2006-2004: INFORMATION ASSURANCE FACULTY DEVELOPMENT WORKSHOP

Douglas Jacobson, Iowa State University

Dr. Doug Jacobson Associate Professor Department of Electrical and Computer Engineering Iowa State University Ames, IA 50011

Thomas Daniels, Iowa State University

Dr. Thomas Daniels Assistant Professor Department of Electrical and Computer Engineering Iowa State University Ames, IA 50011

Information Assurance Faculty Development Workshop

Abstract

The Information Assurance Center at Iowa State University received support from the National Science Foundation to create an "Information Assurance Educational Support Program." Faculty members from universities in the Midwest participate in an intensive workshop on information assurance and security education, with the goal of introducing security concepts into courses in their academic departments. Participants were given access to streaming media version of the lectures from four of our core security classes. They also received support material to help integrate the subject material into their existing courses. Our target audience includes faculty members who are teaching computer science, computer engineering, information systems, or related fields, and are committed to initiating education or research efforts in security in their own departments. We have offered the workshop four times to a total over 60 faculty members from around the United States. This paper will describe the workshop, the intended outcomes, feedback from the faculty involved, the curriculum, and future plans. We will also discuss issues related to recruiting faculty, integration of faculty with different backgrounds, and ongoing faculty support.

Introduction

The growing need for information security professionals is well documented. Few universities offer a comprehensive program in information assurance and security. The end result is a severe shortage of graduates proficient in the technology and policy issues critical to the security of the information infrastructure. While several universities have started programs to address these needs, this only solves a small part of the problem. According to the National Strategy to Secure CyberSpace[1] released by the President of United States in 2003, "Many cyber vulnerabilities exist because of a lack of cyber security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers, chief executive officers, and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructure regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities." In response to the national need to increase the number of graduates who are knowledgeable about security issues, Iowa State University and its Information Assurance Center created the Information Assurance Educational Support Program.

The Information Assurance Educational Support Program provides an opportunity for faculty from other universities to receive an education in information assurance with the goal of being able to teach the core concepts to their students. Participants engage in a two day workshop during the summer designed to explore the issues associated with teaching information assurance, and to provide assistance in developing new courses or integrating security concepts into existing courses. As added help, we provide access to several of our core graduate security courses that are offered via distance education. This includes the videotaped lectures offered through streaming video, on-line chat room support, lecture notes, lab experiments and sample test questions.

The Information Assurance Educational Support Program is synergistic with existing instructional activities at Iowa State University. Four of the core graduate security courses have been offered to a national audience via the Iowa State Engineering Distance Education unit since 1995. In addition Iowa State University offers two graduate degrees in information assurance. A masters of Science in Information Assurance and a 4 course graduate certificate in Information Assurance. Both of these degrees can be obtained via the distance education program[2]. We have found a growing demand over the years for access to the courses from constituents in industry, the military, and even other Universities. The Iowa State University faculty members offering these courses have several decades of experience in distance education and the courses have been designed with distance education in mind. ISU faculty members are also participating in development of national standards for security education and were named as a Charter Center of Excellence in Information Assurance Education by the National Security Agency in 1999.

Our initial target audience for the Information Assurance Educational Support Program is faculty members from four year colleges and universities who are teaching computer science, information systems, or related fields and have a working knowledge of computers.

Workshop Structure

The workshop has three basic components namely, the on-site face-to-face interaction, the instructional materials, and the post-workshop ongoing support. Our initial goal was to have teams of faculty with at least two faculty members from each institution participle in the program each year. The workshop targets faculty members from four year colleges and universities, but we do not limit participation to only these schools.

The funding for the workshop was received in 2001 and during the fall and spring of 2001/2002 the Iowa State University faculty team prepared the course material for the workshop and also developed (with the help of the graduate students) supplemental instructional material for the participants. The workshop is taught by several faculty Iowa State University faculty members. In 2002 the first workshop was held and Iowa State University faculty members facilitated the workshop along with several graduate students.

During our first year the workshop drew twelve faculty members to Iowa State University. The goals of the workshop were:

- To bring participants up to speed on key security concepts and issues taught in our core courses
- To work with participants in finding ways to integrate important security concepts into their own courses
- To work on lab development, support, and funding ideas
- To develop a cohort of faculty that can help support each other
- To provide access to the Iowa State courseware modules and on-going support mechanism

Each faculty member received a $500 stipend in addition to travel costs. At the conclusion of the workshop, participants received access the course lectures and supporting material for the following courses: CprE 531 Computer System Security, CprE 530 Advanced Protocols and

Network Security, CprE 532 Information Warfare, CprE 533 Cryptography. One option is simply to view archived lectures from past semesters. However, we invited and facilitated participants to actually take the courses along with distance education students during the semesters the courses are offered. This gives them access to student chats and other information in real-time so that faculty participants can experience the range of issues that arise during the semester that are not reflected in printed material.

