Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

# A Bachelor of Science Degree in Computer Security: The Experiences of a National Center of Academic Excellence in Information Assurance Education

N. Paul Schembari, Ph.D.

**Abstract—The East Stroudsburg University of Pennsylvania undergraduate Computer Security Program is offered as a model for colleges and universities who would like to incorporate information assurance education, and perhaps a new degree program, into their existing computer science programs. The lessons learned by the faculty involved in the ESU program will be illustrated.**

**Index Terms—Computer Security, Information Assurance, Education**

## I. Introduction

As more universities enter the fields of Information Assurance (IA) and Computer Security at the Bachelor's level, it is important to determine the qualities of good undergraduate programs in these fields. It is also important to determine if four-year institutions can easily incorporate new programs in these fields. Because of the novelty of the discipline, and especially its development at the undergraduate level, these are concerns that IA educators have only begun to address. We attempt partial answers with an analysis of an undergraduate program in computer security. However, we do not infer that this is the only possible methodology for the implementation of an IA Bachelor's program; instead, we share the experiences of our implementation.

East Stroudsburg University of Pennsylvania (ESU) is a National Center of Academic Excellence in Information Assurance Education, one of 59 such institutions in 2004 – 2005. The University has experience with the implementation of a Bachelor of Science degree in Computer Security. In fact, it was the first institution to award Bachelor's degrees in Computer Security, where other institutions offer certificates or concentrations in IA related fields.

In this analysis, we begin by examining the makeup of ESU and its Computer Science Department. We then look at the University's Computer Security program with a deep inspection of the specific IA courses required for the major. Finally, the special experiences of the faculty involved with the program will be shared.

## II. The East Stroudsburg University of Pennsylvania Computer Science Department

East Stroudsburg University of Pennsylvania is one of fourteen institutions in the Pennsylvania State System of Higher Education. The University is located in northeast Pennsylvania in Monroe County, a two hour drive north of Philadelphia or west from New York City. ESU was founded in 1893 as a teacher's college, and has now evolved into a university with three schools. The Computer Security Program is housed in the Computer Science Department, a department in the School of Arts and Sciences.

Attending the University are more than 6,000 students, including over 1,000 graduate students. The Computer Science Department has approximately 140 Computer Science majors, of which over 50 are Computer Security majors. The Department also has approximately 40 graduate students in Computer Science with many performing research in information assurance. Since 1976, the Department has awarded over 500 Bachelor's and over 100 Master's degrees.

The Department offers rigorous Bachelor's and Master's degree programs in Computer Science which closely follow the ACM preparation recommendations [1], and a competitive Bachelor's program in Computer Security. Student admission standards are high, and extensive class work, laboratory experience, and project involvement are required for successful development of students as problem solvers. The quality of the education is a testament to its dedicated and experienced faculty. The Department has ten full-time faculty members with an average of almost twenty years of teaching experience and an average of over five years in industry. The Department also employs a varying number of staff computer scientists for research support.

The Department is the lead partner in the ESU Center for Computer Security and Information Assurance [2]. This center is responsible for the creation and maintenance of the University's IA coursework and for building relationships with outside organizations such as Backbone Security, Northampton Community College (Monroe County, PA),

ISBN 1-933510-99-4/05/$15.00 

Monroe Career and Technical Institute, Drexel University, Rider University, and the Pittsburgh Digital Greenhouse. Such partnerships have lead to research, other curriculum, and projects involving economic development in information assurance.

## III. Overview of the ESU BS in Computer Security

The ESU Computer Security Program was designed to create well-rounded graduates with an excellent foundation in computer science as well as in-depth education in both the technical and non-technical aspects of information assurance. Since graduating security engineers need to communicate clearly with non-technical co-workers and with each other, classes which enhance communication skills are required for the program.

