Abstract – Information Assurance education has become increasingly important in the face of 9/11 and many well-publicized vulnerabilities in the national information infrastructure. The military academies have pioneered education at the undergraduate level with a focus on developing exercises that will lead to direct understanding and practicable experience in computer network defense.

Keywords: Information Assurance, Information Warfare, Cyber Defense, Computer Security, military, education.

1 Introduction

This paper discusses the development of a world-class Information Assurance program at the United States Air Force Academy which has culminated in creating a Technology and Information Assurance Group (TIAG), developing three computer security courses, building three research laboratories, and winning the inter-academy Cyber Defense Exercise (CDX). Half of this paper will discuss the development of the Information Assurance program, while the other half will focus on the CDX.

1.1 IA Motivation

Information Assurance (IA) is primarily concerned with principles and techniques for implementing availability, confidentiality, authentication, integrity, and non-repudiation of data, communication, and people [1]. The military, at least since the time of Sun Tzu, has long recognized that security is a critical feature of winning a military campaign [2]. Since the early 1990s, military strategists and futurists have become increasingly concerned with the vulnerability of the United States to an attack on its information infrastructure [3]. The United States is the most dependent on information technology, and thus, most vulnerable. As early as 1994, security professionals recognized that terrorist organizations would exploit the wide availability of hacker tools and viruses, lack of computer security in virtually all Department of Defense (DoD) and civilian information systems, and increasing government and corporate reliance on information technology to launch a devastating asymmetric attack [4].

Cyber vandalism, vigilantes, and warriors daily launch attacks on the availability, confidentiality, and integrity of information systems. In 2000, amateur hackers known as “script kiddies” wreaked havoc on information networks through “denial-of-service” attacks [5]. Computer viruses have become such a large issue that most large organizations screen e-mail and severely restrict its usage [6]. The DoD has had problems keeping important pieces of classified information away from publicly available networks [7]. The volume and diversity of threat, vulnerability, and attack has led the United States federal government to develop a national strategy for cyber security to protect the nation’s critical infrastructure [8]. Priority III of this national effort to secure the cyber frontier is to develop a “National Cyberspace Security Awareness and Training Program” to “address shortfalls in the numbers of trained and certified cyber security personnel” [8]. To meet this need, the Air Force Academy has created the IA Group with the mission of graduating Air Force officers with the understanding of IA necessary to our nation’s defense [9].

1.2 CDX Motivation

One avenue of producing such officers is the Cyber Defense Exercise (CDX). The purpose of CDX is to raise the level of excellence in IA education so that future military officers will be able to apply the principles of availability, confidentiality, authentication, and integrity to our nation’s defense. Given the shortage of trained and certified cyber security personnel in general and the military’s higher security requirements in particular, this exercise serves as a core educational and training event to help remedy this short fall. The CDX helps the Air Force Academy graduate Air Force officers with the technical and leadership savvy to handle computer network defense in operational Air Force units. The exercise also serves to raise overall awareness, within and without the DoD, of the need for cyber security and education excellence in information assurance.

2 Development of IA Education

It takes several years to develop an effective Information Assurance program. The Air Force Academy had courses in information warfare doctrine and tactics throughout the 1990s, but it created its first computer science course in information warfare in 1996. The early
versions of this course focused more on hands-on computer intrusion and network defense rather than theory. By 2000, the information warfare course had evolved into a fairly comprehensive computer security course that covered basic information security theory, cryptography theory, and network theory, had students use hacking tools such as password crackers, mail encryption utilities, and network sniffers, required students to evaluate software and write a research paper, and placed students in a team exercise where they secured and attacked networks. This team exercise was the genesis for the inter-Academy cyber defense exercise that replaced it.

For most of its history, the computer security and information warfare course, which was the core of the IA program, only had one or two instructors involved. Beginning in 2001, the Academy made a concentrated effort to attract and hire additional faculty with expertise in networking, cryptography, and information security. These new faculty led to a “critical mass” where the Academy could expand its IA program to offer new courses, publish increased research, build more powerful labs, and create the Technology and Information Assurance Group. In 2002, the TIAG held a series of meetings to determine the focus and direction of IA education at the Academy. After much discussion, the IA group developed four goals:

- Integrate IA throughout the curriculum (both in computer science and in other departments)
- Maintain world-class IA research and facilities
- Complete National Security Agency (NSA) IA center-of-excellence certification
- Lead all academies in cyber defense exercise

By 2003, the Air Force Academy had accomplished three of these four goals and was well on its way to the fourth.

