

AC 2007-1394: AN INTERDISCIPLINARY APPROACH TO INFORMATION SYSTEMS SECURITY EDUCATION: A CASE STUDY

Sohail Anwar, Pennsylvania State University-Altoona College

Dr. Sohail Anwar is currently serving as an associate professor of engineering and the Program Coordinator of Electrical Engineering Technology at Penn State University. Altoona College. Since 1996, he has also served as an invited professor of Electrical Engineering at IUT Bethune, France. Dr. Anwar is serving as the Production Editor of the Journal of Engineering Technology and an Associate Editor of the Journal of Pennsylvania Academy of Science.

Jungwoo Ryoo, Pennsylvania State University-Altoona College

Jungwoo Ryoo is an Assistant Professor in Information Sciences and Technology at Penn State Altoona, Pennsylvania. His main research interests include information assurance and security, software engineering, and networking. More specifically, he is interested in software security, network/cyber security, security management particularly in small and medium-sized organizations, software architecture, Architecture Description Languages (ADLs), object-oriented software development, formal methods, and requirements engineering. He has a significant industry experience (Sprint and IBM) in architecting and implementing secure, high-performance software for large-scale network management systems. He received his Ph.D. in Computer Science from the University of Kansas in 2005.

Harpal Dhillon, Excelsior College

Dr. Harpal Dhillon is currently the Dean of the School of Business and Technology at Excelsior College. In the past he has taught undergraduate and graduate Courses in Information Systems, Software Engineering, and Project Management at University of Maryland, Southwestern Oklahoma State University, and George Washington University. Dr. Dhillon worked as owner/senior executive in three systems engineering companies over a period of 20 years. His research interests are in the areas of Human-Computer Interaction, Quality Assurance, and Applications of IT in Telemedicine and Web-based Distance Learning. Dr. Dhillon is a member of the Executive Board of the NASA Oklahoma Space Grant Consortium. He secured a B.S. (Honors) degree in Mechanical Engineering from Punjab University, M.S. degree in Industrial Engineering and Management from Oklahoma State University, and Ph. D. in Operation Research and Systems Engineering from University of Massachusetts

David Barnes, Pennsylvania State University-Altoona College

AN INTERDISCIPLINARY APPROACH TO INFORMATION SYSTEMS SECURITY EDUCATION: A CASE STUDY

Abstract

Society is becoming increasingly dependent upon multi-user distributed information systems. Computer/communication networks facilitate increased productivity in organizations, but these systems also make the information, and information technology assets within the organizations vulnerable in the context of cyber security. Therefore, the designers and users of information technology and other production/logistic functions in these organizations have to be knowledgeable about the cyber security threats, and appropriate responses necessary for protecting the information assets. This growing awareness has led to a demand for information systems security education and training, not only in the information systems domain, but also in practically all engineering and technology activity areas.

This manuscript offers a perspective of how Penn State University-Altoona College, an undergraduate institution in Pennsylvania is taking steps to integrate ISA education into its four-year electromechanical engineering technology program. The college realizes that it is highly important for its engineering students to be knowledgeable about information systems security since engineers are now expected to have at least a basic understanding of current threats, the constant change in the nature of those threats, how these threats affect product development, personal safety, employee productivity, and organizational expenses.

Introduction

The specific intent of an information systems security education curriculum should be to train professionals who are able to analyze, develop, implement, maintain, and protect the appropriate information needed by an organization. An ISA education curriculum should be context sensitive and domain-specific, because it has to be based on unique cyber threat profile applicable to the organization business model. Also, the curriculum should be dynamic because new vulnerabilities are being discovered very frequently. Finally, the curriculum should be multidisciplinary because information assurance includes concepts from various disciplines such as business, computer science, computer engineering, information systems, social sciences, criminal justice, and law.

A universally accepted common body of information systems security knowledge is still being developed for all technical activity areas, except Computer Science and Information Systems. In United States, many educational institutions developed information security assurance (ISA) educational models based on standards and guidelines promoted by the government or other organizations resulting in a large variety of information systems security education curricula [1].

