A COMPREHENSIVE UNDERGRADUATE INFORMATION ASSURANCE PROGRAM

Gregory Conti, John Hill, Scott Lathrop, Kenneth Alford, and Daniel Ragsdale
Information Technology and Operations Center (ITOC), Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY

Abstract: This paper describes the experience of our institution in creating a comprehensive undergraduate information assurance (IA) program. An interdisciplinary approach was undertaken in order to include a larger portion of the student body and faculty and thus influence a broader audience. The program includes a wide variety of mutually supporting information assurance activities including a research center, coursework, an information warfare laboratory, a cyber defense exercise, an outreach program, conferences, trips, summer internships, a guest speaker program, a National Security Agency Liaison program, summer student internships, faculty sabbaticals and a student information warfare club. This paper organizes discussion of these activities into the student experience, building faculty expertise, and organizational support. The catalyst for these activities has been the formation of the Military Academy's dedicated information assurance research center, the Information Technology and Operations Center (ITOC), and the continuing support from and interaction with the National Security Agency. The primary goal of this paper is to provide a descriptive resource to educators who wish to implement an undergraduate or graduate level information assurance program. It is our sincere hope to inspire and aid others in starting similar programs.

Keywords: Information Assurance, Education, Information Warfare, Computer Security Education, Computer Security

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

1. INTRODUCTION

1.1 Motivation

Business, government, military, public utilities, and academia all take advantage of the efficiency, speed, computational abilities, storage, and transport capabilities provided by information systems. These systems are so ingrained into everyday operations that the functions and services they provide would be difficult, if not impossible, to perform without them.

Gene Spafford, the director the Center for Education and Research in Information Assurance and Security (CERIAS), is well known in the information security community. He was called upon in 1997 to testify before congress on the subject of information security education. In no uncertain terms he told the committee that security must be built into information systems, and that in order to make that happen we must properly educate our students: "To ensure safe computing, the security (and other desirable properties) must be designed in from the start. To do that, we need to be sure all of our students understand the many concerns of security, privacy, integrity, and reliability." [1]

It is easy to describe why there is such a need for information security education. As Spafford testified, "Our students and soon-to-be students will be designing our information technologies of the future. We are endangering them and ourselves because the majority of them will receive no training in information security." The way to achieve secure information systems is to provide the appropriate information security education to the people who have to build them.

By November of 1996 (according to Spafford) there were only four "declared, dedicated computer security research centers in degree-granting departments at universities in the United States." Other institutions were performing valuable work in this area, but perhaps didn't have the same institutional or financial support. Fortunately, since that time, information security has been added to numerous programs, new research centers have been established, and additional research funding has been made available. Unfortunately, there is still much to be done. In 2000, Matt Bishop identified the following weaknesses (among others) in our overall efforts: we continue to repeat well-known errors (e.g., buffer overflows), we have not improved how we design systems and programs to account for security constraints, and we don't fully understand how security problems arise from human interaction with systems. [2] Clearly, each of these weaknesses can be addressed by information security education.

Bishop makes clear distinctions in information security education between public awareness and academic education. He further divides

academic education into four broadly stated types: training, undergraduate education, terminal master's education, and doctoral education. [2] Our institution provides education primarily at the undergraduate level (we have no post-graduate program). However, our Information Assurance program and research efforts serve as an effective training ground for our faculty with masters and doctoral degrees.

Recent events in American and world history clearly demonstrate that the demand for information assurance is waxing, not waning. It is our contention that all undergraduate students, regardless of their major or areas of specialization, should receive appropriate levels of information assurance education. At the United States Military Academy, our long-term goal is to introduce *all* of our students to the principles of information assurance and provide in-depth information assurance education to as many students as possible. This paper discusses the actions we are taking to realize that goal.

1.2 Background

The United States Military Academy (USMA) is a medium-sized undergraduate academic institution located at West Point, New York.. There are approximately 4,100 students, all of whom will serve in the military upon graduation. Approximately 200 students are Computer Science, Electrical Engineering, or Information Systems Engineering majors. There are approximately 400 other students taking a three-course engineering sequence (similar to a minor) in either Computer Science or Electrical Engineering. All students take a core information technology (IT) course as a freshman. Beginning in the Fall of 2003, all juniors will be required to take a second IT course.