2.1 Computer Security and Information Warfare

The flagship course in the Academy’s IA program is CS 438, computer security and information warfare. This course is for computer science and engineering cadets to develop a fundamental understanding of cryptography, vulnerability exploits, and computer security and be able to apply these concepts to secure a specific computer network against attack from competent adversaries. The course has seven core curriculum outcomes:

- Understand basic computer security and information warfare concepts and principles.
- Understand how to apply encryption to provide information assurance through confidentiality, integrity, authentication, and non-repudiation.
- Be able to attack confidentiality (cracking, enumeration), authenticity (spoofing), availability (denial-of-service) and integrity (Trojan-horse).
- Be able to secure computer systems and networks and detect and respond to intrusions.
- Be able to find and exploit vulnerabilities in network and system security to gain access and cover penetration.
- Be knowledgeable of legal and ethical issues involved with lawful and unlawful use of computers.
- Be knowledgeable of the resources available to assist computer security personnel.

The DFCS/NSA Information Warfare (IW) Laboratory supports CS 438 by supplying students hands-on experience in computer assurance and information attack. The IW lab consists of 25 student and instructor “attack” machines running VMWare on top of a multiple-boot system configuration. Each attach machine is a dual-hard drive, dual NIC, Dell Power Edge 600SC server with a 2.4 GHz Pentium IV CPU and 2.12 GB of RAM. Each attack machine contains several flavors of Unix, Linux, and Windows operating systems. In addition, the lab contains a stand-alone network for students to attack. The stand-alone IW network consists of a variety of “target” platforms with varying degrees of security, including routers and switches, for cadets to practice their hacking skills. This target network can optionally connect to USAFANet and/or the Cyber Defense Exercise network, but normally does not. It also has one or more firewalls and intrusion detection systems. The floor plan for the lab maximizes student interaction:

Shiva, the Hindu God of destruction, seemed an appropriate name for a cluster of attack machines. (M) is an additional monitor location, and (P) is the printer spot.

2.2 Curriculum Expansion

With the increase in its IA faculty, the Computer Science Department could now create new courses in
The IA Group chose to split CS 438 into its three components: information security (which retained the CS 438 number), secure networks (CS 468), and cryptography (CS 431). The networking, hack-off, and cyber defense exercise portions of the old CS 438 moved into CS 468. The mathematical theory and cryptography fundamentals in the old CS 438 moved into CS 431, which also added advanced cryptography. Finally, the new CS 438 shifted its emphasis to information security and focused more on some of the conceptual and theoretical underpinnings of computer security. In addition, the computer science department’s curriculum committee approved a change in the major’s graduation requirements to make each cadet take at least one of these information assurance courses. By 2003, the Air Force Academy had already witnessed one benefit of this specialization: its CS 468 cadets won the inter-Academy Cyber Defense Exercise.

Other departments also provided courses in Information Assurance and Warfare. The Military Strategic Studies Department continued to teach courses on information operations doctrine and strategy. The Political Science Department continued to offer courses on politics and intelligence. And the Electrical Engineering Department continued to provide course lessons on and waves and signals security. The Institute for Information Technology Applications (IITA) and Institute for National Security Studies (INSS), both at the Air Force Academy, continued to sponsor research in information assurance. Finally, the National Security Agency funded both the Information Warfare Lab and the Cyber Defense Lab in addition to other research efforts.

The IA Group’s rapid expansion and the development of new computer science courses and laboratories led to several important lessons learned:

- **Experienced Faculty.** Faculty must develop skill across the entire spectrum of IA—from computer network defense to cryptography theory to information security. Seek faculty with experience leading teams and implementing aspects of computer security and information operations.

