ABSTRACT
We describe how the Information Assurance Standards from the Committee on National Security Systems, CNSSI / NSTISSI 401x, can be used as a basis for a Master of Science degree in Information Security. While there exists many graduate programs in information security and information assurance, aligning the program to closely follow these national standards enables such a program to target the federal work force and deliver required certifications for those seeking employment or advancement within the federal information security job market.

KEY WORDS

1. Introduction

East Stroudsburg University of Pennsylvania (ESU) is a National Center of Academic Excellence in Information Assurance Education, one of approximately 100 such institutions designated by the U.S. National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS) [1]. This designation was based on the successful ESU Bachelor of Science degrees in Computer Science and Computer Security [2] and the successful ESU Master of Science Degree in Computer Science. The ESU Computer Science Department has recently created a Master of Science degree in Information Security. This program allows students to complete a Master’s degree fully online except for an in-person thesis defense. The program is intended for students with interest in system security administration and allows students who have undergraduate experience in Computer Science, Computer Security, or Information Technology the opportunity to continue their education on the Master’s level. Also, by completion of the program, students are awarded six national certifications [3]:

- CNSSI 4013: National Information Assurance Standard For System Administrators
- CNSSI 4014: Information Assurance Standard for Information System Security Officers
- NSTISSI 4015: National Standard for Systems Certifiers
- CNSSI 4016: National Information Assurance Standard For Risk Analysts

The graduate Information Security curriculum has been designed to follow these national standards closely.

2. Program Need

There are various noteworthy motivating factors for the ESU Information Security Graduate Program. As indicated below, current student desire for a graduate program in information security is very high. Students see a program of this type as beneficial to their education, knowledge, and future employment possibilities. These students also are excited about further research opportunities with faculty in the stimulating world of computer and information security. Second, there is a high demand for students with knowledge in information security, as indicated by employment trend reports [4]. A third motivating factor behind the program is national security. As mentioned in the National Strategy to Secure Cyberspace [5], “Key to any successful national effort to enhance cybersecurity must be a national effort to … maintain an adequate pool of well trained and certified IT security specialists… The Nation must focus resources on training a talented and innovative pool of citizens that can specialize in securing the infrastructure.” The ESU Information Security Graduate Program is designed to help meet this national security need.

The graduate program in information security is considered an important investment for ESU so that the university can continue its leadership role in the field. ESU delivered the first Bachelor of Science degree in Computer Security in the nation; ESU holds multiple national information assurance certifications which apply to its curriculum and students; ESU is a National Center of Academic Excellence in Information Assurance.
Education. These accomplishments show how the current ESU Computer Security Program has succeeded, and a Graduate Program in Information Security is a natural progression to continue the institution’s momentum in this field and enhance the uniqueness of the university.

Another unique aspect of the Information Security Graduate program is its response to changes in the field of information assurance. The coursework has been modeled from a combination of well-known graduate computer science coursework and the CNSS standards. As the computer science curriculum changes, the Information Security Graduate Program will adapt, and as the national information assurance standards change, so will our curriculum. Thus, as the fields of computer science, computer security, and information security evolve, the ESU Information Security Graduate Program must also progress.

The ESU Information Security Graduate Program is necessary to ESU, the Pennsylvania State System of Higher Education (PASSHE, the administrative authority of ESU) [6], the Commonwealth of Pennsylvania, and the Nation. As shown below, the need for students trained in information assurance is great, as required by both private and public interests. Current students are very interested in such a program, and the program has attracted existing corporate and government/military professionals who want to further their education. The program also allows ESU and PASSHE to continue their leadership in the field of information assurance. Finally, the program challenges students, helping to expand their critical thinking abilities. All program candidates perform extensive research, allowing them to learn this critical skill.

2.1 Need as Substantiated by Employment Trends

Employment trends for the field of information assurance are excellent. While some programming employment has been outsourced to other countries, most of these jobs are at lower levels (Associate’s or Technical Degrees). Furthermore, the field of computer and information security is different. Many corporations will not leave the security of their computer and information systems to companies overseas [7]. It is also important to note that many industries have legislative mandates that require they secure their systems, such as the Health Insurance Portability and Accountability Act of 1996 [8] and the Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999 [9]. Other laws which require security of computer and information systems apply to multiple industries (the Sarbanes-Oxley Act or the Public Company Accounting Reform and Investor Protection Act of 2002 [10]) or the entire federal sector (the Federal Information Security Management Act [11]). Because of these mandates, the demand for information assurance professionals is great and growing at a rapid pace.

