Session 2422

Development of a Graduate Certificate in Information Assurance

Dr. Doug Jacobson
Department of Electrical and Computer Engineering, Iowa State University

The growing need for information security professionals is well documented. Very few universities offer more than a single cryptography course, and even fewer engineering departments have a presence in this area. 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 need to for additional education Iowa State University and its Information Assurance faculty created an Information Assurance graduate Certificate Program. Since the creation of the MS degree in Information Assurance there has been a large demand for several of the courses by computer professionals who already had an advanced degree or who are not interested in the MS degree. As part of its land grant mission Iowa State University created a special graduate degree called a certificate which consists of at least 3 graduate courses. Students completing an Iowa State University certificate program receive this indication on their transcripts and receive a paper certificate.

In November 2000, Iowa State University created an interdisciplinary Information Assurance Center[2] with faculty from technology-based disciplines as well as the liberal arts and sciences. Then, as now, the center represented several departments across campus including: Electrical and Computer Engineering; Mathematics; Political Science; Management Information Systems; Industrial and Manufacturing Systems Engineering; Educational Leadership and Policy Studies; and Computer Science. By bringing together faculty members from these disciplines, Iowa State is able to respond to the needs of students and the priorities of funding agencies. The center was designated as a charter Center of Excellence in Information Assurance[3] by the National Security Agency in 1999. The Information Assurance Center provides opportunities for education, research, and outreach to government, business, and academic institutions worldwide. The Information assurance center is the administrative unit for the certificate program.

General description of the graduate certificate

The Information Assurance Graduate Certificate Program provides an opportunity for students to receive in-depth education in information assurance. The certificate was established in fall of 2001 and the courses are offered through Iowa State University's Engineering Distance Education (EDE) office[4], and to students on the ISU campus. The certificate consists of four graduate courses in information assurance. The courses are: CprE 530 Advanced Protocols and Network Security, CprE 531 Information System Security, CprE 532 Information Warfare, and CprE/Math 533 Cryptography. A description of each of the courses is provided at the end of this paper.

Objectives of the graduate certificate.

Students obtaining the graduate certificate will help to fill the current and future needs for well-educated system security specialists in the government, private sector, and academia.
The following program objectives are identified as being critical to the accomplishment of this mission:

- Impart and enhance knowledge about information infrastructure security
- Expand and develop engineering abilities
- Instill and nurture a sense of ethics
- Develop an understanding of strategic and policy issues.

Individual course objectives are provided as part of the course descriptions included at the end of this paper. It should also be noted that these courses meet the government Federal NSTISSI[5] training standards.

Graduate certificate requirements

Our target audience is students who have a BS in Computer Science, Computer Engineering or closely related field. Students can receive the courses locally and via ISU's EDE program. The delivery consists of either video taped lectures, streaming media (available in real-time), or CD-rom. They also receive on-line support through an on-line help desk, chat-rooms, emails, and phone. Several of the courses offer a hands-on learning experience where the students are able to perform experiments and use software systems remotely through the Internet. The admission to the certificate program is through an admission committee consisting of the same faculty members who oversee the admission to the MS in Information Assurance.

The primary prerequisite for admission to the graduate certificate program is a baccalaureate degree in engineering, computer science, mathematics, management information systems, or closely related field. Potential students with baccalaureate degrees in the physical sciences, statistics, or other related fields will be considered on an individual basis, possibly with provisional admission.

Applicants with undergraduate degrees from accredited curricula who are in the upper half of their graduating class are eligible. Graduates of non-accredited curricula may be considered for admission if they meet all other requirements and show outstanding potential for graduate study. Graduates of accredited curricula who fail to meet some admission requirement but otherwise show outstanding potential may also be considered for admission.

If a person who receives a graduate certificate decides to continue for a graduate degree, the person needs to seek approval from that degree program. Credits earned for the graduate certificate may also be used to meet degree requirements for the graduate degree if approved by the Program of Study Committee. If the student wishes to continue and get an MS in Information Assurance they must be admitted to a home department and to the IA degree program.