Information assurance, information security and computer security are of vital importance to the nation, the military, and to us as individuals. It is due to the awareness of this importance and extensive interest by both our faculty members and our students that this program was implemented. Until 1999, our academic program lacked any cohesive information assurance activities. Information assurance education was presented minimally and in an ad-hoc manner. The coalescence of new faculty members with IA experience, increased resources, senior decision-maker support, world events, and heightened public awareness provided the momentum required to establish and build up the current IA program.

1.3 Program Components

In a 2000 report, Corey Schou, the director of the National Information Assurance Training and Education Center (NIATEC) at Idaho State

University and chair of the National Colloquium for Information Systems Security Education (NCISSE), noted that the need for information security professionals still couldn't be met by the output of existing academic programs. [3] Clearly, our academic programs must reach out to more students. He also identified several initiatives for improvement of information security education. Among these were more internships to provide students and faculty with practical information assurance experience, exchanges of government and academic professionals, and improved training resources for students and faculty.

At our institution, we are trying to reach out to as many students as possible. Also, the three initiatives mentioned above represent just a few of the many components that make up our information assurance program. Many of these components started as small faculty member initiatives. Over time, the components have helped us to define what makes a successful overall program. This paper describes the components from the student, faculty, and organizational perspective, and seeks to aid other academic programs avoid the hurdles we experienced as the components matured into a cohesive program

2. RELATED WORK

There is much ongoing work in the area of information assurance education. This activity has dramatically increased due to heightened national awareness and by programs such as the National Security Agency's Information Assurance Center of Excellence program, the Federal Cyber Service Initiative, the Information Assurance Scholarship program and greater overall resourcing of information assurance research. Prior to the recent emphasis, several institutions established computer security and information assurance programs. Recently, many other programs have been formalizing and stepping up their activities in information assurance education. The majority of these activities are at the graduate level. We believe that the interdisciplinary nature and undergraduate focus of the work presented in this paper will help other undergraduate institutions rapidly prototype and implement similar IA programs.

3. THE STUDENT EXPERIENCE

The heart of every academic information assurance program is the student experience. This experience is built upon an overarching framework for information technology and information security education. Hung upon

this framework is an interlocking series of activities that provide mutually supporting information assurance education. The student-focused portion of our IA program includes a student information warfare club, coursework, lecturers, guest speakers, an information warfare lab, an interschool information assurance competition, summer internships and educational trips.

3.1 Framework for Information Technology and Information Security Education

Information Technology Goal: Information technology is a key component of the military's strategy. USMA intends to provide graduates for the military who can operate in an information-rich environment, take advantage of existing information technology, and are prepared to explore and exploit future technology — "The overarching goal of the Academic Program is to enable its graduates to anticipate and to respond effectively to the uncertainties of a changing technological, social, political, and economic world." Additionally, an IT goal was recently added to the overarching goal — "graduates will demonstrate proficiency in information technology." Within the context of our Academic Program, information technology (IT) is defined as encompassing "the knowledge, skills, processes, and tools by which the state of the physical world is sensed and, along with other knowledge, is disseminated, stored, transformed, processed, analyzed, presented, used to make decisions about actions, and used to initiate and control actions." [4] Information technology is embedded in the academic program, and so is information security education. This integration can be seen in most of the course descriptions.

Daily experience: One of the earliest experiences in each student's first academic year is the setup and configuration of their mandatory-purchase student computer. [5] From that moment forward students are immersed in an ubiquitous computing environment — all 4,100 student computers are networked together. Wireless networking is expanding rapidly, energized by the introduction of laptop computers to the Class of 2006. Every academic department and agency on the institution is "wired in" as well. Students are exposed to and intimately engaged with Information Technology as an integral part of their daily routine. The vast majority of courses the students are required to take (*core* courses) take advantage of information technology, ranging from the use of web sites and e-mail for communication through the use of sophisticated automated tools within the classroom. In addition, certain core courses are designated to provide the primary instruction leading to proficiency in specific applications. Other courses are then able to rely on that proficiency. "Throughout their core courses, students learn to use,

evaluate, and select appropriate computing system tools to solve real-world problems. They develop personal skills in the effective use of fundamental computing applications such as word processing, spreadsheet analysis, desktop publishing, database management, presentation graphics, computer security, and telecommunications software." [4]