Of the 120 total credits needed for graduation, over 40% (50 credits) must be completed in the University's General Education Program. In essence, a liberal arts general education program, the University's goal is to provide a broad-based education in history, literature, politics, art, science, economics, and physical education. The Department also requires its majors to complete 31 credits of coursework (with some General Education overlap) with specific objectives. Computer Security graduates must be able to communicate well; hence English Composition, Technical Writing, and Speech Communication are required courses. Computer Security students must also have a firm foundation in mathematics, hence Calculus 1 and 2, Discrete Mathematical Structures, and Statistics 1 are required. Finally, Computer Security students must have a clear understanding of the scientific method; to that end, two semesters of laboratory science are required, with Physics 1 and Electronics recommended.

ESU Computer Security students must complete eight basic courses in computer science: Introduction to Programming and Problem Solving, Computer Organization, Linear Data Structures, Assembler Programming, Operating Systems, Non-Linear Data Structures, Networking and Data Communications, and Database Systems. In addition, three electives must be chosen from a wide range of offerings: Expert Systems, Artificial Intelligence and Heuristic Programs, Machine Learning, Software Engineering, Natural Language Processing, Compiler Construction, Real-Time Systems, Algorithmic Graph Theory, Object Oriented Programming, Web Programming and Security, Programming Using Visual Basic, Programming Languages, Building Graphical User Interfaces, Computer Graphics, etc.

To give majors in-depth background in information assurance, six courses specific to the field are required for the Bachelor's degree in Computer Security. These courses are entitled Fundamentals of Security Engineering, Risk Analysis/Certification and Accreditation, Applied Computer Cryptography, Legal Impacts of Computer Security Solutions, Applied Network Security, and Security Engineering Internship and will be described in Section IV. Graduates of this program emerge as well-educated information assurance professionals, with CNSS certifications NSTISSI 4011 and 4012 [3]. In the near future, ESU expects to be authorized to confer other NSTISSI certifications as well.

## IV. ESU Computer Security Coursework

Six courses in information assurance are required of all ESU Computer Security Bachelor of Science candidates. These courses were designed with the NSTISSI certifications in mind, but reformulated to meet the desires of the Computer Science Department.

### *A. Fundamentals of Security Engineering*

The first IA course for ESU Computer Security majors is *Fundamentals of Security Engineering*, a course taken by junior majors or as an elective by junior and senior Computer Science majors. To ensure student maturity, the upper level sophomore course Non-Linear Data Structures is prerequisite for this course.

*Fundamentals of Security Engineering* is a lecture and discussion based course where students are introduced to the formal concepts of information assurance. We of course cover the basic ideas of confidentiality, integrity, availability, identification and authentication, and non-repudiation. In particular, the course gives an overview of computer attacks and computer crime, access control, elementary cryptography and PKI, Certification and Accreditation (as defined by DITSCAP [4] or NIST Special Publication 800-37 [5]), malicious code, physical security, network security including firewalls, intrusion detection, VPNs, and legal and ethical issues in the field. This is a bold syllabus for a one semester course, but since the focus is to give the students and overview, it is achievable.

The instructors for this course have traditionally chosen Security in Computing [6] by Pfleeger and Pfleeger as a course text. The instructors will typically assign homework and in-class problems as well as giving multiple exams. It should be noted that this course acts as a prerequisite for all other ESU information assurance coursework.

### *B. Risk Analysis / Certification and Accreditation*

The second IA course for ESU Computer Security majors is *Risk Analysis / Certification and Accreditation*, usually taken during the second semester of the junior year. This course allows students to experience the security analysis of an information system. About two-thirds of the semester is spent on a discussion of the NIST Federal Information Security Management Act (FISMA) Implementation Project, a methodology for Certification and Accreditation of federal information systems. This includes lecture and discussion of the NIST Special Publications *800-18: Guide for Developing Security Plans for Information Technology Systems*, *800-37: Guide for the Security Certification and*

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

*Accreditation of Federal Information Systems*, and *800-53: Recommended Security Controls for Federal Information Systems*. We also discuss FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*. The NIST Special Publications and FIPS relating to FISMA implementation are available on the NIST FISMA Implementation website [5].

