparing Our Undergraduates to Enter a Cyber World

Dino Schweitzer, David Gibson, David Bibighaus, Jeff Boleng

Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

Preparing our Undergraduates to Enter a Cyber World

Dino Schweitzer[1], David Gibson[1], David Bibighaus[1], Jeff Boleng[1]

[1]Department of Computer Science, United States Air Force Academy, Colorado, 80840, United States

Abstract. Today's students have grown up with computer-based technology and need to be prepared to enter a career in a digital world. This includes an understanding of the broader implications of technology such as the growing threat of cyber-crime and cyber-terrorism, cyber-ethics, the legal and social implications of technology, and the local and global impacts. At our institution, we have taken a broad look at ways of integrating cyber awareness and education across the curriculum to reach all levels of students, irrespective of their major. We have identified core cyber issues that are taught to all freshmen, developed awareness training that is regularly completed, provided opportunities for interested students to gain more cyber knowledge through a student club and summer program, and developed an in-depth educational program for technical students to graduate with an emphasis in cyber-warfare. This paper will describe our various cyber programs and future plans.

Keywords: cyber-education, cyber-training

1 Introduction

A key priority in the National Strategy to Secure Cyberspace is to increase security training and awareness through enhanced education programs [1]. As a result of this emphasis on security education, more courses and programs are being offered at the undergraduate level in security-related topics such as cryptography, information security, network security, and information warfare. These courses have benefited from an increasing number of textbooks, curriculum development, and student competitions such as the Collegiate Cyber Defense Competition [2].

While much of the focus of cyber education has been on the creation of a professional cyber workforce, at the United States Air Force Academy (USAFA), we feel it is critical for all students to have awareness of the issues and threats associated with cyberspace. In addition, students who have a strong interest in cyber topics, but are not technical majors, should have the opportunity to explore cyber-related areas in greater detail without taking highly technical computer science or engineering courses. Finally, our students who will be starting their careers as cyber professionals need to be able to explore, in depth, both the conceptual aspects of cyberspace as well as receiving hands-on experience in the tools and techniques of the field. This paper will examine these three levels of cyber education and training as implemented at USAFA.

2 Cyber for All

While many recognize the importance of developing the cyber skills of all students, finding a place in the curriculum for cyber education and training can be a challenge. At USAFA, all students receive cyber education in the core curriculum and cyber training in their *First Year Experience* course.

A large core curriculum at our school provides an ideal opportunity for cyber education in the *Introduction to Computing* (CS110) course offered by the Computer Science department and taken by all students as freshman. CS110 consists of 40 lessons covering information representation (5 lessons), algorithmic reasoning (13 lessons), computer system capabilities (7 lessons), computer ethics (1 lesson), software applications (7 lessons), cyber security and warfare (5 lessons), plus a midterm exam and course review (2 lessons). While cyber security topics naturally arise in discussions throughout the course, the 5-lesson cyber security and warfare block is dedicated to cyber education.

CS110's five cyber block topics are: information security, cryptography, cyber warfare and crime, offensive cyber operations, and defensive cyber operations. In addition to introducing the growing importance of cyber security and the prospect of cyber warfare, the information security lesson focuses on the principles of confidentiality, data integrity, availability, and authenticity. The cryptography lesson introduces students to basic symmetric encryption techniques as well as asymmetric public key encryption and digital signatures. CS110's cyber warfare and crime lesson provides students with a political, economic, and military context for cyber warfare and cyber crime before discussing current threats, vulnerabilities, and common cyber attack vectors. The offensive cyber operations lesson explains to students how individuals and organizations conduct cyber attacks with a focus on password attacks and attacks using social engineering. Students do not learn about specific cyber attack tools and techniques in CS110. Finally, the defensive cyber operations lesson focuses on strategies for defending against the attacks described in the previous lesson with a focus on how students can protect themselves and their own computers.

All of our students also learn about cyber topics in several other required core courses. For example, in *Principles of Air Force Electronic Systems* offered by the Electrical and Computer Engineering department, all students learn about circuit and packet switching networks and their respective vulnerabilities to cyber attacks. In *Military Theory and Strategy*, offered by the Military Strategic Studies department, students learn about military cyber capabilities and strategies. In *General Physics II*, students learn about the electromagnetic spectrum which underlies all cyber technologies.