The certificate can be taken by students on campus or off-campus. A majority of the students enrolled in the certificate program are distance education students who are currently employed. The certificate was designed to be obtained in as little as 2 semesters. The two most common options are:

9 month program:

Fall Semester

- CprE 530 Advanced Computer Networking
- CprE 531 Information System Security

Spring Semester

- CprE 532 Information Warfare
- CprE 533 Cryptography

2 year Program:

Fall Semester (Year 1)	CprE 531 Information System Security
Spring Semester (Year 1)	CprE 532 Information Warfare
Fall Semester (Year 2)	CprE 530 Advanced Computer Networking
Spring Semester (Year 2)	CprE 533 Cryptography

Course Delivery

The courses are taught on campus in the EDE classrooms. These rooms hold 60 students on campus and have a series of video cameras, microphones, SmartBoards, and other advanced instructional technologies operated by trained student technicians. The faculty member teaching the course has access to computers for presentations and the cameras can capture the faculty member's notes from either the Smartboard or from an overhead camera shot. In addition the on campus students can view what is being shown on the video stream on several large monitors located around the room. The EDE staff has also created a chat room that can be used by off-campus students to ask questions while the lecture is taking place. However, only a handful of students use this while most students choose to view the lectures at a later time. The only drawback to the chat room system is that the video stream is delayed about 30 seconds, plus the time it takes a student to type the question, the faculty member has often gone beyond the point of the question and on to a new topic. Most faculty do make the streaming lecture available to

on campus students, either the same day or a week delayed. The other limitation is the room size, Information System Security is very popular course for on campus students and we have had to limit enrollment to 60 because of the classroom size.

Issues

There have been many issues that have surfaced since the program was started. The first year of the program we had only a few students who showed interest in the program and we thought we were going to have a hard time getting students. The four courses were already being taught via distance education and had off campus enrollments ranging from 10 to 40. Advanced Computer Networking has been taught to off campus students since the course was created in 1980. Information System Security and Information Warfare have been taught to off campus students since they were created in 1995. Our first few students who enrolled in the certificate program had already taken one or more of the courses and were planning on taking most of the courses anyway. We tried several different things to get interest including making presentations at several regional business meetings. Iowa State University also issued a press release which was picked up in several newspapers.

Unfortunately this led to a problem that we did not anticipate. Since computer security is seen as a hot field we had many inquiries from students that were not well qualified and in some cases did not even have a baccalaureate degree. There was also some confusion over a graduate certificate offered by a university and certification like Microsoft or Cisco. To help overcome this problem we created a web site[6] to help clarify the admission requirements. After the first year we had about 7 students in the program and had graduated two. We continued to try and get the word out about the program by sending emails to any student that had taken one of the courses in the last couple of years. We now have over 20 students in the program and have graduated 7.

Another issue that surfaced was students trying to use the certificate program as a way into the M.S. program. We have had a couple of students who were denied admission to the M.S. in Computer Engineering program that then applied to the graduate certificate program. Due to the very large number of applications to the M.S. in computer engineering program their admission requirements are higher than the certificate program. The students figure if they can take a couple of computer engineering classes and do well in them they can get admitted to the M.S. in computer engineering program. We have started to work closely with the computer engineering department and have included letters to students indicating that admission and completion of the certificate is no guarantee for admission to the M.S. in computer engineering program.