Dedicated IT instruction: This institution has long required that every student take an "Introduction to Computer Science" course, which has recently been reconfigured to focus less on the specifics of computer science and programming and more on information technology. The first year course (IT105) lays a good foundation for students in understanding and using Information Technology. [4] To support the emphasis of the IT goal mentioned above, a new course (IT305), mandatory for juniors, was created to "develop further understanding of the physical and mathematical principles governing sensors and communications as they apply to IT systems" and to "develop their abilities to describe, analyze, and evaluate information systems and their components to build comprehension of selected current and emerging information technologies." A significant component of this course is that "students acquire skills and knowledge relevant to effective information assurance and develop the ability to make informed and rational decisions involving the legal and ethical dimensions of IT." [4]

Majors and Minors: Every USMA graduate receives a thorough grounding in information technology (IT) and an exposure to information assurance (IA). In addition, there are several majors in the academic program that provide special emphasis on IT and on IA. The Computer Science (CS) major develops capabilities in designing, testing, and building computer and information systems, integrating and applying those systems, and being effective users of those systems. CS majors get a thorough grounding in information assurance. [6]. The Electrical Engineering (EE) major focuses on digitization – the exchange of information using computers networked together by digital communications systems, and see information assurance from that perspective. [7] The Information Systems Engineering (ISE) major focuses on providing students with a solid foundation in the development, integration and use of information systems, and focuses attention on the defense of information systems. [8] The equivalent of a minor at the institution is a "core engineering sequence" that focuses on the design-build-test methodology and allows students in any field to expand their knowledge of IT and IA.

3.2 Student Information Assurance Organization

A student information warfare club was formed in February 2001 under the auspices of the Association for Computing Machinery (ACM) Special Interest Group for Security Audit and Control (SIGSAC) and quickly grew to 80 members. It has continued to grow at a rapid pace and now numbers 450+ students (more than 10% of the student population) and six faculty advisors. This is particularly significant when one considers that there are approximately 80 computer science majors at this institution. It was formed due to a realization of the potential of such a club by faculty and extensive interest by students. It was the first student chapter of its kind out of the more than 600 ACM student chapters worldwide. The chapter includes a wide range of interdisciplinary activities and has members from every academic department. It is this wide range of activities and interdisciplinary focus that allow the club to reach a wide audience. It has proven to be an effective vehicle in increasing information assurance awareness, facilitating ethical education and debate, providing leader development opportunities and generating excitement in students for information assurance.

SIGSAC members participate in virtually every aspect of the institution-wide IA program. Members receive invitations to hear guest speakers discuss information assurance topics. This has proven to be very popular, frequently drawing large numbers of students. Members also receive early information about IA-related course offerings and summer internships. During a recent offering of MA489 Mathematical Cryptology over half of the students in the course were chapter members who learned of the course from the SIGSAC mailing list. SIGSAC members are almost exclusively those who compete for and win the IA-related summer internships. Resources can be scarce and SIGSAC is an ideal venue to identify candidates and select those who are most interested and prepared.

The institution participates in an annual collegiate information assurance competition called the Cyber Defense Exercise. While the Cyber Defense Exercise is not a SIGSAC activity, chapter members have been among the most prepared and stood out as leaders. A few members of the faculty draw the analogy that SIGSAC is the junior varsity team, while students in the senior-level CS482 Information Assurance course are the varsity. Trips are another popular activity - chapter leaders coordinate with existing trip organizers and are frequently able to secure seats for SIGSAC members. Using this strategy, students have visited the National Security Agency, the Blackhat Briefings, InfoWarCon, the United States Army's 1st Information Operations Command, the Pentagon and the White House. Recently students have begun a program of Internet safety awareness training for local schools.