Workshop curriculum

The workshop curriculum is delivered over an intense two full day period. We rely on the fact that participants are already accomplished faculty in a related discipline, which allows us to focus on pedagogy, advanced security topics, and the logistics of building a program. We view the workshop as the start of the process; participants see a "proof of concept" and tailor it for their environment and goals. Much of the "learning" then takes place as participants actually develop their own courses or adapt our material for their classes.

Over the four years the workshop has been held the focus of the workshop has shifted from discussions on course content to a lab based focus. All of our security courses at Iowa State University have labs. Several of the courses (see course descriptions in a later section) are very lab focused and the same labs are offered to both on campus and off campus students. We believe the labs make our distance education Masters degree unique. The last two workshops focused on how to create and teach information assurance labs. The curriculum for the workshop consisted of presentations from the faculty members that teach the courses. The faculty created power point presentations that were included in a notebook that was given to every participant. We also included in the notebook a course syllabus and copies of labs experiments for each course.

The workshop schedule for the 2005 workshop is shown below. The focus of the 2005 workshop is lab exercises for computer security courses. The first morning starts with introductions and a survey from the participants gathering information about their programs. The remainder of the day focuses on eight of our security courses and the laboratory exercises. Intermixed with the course presentations are discussions of the high school computer security summer camp and the cyber defense exercise offered by the Information Assurance Center. In the evening we have a dinner with a speaker and a poster session highlighting research projects at Iowa State. The second day provided tours of the teaching and research labs and after lunch a we discussed one additional course. We finished the workshop with a discussion on academic issues, such as obtaining buy-in for computer security as an area of emphasis, and current opportunities for funding and publishing scholarship. We also obtained feedback about what to do next year and how to keep the workshop going after the funding has ended. At the end of the paper we will discuss the future of the workshop.

2005 Workshop schedule

Date/Time	Activity
Sunday, July 10	
6:00 PM	Welcome Reception
Monday, July 11	
7:30 AM	Breakfast/sign in
8:15 AM	Opening remarks
8:30 AM	Participants Program Survey
8:45 AM	Participants Introduction
9:00 AM	Courses 431 & 531 (Introduction to security)
10:30 AM	Break
10:45 AM	Courses 530 & 532 (Network security & Information warfare)
12:00 PM	Lunch
1:00 PM	Computer Security Camp
1:30 PM	Course 535 (Steganography)
2:00 PM	Course 534 (Ethics)
2:30 PM	Course 537 (Wireless Security)
3:00 PM	Break
3:15 PM	Course 536 (Forensics)
4:00 PM	Cyber Defense Competition
5:00 PM	Wrap up of the day
6:00 PM	Dinner and Poster Session
8:00 PM	Tour of ISEAGE
Tuesday, July 12	
7:00 AM	Breakfast
7:45 AM	Travel to campus
8:00 AM	Teaching Laboratory demonstration and tour
9:00 AM	Research Lab
10:00 AM	Forensics Tour Lab
10:30 AM	Distance Education facility tour
12:00 PM	Lunch
2:00 PM	Course 533 (Cryptography)
2:30 PM	Post Workshop Survey
3:15 PM	Round Table
4:30 PM	Wrap Up/What to do 2006
5:00 PM	Adjourn

Course descriptions

A brief description of the courses the participants discussed in the workshop is provided below. For these courses we provided the participants power point slides of the lectures, sample

homework problems, lab experiments, and test questions. In addition we also provide access to the streaming media lectures for the courses offered via distance education (these courses are noted below). The major labs experiments for each course are also listed below and were the focus of the discussion during the 2005 workshop.

