Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Information Assurance Concentration Programs: Integrating Information Assurance in Existing Computer Science Curricula

Stephen S. Yau and Zhaoji Chen

Abstract – Information Assurance and Security is a pervasive theme that must be integrated throughout the information technology curriculum. In this paper, the development of three information assurance concentration programs which is to integrate information assurance topics with existing Computer Science Curricula at Arizona State University. Observations and lessons learned from the development process, including how to arrange and schedule the series of information assurance courses, how to improve student involvement, and what kinds of textbooks are most needed in this area are presented.

Index terms – Information assurance, education, undergraduate curriculum, graduate curriculum, and concentration programs.

I. Introduction

Due to the rapid advances of information technology, it has become indispensable in our daily life, ranging from e-commerce, health care, transportation, communications, online education to intelligence analyses, homeland security, and national defense. With the growing concerns over system availability, data integrity and privacy, information assurance has become an increasingly important and critical area in computer science curriculum. As this area matures, information assurance has changed from an art performed only by experts to a set of well-defined processes which can be followed by non-experts. Besides professional training, universities have also played a very important role in information assurance education. Six comprehensive curriculum standards have been established under the auspices of the Committee on National Security Systems (CNSS) [1]. The principles and practices developed by experts and specified in these training standards need to be introduced and followed by developers in order to build secure robust information systems.

Authors' affiliation: Information Assurance Center, School of Computing and Informatics, Arizona State University, Tempe, AZ 85287-8809, {yau, zhaoji.chen@asu.edu}.

After developing four IA related courses in our Computer Science Programs at Arizona State University, our courseware was certified to satisfy both the NSTISSI-4011 National Training Standard for Information Systems Security (INFOSEC) Professionals [2] and the CNSSI-4012 National Information Assurance Training Standard for Senior Systems Managers (SSM) [3] in 2006. Later that year, as part of our effort to establish the Center of Information Assurance, to be certified as a National Center of Academic Excellence in Information Assurance Education (CAEIAE), we developed three Information Assurance Concentration Programs to integrate information assurance in our existing Computer Science curricula for the degree programs of B.S., M.S., and Ph.D.

In this paper, we will introduce the Computer Science Programs at ASU, and then present the IA concentration programs in Computer Science. Finally, the experiences of our faculty members involved in the program will be discussed.

II. Arizona State University and its Computer Science Programs

Arizona State University is a major metropolitan public research university with four campuses and more than 60,000 students. ASU is rapidly building a comprehensive metropolitan research university with a combination of academic excellence and commitment to our social, economic, cultural, and environmental setting. The Department of Computer Science and Engineering (CSE) in the Ira A. Fulton School of Engineering (FSE) at ASU has been making rapid progress in recent years. A new School of Computing and Informatics (SCI) has been launched, which houses the CSE Department along with the new Department of Biomedical Informatics (BMI).

The CSE Department has 41 tenured and tenure-track faculty members, six full-time lecturers, and a vibrant student body of about 800 undergraduate and 350 graduate students. It offers the B.S. degrees in Computer Science and Computer Systems Engineering. It also

ISBN 1-933510-96-7/$15.00 ©2007 CISSE

offers the M.S., Master of Computer Science, and Ph.D degrees in computer science. The B.S. degree Program in Computer Systems Engineering is accredited by the Engineering Accreditation Commission of ABET, and the B.S. degree Program in Computer Science is accredited by the Computer Science Accreditation Commission of ABET. Our undergraduate programs require students to take the introductory courses on both software engineering and operating systems. The department also offers a list of many technical elective courses covering areas like database and multimedia, computer networks, embedded systems, software engineering, information assurance, artificial intelligence, computer graphics, image processing. And one benefit of having a large number of faculty members is that the department is able to offer courses covering new emerging areas as special topic courses at both undergraduate (CSE 494) and graduate (CSE 591 and CSE 598) levels. The M.S. and Ph.D. programs are research oriented, and require each student to write an M.S. thesis or Ph.D. dissertation. The M.C.S. program requires each student to complete a project. Independent studies on specific topics under the supervision of a faculty member are also part of our graduate programs [4].

