THE ADVANCED COURSE IN ENGINEERING ON CYBER SECURITY

A Learning Community for Developing Cyber-Security Leaders

Kamal Jabbour[1,2] and Susan Older[1]

[1]*Department of Electrical Engineering and Computer Science, Systems Assurance Institute, Syracuse University, Syracuse, NY 13244;* [2]*Next-Generation Security Laboratory, Air Force Research Laboratory, Information Warfare Branch, Rome, NY*

Abstract: The Advanced Course in Engineering on Cyber Security (ACE-CS) is a public-private partnership to develop top ROTC cadets into the next generation of cyber security leaders. Modeled after the General Electric Advanced Course in Engineering, ACE-CS immerses students in the cyber-security discipline through a combination of intense coursework, open-ended problems, and concurrent internships. In this paper, we discuss the ACE-CS pedagogy, the successes and challenges of its inaugural offering, and some future directions for the program.

Key words: Cyber-security education, technical leadership, learning community.

1. INTRODUCTION

The objective of the Advanced Course in Engineering on Cyber Security (ACE-CS) [1] is to develop the next generation of cyber-security leaders, with a particular emphasis on educating future military leaders. Through a public-private partnership among the Air Force Research Laboratory (AFRL), the US Military Academy, and Syracuse University, ACE-CS follows the model of the General Electric Advanced Course in Engineering [2] to help transform top cadets in the Reserve Officers Training Corps into original thinkers, problem solvers, and technical leaders.

The underlying philosophy of ACE-CS is to completely immerse students in the cyber-security discipline, through a combination of intense coursework and internship experiences. Each week, students attend a daylong lecture, given by a domain expert from the military, academia, or industry. They also spend three days a week in cyber-security internships, at either government labs or local industry. In addition, they work in teams to solve open-ended, real-world problems; they then write individual reports to present their solutions.

This paper presents the underlying pedagogy of ACE-CS, discusses the successes and challenges of its inaugural offering, and outlines some future directions for the program.

Specifically, Section 2 describes the program's educational objectives and its approach to meeting those objectives. Section 3 provides more details about the content of the course, including sample real-world problems assigned to students. Section 4 details some of the results of the initial (2003) offering of ACE-CS, as well as adjustments that will be made in the 2004 offering. Finally, we conclude in Section 5 with a summary of the factors that we believe have most influenced the success of ACE-CS.

2. EDUCATIONAL OBJECTIVES AND APPROACH

Critical to the success of any academic program is to identify the desired educational outcomes. Focusing on our expectations for students guides us in developing appropriate learning experiences, selecting topics for inclusion, and assessing student success [3].

The goal of ACE-CS is to develop original thinkers and technical leaders who can solve real-world problems in the area of cyber security. Specifically, when faced with a real-world problem, ACE-CS graduates must be able to do all of the following:

1. Formulate a clear problem statement.

2. Make reasonable assumptions about the problem context.

3. Apply sound analytical techniques and engineering tools.

4. Solve the problem to a specified depth.

5. Perform risk analysis on the solution.

6. Deliver a solution on time.

7. Communicate that solution effectively, both in writing and orally.

2.1 Program Approach

The ACE-CS program structure directly reflects its educational objectives. Modeled after the 80-year old General Electric Advanced Course in Engineering (now known as the Edison course [2]), the program combines (1) an intense classroom environment with real-world problems, (2) mentoring by experienced cyber security professionals, and (3) real-world experience through internships. The overall program–viewed separately from the specific course content–forms a learning community [4] centered on cyber security.

The course itself meets for eight hours once a week. A typical class begins with the timely submission of written reports and the oral presentation of solutions for the previous week's problem. Cadets discuss their solutions with the ACE Director and the instructor, before moving on to a new topic. Each week brings a different instructor, who assigns a substantial real-world problem for the next week and lectures for six hours on the background material for that topic. The instructors–drawn from government, academia and industry–are chosen for their expertise in the given topic.

Cadets work on teams of three to solve the assigned problems, which typically require 40-80 hours per team to solve. They then write and submit individual reports. In addition, each team must give two structured presentations during the ten-week course, one using slides (e.g., PowerPoint) and one using chalk on a blackboard. The presentations provide cadets experience in articulating, justifying, and defending a particular technical point of view. The presentations are nominally 15 minutes in length. However, they typically spark open debates among the class, as different teams attack the validity of others' assumptions and solutions.