1. CprE 530 Advanced Protocols and Network Security

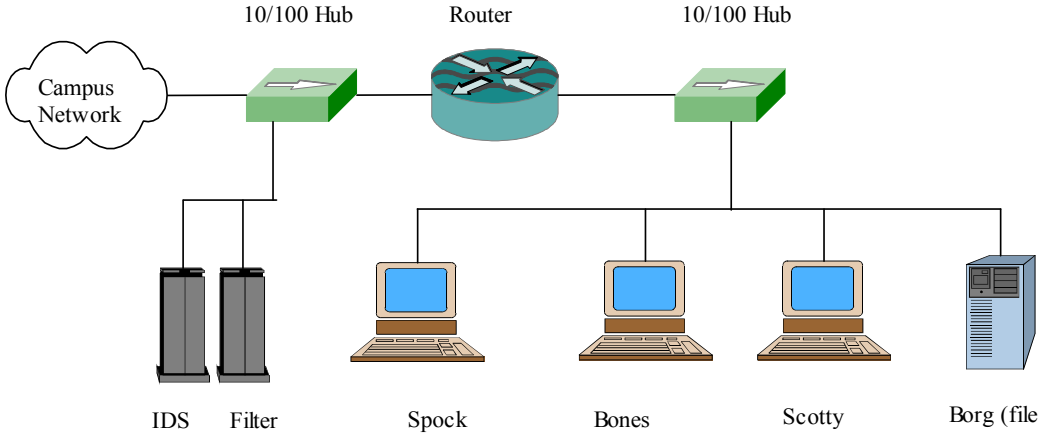
Textbook:

TCP/IP Protocol Suite Second Edition, Behrouz A. Forouzan, McGraw Hill
Course Description:

Design, implementation, and analysis of computer networks and data communications systems. Detailed examination of modern communication standards, protocol systems and their implementation. Transmission technology, packet switching, routing, flow control, and protocols

Lab experiments:

Computer Engineering 530 has a several canned lab experiments where the students have a defined set of activities that are designed to reinforce the lecture material. These include looking at routing tables and network traces, interacting with email and web serves directly, and using DNS. The class also includes 4 programming assignments where the students write a packet sniffer program. The first three programs build on each other and have the students decode the packets they get from an isolated network. The fourth program has the students writing code to send spam email. The figure below shows the test bed network used for CprE 530.



CprE 530 Test bed Network.

2. CprE 431: Basics of Information System Security

Textbook:

Security in Computing, 3rd ed. by Charles Pfleeger and Shari Pfleeger, Prentice Hall 2003. ISBN 0-13-035548-8

Goal:

This is our undergraduate security course. It surveys the basics of information security. It is open to undergraduates with credit or enrollment in an operating systems and networking class. This is primarily composed of senior computer engineering students. Our focus is on the application of principles in practical system administration and programming exercises.

Course Description:

Introduction to and application of basic mechanisms for protecting information systems from accidental and intentional threats. Basic cryptography use and practice. Computer security issues including authentication, access control, and malicious code. Network security mechanisms such as intrusion detection, firewalls, IPSEC, and related protocols. Ethics and legal issues in information security. Other selected topics. Programming and system configuration assignments.

Laboratory Experiments and Homework:

Developed in Spring 2005, our CprE 431 experience led us to the realize that we needed a scaleable, inexpensive method of providing homework environments to many students. Hence, we are developing an open source system to provide entire network environments of multiple virtual machines to every student in the class. In 2005, we developed the first prototype based on the Xen 2.0 hypervisor system developed at University of Cambridge. The prototype used a single 2GB Pentium 4 machine (2.8 GHz) to provide 35 students with one virtual machine each. Projects included development of file system configurations based on policies, network sniffing and scanning, and vulnerability exploitation on hosts.

3. CprE 531: Information System Security

Textbook:

Computer Security Art and Science, Matt Bishop, Addison and Wesley, ISBN: 0-201-44099-7

Course Description:

Computer and network security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

Goals:

Introduce graduate students to basic cryptography and applied theory in information security. This is a variant of CprE 431 except more access control and multilevel security theory is covered.

Laboratory and Homework Experiments

Students do written assignments regularly and typically do a large 10-15 page paper on one of several topics. Future work may integrate the Xen testbed.

4. CprE 532 Information Warfare

Textbook:

Hacking Exposed, 4th ed, McClure, Scambray & Kurtz, McGraw-Hill Osborne Media, ISBN: 0072227427

Goal:
This is the second course in a sequence. This course is intended to provide students with hand-on experience in installing, configuring, and testing state-of-the-art security software and hardware. Methods of attack will be examined to better understand how to detect and prevent attacks.

Course Description:

Computer Systems and network security: implementation, configuration, testing of security software and hardware, network monitoring. Computer attacks and countermeasures. Emphasis on laboratory experiments.