Clearly, during this lecture and discussion time, students obtain the experience of analyzing and creating security policy, one of the major goals of the course. Exercises also reinforce the creation of Security Plans, Acceptable Use Policies, an analysis of threats to and vulnerabilities of an information system, etc. Then for the final portion of the course, the students perform a C&A exercise on a live information system. For such systems, we have been able to gain the cooperation of the University and local high schools.

During the C&A exercise, a multiple week experience, students visit the site of their assigned information system. Then, they analyze existing documentation of their assigned system and develop new Acceptable Use Policies and new Security Plans for the systems. Following the C&A process, they next design tests in order to analyze possible threats and vulnerabilities which are then approved by the volunteer site. After running the tests, a Security Test and Evaluation Report is generated by the students. They complete their projects by compiling a partial Certification Package and parts of the Accreditation Package. Throughout the exercise, students play various roles: sometimes the System Owner, sometimes the Certification Agent, and sometimes the Accrediting Official.

Finding a textbook for our *Risk Analysis / Certification and Accreditation* course has been troublesome. Two instructors have tried Information Security Risk Analysis by Peltier [7], and both found the book lacking. In the latest run of the course, the instructor chose to use only the FISMA Implementation documentation from the NIST website.

### *C. Applied Computer Cryptography*

As students enter their senior year in the ESU Bachelor's Program in Computer Security, they next take the *Applied Computer Cryptography* course. The Department feels that no degree in Computer Security could be complete without knowledge in basic cryptology. In this class, students begin with a study of basic encryption and continue onto the difference between block and stream ciphers, as well as symmetric and asymmetric ciphers. We discuss the elementary substitution and transposition ciphers, as well as the use of XOR. The cryptanalysis of each of these ciphers is also studied.

After discussing the basic historical ciphers, we move to more modern ciphers. We begin analyzing DES. One of the instructors has found the use of S-DES, as defined by Edward Schaefer [8, page 56], to be an invaluable tool for greater student insight. To complete the study of symmetric ciphers, AES is discussed. The class also studies modes of operation with regard to these modern symmetric ciphers. For the remainder of the course asymmetric ciphers and digital signatures are analyzed. The focus here is on RSA and Diffie-Hellman, with some time spent on Elliptic Curve Cryptography and the Digital Signature Standard.

An important point for this course is to allow students to "immerse themselves" in the ciphers. To this end, exams are used to test concepts, and programming exercises are used to determine the depth of student knowledge. Each student writes approximately 10 programs in a semester, each of which involves the programming of ciphers.

Two different books have been used as required texts: Applied Cryptography [9] by Bruce Schneier and Cryptography and Network Security [8] by William Stallings. The second text has the advantage of covering AES while the first has the advantage of more information with regard to other ciphers and protocol analysis.

### *D. Legal Impacts of Computer Security Solutions*

Students complete the *Applied Computer Cryptography* class in the first semester of their senior year along with our "Law and Ethics Class", *Legal Impacts of Computer Security Solutions*. Again as a lecture and discussion class, students are exposed to various laws relating to Computer Security as well as ethical issues. Two different instructors for this course have followed the development in Bowyer's text, Ethics and Computing [10], adding law and more ethical case studies to the mix. One instructor has used Spinello's Case Studies in Information Technology Ethics [11] for such applied situations.

Following Bowyer's development, the class begins with a discussion of ethics in general. We then look at critical thinking skills, and professional codes of ethics. With regard to these topics, some laws are discussed, but the focus for this beginning part of the course is ethics. When we arrive at the next topic – cracking and computer security, we spend much time on the discussion of various laws. Roy Girasa's text Cyberlaw [12] is used as a reference. Discussed laws include the First Amendment, the Computer Fraud and Abuse Act, laws on wire fraud, the Racketeer Influenced and Corrupt Organizations Act, the National Stolen Property Act, and the Identity Theft and Assumption Deterrence Act. We also discuss the old Federal Sentencing Guidelines, but with the latest Supreme Court decision on these guidelines, this topic may be dropped.