The Computer Science Program at ASU strives to reflect the depth and breadth of computer science. To this end, we have engendered strong collaborations with other engineering departments in the FSE as well as academic departments throughout ASU, such as the School of Life Sciences, the W.P. Carey School of Business, the Herberger College of Fine Arts and the College of Liberal Arts and Sciences.

Key research areas in the department include embedded systems, information assurance, distributed computing systems and networks, software engineering, database systems, multimedia and graphics. Faculty members are also collaborating on trans-disciplinary projects with the Translational Genomics Institute (T-Gen), the Biodesign Institute at ASU, the Decision Theater at ASU, Banner Health Systems and Mayo Clinic, and Center for Health Information and Research.

III. Information Assurance Concentration Programs

The Information Assurance Concentration Programs were designed to complement the existing computer science degree programs and specifically for those students who wish to pursue educational programs concentrated on information assurance area. It aims at providing students with excellent foundation, in-depth knowledge on the technical issues, as well as the non-technical aspects of information assurance. It helps them build a competitive advantage to pursue further study or seeking employment opportunities in information assurance area.

We have established information assurance concentration programs with the B.S., M.S. and Ph.D. degrees in computer science. Each student must satisfy all the requirements for the appropriate computer science degree program [5-7]. In order to provide students with in-depths training in information assurance, several courses in the field are required for the concentration programs. These courses cover a wide range of information assurance topics ranging from the foundation and background to specific advanced techniques, like network security, applied cryptograph, software security, data security and privacy, and computer system security, which will be described in detail in Section IV. Due to the cross-discipline nature of information assurance, the students are required to take additional courses to cover other computer science areas of their interests.

For the B.S. IA Concentration Program, students are required to take four information assurance courses covering information assurance background, computer system security, data security and network security. Students are also required to take one additional course from a list of technical electives, including database management, software analysis and design, human computer interaction, computer network and artificial intelligence. These courses are considered technical electives in their B.S. Program in computer science.

For the M.S. IA Concentration Program, out of the 30 credits required for the M.S. degree, students are required to take four information assurance courses covering information assurance background, software security, applied cryptography and advanced network security. In addition, students also need to take one additional course from a list, including distributed operating systems, advanced compute networks, and software verification and testing.

For the Ph.D. IA Concentration Program, the students are also required to take the four graduate level information assurance courses like the M.S. program. As part of the total 84 credits required for the Ph.D. degree, including the 30 credit hours from a M.S. degree, it requires two additional courses from a list of electives with a wide range of topics from data mining, artificial intelligence, advanced computer networks, distributed and multi-processor operating systems, distributed database to modeling and simulation.

In addition, we would like to have graduates of these IA Concentration Programs to have first-hand experiences in information assurance by requiring students enrolled in the B.S. degree program to have a major portion of their capstone projects (CSE485 and CSE486) in the

information assurance area, and students in the M.S. and Ph.D. degree programs to have a major portion of their theses or dissertations in the information assurance area.

IV. Information Assurance Courses

Eight courses in information assurance have been developed at undergraduate and graduate levels. Beside the four courses we originally had when we applied for the 4011 and 4012 certificates, we have developed four additional courses to cover additional topics and strengthen the three IA Concentration Programs. Each of these courses carries 3 credit hours.

According to the IT2005 report of the ACM SIGITE Curriculum Committee [8], some topics are referred as *pervasive themes*, should be addressed "multiple times in multiple classes, beginning in the IT fundamentals class and woven like threads throughout the tapestry of the IT curriculum". *Information assurance and security* is listed as one of the pervasive themes. Thus, we designed our information assurance courses in a way that we first introduced the foundation courses and then have individual courses to cover specific aspects of information assurance. There is an appropriate amount of overlapping information on the topics covered by these courses to achieve the "thread weaving" effect to reinforce some of the topics the students learn in previous courses.

A. Foundation Courses for Information Assurance

We have designed two courses to cover the information assurance foundation, and each student in the IA Concentration Programs is required to take one of these two courses: the undergraduate course *CSE465 Information Assurance* and *CSE543 Information Assurance and Security*. Both courses are lecture and discussion based, introducing most aspects of information assurance and security. With one of these two courses, the students can have a basic and comprehensive understanding of the problems in the information assurance area and the solutions to these problems. The graduate level course CSE543 is mainly for students who are enrolled in the graduate concentration programs, but did not take CSE465 or a similar course in their undergraduate study.