This strategy has resulted in a great deal of enthusiasm and participation. As a result of these activities, the chapter won a 2001-2002 ACM Outstanding Activities Award. More details can be found at http://www.itoc.usma.edu/sigsac/.

3.3 Courses Providing Breadth and Depth in Information Assurance

Information Assurance coursework is at the heart of the program. Some courses are primarily information assurance related, others have a large information assurance component or otherwise play a supporting role.

CS482 *Information Assurance*: CS482 is the flagship information assurance course in the curriculum. It provides depth and is taught in the Information Warfare (IWAR) laboratory. This lab contains an isolated network designed to allow a much greater range of action beyond what would be allowed in a traditional lab on the official academic network. The course teaches students how to employ strong network defenses by exposing them to core information assurance principles as well as the tools and techniques of attackers. This course is highly technical and is limited to students with a substantial background in Computer Science or Electrical Engineering. It is offered each spring and culminates with a demanding three-day Cyber Defense Exercise (CDX), which is described in more detail later in this paper.

SS490 Policy and Strategy of Cyberwar This course is offered by the Department of Social Sciences and provides additional depth and complements CS482. While CS482 focuses on the technical aspects of information assurance, SS490 focuses on the political, economic and social issues. The course is open to a much wider population of students and is offered each fall. The prerequisites are the mandatory IT105 course and SS307 *International Relations*.

MA489 Mathematical Cryptology: This course is offered by the Department of Mathematical Sciences and exposes students to manual and machine cryptosystems, the history of the art, and cryptanalytic techniques.

LW489 CyberLaw: This course is offered by the Department of Law and exposes students to the legal issues associated with information technology and cyber war.

Information Security Integration Throughout the Curriculum: While CS482, SS490, MA489 and LW489 provide specific and in-depth exposure to information assurance, a variety of other courses (primarily in the CS and IT programs) provide support. A deliberate decision was made in these courses to weave security throughout applicable lessons rather than relegate the subject to only a lesson or two at the end. The core information

technology courses, IT105 and IT305, expose freshmen to information assurance and include an information warfare lesson and exercises in the IWAR lab, and addresses security throughout the spectrum of military information systems. CS385 *Analysis and Design of Algorithms* covers the mathematical foundation for encryption algorithms. The CS481 *Operating Systems* course delves into threats against computer system assets and operating system design issues associated with countering those threats. CS484 *Computer Networks* teaches information assurance and network security by complementing traditional theory based instruction with hands-on exercises utilizing white hat and hacker tools and techniques. Every layer of the OSI model can be exploited and these exercises illustrate to the students the respective strengths and weaknesses.

3.4 Lectures and Guest Speakers

Formal classroom instruction is augmented with a wide range of lectures and guest speakers. Student attendance is typically optional for the majority of the student body and for SIGSAC members. In some instances, CS482 *Information Assurance* in particular, students taking the course were required to participate. In 2001 and 2002 speakers came from several activities, including the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), White Wolf Security Consulting, the Secret Service Electronic Crimes Task Force, a Department of Defense Computer Crime Investigative Unit, the Department of Defense Joint Task Force for Computer Network Operations, and the Honeynet Project. Bringing in outside speakers helped to build bridges with other organizations as well as foster enthusiasm among the students and faculty. For the general student population, this series of speakers proved to be the most successful portion of the IA program.

3.5 Information Warfare (IWAR) Laboratory

We decided early in the process of building our Information Assurance program that simply discussing Information Assurance topics was not enough. In order to meet the institution's goal of providing an "active learning" approach to education, only a facility where students could obtain hands-on experience with cyber attacks and technical countermeasures would suffice. The Information Warfare Analysis and Research (IWAR) laboratory has evolved over the last two years to provide such an environment and is the centerpiece of our IA education.