The class then proceeds to discuss the relationship between encryption, privacy, and the law enforcement need for legal eavesdropping. With this regard, ethical issues are raised as well as related laws, such as the Fourth Amendment, the Electronic Communications Privacy Act, the

Communications Assistance for Law Enforcement Act, and laws related to the export of encryption. With regard to privacy, the class also discusses California's new privacy protection law, the Health Information Portability and Accountability Act, the Financial Modernization Act, the USA Patriot Act, the Total Information Awareness program, and issues with regard to the use of biometrics.

The course finishes with a discussion on intellectual property. We discuss Article 1 of the U.S. Constitution and laws and ethical situations with regard to patents, copyrights, trade secrets, and trademarks. Other laws such as the Anticybersquatting Consumer Protection Act, the Truth in Domain Names Act, and the Digital Millennium Copyright Act are discussed. Since students in this class are close to internships and employment Non-Disclosure Agreements and Non-Compete Agreements are also part of the curriculum.

While the instructors have followed the development of Bowyer's text, the lack of any legal issues in this book has been quite troublesome. Instructors have discussed once again moving away from using a text in this course, and instead using online materials as we do in the *Risk Analysis / C&A* course.

### *E. Applied Network Security*

*Applied Network Security* is the capstone course for the major. Students in this course experience lecture and discussion of applied security topics as well as a two-hour weekly lab. The class takes the material learned in all previous IA classes and applies it in a laboratory setting. For lecture and discussion, different instructors have followed different approaches. One instructor chose to follow the work of Holden in Guide to Network Defenses and Countermeasures [13]. Here the topics covered include foundations of network security, designing a network defense, risk analysis and security policy design, choosing and designing firewalls, strengthening and managing firewalls, setting up a VPN, intrusion detection, incident response, and ongoing management. The instructor found this text a bit elementary for a senior level undergraduate course and will probably change in the future.

For lecture and discussion, the second instructor chose Skoudis's Counter-Hack [14]. This text seems more appropriate for the level of the student and will probably be used again. Topics covered following this development include the analysis of how an attack can occur on an information system and the appropriate defenses. The actual topics include an introduction to attacks and attackers, an overview of networking, UNIX, and Windows systems, an attacker's reconnaissance, scanning networks, application and operating system attacks, network attacks, Denial of Service attacks, Trojans and backdoors, and how an attacker avoids detection.

The more valuable portion of the course consists of laboratory research and experimentation by students. The lab work has been used to reinforce the development during lecture and discussion, and this seems to be successful. Lab topics have included using networking tools, analyzing network traffic, sniffing, improving policy, performing limited risk analysis, detecting weak passwords, working with Linux iptables, working with a commercial firewall, working with a commercial IDS, setting up a VPN, performing elementary forensics, etc. A good reference for laboratory work, which we may use in future offerings of this course, is Whitman and Shackleford's Hands-On Information Security Lab Manual [15].

### *F. Security Engineering Internship*

While *Applied Network Security* acts as the capstone course in the major, the *Security Engineering Internship* acts as the capstone experience. In this course, students are required to work at a job site for 180 hours in order to earn three credits, as required by the major. Some students work longer to receive more credit with a maximum of 12 credits allowed.

There are no class sessions for such a course, but the instructor is responsible with keeping in contact with students, reviewing student logs, and meeting with the student and supervisor on site. Students will also write a paper on their experience and sometimes make an oral presentation. Students taking this course have completed varied assignment from working on network security at a local hospital to helping in the development of a security product. Some have worked with a local security firm, Backbone Security, on their products, while others have worked on the development of their own products, in the application of economic development. The Department has received funding from the state (PA) to help its students with such product development. Some of our students have also won product development competitions using their internship projects.