Because many students from local industry are interested in this subject, but it is not convenient for them to come to campus for taking CSE 543, we offered this course online last year as part of our Professional Development Programs.

B. Computer Network Security

Because most information systems are networked and often include software systems running on interconnected computing devices, we believe that network security is an important part of our IA Concentration Programs. We have developed two courses on network security: an undergraduate level course *CSE468 Computer Network Security*, and a graduate level course *CSE548 Advanced Computer Network Security*. These courses provide the students with a comprehensive understanding of network security theories and problems as well as the current state-of-art solutions to these problems. Topics range from protocols for authentications, maintaining confidentiality of email and information transmissions to secure web transactions and distributed group key management. These two courses also have laboratory assignments which will be discussed in Section V.

C. Software Security

As discussed in [9], we have developed a graduate-level course *CSE545 Software Security* on secure software engineering. The course covers secure software design, threat analysis and modeling, security coding and testing. It aims at providing the students with thorough understanding and knowledge on various theories and tools for improving software security. The course consists of a series of lectures, student presentations of selected recent research results, and a software development project focusing on software security. The students also test and try to break other students' project deliverables at the end of the semester so that they can have some experience on how to think like an attacker when they are trying to defend their own software packages.

D. Applied Cryptography

CSE539 Applied Cryptography is a popular computer science course, which has been offered almost every year, long before the establishment of our IA Concentration Programs. With the advent of electronic commerce, online transactions, consumer computing and authentication, cryptography is playing an important role in securing the privacy and authenticity of electronically stored and transmitted information. We believe that no students should complete the graduate IA Concentration Programs without sufficient knowledge of cryptography and its applications, and hence this course is included as one of the required courses for the graduate IA Concentration Programs. This course covers three major parts: cryptographic algorithms, cryptographic protocols and cryptographic techniques. The cryptographic algorithms embody the art of encryption. The cryptographic protocols expose the students to the fascinating world of building trust on untrusted

relationships. Finally, the cryptographic techniques will include those used in key management and selection of cryptographic algorithms.

The following two courses are newly designed information assurance courses, which will be offered in the next semester.

E. Computer System Security

Currently, basic computer infrastructures, ranging from consumer desktops to business servers, are under continual attacks from a variety of miscreants (or "hackers") for both fun and monetary gain. The designs of computer systems often have many vulnerabilities and the attacks exploit these vulnerabilities for stealing private information, performing unauthorized operations, destroying data, etc. *CSE466 Computer System Security* has been developed to cover these system aspects in information assurance. This course will cover the countermeasures to attacks on general purpose systems, operating systems, applications and the end-users. The topics provide the students a keen insight into the methods employed by the miscreants, the loopholes that exist and how they come about and the methodology to prevent and defend against such attacks. As a part of the course, and for the sake of completeness, it will also cover some basic topics from cryptography and network security.

F. Data and Information Security

It is important for information assurance professionals to protect not only the information systems from various attacks, but also the integrity and privacy of the information which is being stored, processed and transmitted by these information systems. Thus, it is necessary to offer a course focusing on the privacy and integrity of the information itself. We have developed a course *CSE467 Data and Information Security* to fill this need. The course will introduce basic concepts of authentication, confidentiality, integrity and privacy; data and database security; access controls; authentication in distributed information systems; trust models; watermarking; and private information retrieval.

V. LESSONS LEARNED

A. Course Scheduling and Course Levels

While we developed various courses for undergraduate and graduate IA Concentration Programs and tried to offer them in different semesters, we have found that students sometimes will have difficulties to take all the required courses within their planned schedules, especially for undergraduate students. Because information assurance is a rapidly growing field, and needs a substantial amount of background knowledge, all the undergraduate information assurance courses are currently offered at 400 levels. Thus, the undergraduate students have to take all four required information assurance courses during their senior year in order to satisfy the course requirement of the B.S. degree program in the normal four-year period, which is not an easy task. In addition, because only a few of the current faculty members in the information assurance area can schedule to teach these courses, and it takes a quite long time to recruit outstanding faculty members in information assurance area, it is very challenging to keep offering these courses annually. Therefore, the undergraduate students who enroll in the information assurance concentration program will only have one chance to take a specific information assurance course during their senior yea without staying an extra year.