Few colleges and universities have a large core curriculum like USAFA's. Nevertheless, opportunities exist at many schools for introducing cyber topics to a broad group of students in general education elective courses. One target of opportunity may be the first year experience course required for all freshmen at many schools. At USAFA, one of the first lessons of the *First Year Experience* class teaches cadets how to access and use the institution's computer network safely and securely.

3 Cyber Training

In addition to the exposure to cyber topics provided all students in the core curriculum, our department has created opportunities for greater hands-on cyber training to interested students outside of the classroom. We accomplish this through two primary mechanisms: a summer cyber training program and an active Cyber Warfare Club.

3.1 Basic Cyber Training

This summer, we will offer our newest training course in Cyber Warfare – Basic Cyber (Cyber 256) which was first prototyped in the summer of 2009. The course is a ten-day introduction to cyber operations and is open to all sophomores. The goal of the class is to "explore … cyber … with hands-on training designed to teach the fundamentals of establishing, operating, attacking, defending, and exploiting computers and networks." The course was modeled on our USAFA's basic sailplane course. There are three distinctive aspects of the basic sailplane course that we are incorporating into the Cyber 256:

- Light on Theory – heavy skills training. In soaring, students receive very little classroom learning (just enough to keep them safe) and spend most of their time in the cockpit. The goal is to provide enough real-world exposure early in their experience with the subject to allow students to intelligently decide if they are motivated to delve deeper into the subject (which will naturally require a more in-depth classroom experience). Likewise, our cyber class is designed to give them enough hands-on training with real world tools in a carefully controlled environment to allow them to decide if they want to pursue the discipline at a deeper level.
- Student Led – One of the amazing things at our institution is to watch the hundreds of glider flights that occur safely every week and realize that they are being taught by undergraduate instructors. This has two benefits: for the student, it makes the skills seem not so far "out of reach" and removes some of the mental limitations that students often place on themselves. For the student instructor, it not only builds a deeper level of competency in the subject area, but also develops the ability to lead and communicate effectively about their discipline. Since cyber warfare is often perceived as a dark art, having students lead the training is important to make the topics appear more accessible to the students. In addition, the nation needs young men and women who can effectively communicate and lead in cyber matters.
- Task Oriented – The soaring program is centered on students being able to perform a series of tasks needed to safely and effectively fly an aircraft. For the Cyber course, students will be presented with a series of scenarios that require them to perform specific tasks and will be evaluated on whether or not the student performed them satisfactorily.

The Cyber 256 class will expose students to cyber-warfare primarily from an attacker's point of view. Students will begin by exploring some of the basics of establishing a network and then quickly proceed to use some of the more commonly used network security tools. The idea is not to provide in-depth training on these tools, but rather provide enough exposure for the students to understand the basic process and appreciate some of the avenues of attack. In addition, the course is designed to be cross-disciplinary. Special emphasis is placed on the larger context of cyber warfare including social engineering, the legal aspects of cyber warfare, current threats, and how the Air Force is organizing itself to address them. Table 1 shows a list of the topics taught during the Basic Cyber Warfare course.

Table 1. Topics in Cyber 256.

	Morning Topic	**Afternoon Topic**
Day 1: Establish	Basic Network Training	Advanced Networks
Day 2: Cyber Intel	Network Mapping	Denial of Service
Day 3: Penetrate	Computer Penetration	Web Vulnerabilities
Day 4: Operations	Air Force Cyber Mission	Cyber Threat
Day 5: Social Aspect	Social Engineering	Law
Day 6: Wireless	Wireless Vulnerabilities	Password Cracking
Day 7: No Training		
Day 8: Forensics	Forensic Tools	Hard Drive Analysis
Day 9: Advanced Threats	Root Kits	Intrusion Detection
Day 10: Capstone	Capstone Part I	Capstone Part II

The Cyber 256 course has some similarities to the Advanced Couse in Engineering Cyber Security Boot Camp (ACE) course that was developed by the Air Force Research Laboratory and administered to Air Force ROTC students [4]. Our course has several important differences. First the course is offered to all rising sophomores. This is one year earlier than the ROTC program and therefore cannot be limited to students of a particular major. In addition, it is a ten-day course as opposed to the current ten weeks for ACE. Because of the compressed timeline and less-restrictive pre-requisites, the course is, by design, much more training-focused as opposed to education-focused.