Consisting of over 200 computers and networking nodes, the IWAR lab is an isolated network of heterogeneous operating systems, applications, and

networking equipment where students enrolled in our courses and members of our ACM SIGSAC student chapter can learn about the capabilities of known computer attacks and discover the technical countermeasures to defend an information system against such exploits. Except for a few administrative machines, the students are given full administrative privileges on systems within the lab. This enables them to experiment with offensive and defensive tools such as port scanners, vulnerability scanners, Trojan horses, worms, viruses, firewalls, intrusion detection systems, password crackers, and any published exploits without running the risk of releasing malicious code onto our production network or into the "wild." Just as a soldier would only fire a weapon on the range or in combat, our policy only permits users to experiment with the malicious tools in the controlled confines of the lab.

Currently the IWAR lab supports CS482 *Information Assurance,* CS484 *Computer Networks*, SS490 *Policy and Strategy of Cyber War*, several lessons in IT305 *Military Information Systems* and one lesson in LW489 *CyberLaw*. Faculty members reserve the lab and use it to teach components of their courses that would best not be done on the official academic network. A good example is running the Ethereal software package (http://www.ethereal.com). Ethereal is packet sniffing software that is very useful for demonstrating encapsulation techniques within the OSI network stack and for demonstrating network protocols in action. The risk is that it also can capture personal information and capture passwords. The IWAR lab provides on ideal venue for such a tool.

The lab is also used as a focal point for congressional, academic, military, and other visitors interested in observing or replicating our work; and is used for information warfare demonstrations during a once-per-semester "technology tour" for the freshmen students. The purpose of this demonstration is to motivate the freshmen to take advantage of the lab and Information Assurance courses during their time as students. Finally, the lab provides a facility for faculty members to conduct research and work on projects in Information Assurance topics. The website at http://www.itoc.usma.edu provides more information and includes labs used in the IA course as well as the standard operating procedures.

3.6 Cyber-Defense Exercise (CDX)

The Cyber Defense Exercise (CDX) is the most demanding activity in our IA program. As the capstone project in the CS482 *Information Assurance* course, the exercise is an intensive three-week competition allowing students to apply their IA skills in a team setting. Given a set of constraints and required network services, students from each of the military

academies (Military, Air Force, Naval, Coast Guard, and Merchant Marine) and the Naval Postgraduate School design, build, harden and defend their network against attacks by professional red teams from the NSA and the 1st Information Operations Command. The primary sponsor of the event is the National Security Agency who awards the Information Assurance Director's Trophy to the undergraduate team whose network provides the required functionality while proving to be most resilient to attacks. This annual event has been held twice, with USMA winning the trophy both times. The Naval Postgraduate School participates in the exercise and does very well, but is not involved in the competitive scoring of the undergraduate institutions.

During the first two weeks, or preparation phase of the exercise, students build their network and secure their systems. Certain constraints in the exercise directive require the students to use several different operating systems on one or more of their end systems. For example, in last year's competition student's employed Solaris 8.0, Linux kernel 2.4.8, Windows 2000 Advanced Server, and Windows NT 4.0. Certain services such as web, email, and file servers must be provided by the students' system. In order to establish a defense-in-depth and defense-in-breadth posture, security measures are limited to open source tools to include, but not limited to, open-source port scanners, vulnerability scanners, network monitoring tools, intrusion detection, and host-based and network-based firewalls. For example, in the recently completed exercise, the students established an intrusion detection system using Snort running on a Linux machine. In order to prevent traffic from leaving their network interface card, they built a one-way Ethernet cable that allowed only one-way traffic into their intrusion detection machine, aptly named *Narc*. More information on the exercise can be found at http://www.itoc.usma.edu.

3.7 Summer Internships

Many students are given the opportunity to participate in three to four week summer internships. This is a longstanding program at this institution, but until recently, there were no internships within the information assurance community. The institution's information assurance research center actively develops relationships with external organizations and coordinates a wide variety of information assurance related opportunities for students. Recent internships included assignments at the newly established Homeland Security Office in order to assist the creation of national policy for the nation's critical infrastructures; the evaluation of network security with the National Security Agency; research of wireless tracking devices with the Secret Service; and investigation of hackers breaking into military networks at a Department of Defense Computer Crime Investigative Unit (CCIU).

Students are encouraged to bring back the work they begin on these summer internships and to continue the work as either part of an individual study class or as part of their senior project. These internships reinforce in the students' minds the emphasis and priority Information Assurance initiatives receive in real world settings and motivate the students to continue to delve deeper into their studies.