Increased marketing has led to increased off campus enrollment, which was to be expected but does pose a problem for the instructors of the courses. The two courses with the highest off campus enrollments are Information System Security and Information Warfare, each with typically over 60 off campus students. The former has several large projects which creates a grading increase for the instructor. The department has provided Teaching Assistants (TA) to help with the overload. Information Warfare has a lab component with one large “break-in” lab that lasts several weeks. Since the labs are all designed to be accessed over the internet the problem is not with the number of seats in the lab, but just with the shear number of students

accessing the computers and performing the labs. The lab requires constant monitoring and several times each week during the semester the instructor must fix problems at night or on the weekend. The other two courses have also seen an increase in enrollment. Cryptography has an off-campus enrollment of over 30 and this course also has a TA. Advanced Computer Networking also has a lab component, but to add to the difficulty the course is offered three times a year. In the fall semester it is taught live to over 60 on-campus students and to over 40 off-campus students. During the spring and summer semesters the course is replayed to off-campus students. Occasionally on-campus students are given access to the off-campus version during the spring or summer semesters. These are often undergraduate students who are graduating and could not fit the course into their schedules during the fall semester. Offering the course three times a year creates its own set of problems since the lab for this course must be kept running all year long and the faculty member must deal with student questions and grading all year. Typical enrollment for Advanced Computer Networking during the spring is 20 and about 10 in the summer. One advantage to offering this course in the spring semester is that students can start the certificate program. We found they often did not want to start with the Cryptography course and since Information Warfare has a prerequisite of Information System Security, they had to wait until fall.

We have also discovered that by using the message board feature of our web course management tool, WebCT[7] , the students interact with each other outside of class. This is used primarily by the off-campus students, but with encouragement by the faculty members we have been able to get on-campus students using the system. The students start talking about issues and problems, and many times we find that the students answer their own questions. This helps connect the off-campus students with the on-campus students making for a richer classroom environment. I have had cases where the off-campus students have talked about their personal experiences in the discussion rooms, which have benefited the on-campus student experience.

Another set of problems are due the large number of undergrads who take these courses as technical electives. While it is not a problem to have these students in class, it is a problem if they wish to get either the certificate or the MS in Information Assurance, since they can not count the courses twice. The undergraduate advisors have started to ask students wishing to enroll in these courses if they are interested in graduate school. In which case they are advised about the issues and can make informed decisions. We do allow one substitute course in the certificate program. The newest problem with the undergrads is that a couple of them want to take the four courses for the certificate while they are enrolled as an undergraduate and get both a B.S. and the graduate certificate. Often they can do this with only one additional semester. Iowa State has a process for students to dual enroll in a B.S. and M.S. program. We have now started to allow students to dual enroll in a B.S. and certificate program.

The last issue is the way in which Iowa State distributes the money received from distance education fees and tuition. The faculty member is paid extra compensation based on the number of off campus students which works out to about $100 per student. The departments are given about $300 per student out of which they pay the faculty. Since this program is administered by a university center it does not get access to the money to help defer the cost of administration or to help with up keep of the labs.

Since the program was started we have made several changes some of which were outlined above. We have made a few additional changes to help make the program work better and to help meet demand. We just added another course to the list of possible courses. The course is entitled "Digital Data Hiding". This is a new course that can be used to replace Cryptography. Cryptography presents the biggest challenge to our students who have been away from math for many years. To address this issue, the instructor has created a set of on-line (streaming video) bridging lectures to review fundamental math concepts important for student success in the course.

Despite these challenges, we have seen a steady increase in the number of students applying to the program and an increase in the number of inquiries.

Conclusions

Since starting the program we have experienced some problems that we anticipated and several problems we did not. The program has increased off-campus enrollment in the courses which has increased revenues to the academic departments and the EDE office. The department of Electrical and Computer Engineering has since started a certificate in power systems engineering that is also offered to off-campus students. There has been discussion about creating additional certificate programs to help recruit students.

As someone who teaches two of the courses (Advanced Computer Networking and Information Warfare) I have seen several benefits to having the certificate program. The first benefit is the experience level the off-campus students bring to the classroom. In the Information Warfare class I often have off-campus students that are working in computer security helping to defend a company network. They contribute to the classroom discussion via the chat room and via the WebCT discussion board. They also provide additional feedback via email in the form of actual events they have seen or issues they have confronted which I have been able to share in class. The off-campus students also provide contacts into companies which can help in developing research partnerships. A few of these students do plan to go on to get an M.S. degree. Of course as we get more students in the certificate program they will tell others in their company about the experience which will further increase enrollment.