Lab experiments

The information warfare course looks at computer security from an attack/defend standpoint. We spend the first couple of weeks in class looking at the processes attackers use to identify, study, and then attack a system or network. We develop our own process for attacking computer systems. We also look at risks and potential effects of information warfare on computer systems and critical infrastructure. We then spend the next 6 weeks looking at various subsystems and protocols used in a typical information system. A topic will be introduced like authentication and the attack methodologies will be studied. That will be followed by looking at various defense mechanisms. During this time there are numerous lab experiments which help drive home the concepts introduced. Some of the lab experiments have the students actively probing networks and gaining information that could be used in an attack. About two thirds of the way through the course the break-in lab is assigned. After the break-in lab we spend time looking at the results and studying the defenses used by the company.

The labs for CprE 532 are listed below. The break in lab[3] is described in more detail.

Lab 1 find out everything they can about ISU's network from only public information

Lab 2 Scan an isolated subnet
Lab 3 Crack password & S/Key
Lab 4 Kerberos
Lab 5 Email spoofing & PGP
Lab 6 SSH
Lab 7 Web Security
Lab 8 Break-in lab

The major lab experiment in CprE 532 is the break in lab where students have three week to try and break into a company network designed for the class. The lab assignment is shown below:

Using (bones.ee.iastate.edu or spock.ee.iastate.edu) and any of the tools we have discussed during the class (both installed on bones/spock and those that have not been installed) perform the following:

Break into the computers belonging to the company 532 Corp (domain 532corp.issl.iastate.edu)

The goals are:

- Obtain as many user names and passwords as you can
- Obtain any files ending with .secret that are found in the users home directories. Some maybe encrypted and should be decrypted if possible.
- Obtain any diagrams of the corporation network

Turn in the following:

- The user names and passwords for all users on each of the machines you broke into.
- The step by step method used to gain access to and decode the files. List both successes and failures and the time required to obtain and decode the files.
- Provide a detailed description of how you would plug the holes you found along the way.

Notes:

- There are many methods to gain access to the computers in the 532 corporation. I have intentionally left several security holes in place.
- There are several machines on the network 129.186.215.0 which are possible targets. Please limit your attacks only to machines in the 532corp.issl.iastate.edu domain.
- You will not be able to get all passwords for all users.
- Also do not change any files on the machines or leave behind files. The goal is to break in undetected.
- This lab should be worked on individually. You should NOT discuss methods or solutions with other students.

- You may not be able to solve the problem completely. Turn in what you have finished.

5. CprE 533 Cryptography

Textbook :

Cryptography: Theory and Practice, 2nd ed, Stinson, Douglas, CRC Press, ISBN: 1584882069

Introduction to Cryptography with Coding Theory, Trappe, Wade &Lawrence Washington, Prentice Hall, ISBN: 0-13-061814-4

Course Description:

This course will cover the basic concepts of secure communication. Secret-key and public-key cryptosystems. Zero-knowledge proofs, key distribution, hash (a.k.a. message digest) algorithms. The relevant number-theory will be covered in class.

Course Learning Objectives:
Upon completion of this course, a student will understand the mathematical foundations of common cryptosystems: why they work, how the security of the system is tied to the underlying structure, and how different systems are related. The student will be able to evaluate a cryptosystem from the standpoints of security and practicality. A student will understand how the component parts of a cryptosystem work together to create a secure environment.

6. CprE 534 Legal and Ethical Issues in Information Assurance

Text Book:

Case Studies in Information Technology Ethics by Richard A. Spinello
Many other readings from the web are selected by students.

Course Description:

Legal and ethical issues in computer security. State and local codes and regulations. Privacy issues.

Students perform reading and writing assignments on ethical issues as well as contemporary legal issues in information assurance. Groups of students present issues to the class.

7. Math/ CprE 535 Steganography and Watermarking

Textbook:

Course Description:

Basic principles of steganography and watermarking. Algorithms based on spatial domain approaches, transformations of data, statistical approaches. Techniques for images, video, and audio data. Communications models for data hiding. Analysis, detection and recovery of hidden data. Military, commercial and e-commerce applications. Known theoretical results. Software packages for data hiding. Social and legal issues, case studies, and digital rights management issues that affect technological development of steganography and watermarking. Current developments in the area.

Lab Experiments:

The students use public domain software to hide data within images. They also MatLab to study the math behind the concepts introduced.

8. CprE 536 Computer and Network Forensics

Textbook:

Course Description

Fundamentals of computer and network forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity and pseudonymity, privacy-protection techniques, cyber law, computer security policies and guidelines, court testimony and report writing, and case studies. Emphasis on hands-on experiments.