3.8 Student Trips

Trips to Information Assurance conferences and to governmental agencies working in Information Assurance also contributes significantly to motivating students and faculty to start or continue their educational experience in IA topics. Conference participation provides a source of new ideas. Each trip brings both direct and subtle thoughts as well professional contacts and exposure that benefit the program. Although some of the material being presented may be somewhat over their heads, students begin to appreciate the complexity and issues associated with securing information systems.

Within the past two years there have been four major trips scheduled each year. Participation in conferences is carefully synchronized with other program activities and the academic year to provide maximum impact. Table 1 displays this careful timing. Approximately 30 students and four to five faculty members accompany the students on each trip. The priority for the trips is to those students who are either enrolled in one of the IA course or actively involved in the SIGSAC program.

Table 1: Conference/Trip Timeline

When	What	Why
September	InfoWarCon/Visit D.C. Area Agencies	Motivate Students to pick IA topics for their senior projects. Build underclass (SIGSAC) understanding of the issues.
February/ March	Blackhat/SANS type conference	Provide instruction and motivate students enrolled in Information Assurance Course for upcoming Cyber Defense Exercise.
March/ April	NSA Trip	Provide overview of NSA's priority on IA to students involved with SIGSAC.
June	IEEE Information Assurance Workshop	Contribute to the education of the IA community. Promote our own program and faculty.
July	Blackhat/Defcon	Stimulate faculty interest and keep them up to date on the latest exploits coming from the BlackHat community.

A trip in the fall centers on the InfoWarCon, www.infowarcon.com, conference in Washington D.C. In conjunction with the conference, the students visit with a senior Department of Defense Chief Information Officer (CIO) at the Pentagon, discuss network security issues with the Pentagon's Computer Network Security Defense team, receive a presentation and tour of the Homeland Defense Office's Critical Infrastructure Protection, and view the 1st Information Operations Command and control center for military computer network defense. There are two trips scheduled in the spring: one is to tour the National Security Agency's Information Assurance operations, and the other trip is to a conference. Last year the students attended the Blackhat conference in New Orleans (http://www.blackhat.com/). The topic of discussion was focused on Windows Security, which proved beneficial to the students in the Cyber Defense exercise. This year the students will attend the SANS conference (http://www.sans.org/).

4. BUILDING FACULTY EXPERTISE

The success of the student experience depends in large measure upon faculty expertise in Information Assurance. Information Assurance, like many areas of computer science, is fast moving and faculty members require constant maintenance to remain current. To facilitate continued development, our program includes an aggressive program of outreach, publication, trips and professional exchanges.

4.1 Faculty Outreach

An important aspect of building faculty expertise in information assurance is the integral outreach activities to government, academia, industry and the local community. The relationships built provide a give-and-take of ideas, professional contacts and possibly even identification of resources or funding. Some of the government agencies involved in the faculty outreach effort are the National Security Agency (NSA), the Defense Advanced Research Projects Agency (DARPA), the Defense Information Systems Agency (DISA), the Army's First Information Operations Command (formerly the Land Information Warfare Activity (LIWA)) and the Department of Defense's Joint Task Force for Computer Network Operations (JTF-CNO). These agencies (and others) have active information assurance programs, and have provided valuable support ranging from simple collaboration through provision of expertise and funding.

Faculty members participate in professional organizations such as the Association for Computing Machinery (ACM), the ACM Special Interest

Group for Security Audit and Control (SIGSAC), the NSA Information Assurance Center of Excellence program, the IEEE Computer Society, the IEEE Task Force on Information Assurance, the Federal Information Systems Security Educators Association (FISSEA), and the National Colloquium on Information Systems Security Education (CISSE). Faculty members also participate in information assurance conferences and work with some of the leading information assurance research centers, in particular Texas A&M University and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue.

There is a growing awareness of the need to pass information assurance principles beyond the professional community to the population at large. Students and faculty members are building information security and Internet safety training packages and plan to teach students at local schools.