Our plan is to rearrange some of the information assurance topics based on our observations and experience after the IA Concentration Programs have been running for a couple of years. We could shift some information assurance topics into some lower level courses required by the B.S. degree, and reduce the number of required information assurance courses. Or we may gather the basic concepts and background information and change the foundation course to be a 300 level course, which students can take during their junior year.

B. Student Involvement

We strongly encourage active student involvements in curriculum activities, which are important for generating good results. Based on our observations, students are most involved when they work in a team environment with peer-evaluation, compared to a lecture environment. Hence, all the information assurance courses have a group project with hands-on experience. We have established a designated network security laboratory with isolated Intranet, consisting of 21 PCs, one server, and one switch with 48 ports. Each PC has two ethernet interface cards belonging to two subnets for having various network configurations. Now, it has been used by the courses *Software Security*, *Computer Network Security* and *Advanced Computer Network Security* for their individual laboratory assignments. For the *Computer Network Security* courses, students will also gain hands-on experience on (1) network service setup and configuration, (2) iptable firewall setup and configuration, (3) intrusion detection system (IDS) administration, and (4) kerberos server administration through four carefully designed laboratory projects carried out in the isolated network. For *Software Security* course, we have developed an experimental laboratory assignment on

various attacking techniques listed in Whittaker and Thompson's book [10] using Holodeck[1] as the testing tool and Internet Explorer as the target application. More courses will use the laboratory, and we will continue to work on establishing excellent information assurance laboratory experiments.

In addition to projects and laboratory experiments in the *Software Security* course, each student also is required to select one important research paper in the software security area provided by the instructor, study it and present the study result to the whole class. They are not only introduced to the latest research results, but also learn how to think independently and figure out ways to solve challenging problems in information assurance area. This experience should be very helpful when they start to do research in this area.

We also seek partners in local industry to participate in internship programs which will give our students the opportunities to experience the real-world applications, problems and solutions. Motivating and increasing student involvement will remain to be a key factor for the success of our information assurance programs.

C. Textbooks

The time for the instructors during classes is always limited. Thus, it is very helpful to have an informative textbook to cover most of the lecture material and provide students with the necessary background information and further reading materials. However, because information assurance area is a rapidly developing area, based on our observations during the establishment of our information assurance courses and the concentration programs, it is clear that right now we do not have enough good textbooks in this area.

There are some good textbooks for some specific topics, for example Bruce Schneier's *Applied Cryptography* [11] and the *Network Security* [12] by Kaufman *et al*. But, we have not found a general textbook to cover all the basic concepts, fundamental theories and necessary background information for our foundation courses CSE 465 and 543. Right now, these course materials are generated based on several books focusing on different topics and latest research papers. We have also found that textbooks are most needed for the following two topics since they are relatively new.

The first topic is the legal and ethical issues related to information assurance. The textbook should cover related laws and regulations for information assurance, such as the Foreign Intelligence Surveillance Act, Computer Fraud and Abuse Act, Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act. It should help the students specialized in the information assurance area to have a clear understanding about the legal and ethical issues. On the other hand, since laws are continuously evolving, it is also beneficial to have students engaged in the discussions about how the technical inputs and important events influence the legislations and executive orders in information assurance area.

The second topic is computer forensics. As computer crimes on the rise, we not only need to discuss the legal issues related to computer crimes, but also to prepare our future IT professionals on how investigations are conducted when a computer crime is suspected. Although currently we can find several books on computer forensics, they often specialize in certain application domains, contain too much technical details and require a great amount of background knowledge, which make them good reference books for well-trained IT professionals, but are not suitable to be used as textbooks for students who are interested in information assurance area. We cannot expect all students to become computer forensic experts just after taking a class on this issue, but we hope we can introduce all students with the fundamental concepts and techniques on computer forensics so that it will be much easier for them to read those reference books later on if they would like to know more about computer forensics.