In 2005, the ACM Special Interest Group for Information Technology Education (SIGITE) Curriculum Committee developed a list of the topical areas for the information assurance and security (IAS) domain of the information technology body of knowledge [2]. The topical areas include:

- Fundamental Aspects of Information Assurance and Security

- Security Mechanisms (Countermeasures)
- Operational Issues
- Policy
- Attacks
- Security Domains
- Forensics
- Information States
- Security Services
- Threat Analysis Model
- Vulnerabilities

Several colleges and universities in the USA have made efforts to integrate most of the above mentioned IAS topical areas into their existing information technology curricula. For example, two senior level IAS classes have been integrated into the undergraduate information technology curriculum at Purdue University. The first one is titled “Network Security” and the second one is “Introduction to Computer Forensics”. At Weber State University [3], the undergraduate Information Systems and Technology (IS&T) majors are required to select either a software development emphasis consisting of three specialty courses (9 units) or the information security and networks emphasis comprising four specialty courses (12 units). Required courses for the information security emphasis include: data communications, LANs, computer crime, and computer forensics. The required coursework for the information security emphasis focuses on technical skills, emphasizes security issues, and introduces the ethical and legal concerns of managing security. The computer forensics course is the capstone course for the Weber State University IS&T majors. This course includes desktop and network investigations and security implementation. At Brigham Young University, the IAS concepts have been integrated into the entire undergraduate information technology curriculum. However, many educational institutions which are including the above mentioned topical areas in their undergraduate information technology curricula have done so by adding one or two electives focusing on network security, computer system security, or computer forensics.

In addition, many educational institutions are now offering information systems security certificate programs. Typically, these programs consist of a sequence of three or four courses covering several IAS topical areas. For example, the Information Security and Networking Management Certificate offered by Ferris State University consists of four 3 credit-hour courses which include principles of information security management and advanced security management. The 18-credit Information Systems Security Certificate offered by the Penn State University-Altoona College requires completion of four courses which include introduction to information systems, organization of data and information assurance, networking fundamentals, and networking security. In addition, upon approval from the Certificate Program Coordinator, students take two other information technology courses. Examples of such courses include secure web design and computer forensics.

This manuscript describes how Penn State University-Altoona College, an undergraduate educational institution in Pennsylvania is taking steps to integrate the IAS concepts into its four-year electromechanical engineering technology degree (BSEMET). The manuscript also describes an 18-credit information systems security certificate program recently instituted by

Penn State University-Altoona College to provide students with a set of courses that can be used as an individualized option or focus within an undergraduate degree program.

Rationale for Undergraduate Information Security Education

There is a well-recognized need to increase awareness and education on information systems security at all levels. Organizations of various sizes and types are constantly exposed to security threats such as malware, hacking attempts, thefts, social engineering, etc. The problem is exacerbated by the fact that more and more systems are interconnected and therefore it takes just one unsecured device to compromise an entire computer network. As a result, it is extremely important for individuals in an organization to clearly understand the nature of potential threats they are facing everyday and to do their best to minimize the risk.

However, before a threat is understood, it must be realized. Security attacks are often very difficult to detect because of their deceptive and secretive nature. Complacency makes the problem even worse. Everyday users of information systems should be more proactive to effectively defend themselves and their organizations against numerous threat agents. A drastic change in the mindset of people is necessary to accomplish any meaningful security objectives.

Once being well aware of security threats, one must acquire practical knowledge to mitigate risks associated with the threats. Computer literacy can lay a foundation for this. However, it is not sufficient. In order to be effective, one should attain an appropriate level of competency in *security literacy*.

The curricular materials could be leveraged to offer an academic program (such as a certificate program in information systems security) to full-time students. In essence, the authors of this manuscript have developed an interdisciplinary program that can be used in several majors. It provides students who are pursuing Business, Criminal Justice, or Liberal Arts degrees with a set of courses that can be used as an individualized option or focus in their major. It also offers a meaningful information systems credential that can lead to improved career opportunities.