While the U.S. Department of Labor (DOL) does not keep statistics on the field of information assurance, it does report on “Computer Support Specialists” and “Computer Systems Analysts.” The following are taken from DOL web pages [12], [13]:

“... Demand for computer security specialists will grow as businesses and government continue to invest heavily in ‘cyber security,’ protecting vital computer networks and electronic infrastructures from attack. The information security field is expected to generate many opportunities over the next decade as firms across all industries place a high priority on safeguarding their data and systems.”

“These workers with formal education or experience in information security, for example, are in demand because of the growing need for their skills and services.”

“Also, the increasing importance being placed on ‘cybersecurity’ – the protection of electronic information – will result in a need for workers skilled in information security.”

“The introduction of the wireless Internet, known as WiFi, creates new systems to be analyzed. The spread of such new technologies translates into a need for information technology professionals who can help organizations use technology to communicate with employees, clients, and consumers. Explosive growth in these areas also is expected to fuel demand for analysts who are knowledgeable about network, data, and communications security.”

A brief survey of available Master of Science programs across the nation reveals the existence of approximately 120 programs in Computer Security or Information Security [14]. In order to differentiate the program at ESU from these other programs, the decision was made to follow the successful example of the existing Computer Security undergraduate degree and align the graduate program with the previously mentioned national standards in information security. This decision was made to enable the ESU program to target the federal government workforce (and those working in environments that follow the federal standards). The ESU graduate program delivers the required certifications for those seeking employment or advancement within the information security job market of these employers. The focus on this employee population was a natural extension of the undergraduate program; several good relationships have been cultivated between ESU and numerous federal government agencies via successful placement of ESU computer security undergraduate students. The graduate program was established in part due to the demand for workers to obtain the additional certifications needed to work and
advance in these environments, in addition to the previously discussed student demand for such a program.

2.2 Demand for the Program Among Current and Prospective Students

Two methods were used to determine demand among local students and local employers. For local students, a survey was conducted including computer science and computer security students in the second, third, and fourth undergraduate years at ESU. Sixty-five (65) students were asked the following two questions in written survey form, and their responses are given in Table 1.

Question 1: “Are you interested in a Master’s program in computer security?”

Question 2: “Are you interested in an online Master’s program in computer security?”

Table 1. Survey of interest in Information Security Master’s Programs by undergraduate students.

<table>
<thead>
<tr>
<th>Response</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 1 = Yes, Question 2 = Yes</td>
<td>41</td>
</tr>
<tr>
<td>Question 1 = Yes, Question 2 = No</td>
<td>13</td>
</tr>
<tr>
<td>Question 1 = No, Question 2 = Yes</td>
<td>8</td>
</tr>
<tr>
<td>Question 1 = No, Question 2 = No</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>65</strong></td>
</tr>
</tbody>
</table>

As we can see, less than 5% of the students (3/65) surveyed have no interest (a “No” answer to both questions) in an on-campus or online information assurance graduate program. That is, over 95% of the surveyed students are interested in completing graduate work in information assurance. In discussion with students after the survey, we found that students are very interested in learning more of this exciting field, but they are also very interested in pursuing applied collaborative research with faculty and other students.

Local employers have also been canvassed to judge their needs in information assurance. In a recent project completed by a partnership between ESU and Backbone Security, the Stroudsburg computer security company which was a member of the ESU Business Accelerator, an Information Assurance Career Development Program was developed. Part of this program included the involvement of multiple local companies to judge their needs in information assurance, with a focus group of companies coming to the ESU campus. While no formal written surveying was completed with this group, the majority of the focus group discussion involved corporate information assurance needs with regard to employees. This focus group indicated that Master’s level students in information assurance would be highly desirable future employees.