Three days a week, cadets work with mentors at local private or government cyber-security laboratories during the day. These internships expose the cadets to the practical challenges of cyber security and help them establish professional relationships with domain experts. The ACE-CS Director matches students and internship opportunities before cadets arrive in June, based on employer needs and student background. Employers provide a paragraph describing the tasks they have for an intern, and students provide a 100-word bio describing their background and interests. Companies such as Par Technologies and Dolphin are looking for civilian students who may be interested in working for them full-time after graduation. Classified labs such as the Northeast Air Defense Sector (NEADS) need students who already have security clearances.

Fridays generally provide the military component of the ACE-CS experience. In addition to a weekly 8-mile run with the ACE-CS Director, cadets participate in flag ceremonies on base. There are also several field trips to military installations. For example, the 2003 cadets visited Fort Drum to observe the Phoenix Warrior live war games, the 174th Air Wing of the National Guard in Syracuse to see an operational Air Wing, and NEADS to observe the operation of a net-centric command and control center.

2.2 Student Assessment

The written reports serve as the primary assessment mechanism for gauging student progress. Although there is no mandated length for the reports, they typically run 30-40 double-spaced pages. The ACE-CS director and the instructors evaluate the reports with respect to the desired educational outcomes. Specifically, each report is graded on a 100-point scale, with the following weights: 10 points for the problem statement, 10 points for quality assumptions, 10 points for the use of analytical techniques and tools, 20 points for the solution itself, 10 points for the risk analysis (i.e., determining how dependent on the initial assumptions the solution is), and 40 points for the quality of writing (e.g., style, grammar, neatness, format, references). Students receive zero credit for a report not submitted on time; a second late submission results in expulsion from the program.

Like the reports, presentations are evaluated for both their content and their adherence to a strict format. PowerPoint presentations are limited to seven slides, and the first three slides must provide (respectively) a clear statement of the problem, the assumptions upon which the solution depends, and a summary of the tools and techniques employed in solving the problem. The remaining slides are devoted to the solution itself.

Cadets also evaluate themselves and their peers at the end of the course. Specifically, they must indicate what each team member's contributions were, and what percentage of the work each member performed. These evaluations influence the final grade that students receive for the course, which carries four credit hours of academic credit from Syracuse University. Students who successfully complete the program can apply the earned credit towards their programs of study at their home institution.

3. COURSE CONTENT

ACE-CS was first offered in Summer 2003, with an enrollment of seventeen students from across the country: twelve Air Force ROTC cadets, two civilian undergraduates, and three civilian graduate students. (In this paper, we shall follow the ACE-CS lead and use “cadets” to refer to all students, regardless of their ROTC status.) All but one cadet had completed at least three years in a computer-related discipline (electrical engineering, computer engineering, computer science, or information studies) and had experience in both programming and operating systems. Previous networking experience was desirable, but not necessary. The average grade-point average (GPA) was 3.2, on a 4.0 scale.

There were ten separate lectures, each covering a different aspect of cyber security. The lectures primarily focused on technical aspects, but they also covered legal and policy aspects of security. The full assortment of topics, along with the instructors who taught them, appears in Table 1. In addition to lecturing, the instructors also designed the problems that cadets worked on for the next week. These open-ended problems reflected the sorts of situations that cyber-security professionals encounter in the real world.

Table 1. Week-by-week syllabus of the ACE-CS course.

Week and topic	Content	Instructor
1. Legal Issues	Internet laws and cyber crime, the Fourth Amendment of the US Constitution, search and seizure of data, rights and privacy issues, government versus private workplace, search warrants and wiretap laws, the PATRIOT Act.	Prof. Lisa Dolak, *SU Law Professor*
2. Security Policies	Establishing and implementing security policies, confidentiality integrity and availability considerations, identifying vulnerabilities and threats, establishing disaster response and recovery procedures.	Joseph Giordano, *Technical Advisor, Information Warfare Branch, AFRL* LT Chad Korosec, *US Naval Reserve Officer*
3. Cryptography	Mathematical basis for data encryption, substitution ciphers and the Data Encryption Standard, private-key and public-key cryptography, key distribution and trusted authority, digital signatures.	Prof. Shiu-Kai Chin, *SU Professor*
4. Computer Security	Operating systems and file system security, passwords and one-way hashes, user-space administration, archiving and back-up strategy, intrusion detection, disaster response and recovery.	Prof. Steve Chapin, *SU Professor*
5. Digital Forensics	Procuring and analyzing digital evidence, preserving the chain of custody of digital evidence, recovering hidden data on hard drives, classifying file systems, analyzing slack and sector data,	Mr. Chet Hosmer, *CEO of Wetstone*