Another benefit of the program is not as tangible, but in the era of increased budget cuts by the state and increased pressure to show how the university can help the state. This program has been highlighted as a benefit to the state.

All things considered the graduate certificate program has a positive effect on the university and on the classroom and is a model that should be adopted by other universities looking to increase enrollment in distance education programs. For Iowa State which was already teaching the course via distance education the additional overhead of offering a certificate program is minimal.

The detailed course outlines are provided below.

Course descriptions

CprE 530 Advanced Protocols and Network Security

Textbook:

TCP/IP Protocol Suite Second Edition, Behrouz A. Forouzan, McGraw Hill
ISBN: 0-07-246060-1

Course Length: 45 hours in 15 weeks, 2 75-minute meetings per week

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

Course Learning Objectives:

Upon completing this course a student will:

- Understand the relationship between network layers, network services and functions.
- Understand the function of each of the layers in the TCP/IP protocol suite.
- Be able to describe the TCP/IP network protocols and the effect of an open network protocol on security
- Be able to snoop traffic from a network and decode the data
- Be able to write programs the use the TCP/IP socket level interface.
- Understand the tradeoffs used in the design of the network protocols
- Be able to setup routing table for IP
- Be able to describe the functions of the packets used in each of the upper layers
- Be able to describe the function of each of the packets in the most common TCP/IP applications

Major Topics:

- Introduction
- Data link Layer
- Network Layer
- Transport Layer
- Sockets
- Application Layer

- System Issues
- IPv6

CprE 531: Information System Security

Course Length: 45 hours in 15 weeks, 3 one-hour meetings per week

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.

Course Learning Objectives:

Upon completing this course a student will:

- Understand the varied types and sources of threats to computer security
- Be able to choose appropriate security mechanisms given the value of the data and the types of threats anticipated
- Understand the different categories of cryptographic algorithms and be able to explain or demonstrate the underlying mathematical problem they are based on, explain their strengths and weaknesses, and determine appropriate uses
- Understand authentication and access control, as implemented in different information models and real-life operating systems. Be able to analyze a real computer system and note exploits in the authentication and access control policies and implementation that could lead to a security exploit.
- Understand the capabilities and limitations of contemporary security technology and determine it's appropriate use.
- Understand local and state code, and rules of evidence, as it pertains to computer crime
- Understand the issues the various perspectives in the ongoing debate about security and privacy

Major Topics:

- Sources for security threats; risk analysis; appropriate reactions
- Cryptographic techniques: alphabetic ciphers, one-time pads, block ciphers, etc.
- Secure encryption systems: RSA, DES, Clipper, public and private key systems
- Key exchange schemes and more elaborate protocols (arbitrated, adjudicated, and self-enforcing protocols)
- Authentication mechanisms: Kerberos, X.509, etc.
- Trusted computer systems; TCB OS design; TSEC evaluation (Orange Book, Common Criteria)

- Access control mechanisms and information models: DAC, MAC, BLP, Biba, Chinese Wall, Principle of Least Privilege, lattice models
- Security technology: PGP, packet filtering, TCP wrappers, firewalls
- Network and system intrusion detection
- Policy and legal aspects of computer security

CprE 532 Information Warfare

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.

Prerequisite: CprE 531

Course Length: 45 hours in 15 weeks, 2 eighty minutes meetings per week

Textbook:

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

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.