3.2 Cyber Warfare Club

The Cyber Warfare Club at USAFA was created as a multidisciplinary club with members from all academic majors. It is similar to the club described at the United States Military Academy [5]. Among the current 100+ club members, there is a diversity of academic majors, to include aerospace engineering, biology, chemistry, computer science, economics, electrical engineering, English, military strategic studies, physics, political science, space operations, and systems engineering. One of the goals of the club is to make it inclusive and attract a diversity of students. This decision was based on the realization of the importance of cyber education to all of our graduates.

In September of 2008, we began to survey the interest of students at our institution in cyber warfare by demonstrating some simple Backtrack tools at semi-annual majors nights where we typically recruit young students into the computer science major. The response was overwhelming. Several planning meetings were held with many of the interested students leading to a vote for student leadership in January of 2009. The club was officially recognized by the institution club regulatory body at the end of March the same year. In the short history of the club, we have had many successful training opportunities, invited talks, and members have participated in several competitions learning a great deal along the way.

We have had to carefully design club activities to ensure opportunities for all members because of the diverse nature of our membership. One way in which we have done this is through talks given by experts from the field. One of our first talks was given by the Director of Communications and Information at our institution and detailed a plan for the future network architecture. Since that first talk we have had others including a presentation on current trends in cyber warfare by the Research Director at Gartner, threats and case studies by the NSA Information Assurance Directorate Technical Director, and Public Key Infrastructure by the Air Force PKI Team. Recent talks include a discussion of Microsoft's work to mitigate threats by a senior Microsoft Security specialist and a discussion of the policy, law, and ethics of cyber attack by the Chief Scientist of the Computer Science and Telecommunications Board, National Academy of Sciences. By providing a mixture of technical and policy discussions we have been able to entice a mixture of all of club members to attend and participate.

Hands-on training in network attack and defense is another major goal of the Cyber Warfare Club. Development of the appropriate level of hands-on labs has been challenging. One of the approaches we have used is to introduce security concepts through web-based simulations of cyber threats such as buffer overflow and SQL injection which do not require a highly technical background to understand [6]. We identified the following topics as a starting point for hands-on lab development:

- vulnerability analysis and penetration testing,
- the hacker methodology,
- incident response,
- forensics,
- reverse engineering,
- networking fundamentals, and

- service fundamentals

A key concept in our hands-on labs is the idea of a "check ride". In aviation, a check ride is where a student takes control of a plane (under the close supervision of a qualified pilot) and demonstrates techniques and is either verified as being qualified or needing additional training. We utilize our senior club members to provide cyber check rides to the more junior students. We are pursuing the development of multiple training modules in parallel. Additionally, there are several opportunities to leverage work being done in various cyber organizations to provide additional training to club members. Several organizations have expressed an interest in collecting club materials and training modules developed at our institution.

Besides the training opportunities, we have used the club as an opportunity to select students for additional training provided commercially. Over spring break in 2009 and 2010, we sent ten students to Certified Ethical Hacker training. This course was well received by the students.

In its short history, students from our Cyber Warfare Club have participated in multiple cyber competitions. Two of these competitions had the students on blue teams protecting systems and services while another allowed them experience on a red team in a capture the flag event. We recently competed in the 2010 International Capture The Flag (ICTF) competition and had a respectable placing in the top 20 of all teams worldwide [7]. These competitions serve as capstone events and tie all of the education and hands-on training together to provide students an opportunity to integrate all their skills and get a feel for the bigger picture.

4 Cyber in Depth

Along with the cyber education given to all students, and the cyber training providing additional experience to interested students, we offer students the opportunity to explore cyber topics in much greater depth through the cyber warfare track of our computer science major, through the cyber instructor course, and through cyber research opportunities.

4.1 Cyber Warfare Track

Our Computer Science major has been recognized by NSA and DHS as a Center of Academic Excellence (CAE) in Information Assurance Education. We have integrated computer security principles in several of our major courses where appropriate. In addition, all CS majors are required to take the Information Warfare course which is a concepts course in cyber security.

For students that want to focus on cyber warfare, we offer two additional courses, a cryptography course and a network defense course. Students that complete both of these as optional courses in the major receive a designation on their diploma as having completed the cyber warfare track of the Computer Science major.