Lab Experiments:

This course uses the cyber forensics lab at Iowa State University for several lab experiments. Students use public domain software to analyze digital media. They also use commercial software from Guidance Software[4] to analyze disk images. The only drawback to using the commercial software is the hardware license system, where the software can only be run on a machine with a USB key. This was not a problem until the course was offered via distance education. In order to give the remote student access to the lab the faculty member had to install the software on machines running windows terminal server. He then needed to have a signup system to insure only one student used the software at once. The cost of the software limited the number of computers that could be used for the lab.

9. CprE 537 Wireless Network Security

Course Description:

Introduction to the physical layer and special issues associated with security of the airlink interface. Communication system modeling, wireless networking, base stations, mobile stations, airlink multiple access, jamming, spoofing, signal intercept, wireless LANS and

modems, cellular, position location, spread spectrum, signal modeling, propagation modeling, wireless security terminology.

Workshop recruitment

The primary target of recruitment is universities and colleges in the Midwest because we have a large network of contacts in the region; however participants are welcome from any university. Recruitment is handled in a variety of ways including, direct contact with CS, CprE, and MIS department chairs, and advertising brochures mailed to departments. Information and registration was made available through a web site. The first year we sent out invitations to CS departments in the Midwest and had twelve faculty members enroll in the workshop. The second year, we also emailed invitations and Iowa State faculty members gave presentations at regional conferences. The result was an increase to nineteen participants. The table below shows the number of participants each year of the workshop. Over the four years of the workshops the participants represented 26 different colleges and universities. The cost to hold each workshop is about $1000 per attendee.

Year	New Attendees	Returning Attendees	Total
2002	12		12
2003	18	1	19
2004	12	6	18
2005	9	6	15

Participating University Commitment

The participating universities are asked to commit to the following:

- Provide time for the participating faculty members to view the courses
- Offering new information assurance and security courses or add security topics to existing courses
- Release time to attend the summer workshop

To date, this level of commitment has not been an issue for participating Universities.

Ongoing support

The goal of the project is to establish a mechanism to provide on going support to the participants via the web, and through continued personal contact. A web site will be maintained that will support a chat room, on line help, an email list server, and access to the courseware modules. We will also provide on going assistance to help the participants develop laboratories to support the courses and will assist in assessment, by posting experiments, tests, quizzes and other materials to the web site for use by the participating faculty.

Feedback and lessons learned

The four workshops held thus far have been successes. In every case, participants from the four-year Universities have been able to create new courses or introduce security into an existing course. A few of the faculty members have written successful NSF proposals to secure funding

to expand their emerging security programs. Feedback has been strongly positive. One requested change was to allocate more time workshop time for a dialog on the politics and logistics of creating a new security area in a department. We made that adaptation in the second year, which was well received by attendees. There was also a concern expressed about better articulating the prior knowledge needed by students for each of the courses. For example, some participants were concerned that the curriculum for our cryptography course required a more mature mathematics background than students might normally have; similarly, the first security course assumes that incoming students have a solid understanding of operating systems and software engineering principles. In response, we have endeavored to look at the content of our courses in terms of skills and knowledge rather than prerequisite courses.

A New Conference in Information Security Education

With a modest reserve of funding, we chose to devote a portion of the fourth workshop to finding ways to continue this activity so that it is self-sustaining. Although the participants agreed that NSF support for their attendance was very desirable, another option was agreed upon—the formation of an academic-oriented conference for dissemination of information security education research. In September 2006, Iowa State will host the First Annual Conference on Education in Information Security (ACEIS)[5]. With approval from NSF, we will devote the remaining workshop funds to the conference.

ACEIS will accept peer-reviewed papers on all aspects of education in information security and assurance education. ACEIS will publish accepted papers in a printed proceeding with the goal of inclusion into either the IEEE or ACM digital library. We hope that this gives faculty in the area a valuable archival publication venue thereby allowing faculty to demonstrate their scholarship in security education. Eventually, this will improve the overall state of education in the area as well as make scholarship in the area more compatible with promotion and tenure processes.

Acknowledgements

We would like to thank our colleagues who have contributed to the workshop: Clifford Bergman, Johnny Wong, Barb Licklider, Jan Wiersema, Steffen Schmidt, Yong Guan, and Jim Davis. The material is based upon work supported by the National Science Foundation under grant No. DUE-113549.

Bibliography

1. Federal Government "The national strategy to secure cyberspace", http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf, February 2003.
2. Engineering Distance Education Program www.ede.iastate.edu
3. Doug Jacobson, "Teaching Information Warfare with a Break-in Laboratory", Proceedings of the 2004 American Society for Engineering Education, Salt Lake City, June 2004.
4. Guidance Software http://www.guidancesoftware.com/
5. ACEIS website at http://www.aceis.org/