Week and topic	Content	Instructor
	recovering lost clusters.	*Technologies*
6. Network Security	TCP-IP packet format and vulnerabilities, protocol and implementation flaws, buffer overflow, denial-of-service attacks, distributed attacks, email, domain name system, web servers.	Prof. Heather Dussault, *SUNY-IT Professor*
7. Steganography	Data hiding in images, classifying steganography algorithms and tools, categorizing vessel capacity, detection and recovery of hidden data, digital watermarking, streaming media steganography, multilingual steganography.	Dr. Leonard Popyack, *Director of Adversarial Science Unit, AFRL*
8. Network Defense	Host and network security, firewalls and periphery intrusion detection systems, bastion hosts, network monitors and traffic analyzers, network logfiles, detecting anomalous behavior, network recovery.	Lt. Col. Daniel Ragsdale and Major Ronald Dodge, *United States Military Academy*
9. Wireless Security	Wireless local area networks, wireless encryption protocols, wardriving.	Mr. Paul Ratazzi, *AFRL/IFGB*
10. Next-generation Cyber Security	Next-Generation Internet Protocols IPv6, embedded systems, 3G cell phones and personal data assistants.	Prof. Kamal Jabbour, *SU Professor*

For example, the *Security Policies* problem required cadets to develop the security policies and procedures for an Air Force Air Operations Center (AOC) that contains a weather cell, a logistics cell, a Command and Control (C2) center, and an intelligence-gathering and processing center. The different cells and centers must operate at different security levels. In addition, the C2 center involves primarily Air Force personnel, but also includes Army, Navy, and some British military personnel. Given an initial high-level AOC architecture, cadets had to review and appropriately modify the architecture; perform a risk assessment on the AOC; develop a security architecture to overlay on the AOC architecture; and develop and define the AOC's security policies and procedures.

For the *Computer Forensics* problem, the instructor completed his lecture by tossing a USB thumb drive on the table. He informed the cadets that customs officers had seized it from a suspected drug dealer trying to enter the United States at Niagara Falls. He then asked the cadets to analyze the drive for (simulated) evidence that might support an indictment. To accomplish this task, the cadets faced the challenge of making 5 copies without modifying the device, calculating a hash, making assumptions, analyzing files and images, recovering stegoed data from an image of the Falls, restoring deleted email from the drive slack, translating foreign information, interpreting addresses and identifying the country, mapping drug slang into English, and then compiling a long list of circumstantial and forensic evidence.

The background scenario for the *Wireless Security* problem made the cadets part of an Air Force Office of Special Investigation (AFOSI) cyber-crime team attempting to gather preliminary evidence in a computer-crime investigation. Cadets were given authorization to search the Air Force premises of Griffiss Business & Technology Park in

Rome, NY to find a hidden wireless network. To ensure that they did not accidentally start analyzing the wrong networks, cadets had to report the location and identifying information of the suspected network to Air Force authorities. Once given the authorization to continue, cadets could move on to their primary task, which was to use any available tools and techniques to gather as much information as possible, including network configuration, identity of devices on the network, and contents of the data on computers and traversing the network. For their reports, students had to document their procedures and findings, and also determine whether the various vulnerabilities they found were fixable by the (hypothetical) criminal suspects or represented inherent vulnerabilities of the technology.

4. EXPERIENCES AND ADJUSTMENTS

All seventeen students successfully completed the 2003 offering of the course, and all but one student received an A or B. Eight of the nine problems were solved by all teams. However, only one team completely solved the *Wireless Security* problem, which ultimately required the cadets to find the hidden network (i.e., wardriving), determine the level of encryption, capture enough packets to crack the encryption (around 4 million packets, which took several hours), outline the topology of the network, find vulnerabilities (a misconfigured FTP server), compromise and penetrate the server, and then recover a password from a hidden directory. Only one team realized that they needed to write a C-program to strip the unencrypted headers from the encrypted packets before attempting to crack the encryption.

During the summer, cadets requested to play a cyber war game. On their own initiative, and with logistical support from the engineers in the Next-Generation Cyber Security Laboratory at AFRL, the cadets divided into a Blue Team and a Red Team. The Blue Team designed the target network, with a strategically placed series of “flags” (i.e., vulnerabilities). The Red Team deployed an extensive arsenal of off-the-shelf and custom computer-network attack tools, and systematically attacked the blue network over the course of one Friday. John Gilligan, Chief Information Officer of the US Air Force, met with the cadets near the end of the exercise and discussed their ACE experiences.