## V. LESSONS LEARNED

### *A. Textbooks*

It is clear from our analysis of the ESU IA coursework that the need for good textbooks has not been answered. We make this challenge to the IA academic community – improve the textbooks in the field, especially with regard to security analyses and legal issues.

An informative book that teaches students and professionals how to perform a security analysis of an information system is needed. Miles, et al, have recently come out with the text Security Assessment: Case Studies for Implementing the NSA IAM [16] which gives an overview of the NSA INFOSEC Assessment Methodology, but it lacks a companion text of the NSA INFOSEC Evaluation

Methodology. For a description of the IAM/IEM see the NSA website [17].

We believe that the needed text on security analyses of information systems would cover the existing standardized methodologies such as the FISMA Implementation Project and the NSA IAM/IEM. It could also include techniques used by industry which many feel are effective yet not standardized. The text should give students the opportunity for hands-on labs applying related investigative techniques. The culminating exercise in the text would be the analysis of a "live" information system following the text development. While the course instructor could arrange for students to perform such an exercise, the text should give examples of previous student results.

The second area of text need is ethical and legal issues in IA. While a combination of Bowyer's and Girasa's texts can be used, a merged text would be preferable. We are now investigating Gift of Fire [18] by Sara Baase as a possible replacement, but it may lack the legal background that is necessary for IA students.

We believe that the needed text of ethical and legal IA issues should cover the necessary topics of computer crime, encryption and law enforcement's need for wiretapping, privacy, and intellectual property. It should also give students the opportunity to have active discussions on the ethical issues related to these topics. Open questions on the covered topics should be illustrated to facilitate student discussion. Finally, since laws constantly evolve, the text should give students the opportunity to research the up-to-date laws in the covered areas.

### *B. Class Calendar and Level*

While the ESU IA coursework has been presented in the order intended for student enrollment, we have found that students will sometimes take classes in a different order. For example, juniors have taken the *Applied Network Security* and *Legal Impacts of Computer Security Solutions* classes with success, and seniors have taken the *Risk Analysis / C&A* class while it is meant for juniors. The *Fundamentals of Security Engineering* class acts a prerequisite to all other classes, and this seems to allow students enough background to succeed in the other courses.

We have also determined that the *Fundamentals of Security Engineering* and *Applied Network Security* (ANS) courses may be listed at too high a level. Here, we mean that the first course may not be comparable to other courses the Department offers on the junior level, and the second course may not be comparable to senior courses. We have considered placing "Fundamentals" on the sophomore level and ANS on the junior level. We would then create a senior level project course more advanced than ANS with students developing tools instead of using tools.

### *C. Student Involvement*

As is often the case, we have found that active student involvement leads to the best learning. For example, in "Fundamentals", when the students work on group exercises with regard to securing a network, they are the most involved, and seem to get more out of the class. During the lecture and discussion portion, the students seem less involved with some adding to discussion, but others not.

In the *Applied Computer Cryptography* class, students get the most out of the programming of the ciphers, again "getting their hands dirty". This leads to more knowledge on the ciphers. In the *Legal Impacts of Computer Security Solutions* course students seem most involved in the class discussions, and especially when they have researched the issues and laws before class. A technique that has worked in this class is to ask students to produce a "brief" on the issue to be discussed in the following week. This student involvement has generated the best classes after the student research is complete.

The *Risk Analysis / C&A* course which involves students in the security analysis of a "real live" system has been quite successful. Students have enjoyed this experience and remember what they have learned. In *Applied Network Security*, students work with real tools in the lab situation and again remember what they have learned. Finally, many students have informed us that the best experience in the major is the *Security Engineering Internship* which allows them to work side-by-side with practicing security professionals.