- **Hands-on Exercises.** Students learn high-level IA concepts better when provided hands-on technical assignments where they can apply classroom concepts. For example, in cryptography, actually write software for computer cryptanalytic attack as well as encryption/decryption programs. Or, in secure networks, actually install, configure, and secure operating systems and computer networks.

- **Real-world Application.** The relevance of much IA has to do with real world application. In the same way that students learn algorithms and data structures by writing computer programs, they learn availability, confidentiality, and integrity by implementing secure networks and secure software programs.

- **Student Focus.** Keeping the IA curriculum current is time-intensive since the information technology changes rapidly and security threats evolve faster. Expect to dedicate more time on student learning, curriculum updates, and lab maintenance versus attending conferences and publishing papers.

- **Research Funding.** Seek donors early to obtain funds for research, lab equipment, and faculty. Expect to need to replace a whole lab about every two years.

Ultimately, the Air Force Academy’s success in its IA program rests on the commitment of exceptional faculty who work well together and are obsessed with student learning. An emphasis on good teacher-student interaction in addition to relevant, up-to-date course ware and lab facilities has also been critical.

## 2.3 Evolution of Cyber Defense

In 2003, TIAG officially separated CDX from CS 438 and moved it into CS 468. However, students enrolled in CS 438 still helped their counterparts in secure networks prepare by acting as the in-house “red teams” verifying and evaluating the CS 468 cadet’s networks. CS 438 students used both passive and active foot printing, scanning, and enumeration tools to determine type and number of machines and services offered by the secure networking students. They then used vulnerability assessment tools like Nessus and SARA to discover holes in the security of the cyber defense network. Finally, they attempted to exploit vulnerabilities they found in the network using scripts and code downloaded from the internet. In this early test, the information warfare students were unable to gain access, either as users or as root, on the network security students’ machines. Although frustrating for the CS 438 students, it gave the secure networking students a confidence boost that they were on the right track—a fact eventually verified by their nearly perfect defense against the “professional” red teams from the NSA, Air Force, and Army. Below is a diagram illustrating the network configuration between the information warfare student network and the cyber defense network:
3 Cyber Defense Exercise

An ideal capstone project for an undergraduate concentration in information assurance, the cyber defense exercise requires students implement and secure a production-level computer network and its applications. Successfully incorporating a CDX is time consuming and resource intensive for faculty and students. Yet, doing so at the Air Force Academy has yielded outstanding student feedback and educational results.

3.1 What is a Cyber Defense Exercise?

A Cyber Defense Exercise is an event that allows students to get realistically involved with designing, implementing, defending and analyzing a small computer network. The CDX in which the Federal service academies (United States Air Force, Naval, Military, Coast Guard and Merchant Marine) participate contains three groups: “white cell” members who play the role of mediators, “red cell” members who play the role of the adversary, and “blue teams” played by each of the schools.

Each school is presented with the same requirements (e-mail, web servers, DNS, etc.) and guidelines as well as the same hardware and time to complete the project. The exercise ends with a four day “execution period” where the networks are actively in use and under attack. The team providing the most stable and operational services, and who analyzes attacks with the most accuracy is declared the winner.

The Air Force Academy (AFA) has participated in all three of the CDX competitions. Each year the exercise has been integrated into the Academy computer science curriculum and has received highly favorable feedback from students involved. The first two years the CDX was much smaller in scale and did not allow each team to design its own network. The 2003 exercise was a significant improvement over the previous two years, primarily because each school was free to design the network they wanted to implement.

The exercise is a team project that can provide the ultimate experience to undergraduate students who will soon be commissioned as second lieutenants in the Air Force, where most of them will be actively applying the
information assurance lessons learned while participating in the exercise.

3.2 Computer Science 468 Secure Networks

A new course was developed to give adequate coverage of topics such as perimeter design, intrusion detection, computer forensics, secure protocols, weaknesses in existing network protocols, risk analysis, and survivability. This course was known as CS 495b Analysis and Design of Secure Networks during its first offering in the spring of 2003. It is now a permanent spring offering as CS468 Secure Networks. CS 495b used popular literature readings and two textbooks for readings.