The internship component was very successful. Two cadets interned at NEADS, two cadets interned at local companies, and the remaining cadets worked in various labs throughout AFRL. The only complaint expressed by employers was a desire to have more of the cadets’ time allocated to the internships.

The cadets were very candid in their ACE-CS evaluations. They expressed strong views about various instructors, particularly complaining about those problems they found insufficiently challenging. Throughout the summer, they also expressed unhappiness with the ACE-CS Director’s insistence on correct written English and the stringent writing criteria he imposed. However, this reticence slowly turned into self-congratulatory praise as they appreciated their newfound ability to communicate professionally. The cadets also expressed appreciation for the 8-mile runs and indicated that the runs should remain a component of the program.

The 2004 offering of ACE-CS begins in early June. Out of 57 applicants, a total of 26 students will be participating in the program. Of these, seventeen are ROTC cadets (14 Air Force, 1 Navy, and 2 Army), and nine are civilian students. The average GPA is 3.4. All but two of the students are in computer science, computer engineering, or electrical engineering; the remaining two are in global studies and information security, which is a feeder program for Army Intelligence.

The most significant change planned for this year's curriculum is that legal aspects will be incorporated into the *Security Policies* lecture rather than be taught as a separate topic. Replacing the *Legal Issues* lecture will be a *Network Attack* lecture. There will also be a formal hack fest: Symantec will be sending a dozen of their security experts to set up a weeklong attack-defend exercise in July.

The 2004 offering will also introduce a summer-long competition among teams. Although all students worked hard in 2003, teams tended to share results with one another, effectively resulting in a 17-person team on some problems. Teams will receive points for their academic performance, success in the war game, completion of the 8-mile runs, peer and faculty evaluations, and possibly other activities. Members of the winning team will receive cyber-security gadgets as prizes at the end of the summer, as well as the bragging rights that accompany them.

5. CONCLUSIONS

The initial offering of ACE-CS was well received by the cadets, the military, and the laboratories that provided internships. Every ROTC graduate has been placed into a job where their cyber-security training can be used. There are more requests for ACE-CS interns than there are students in the program: every laboratory that provided internships in 2003 requested interns for 2004. We expect ACE-CS to expand into a multi-service leadership-development program in the coming years, as the US military transforms itself into a net-centric war-fighting force [5].

Without a doubt, ACE-CS benefits significantly from the partnership between Syracuse University and the Air Force Research Lab. However, ACE-CS is built upon fundamental principles that apply more widely than just to the military context. The five basic tenets that we believe have contributed most to the program's success are: (1) quality control through highly selective admissions; (2) domain experts in the classroom; (3) real-world, open-ended problems; (4) concurrent internships; and (5) the bonding of students through shared activities and hardship.

In effect, the ACE-CS program has been successful in creating what experts in Higher Education term a *residential learning community* [4] in the area of cyber security. Many universities are introducing learning communities to enrich the academic experience of students by integrating curricular and co-curricular activities. Learning communities bring together students with shared interests and values, engage them in shared activities (both academic and social), provide peer and faculty mentoring, and increase the intellectual interaction between students and faculty. These aspects of learning communities echo the basic tenets employed in the structure of ACE-CS. Cadets bond through many shared activities, such as field trips, life in the dorms, the weekly problems, and the 8-mile runs with the ACE-CS director. The ACE-CS structure fosters interaction with a diverse collection of instructors, and the internships provide cadets with both professional mentors and immersion in the discipline.

ACKNOWLEDGMENTS

The Advanced Course in Engineering on Cyber Security was made possible with grants from the Air Force Research Laboratory Information Directorate, the Air Force Office of Scientific Research, the CASE Center at Syracuse University (funded by the New York State Office of Science, Technology, and Academic Research), and the Griffiss Institute on Information Assurance.

REFERENCES

1. Kamal Jabbour, “Advanced Course in Engineering on Cyber Security”, course home page, http://Ace.syr.edu.

2. General Electric Corporation, “Edison Engineering Development Program”, 2003, http://www.gecareers.com/GECAREERS/jsp/campus/eng_program_guide.jsp.

3. Susan Older and Shiu-Kai Chin, “Using Outcomes-based Assessment as an Assurance Tool for Assurance Education”, *Journal of Information Warfare*, Volume 2, Issue 3, pages 86–100, August 2003.

4. Sandra N. Hurd and Ruth Federman Stein, *Building and Sustaining Learning Communities: The Syracuse University Experience,* Anker Publishing Company, Boston, MA, 2004.

5. US Air Force Modernization Planning FY 2006, Information Warfare Mission Area Plan, 2004.