### *D. Double Major*

Because of the extensive background in computer science during a student's first two years, students have found it easy to actually complete Bachelor's degrees in both Computer Science and Computer Security. Courses in one program will count as electives in the other program, so a student need only complete a few extra courses to earn both degrees. Such a student must complete the following courses in the ESU Computer Science Department plus one Computer Security elective:

- Introduction to Computer Programming and Problem Solving
- Computer Organization
- Linear Data Structures
- Assembler Programming
- Operating Systems
- Non-Linear Data Structures
- Issues in the Practice of Computer Science
- Fundamentals of Security Engineering
- Risk Analysis / Certification & Accreditation
- Programming Languages
- Networking and Data Communication
- Applied Network Security
- Database Systems

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

- Applied Computer Cryptography
- Legal Impacts on Computer Security Solutions
- Computer Science Internship
- Security Engineering Internship

Note the two internships – one for each major.

## VI. Conclusion

The ESU Computer Security Bachelor of Science degree is a rigorous program of study which leads students to become well-educated security engineers after only four years of undergraduate study. We believe that colleges and universities can use this program as a model for their own programs. In fact, since the ESU Computer Science program closely follows the ACM recommendations for undergraduate programs, it is possible for other institutions that follow ACM to incorporate the ESU Computer Security program. The retraining of a university's faculty and an eagerness to succeed in IA education will allow such an institution to have success with their own program.

*The author offers thanks to the ESU Center for Research and Economic Development for help with the description of East Stroudsburg University given in Section II.*

## VII. References

[1] Association for Computing Machinery; *ACM Curricula Recommendations*, January 2005; Retrieved on March 1, 2005 from http://www.acm.org/education/curricula.html.

[2] East Stroudsburg University; *East Stroudsburg University Center for Computer Security and Information Assurance*, January 2005; Retrieved on March 1, 2005 from http://www.esu.edu/compusec/

[3] Committee for National Security Systems; *CNSS Library*; Retrieved on February 15, 2005 from http://www.nstissc.gov/

[4] US Department of Defense; *DoD Information Technology Security Certification & Accreditation Process*, January 2005; Retrieved on March 3, 2005 from http://iase.disa.mil/ditscap/ .

[5] National Institute of Standards and Technology; *FISMA Implementation Project*, March 2005; Retrieved on March 3, 2005 from http://csrc.nist.gov/sec-cert/.

[6] Pfleeger, Charles P. and Pfleeger, Shari Lawrence; Security in Computing, 3rd edition; Prentice Hall Publishing, Upper Saddle River, New Jersey, 2003.

[7] Peltier, Thomas R.; Information Security Risk Analysis; Auerbach Publishing, Boca Raton, FL, 2001.

[8] Stallings, William; Cryptography and Network Security, 3rd edition; Prentice Hall Publishing, Upper Saddle River, New Jersey, 2003.

[9] Schneier, Bruce; Applied Cryptography, 2nd edition; John Wiley and Sons Publishing, New York, 1996.

[10] Bowyer, Kevin W.; Ethics and Computing, 2nd edition; IEEE Press, New York, 2001.

[11] Spinello, Richard A.; Case Studies in Information Technology Ethics, 2nd edition; Prentice Hall Publishing, Upper Saddle River, New Jersey, 2003.

[12] Girasa, Roy J.; Cyberlaw; Prentice Hall Publishing, Upper Saddle River, New Jersey, 2002.

[13] Holden, Greg; Guide to Network Defenses and Countermeasures; Thomson Course Technology Publishing, Boston, MA, 2003.

[14] Skoudis, Ed; Counter-Hack; Prentice Hall PTR Publishing, Upper Saddle River, New Jersey, 2002.

[15] Whitman, Michael E. and Shackelford, David M.; Hands-On Information Security Lab Manual; Thomson Course Technology Publishing, Boston, MA, 2003.

[16] Miles, Greg, et al; Security Assessment: Case Studies for Implementing the NSA IAM; Syngress Publishing, Rockland, MA, 2004.

[17] US National Security Agency; *INFOSEC Assurance Training and Rating Program*, October 2004; Retrieved on March 3, 2005 from http://www.iatrp.com/main.cfm.

[18] Baase, Sara; A Gift of Fire, 2nd edition; Prentice Hall Publishing, Upper Saddle River, New Jersey, 2003.