VI. MIGRATION OF RESEARCH RESULTS TO INFORMATION ASSURANCE COURSES

Information Assurance is a very active research area, where new ideas and techniques are continuously generated. We believe that migrating new important research results to information assurance courses is critical to keep the courses fresh and attractive. It is also helpful to lead students to conduct cutting-edge research in this area, which is especially important for graduate students. Currently, we have faculty members active in research in cyber trust modeling, group key management, personal identify protection, access control mechanism, privacy preserving information retrieval, software security, trust management, and secure service discovery Besides publishing research results in journals and conferences, our faculty members also migrate these results to the relevant courses.

Currently, we have migrated research results on security requirement specifications and management to *CSE545 Software Security*. The two network security courses also include research results done by the instructor, such as distributed group key management. Research results on privacy-preserving information retrieval and personal

[1] *Information about Holodeck can be found at: http://www.securityinnovation.com/holodeck/index.shtml*

identity protection will also be included in the new courses *CSE466 Computer System Security* and *CSE467 Data and Information Security*, respectively.

VII. Conclusions and Future Plan

Because we increasingly depend on the continuous services of various information systems, there are growing concerns with information system availability, data integrity and privacy. It has generated great demands for well-educated students in information assurance area. We have created three IA Concentration Programs associated with the Computer Science degree programs at B.S., M.S. and Ph.D. levels, which aim at educating students to become IA professionals with excellent foundation, in-depth knowledge on the technical issues, as well as the non-technical aspects of information assurance.

Information assurance is a rapidly developing area. Thus, we need to continuously updating our information assurance programs with the advances in this area. New information assurance topics will be incorporated in existing courses or new courses when sufficient new research results have emerged

Our information assurance programs can be used as a model for other colleges and universities who are interested in establishing their own information assurance educational programs in computer science. We are also working on expanding our outreaching programs and collaborate with local community colleges to improve their information assurance training and education. We also plan to collaborate with industry partners to create appropriate training programs in information assurance and security for practitioners.

VIII. Acknowledgment

The authors would like to thank all the participating faculty members at Arizona State University in the information assurance programs, especially Drs. Slecuk Candan, Partha Dasgupta, and Dijiang Huang for developing the new information assurance courses.

IX. References

[1] Presidential Decision Directive 63: The Clinton Administration's Policy on Critical Infrastructure Protection, available at: http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

[2] NSTISSI-4011 National Training Standard for Information Systems Security (INFOSEC) Professionals, available at: http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

[3] CNSSI-4012 National Information Assurance Training Standard for Senior Systems Managers (SSM), available at: http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf

[4] Computer Science and Engineering Undergraduate and Graduate Programs at ASU, available at: http://cse.asu.edu/students/undergrad/index.php and http://cse.asu.edu/students/graduate/index.php

[5] Requirement for Bachelor of Science in Computer Science at ASU, available at: http://cse.asu.edu/students/undergrad/checkflowBS.php

[6] ASU M.S. Degree in Computer Science Requirements and Procedures, available at: http://cse.asu.edu/students/graduate/masterpolicy.php

[7] ASU Ph.D. Degree in Computer Science Requirements and Procedures, available at: http://cse.asu.edu/students/graduate/phdpolicy.php

[8] SIGITE Curriculum Committee, Computing Curriculum: Information Technology Volume 2005, available at: http://www.acm.org/education/curric_vols/IT_October_2005.pdf

[9] S. S. Yau and Z. Chen, "Software Security: Integrating Secure Software Engineering in Graduate Computer Science Curriculum", *Proc. 10th Colloquium for Information Systems Security Education (CISSE)*, 2006, pp. 124 - 130.

[10] James A. Whittaker and Herbert H. Thompson, *How to Break Software Security: Effective Techniques for Security Testing*, Addison Wesley, 2003

[11] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, Jonh Wiley & Sons, Inc., 1995

[12] C. Kaufman, R. Perlman, M. Speciner, *Network Security*, 2nd Edition, Prentice Hall, 2002.