Table 1

<table>
<thead>
<tr>
<th>Topic</th>
<th>Number of Lessons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Threats</td>
<td>1</td>
</tr>
<tr>
<td>Survivable Systems</td>
<td>2</td>
</tr>
<tr>
<td>TCP/IP Protocol Weaknesses</td>
<td>2</td>
</tr>
<tr>
<td>Analyzing Network Traffic and Protocols</td>
<td>2</td>
</tr>
<tr>
<td>DNS Design and Weaknesses</td>
<td>1</td>
</tr>
<tr>
<td>Assessment Techniques</td>
<td>1</td>
</tr>
<tr>
<td>Secure Design Principles</td>
<td>1</td>
</tr>
<tr>
<td>Perimeter Security Fundamentals (packet filters, proxies, NAT,)</td>
<td>4</td>
</tr>
<tr>
<td>Security Policies</td>
<td>1</td>
</tr>
<tr>
<td>Routing and NAT</td>
<td>1</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>2</td>
</tr>
<tr>
<td>Virtual Private Networks</td>
<td>2</td>
</tr>
<tr>
<td>Network Software Architecture</td>
<td>2</td>
</tr>
<tr>
<td>Design Discussion</td>
<td>2</td>
</tr>
<tr>
<td>CDX Lab Preparation</td>
<td>5</td>
</tr>
<tr>
<td>CDX Execution</td>
<td>3</td>
</tr>
<tr>
<td>CDX Discussion and Briefing</td>
<td>2</td>
</tr>
<tr>
<td>Auditing and Computer Forensics</td>
<td>3</td>
</tr>
<tr>
<td>Analysis of Attack Trends</td>
<td>2</td>
</tr>
<tr>
<td>Administration, Tests</td>
<td>3</td>
</tr>
</tbody>
</table>

CS 468 was designed around CDX so that all of the lessons learned during the semester could be applied to the exercise (which takes place in mid-April). Analysis and discussions afterward round out the class. Three large homework assignments were assigned before CDX and focused on mixing hands-on lab time with traditional-style homework questions and analysis. Before ever configuring the CDX lab to their design specifications, the students were using the hardware throughout the semester to complete the homework assignments, which helped them become very comfortable with the equipment. Also, the software they were using in the homework were items that would be available for use in the CDX (if they chose), further helping them become accustomed to the environment of the exercise. Table 1 lists each of the lesson topics (each lesson is 50 minutes of contact time).

The primary theme in CS 468 is survivability. The course instructor incorporated lessons based on personal experience in managing a large series of networks at an Air Force base prior to teaching at the AFA. Each topic was tied back to relevant Air Force network examples or possible application to CDX.

3.3 Incorporating CDX

Successful participation in CDX requires significant planning and resources. Finding the proper place in our curriculum has been challenging for each of the three years we’ve participated in the exercise. The most significant challenge is allocating enough time for preparation and execution. Execution of the exercise takes place roughly ¾ of the way through the semester, and lasts for four days. During the day, students must be available to monitor the systems and respond to incidents or activity on the systems. In the evening, the students must analyze the day’s activity and provide a written situation report, which can stretch late into the night. Preparation for the exercise takes a minimum of two to three weeks as well, which means a conservative estimate for how much time participation in the exercise takes is around four weeks.

In addition to the significant time that must be dedicated to the CDX, there are hardware requirements that ensure each participant does not have an advantage over the other teams. NSA sponsorship of the exercise ensure that the five participating undergraduate schools have the same hardware. Other schools wanting to start a CDX competition could establish hardware guidelines that would be more flexible, allowing a wider variety of existing hardware to be used, increasing the number of possible participants.

Another consideration when planning for CDX involvement is that the lab housing the CDX equipment must be dedicated to the exercise for at least a month. During the preparation and execution phases, it is extremely difficult to share the lab with any other classes or for any other use.

The final project in CS 468 is analyzing the CDX requirements and designing an implementation. The overall architecture used in the exercise was evolved by working in small teams in class. Each team designed their own rough solution, which was presented to the rest of class for critique. Each team then incorporated the best traits discussed during the critique process and improved the design. By the end of the process, the teams had agreed on the general architecture of the network. A detailed solution including a complete design, security
policy, and assessment based on the Survivable Network Analysis Method presented in [10].