The Information Security Graduate Program has also allowed ESU to tap multiple student markets. Firstly, this program draws in a similar manner to our current populations – many students from the Pocono, Lehigh Valley, Scranton, and northwest New Jersey areas, some students from outside these regions, and some international students. With the online offering of the program, ESU has also been able to grow into a worldwide market. For example, ESU was recently approached to discuss information assurance opportunities for students in Japan. The Graduate Program in Information Security has enabled international students or students from remote location to enroll in the Information Security at ESU.

3. Academic Integrity

The ESU Information Security Graduate Program is a rigorous technical program for students with undergraduate experience in Computer Science, Computer Security, or Information Technology, and interested in furthering their knowledge in system security administration. All students in this program are required to complete a thesis under the direction of a faculty member, which is judged by a thesis committee of faculty members.

3.1 Program Goals

The ESU Information Security Graduate Program curriculum has been designed with multiple goals. One goal was that the design should be based on two models of curriculum. First, the existing ESU Master’s degree in Computer Science was used as a model. In the Computer Science Program, students are required to complete rigorous courses which give them theoretical as well as practical abilities. Students are also required to complete a major research project and to successfully defend their written thesis document. All of these elements have been included in the Information Security Graduate Program.

The second curriculum model used for the Information Security Graduate Program comes from the CNSS standards. Six of the courses included in the program are dictated by these standards. These six courses are mapped directly to six standards, namely CNSS 4012, 4013, 4014, 4016, and NSTISSI 4011 and 4015. The remaining courses consist of those which already exist in computer science and those which instruct the students in graduate level research. The combination of these two models with well-known rigorous computer science and research courses lead to the development of the Information Security Graduate Program which gives students both broad and deep understanding of computer and information security.

The CNSSI standards are very broad and do include an amount of overlap from one standard to the next. When developing the course syllabi, care was taking to ensure
that, while mapping each course to its respective standard, duplicate material was spread out to be covered only once throughout the curriculum. The mapping of courses to standards is as follows:

- CPIS 511 – NSTISSI 4011
- CPIS 512 – CNSSI 4012
- CPIS 513 – CNSSI 4013
- CPIS 514 – CNSSI 4014
- CPIS 515 – NSTISSI 4015
- CPIS 516 – CNSSI 4016

Another program goal was to create a unique program which serves numerous markets. Multiple factors point to the uniqueness of the Information Security Graduate Program. First, many schools which offer graduate coursework in information assurance do so by offering a certificate program. ESU’s program, with a full-fledged Master’s degree, encourages students to study information assurance with more depth. Second, as the program also allows students to earn six national certificates, it also acts as the certificate programs of other schools. Finally, the program is quite unique in the fact that it allows students to earn all six national certifications sponsored by the U.S. Committee on National Security Systems. There are only approximately 10 institutions in the nation which offer all six of these certifications.

Another goal of the program design was the use of multiple instructional technologies. First, the use of distance education, especially via the Internet, was desired. Second, because the target audience was to include military personnel and professionals from outside the East Stroudsbury area, the creation of a full Master’s program online with asynchronous delivery was implemented. This combination allows for maximum flexibility for the students.

### 3.2 Student Learning Outcomes

The major learning outcome of the program is to induce students to have a graduate level understanding of information assurance. This includes knowledge of the standard areas of Confidentiality, Integrity, Availability, Identification and Authentication, and Non-Repudiation. Students learning outcomes in these areas include both theoretical and practical knowledge. With regard to theoretical knowledge, students learn information assurance with an approach that is almost mathematical, as much instruction in graduate level computer science occurs. That is, students learn how to define the basic building blocks of information assurance, and then work examples related to the field. A second aspect of the theoretical approach is the required research project or thesis. All students in the Information Security Graduate Program perform an extensive, year-long, research project that leads to a written thesis and a public defense of the students’ work. As is the case with most graduate programs, the students’ work on this project is counselled by faculty, and then judged by a committee of faculty. Students also learn the tenets of information assurance on a practical level. For example, some courses in the Information Security Graduate Program use experimental learning, allowing students to work with computing technologies to determine their vulnerabilities.

Finally, student learning outcomes are dictated by the CNSS certifications which modeled the curriculum, and employment needs. The Information Security Graduate Program ensures that students’ learning allows them to fulfill the requirements of the national standards as well as meet the needs of future employment.