Course Learning Objectives:

Upon completing this course a student will:

- Understand the ethics of using hacking tools
- Be able to describe the TCP/IP network protocols and the effect of an open network protocol on security
- Be able to snoop traffic from a network and decode the data
- Be able to describe methods to counter traffic attacks like snooping, spoofing, redirection, and flooding.
- Understand the importance of passwords and methods to select good passwords
- Be able to crack passwords and understand the importance of authentication
- Understand the issues of social engineering when used to discover passwords
- Be able to describe a centralized key distribution center and its uses in authentication
- Be able to use one-time passwords, Kerberos, and other authentication systems.
- Understand the issues of anonymous email and email forgery, email privacy.

- Understand and be able to use an encrypted email system
- Understand the relationship of public and private keys to email and the uses of a Public Key Infrastructure
- Be able to identify the security problems with standard terminal based protocols like telnet, ftp, NFS, and web.
- Be able to identify solutions to the security problems with telnet, ftp, NFS, and web traffic.
- Understand how secure protocols like SSH, SSL, and VPN's operate and how they can be used to enhance security.
- Be able to develop a plan to attack a network of computer systems and then be able to develop a plan of countermeasures.
- Understand the use of firewalls and the strengths and weaknesses of a firewall
- Be able to read and identify information in log files for possible security violations
- Be able to use screening routers and software filters to defend a computer system from attack.
- Be able to use probe software to determine the weaknesses of a computer system.
- Understand how intrusion detection system operate and how they can be used to detect attacks

Major Topics:

- Introduction & Ethics
- Network Protocols
- Traffic attacks and defenses
- Authentication attacks and defenses
- eMail Attacks and defenses
- Terminal Services, NFS, and X
- WEB
- Intrusion detection
- Firewalls
- Screening Routers
- Link encryption
- Encryption tools
- Trapping a hacker
- Probe software
- Security management

Method of Instruction:

The course is taught using lectures which are also videotaped to the off campus students. The course also has a strong laboratory component where the students connect to the lab remotely to carry out experiments. The labs range from using tools (both attack tools and defend tools) to looking at network protocols. The largest lab is the attack and defend lab where the students try to break into a small company designed by the faculty. The students must detail the attack plan and then provide a detailed description of how to defend against the attacks.

CprE 533 Cryptography

Course Length: 45 hours in 15 weeks, 3 50-minute meetings per week

Textbook (optional):
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.

Major Topics:

1. Overview
2. Concepts of Information Theory
3. Symmetric Key Cryptosystems
    1.DES
    2.IDEA
    3. Rijndael
4. Differential and Linear Cryptanalysis
5. Public Key Cryptosystems
    1.Relevant Number Theory
    2.RSA
    3.El Gamal
    4.Signature Schemes
6. One-way Hash Functions
7. Key Exchange Algorithms
8.Stream Ciphers and Random Number Generation
    1.Linear Feedback Shift Registers and Variations
    2.Blum-Blum-Shub Generator
9. Field Theory and Elliptic Curves
    1.Fields and polynomials
    2.Elliptic Curve Cryptosystems

3.More about Linear Feedback Shift Registers

Method of Instruction:

The course is taught in a traditional lecture format. The lectures are also videotaped and shipped out to the off campus students. Bi-weekly homework assignments are used to give students practice in the kind of analysis demonstrated in class, and to pursue subtle questions not addressed in the lectures. An effort is made to accommodate students who are primarily interested in the theoretical underpinnings of the subject as well as those more concerned with the implementation aspects of cryptography.

Bibliography

1. "The national strategy to secure cyberspace", February 2003 http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
2. http://www.iac.iastate.edu
3. http://www.nsa.gov:8080/isso/programs/coeiae/index.htm
4. http://www.ede.iastate.edu
5. http://www.nstissc.gov/html/introduction.html
6. http://www.ede.iastate.edu/info.grad.program.asp
7. http://www.webct.com/

Biography

DOUG JACOBSON

Doug Jacobson is an Associate Professor of Electrical and Computer Engineering at Iowa State University and director the ISU Information Assurance Center. He has received two R&D 100 awards for security technology and has two patents in the area of computer security. He has given over 40 presentations in the area of computer security and has been teaching security and networks courses for over 15 years.