3.4 CDX Team Selection

Participation in CDX is time consuming and requires an above average dedication to working outside of class. Given that the faculty and students both had high expectations for the class, and that the faculty decided the class would run better if each student had a dedicated lab server, enrollment was limited to 14 students. These students were selected on a first-come, first-served basis. Future offerings of this course will give priority to cadets who are pursuing an information assurance concentration.

This year’s class consisted of 14 students, 10 seniors and 4 juniors. There were eleven computer science majors, one computer engineering major, one mathematics major, and one behavioral science major. Both the mathematics and behavioral science major were computer science minors.

In many ways CDX is as much a leadership and teamwork exercise as it is a network security exercise. The course instructor chose the team leader from those who volunteered for the position. This year, the team leader was a math major and computer science minor. During the design phase of the exercise, the team leader worked with the rest of the class to organize into specialized teams. The students decided that they would organize functionally into four groups; perimeter security, services, intrusion detection, and forensics and disaster recovery.

Probably the most difficult challenge for the team during the exercise is communication. This year’s team was much more successful at communicating and maintaining written logs of activity throughout the day. Consequently, one of the most valuable lessons students learn from the exercise is the importance of continuity of operations.

From the instructor’s point of view, a smaller team worked much better than a larger one. In the prior year’s competition, the Academy fielded a team of 25 students. The large size created problems in communication and hurt teamwork in general. 14 students were probably close to an ideal size, and twenty could be an upper limit.

3.5 Preparing for CDX

Preparation for CDX primarily involves establishing a laboratory environment for the students to implement their design. A laboratory technician or faculty member should be well versed in UNIX and Windows system administration to help the students troubleshoot problems.

A key element to being successful in CDX is to have as many students as possible involved during the execution phase. Achieving this can be quite difficult, as excusing students from all the duties at a military academy over the course of four days is not a trivial challenge. This year, the Academy team kept about four cadets available (as a minimum) throughout the day. Additionally, each night the team leader held a team meeting where all members would be present to contribute to the daily situation report. Recovery and other analysis, or improvement to the network could also be made at this time.

Providing after hours support for the CDX team is also important. Although not a problem this year, in the past teams have often stayed late rebuilding systems, changing configurations to improve the security or applying new patches. Often, the students will be treading on new ground and will require some technical assistance. It is also important to note that CDX is not an exercise in system administration.

3.6 Benefits of CDX

Before the results for this year’s CDX were announced, students submitted written feedback and engaged in informal discussions with each other and faculty. The overwhelming response was that participation in CDX was one of, if not the most fulfilling academic event the students had been involved in. Though many cadets admitted the amount of time and effort put into the exercise was more than expected, they also felt the effort was worth it. Two of the junior students have expressed an interest in doing independent research in information assurance topics.

End of course critiques for the class showed that students rated the class an average of excellent (a numeric value of 6, from 1 to 6) in three categories, intellectual challenge, relevance and usefulness, and amount learned. The course also earned a nearly perfect 5.9 average in three other categories, reasonableness of work, evaluative and grading techniques, and course as a whole. When compared with all other courses offered during the same semester at USAFA, this course scored an average of 1.5 points higher. A highly rated capstone course is an obvious benefit when advertising the concentration, and winning the CDX is a source of pride for the whole institution.

4 Conclusions

It has taken the Air Force Academy several years to develop a mature, effective IA program. Information Assurance (IA) is primarily concerned with principles and techniques for implementing availability, confidentiality, authentication, integrity, and non-repudiation of data, communication, and people. A Cyber Defense Exercise (CDX) raises the level of excellence in IA education and
get students realistically involved with designing, implementing, defending and analyzing a small computer network. Experienced faculty, hands-on exercises, student focus, and top-notch research facilities are all critical to success in building an IA program. Successful participation in CDX required significant planning and resources by faculty and required students to have an above average dedication to working outside of class. The overwhelming student response was that participation in CDX was one of the most fulfilling academic events in which they had been involved. They learned a lot and loved learning!

References