Academic institutions can play a valuable leadership role in promoting information security and become an important partner, particularly to small and medium-sized organizations, that do not have all the resources generally available to larger organizations.

Design and Implementation of the Information Security Certificate Program

The curricular design process used to develop the above mentioned set of courses somewhat followed the steps proposed in [4] and [5]. These steps are listed as follows:

STEP 1. Identify job roles to be performed by graduates of the curriculum.

STEP 2. Identify revealing questions which uncover enduring concepts required and shared by these job roles.

STEP 3. Identify a body of knowledge consisting of topics and learning objectives that will be

achieved while investigating these questions and concepts.

STEP 4. Identify outcomes that demonstrate preparation for the job roles identified in STEP 1.

Following the above mentioned steps, an 18-credit information systems security certificate program was developed by Penn State University-Altoona College to help students develop proficiency in each of the following topical areas:

- computer networking and security for both wired and wireless systems
- installation and configuration of firewalls
- intrusion detection and prevention
- risk analysis and management
- security management using policies and access control
- fault tolerance
- disaster recovery planning
- computer forensics and investigations
- cryptography
- physical security

The following 3-credit courses constitute the above mentioned certificate program:

Required Courses:

- **Introduction to Information Systems:** This introductory course lays a foundation for studying more advanced, security-specific issues later in the curriculum and will introduce students to core issues in information sciences and technology assurance and security. Students are presented with many everyday security attack scenarios in which they are asked to develop appropriate defense mechanisms. For instance, one of the scenarios asks students to find concrete ways to defend their home computers against identity theft attempts like phishing. In addition to being well versed in common security problems and solutions, students are exposed to a broad spectrum of contemporary topics in the field of information systems security, which include social and legal issues, risk analysis and mitigation, crime intelligence and forensics, and information warfare and assurance.
- **Organization of Data and Information Assurance:** This course introduces the secure storage, retrieval, manipulation, analysis, and display of information. During the first half of the class, students learn all the essential skills required for effectively manipulating data. For example, they learn how to use Entity Relationship diagrams and query languages such as SQL in designing databases and implementing them. Once they are familiar with the basic database concepts, students are guided to delve into more security-oriented topics such as table access control, real-time alerts (for automatic notifications whenever certain policies are violated), restricting database access, etc for the second half of the semester.
- **Networking and Telecommunications Fundamentals:** Through many hands-on exercises, this course offers practical knowledge on installing and managing different types of networks, including Local Area Networks (LANs), Wide Area Networks (WANs), and the internet. . In particular, students learn (1) different types of data

communications networks, (2) the Open Systems Interconnection (OSI) seven layer model and vertical communication among the layer processes, (3) well-known networking/ telecommunications standards and protocols, (4) the roles and functions of different network devices such as hubs, switches, and routers, (5) the principles of wire-line and wireless telephony, and (6) network security threats and mechanisms for mitigating potential security attacks.

- **Network Security:** This course teaches how to effectively protect computing and networking infrastructures from external security threats in this course, by using freely available software tools such as firewalls, intrusion detection systems, encryption utilities, and network surveillance/management applications. The course consists of four major modules as shown below:

Module One	Security Fundamentals, Access Control, and Firewalls
Module Two	Encryption and Host Security
Module Three	Intrusion Detection and Application Security
Module Four	Incident and Disaster Response, and Security Management

Additional Courses:

- **Secure Web Design and Electronic Commerce:** This course teaches the development and maintenance of Web sites as well as E-commerce applications using the latest Internet Security technologies. First, students learn basic Web-authoring skills involving Hyper Text Mark-up Language (HTML) and scripting languages such as JavaScript. Building on the basic programming knowledge, they then acquire security-specific proficiency covering latest e-commerce security technologies (for example, Secure Socket Layer, third party payment services, Public Key Infrastructure, etc.) and different types of e-commerce security threats such as SQL injection and cross-site scripting attacks.
- **Cyber Forensics, Investigations, and Laws:** This course teaches how real-life cyber crime investigations are conducted using the latest forensics tools that help the handling of digital evidence, data analysis, and E-mail investigations.
- Other information technology courses can be also counted toward the certificate program if approved by the coordinator.