### 3.3 Curriculum Overview

The Information Security Graduate Program is a technical program for students with undergraduate experience in Computer Science, Computer Security, or Information Technology and those who are interested in improving their knowledge in system security administration. All students in this program are required to complete a thesis under the direction of a faculty member, which are judged by a thesis committee of faculty members.

Nine new courses were created as program requirements for the Graduate Program in Information Security implementation. In the courses listed below, the rubric CPIS is used, indicating Computer / Information Security, since the program is housed in the Computer Science Department:

- CPIS 511: Information Systems and Information Security
- CPIS 512: Information Security for Senior System Managers
- CPIS 513: Information Security for System Administrators
- CPIS 515: Information Security for System Certifiers
- CPIS 516: Information Security Risk Analysis
- CPIS 570: Introduction to Information Security Research
- CPIS 574: Information Security Research 1
- CPIS 575: Information Security Research 2

One required course already existed at the university (as an undergraduate course) and was adapted as a graduate course and for online offering:


Information Security MS candidates are expected to progress through the program as shown in Table 2. Some students may not follow this sequence, especially those
who are seeking to obtain only a few of the national certifications associated with the program.

Table 2. MSIS Course progression.

<table>
<thead>
<tr>
<th>Year 1, Fall:</th>
<th>CPIS 511, CPSC 516</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year 1, Spring:</td>
<td>CPIS 513, CPSC 515</td>
</tr>
<tr>
<td>Year 1, Summer:</td>
<td>CPIS 512, CPIS 570</td>
</tr>
<tr>
<td>Year 2, Fall:</td>
<td>CPIS 515, CPIS 574</td>
</tr>
<tr>
<td>Year 2, Spring:</td>
<td>CPIS 561, CPIS 575</td>
</tr>
<tr>
<td>Year 2, Summer:</td>
<td>Residency: Thesis Defense</td>
</tr>
</tbody>
</table>

Below we provide a brief description of each of the 10 courses in the program.

CPIS 511: Information Systems and Information Security – This online course will introduce the student to information systems and information security, especially with regard to the management of information systems. Topics include information and communication system basics, information assurance, national information security policies, operational security, and security planning. Prerequisite: Permission of the Information Security Graduate Coordinator.

CPIS 512: Information Security for Senior System Managers – This online course will allow students to delve more deeply into the concepts of information system security management, especially with regard to Senior System Managers. Topics include system approval to operate, system accreditation, compliance verification, security control management, acquisition management, roles and responsibilities of security management officials, criticality and sensitivity of systems, resource allocation, and assessment of network security. Prerequisite: CPIS 511, CPSC 561.

CPIS 513: Information Security for System Administrators – This online course will allow students to delve more deeply into the concepts of information system security management, especially with regard to System Administrators. Topics include secure use of information systems, incidents and incident response, system configuration, system anomalies and system integrity, and security administration. Prerequisite: CPIS 511, CPSC 561.

CPIS 514: Information Security for Information Systems Security Officers – This online course will allow students to delve more deeply into the concepts of information system security management, especially with regard to Information Systems Security Officers. Topics include certification and accreditation and its support by the ISSO, security policy and the verification of policy, and security status reporting. Prerequisites: CPIS 511, CPSC 561.

CPIS 515: Information Security for System Certifiers – This online course will give students a deep understanding of system certification and accreditation, and allow students to act as system certifiers. Topics include system certification and accreditation, prerequisites to certification, system registration, life-cycle management, system evaluation, and certification reporting. Prerequisites: CPIS 511, CPSC 561.

CPIS 516: Information Security Risk Analysis – This online course will provide students with an understanding of risk analysis for information security professionals. Topics include life cycle activities, identification and implementation of controls, certification and accreditation, testing and evaluation, threat and adversary analysis, mission and asset assessment, vulnerabilities analysis, and training and awareness. Prerequisites: CPIS 511, CPSC 561.

CPIS 570: Introduction to Research in Information Security – This online course will introduce the student to the professional open literature as well as other sources in Information Security. The student will investigate multiple areas or problems, and assimilate, integrate, and present the findings in multiple scholarly online seminars. Prerequisite: Permission of the Information Security Graduate Coordinator.