4.2 Faculty Publications, Conferences and Trips

Faculty members submit their work to professional journals and to conferences to share their ideas, successes, and lessons learned. Conference participation is the source of new ideas for the information assurance program. Each trip brings both direct and subtle ideas as well professional contacts and exposure that benefit the program. Our institution directs resources to support the widest possible participation by both students and faculty. To the maximum extent possible, funding is provided to send at least one author of an accepted paper to present it and to encourage faculty members to attend IA-related conferences. Participation in such conferences is carefully synchronized with other program activities and the academic year to provide maximum impact.

Several members of the faculty attend the Blackhat conference in Las Vegas with some staying on for the hacker convention, DEFCON (http://www.defcon.org/). The Blackhat Briefings are an excellent source for an update on the current state of the Information Assurance community. Faculty members have participated during the past several years and brought back a wide variety of tools and techniques. The Blackhat Briefings occur several times per year and our faculty members have participated in both the summer and spring offerings. DEFCON provides invaluable cultural exposure to some of the more visible members of the underground hacker community.

It is the program's goal for each computer science faculty member to attend at least one Blackhat and DEFCON conference. Again, this not only stimulates the faculty intellect but also keeps them current with the latest exploits and serves as a motivational tool to emphasize the necessity to continue improving our program. The Blackhat Briefings organization and

DEFCON freely distribute the briefings and tools via their websites. Faculty members frequently use these tools to create in class exercises for the information assurance aspects of their courses.

In addition to trips to other conferences, the ITOC organizes and executes the annual IEEE Information Assurance Workshop. This event has been held for three years and includes presenters who are subject matter experts in a wide variety of IA topics such as wireless networking, honeynets, agent architectures in coalition environments, intrusion detection and response. The conference targets academia, business, and government employees and thus provides a balance between theoretical and practical application of the Information Assurance topics. It has proven to be a very effective means of outreach and interaction with the larger Information Assurance community. This institution is unique in that it selects military officers for advanced schooling with follow-on military teaching assignments. It has proved to be successful to invite the soon to be faculty members and their advisors to participate. More information can be found at www.itoc.usma.edu/workshop.

4.3 Professional Exchange

Sabbaticals: Tenured faculty members are offered the opportunity to participate in a sabbatical once every seven years. Typically of one-year duration, they allow faculty members to step away from traditional responsibilities and gain a fresh perspective by working at another academic institution (even outside the U.S.) or at agencies within the United States government. The most recent participant in the program worked with members of the ITOC to arrange their sabbatical at the National Security Agency working in their research and engineering program. While this is a first attempt at tying in the sabbatical program with information assurance there is much future potential. The insights gathered from working at the front line of information assurance and personal contacts made are expected to prove very valuable.

NSA Fellow: The Department of Electrical Engineering and Computer Science hosts a Visiting Fellow from the National Security Agency. This NSA Fellow brings a wealth of experience and expertise in information security and is actively involved in both the academic and research programs in the department. The current NSA fellow contributed in the following ways:

- taught CS407/CS408 Information Systems Design and CS482 Information Assurance
- directed research in support of the ITOC.

- developed and shared IA curricula with academic programs at other military academies
- participated in the successful effort to obtain NSA certification as a Center of Academic Excellence for Information Assurance Education
- helped establish the annual Cyber Defense Exercise.

Endowed Chair: The Department of Electrical Engineering and Computer Science has an endowed chair (The Adam Chair) that allows the department to bring in a faculty member with significant qualifications in an area of interest. The current occupant of the Adam Chair is actively involved in supporting the research efforts of the ITOC.

5. ORGANIZATIONAL SUPPORT

For an academic information assurance program to be successful it must be supported with adequate personnel, financial, and physical resources. Successful programs also require two additional components—a champion and additional outside help. The IA program at this institution is fortunate to receive adequate resources in each of these areas.

The Information Technology and Operations Center (ITOC) has served as our "IA champion." This center is the driving force behind the success we have experienced. Formally, the center's mission is to "support the educational mission through curriculum development, research, and outreach to the Army that addresses the acquisition, use, management, and protection of information."