The courses described above are leveraged from an existing Information Sciences and Technology (IST) curriculum. For example, courses such as Introduction to Information Systems, Organization of Data and Information Assurance, and Networking and Telecommunications Fundamentals are core courses required for a four year IST program offered through the college of IST at the Pennsylvania State University. These courses are chosen for the certificate program since they are prerequisites for more security-oriented courses like Network Security. Note that the first course in the certificate program (namely, Introduction to Information Systems) plays a crucial role since it gives an introduction to the field of information assurance and security, and is meant to generate an interest so that students can

enthusiastically carry on with the rest of the certificate program. The course is also a general education course, and many students taking the course don't necessarily pursue a certificate in the beginning. An ideal scenario is that a significant number of students realize the importance of information systems security in their own respective disciplines and benefits it brings to their career opportunities once they are exposed to the various aspects of the field.

Integration of Systems Security Concepts into the BSEMET Degree

The Penn State University Altoona College Electro-Mechanical Engineering Technology baccalaureate degree program (BSEMET) is designed to provide graduates with the knowledge and skills necessary to apply current methods and technology to the development, design, operation, and management of electro-mechanical systems. The program is specifically intended to prepare graduates for careers in industries where automated systems are used and to prepare them both to meet current challenges and to be capable of growing with future demands of the field. It accomplishes this by accepting associate degree students from either mechanical or electrical engineering technology programs, cross-training them in the alternate discipline, and then exposing them to a spectrum of instrumentation and industrial controls concepts. The program culminates with a capstone project design course that requires students to assimilate the skills and knowledge from all their electrical, mechanical, instrumentation, and controls courses to develop and demonstrate a practical, working electro-mechanical device.

The primary objective of the BSEMET program is to provide graduates with the range of practical skills needed to be a successful technologist/engineer in any industry where modern industrial and manufacturing control systems are heavily used. This objective is accomplished by exposing students to a core of electrical and mechanical engineering topics, which are capped off with extensive studies in modern instrumentation and controls concepts.

Training in the technical subjects is supported by foundation courses in differential and integral calculus, ordinary differential equations, chemistry, thermofluids, statistical process control, and engineering economics. Students' written and oral communications skills are refined through a technical composition course and through extensive writing and speaking activities in the technical courses. These same activities support the secondary objective of the BSEMET program, which is to prepare graduates for life-long learning once their formal education is completed.

The Altoona College realizes that it is very important for its BSEMET degree students to be knowledgeable about information systems security since engineers are now expected to have at least a basic understanding of current threats and how these threats affect product development, personal safety, employee productivity, and organizational expenses. It is due to this realization that the Altoona College has started making efforts to integrate the information systems security concepts into its BSEMET curriculum. However, the BSEMET program requires students to complete a rigid 135-credit hours curriculum. There is absolutely no room in the curriculum for an additional course dealing with the basic concepts of information. Therefore, it has been proposed that the information systems security concepts be integrated into the selected BSEMET courses. The BSEMET courses targeted for the integration of information systems security concepts are described as follows:

- ED&G 100 (Introduction to Engineering Design): Introduction to engineering design processes, methods, and decision making using team design projects; design communication methods including graphical, verbal, and written methods. 3 credit-hours.
- EET 220 (Programmable Logic Controllers): An introduction to Programmable Logic Controllers (PLCs). Topics covered include PLC programming, troubleshooting, networking, and industrial applications. 2 credit-hours.
- EMET 430 (Programmable Logic Controls II): A second course in PLCs covering sequencing/shift instructions, program flow control, data and math instructions, PID loops, and machine communication. 3 credit-hours.