CPIS 574: Information Security Research 1 – This online course will provide practical experience in applying information security research techniques and methodologies from a number of different areas over an extended period of time. The student will analyze, design, evaluate, and apply new research findings or technological advances, develop a final product, and present the work in a formal oral presentation. Prerequisite: CPIS 570.

CPIS 575: Information Security Research 2 – This online course is a continuation of CPIS 574 and will provide practical experience in applying information security research techniques and methodologies from a number of different areas over an extended period of time. The student will analyze, design, evaluate, and apply new research findings or technological advances, develop a final product, and present the work in a formal oral presentation. Prerequisite: CPIS 570, CPIS 574.

CPSC 561: Legal Impacts of Computer Security Solutions – This course in computer security focuses on the foundation laid in CPSC 325 and CPSC 326. Students are presented with the legal rational behind the technical solutions studied in CPSC 325 and CPSC 326. Criminal, civil, regulatory and intellectual property law will be discussed in the context of professional computer environments. Federal and State computer security statutes will guide discussions. Student reports and presentations will reinforce the subject matter. This course may not be used as an elective by Computer Science Master’s candidates.
3.4 Learning Experiences and Instructional Methods

Many different learning experience and instructional methods are used in the Information Security Graduate Program. Some courses use experimental learning, working with computing technologies to determine their vulnerabilities. Students working online are required to participate in class discussion through chat room style applications. Students are able to make presentations to the entire class via webcam technologies. Other methods for practical learning include the types of assignments which are used to assess students. Each of the assessment techniques are used to allow for a good variety of practical experiences.

Practical or experiential learning is incorporated by requiring student to complete laboratory assignments that typically involve configuring, maintaining, or administering various tools or systems in a virtual computing environment (e.g., VMWare or VirtualBox running on a guest machine that in turn runs machine images for various assignments [16], [17]).

- Exams: As in on-campus courses, with the student responsible for finding a proctor.
- Class Participation and Discussion: Use of chat-room technology for discussion, as available in WebCT, Moodle, or other web-based learning management systems.
- Interactive In-Class Work: Again, using chat-room technology where the students respond to exercises given by the instructor.
- Case Studies: Students are required to report on real-life scenarios as assigned by the instructor. Reports can be in written form, or as part of discussion.
- Projects: Typically computer programming or implementation projects.
- Research Papers: As in on-campus courses.
- Student Presentations: Students record a presentation and then submit it to a server so that others in the class can view the presentation.
- Team Exercises: Groups of students working on exercises as above, and then submit a report in writing or as part of discussion.

The implementation of the program was initially designed around the cohort model, where students enroll into the first year of the program, then progress together with an establish cohort of students. This model was chosen to provide the opportunity to establish student support relationships so that students might help each other more readily, when needed, based on an established relationship via the cohort. We learned early on that the cohort model imposes certain restrictions on student that may not always prove to be in the best interest of every student. As such, we have moved to a more flexible cohort, whereby we will accept new students into the program during any stage of the first year of classes. In this way, students have more flexibility as to when the start their graduate education. After the first year of open admissions, the cohort is closed until the completion of the second year of classes.

4. Conclusion

The ESU Information Security Graduate Program is a rigorous technical program for students with undergraduate experience in Computer Science, Computer Security, or Information Technology, and interested in furthering their knowledge in system security administration. The program was designed based on the 6 CNSS Standards and includes research opportunities and a required thesis.

During the summer of 2011, the first cohort completed the program. Besides completing the courses based on the CNSS Standards, at the time of this writing, four students have successfully defended their theses in the areas of Compromising Physical Access Control Systems, SSL Vulnerabilities, Layer 2 Network Security Protocols, and Privacy in Online Social Interactions. The other four full-time students in the program are planning theses in the areas of Open Source Intelligence, Electronic Voting, Information Warfare, and Intrusion Detection Systems. We have improvements to the courses and the program during the Summer of 2011 and started our second cohort in the Fall of 2011. Overall, it has been a successful experience.

References:


[16] VMWare. VMWare Virtualization. [Online]. http://www.vmware.com/