With only four full-time and several part-time positions (which include a National Security Agency fellow and chaired professor), the center is a lean organization, but it has been able to accomplish a great deal in tying independent IA initiatives into an integrated whole. The computer and research scientists in the center are responsible for:

- conducting information assurance research
- maintaining outreach programs
- coordinating guest speakers
- maintaining the IWAR lab
- organizing participation in the annual Cyber Defense Exercise
- teaching CS482 Information Assurance
- developing IA course materials for other courses
- having primary responsibility for the IEEE Information Assurance Workshop held each summer

- coordinating faculty and student attendance at IA conferences
- arranging IA educational trips for faculty, staff and students
- assisting in teaching other IA courses or lessons
- providing essential support to the student Information Warfare club (ACM SIGSAC)
- coordinating IA related student internships and faculty sabbaticals

The center's staff is augmented by support from faculty and staff of the Department of Electrical Engineering and Computer Science and others from across the institution and country in support of their IA program. These "augmentees" support the Information Warfare club, organize IA trips, assist in coordinating summer internships, assist in the planning and execution of the IEEE Information Warfare Conference, conduct IA research and arrange for guest speakers.

We are deeply indebted to the support and resources provided by the National Security Agency (NSA) which include a full-time fellow, co-sponsorship of an annual IEEE Information Warfare Conference, an annual student and faculty "field trip" to visit NSA headquarters, NSA summer student internships, sponsorship of the annual Cyber Defend Exercise, program certification through their Information Assurance Centers of Excellence program, and research assistance.

In addition to resources provided by the institution and NSA, several other organizations have been extremely supportive in establishing a viable IA program. These include the Defense Information Systems Agency, the Department of Defense Joint Staff, and several Department of Defense program and project managers.

6. FUTURE WORK

The IA program continues to evolve and improve as lessons from past experiences are learned. There is a large amount of future work that needs to be done across all aspects of the program, to include:

- Establish a fellowship program for recent top information assurance graduates in order to allow these graduates to continue their education
- Develop "IWAR in a box" — create a virtual IWAR laboratory inside a single computer.
- Implement Honeypot within the IWAR lab in order to capture live attacks.
- Expand the Cyber Defense Exercise to include coalition forces and insider attacks.
- Increase the number of summer internships and include stints at Computer Emergency Response Teams (CERTS) located around the world.
- Continue education of faculty members from all academic departments

7. CONCLUSIONS

This paper described the methodology, implementation and results from the creation of a comprehensive undergraduate information assurance program. The interdisciplinary approach is very successful in reaching a large portion of the student body and faculty. The overall program of mutually supporting information assurance activities is successful in fostering a high degree of learning by both students and faculty. Hopefully this will prove useful to other undergraduate institutions considering the development of their own information assurance program.

DISCLAIMER

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense or the U.S. Government.

REFERENCES

Spafford, Eugene H. (1997). "One View of A Critical National Need: Support for Information Security Education and Research." Testimony Before the US House of Representatives Committee on Science. Washington, DC, February 11.

Bishop, M. 2000. "Academia and Education in Information Security: Four Years Later." Fourth National Colloquium on Information System Security Education, Washington, DC.

Schou, C., D. Frincke, et al. 2000. "Meeting the Information Assurance Crisis - Now." EDPACS: The EDP Audit, Control, and Security Newsletter.

Office of the Dean. "Educating Future Army Officers for a Changing World." United States Military Academy. Available online [accessed December 24, 2002] at http://www.dean.usma.edu/AAD/EFAOCW.pdf

Office of the Dean. "Computing@West Point." United States Military Academy. Available online [accessed December 29, 2002] at www.dean.usma.edu/dean/computingatwestpoint

Ray, C. "Computer Science Program." United States Military Academy. Available online [accessed December 29, 2002] at www.eecs.usma.edu/programs/cs/default.htm

Dudevoir, G. "Electrical Engineering Program." United States Military Academy. Available online [accessed December 29, 2002] at www.eecs.usma.edu/programs/ee/default.htm

Blair, J. R. S. "Information Systems Engineering Program." United States Military Academy. Available online [accessed December 29, 2002] at www.eecs.usma.edu/programs/ise/default.htm