Efforts are currently underway to incorporate information systems security concepts into all of the above three courses. Since ED&G 100 is a required course for all the first-semester BSEMET students, it is an ideal course for exposing the BSEMET students to some form of basic information systems security principles. The systems security concepts to be incorporated into ED&G 100 course include:

- Basic networking concepts (OSI seven layers, Network Address Translation (NAT), wireless Local Area Networks (LANs))
- Types of security threats
- Basic security countermeasures (malware removal tools, personal firewalls, setting up routers properly, data back-ups, password management, Internet security including e-mail security, and encryption/decryption methods)
- Wireless LAN security
- Security principles (confidentiality, integrity, and availability)

The EET 220 is a sophomore level BSEMET course focusing on programmable logic controllers (PLCs). It is proposed that since the PLC technologies taught in this class use the Ethernet standard, students shall have some networking background. Assuming that the existing networking course module does not cover any security-related topics, a new course module can be introduced to supplement the current, general networking instructional module. The following security topics are technical in nature and highly relevant to the types of networking discussed in EET 220.

- access control (identification, authentication, authorization, accountability, access control models, access control technologies, and access control administration)
- firewalls (different types of firewalls, firewall architectures, and configuring, testing, and maintaining firewalls)
- intrusion detection systems
- basic cryptography (methods of encryption, public key infrastructure, and key management)
- physical security

The EMET 430 is a senior level BSEMET course focusing on advanced PLC concepts. It is proposed that since most of the students taking this class must be near their graduation, they

should be able to integrate their knowledge acquired by various other lower-level courses. For example, students should be able to use the technical security knowledge taught in EET 220 and to apply it in a broader context (particularly, in terms of system integration). A module focusing on security management can help students cope with this phase of their learning process. The module could teach the topics shown below.

- risk analysis,
- policies, standards, procedures, guidelines, and baselines,
- information classification,
- responsibility hierarchy, and
- security awareness.

The above mentioned efforts to integrate the information systems security concepts into the 4-year BSEMET curriculum are presently underway. It is expected that these efforts will be completed in the next two years. Once the above mentioned systems security concepts are integrated into the selected BSEMET courses, a formal assessment will be conducted to determine the effectiveness of these concepts in helping the BSEMET students develop a basic understanding of information systems security.

Conclusion

This manuscript describes how Penn State University-Altoona College, an undergraduate institution in Pennsylvania, is making efforts to integrate information systems security concepts into its four-year electromechanical engineering technology (BSEMET) degree program. The BSEMET courses targeted for the integration of the systems security concepts are described. The rationale for selecting these BSEMET courses is discussed. Additionally, the manuscript describes the 18-credit information systems security certificate program recently instituted by Penn State University-Altoona College to provide students with a set of undergraduate level courses that can be used as an individualized option or focus within a 4-year degree. The curricular design process used to develop this set of courses is outlined.

All the above mentioned efforts undertaken by the Penn State University-Altoona College to provide information systems security education to its students stem from the realization that there is a well-recognized need to promote awareness in information systems security at all levels. At present, no formal assessment has been conducted by the Penn State University-Altoona College to determine the effectiveness of its above mentioned efforts. However, such an assessment is planned for the near future.

Bibliography

1. Hentea, M., H. Dhillon, and M. Dhillon. "Towards Changes in Information Security Education." *Journal of Information Technology Education*, Volume 5, 2006.

2. Dark, M., J. Ekstrom, and B. Lunt. *"Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice."* Journal of Information Technology Education, Volume 5, 2006.
3. Logan, P. *"Crafting an Undergraduate Information Security Emphasis Within Information Technology."* Journal of Information Systems Education, 13 (3)
4. Reynolds, C. *"An Undergraduate Information Assurance Curriculum."* Proceedings of the 2003 IEEE Workshop on Information Assurance, 2003.
5. McTighe, J., G. Wiggins. *Understanding by Design.* Association for Supervision and Curriculum Development, Alexandria, Virginia, 1998.
6. Anwar, S. and P. Ford. *"Use of a Case Study Approach to Teach Engineering Technology Students."* International Journal of Electrical Engineering Education, 38 (1), January 2001, pp 1-10.