4.2 Cyber Instructor Course

As stated earlier, undergraduate students are the primary instructors of the Cyber 256 class. Each 10-day offering will have fifteen students and three undergraduate instructors. These student instructors have been hand-picked by the faculty because of their leadership potential and demonstrated proficiency in the cyber warfare club. As previously described, this instructor model draws heavily from the sailplane instructor paradigm. For each skill, student instructors will demonstrate a skill, allow students to practice the skill with instructor help and finally have the student perform the skill for evaluation. If the sailplane program is any indication, the biggest challenge for these instructors will be to restrain themselves from correcting student mistakes too quickly.

The Cyber Instructor Course fulfills a very important and often underappreciated need within the cyber warfare discipline, namely to develop cyber leaders. Too often cyber warfare courses emphasize the technical nature of the discipline. Yet what is in demand are people who not only understand the technical challenges cyber warfare presents, but can communicate those challenges to non-technical people. Student instructors will be required to train their non-technical peers to use sophisticated cyber security tools to perform basic tasks. In the process, they will develop both their technical and leadership skills. In fact, USAFA is allowing these cyber instructors to teach the cyber warfare class in-lieu of other leadership requirements.

4.3 Cyber Research

Although we are an undergraduate-only institution, we believe that research is an integral part of the undergraduate experience. Students have the opportunity to explore a cyber-research topic in-depth through an independent study course which matches the student with a faculty mentor conducting research on a specific project. In addition, our institution offers a 5-week summer research program made available to the top students in each major. Between their junior and senior years, students in this program attend institutions such as NSA, NRO, MITRE, Intel, and research organizations to work on a real-world research problem. The program is highly rated by students and gives them an excellent exposure to the cyber world outside of academia.

We believe that research should not be relegated to just the top students. In our Information Warfare course required of all computer science majors, we have created a final course project that provides a research experience [8]. Students pair up with a faculty mentor to work on a current research topic throughout the semester. The project is broken into the phases of a research effort where students have to conduct background investigation, develop a research plan, collect data, perform analysis, and document their findings in both a research poster and a conference-level research paper. Several of the projects have been published in various conference proceedings.

5 Future Plans

Our current program is successful in providing all of our graduates a fundamental exposure to important issues they will be facing in their professional careers. Students with an increased level of interest have access to training opportunities that take into consideration the fact that they may not be technical majors. Our graduating cyber professionals have a high rate of accomplishment in their careers and a proven track record of successful performance.

To continue our success, however, requires evolving our program as technology changes and as the demands of our students future career field change. We are constantly updating our educational cyber curriculum and have faculty actively involved in cyber-education working groups. We also have faculty who actively participate in defining training standards and programs for the Air Force cyber career field. We try to take the lessons learned to improve our cyber training opportunities for students. As we gain more experience with Cyber 256 and the associated student instructors, we will need to tweak the program to keep it fresh, challenging, and relevant. Similarly, we are constantly in touch with our peers in the commercial and research sectors to understand the current challenges and find interesting projects for our students to work on. By maintaining currency, we hope to keep our broad-based program at the forefront of cyber education and best prepare our students to enter the cyber world.

References

[1] Critical Infrastructure Protection Board, National strategy to secure cyberspace, http://www.whitehouse.gov/pcipb
[2] Conklin, A.: The Use of a Collegiate Cyber Defense Competition in Information Security Education. Proceedings of the 2nd annual conference on Information security curriculum development, 16-18 (2005)
[3] The National Centers of Academic Excellence in Information Assurance Education Program, http://www.nsa.gov/ia/academia/caeiae.cfm
[4] Jabbour, K., Older, S.: The Advanced Course in Engineering on Cyber Security: A Learning Community for Developing Cyber-security Leaders, The Sixth Workshop on Education in Computer Security, (2004)
[5] Conti, G., Hill, J., Lathrop, S., Alford, K., Ragsdale, D.: A Comprehensive Undergraduate Information Assurance Program. Security education and critical infrastructures, Cynthia Irvine and Helen Armstrong (Eds.). Kluwer Academic Publishers, Norwell, MA, 243-260 (2003)
[6] Schweitzer, D., Boleng, J.: Designing Web Labs for Teaching Security Concepts. Journal of Computing Sciences in Colleges, 25, 2, 39-45 (2009)
[7] The UCSB iCTF, http://ictf.cs.ucsb.edu/
[8] Schweitzer, D., Boleng, J., Hadfield, S.: Providing an Undergraduate Research Experience in a Senior Level Security Course. Proceedings of the 13th Colloquium for Information Systems Security Education, (2009)