A FRAMEWORK FOR THE INTEGRATION OF INFORMATION SECURITY AND RISK ANALYSIS CONCEPTS INTO AN UNDERGRADUATE ENGINEERING TECHNOLOGY DEGREE

Sohail Anwar, Ph. D, Jungwoo Ryoo, Ph. D
Division of Business & Engineering
Penn State University, Altoona College

Abstract

Although information systems increase productivity in organizations, they also make the Information Technology (IT) assets within these organizations vulnerable in the context of cyber security. Thus, the designers and users of IT in these organizations need to have adequate education in the cyber security threats and be ready to take appropriate actions necessary for protecting their IT assets. The growing awareness has resulted in a significant demand for information systems security and risk analysis education. Proper training in security and risk analysis can be very helpful in confronting cyber security threats and protecting vital information. Problem solvers with appropriate skills and relevant experience are needed in the security and risk analysis domain. The Penn State University Altoona College realizes that it is very important for its BSEMET degree students to be knowledgeable about information systems security and risk analysis 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 and risk analysis concepts into its BSEMET curriculum. The main focus of this manuscript is a perspective on how Penn State University-Altoona College is taking steps to integrate the information security and risk analysis concepts into its four-year electromechanical engineering technology program.

Introduction

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 system should be more proactive to effectively defend themselves and their organizations against numerous threat agents. A drastic change in 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* [1].

The designers and users of information technology have to be knowledgeable about the cyber security threats, and appropriate responses necessary for protecting the information assets of their organizations. 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 [2].

The Pennsylvania State University-Altoona College has recently adopted and implemented a multidisciplinary Bachelor of Science degree program in Security and Risk Analysis (SRA). This undergraduate degree program is intended to teach students general framework and multidisciplinary theories that define the area of security and related risk analysis.

The above mentioned SRA undergraduate degree program provides a grounding in the analysis and modeling efforts used in information search, visualization, and creative problem solving. Courses in the SRA major also engage students in the multidisciplinary challenges and problems associated with assuring information confidentiality, integrity, and availability as well as the strengths and weaknesses of various methods for assessing and mitigating risks. The degree program also includes a detailed study of network management that plays a critical role in identifying, preventing, and responding to security-related incidents.

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 system.

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.

Integration Into the BSEMET Program

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 security. 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:

- EDSGN 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 275 (Programmable Logic Controllers): An introduction to Programmable Logic Controllers (PLCs). Topics covered include PLC programming, troubleshooting, networking , and industrial applications. 3 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.

- CMPET 211 (Embedded Processors and DSP): A study of Machine language architecture, and interfacing of microprocessor-based systems emphasizing applications of microprocessors and microcontrollers.

Efforts are currently underway to incorporate information systems security concepts into all of the above three courses. Since EDSGN 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 the EDSGN 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 275 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 275.

- 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 the 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 275 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
- Security awareness

The CMPET 211 (Embedded Processors and DSP) teaches machine language programming, architecture, and interfacing for microprocessor-based systems. Since the course focuses on software, this class provides an excellent opportunity to expose engineering students to software security concepts.

The Software Assurance Common Body of Knowledge (SwACBK) developed by the Department of Homeland Security (DHS) suggest that there are three core software security areas to be covered as shown below [3].

- The adverse: something or someone intending to do harm,
- The system: a software-centric mechanism exposed to the attacks by the adverse, and
- The environment: a context in which the adverse and the system interact with each other.

For the adverse part of SwACBK, we propose the following as the relevant topics for engineering students taking CMPET 211 include:

- Adversaries: this topic area characterizes different types of entities behind various software security attacks (e.g., cyber terrorists, script kiddies, black hat , etc.) so that students learn how to think like an attacker to be a better defender.
- Microprocessor or microcontroller-relevant attacks: Since CMPET 211 teaches students low-level programming languages such as Assembly and C, the class provides an excellent opportunity to introduce attacks that take advantage of vulnerabilities found in those languages. Therefore, threats such as buffer overflow attacks can be discussed in conjunction with computer memory management concepts such as stack, heap, NOP, and return addresses.
- Secure System Development Life Cycle (SecSDLC): In software engineering, there are a number of well-established software development methods collectively called software development life cycle (SDLC). SecSDLC refers to specialized SDLCs that have extra steps designed to produce secure software.

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.

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. Such an assessment will be conducted to determine the effectiveness of the information security and risk analysis concepts in helping the BSEMET students develop a basic understanding of information systems security.

References

1. Hentea, M., Dhillon, H., and Dhillon, M. (2006) “Towards Changes in Information Security Education.” Journal of Information Technology Education, Volume 5, 2006.

2. Anwar, S., Ryoo, J., and Dhillon, H. (2007) “An Interdisciplinary Approach to Information Systems Security Education: A Case Study”, Proceedings of the 2007 American Society for Engineering Education Annual Conference & Exhibition.

3. Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software, Department of Homeland Security, October 2007.

Biographical Information

Dr. Sohail Anwar is an Associate Professor of Engineering at the Altoona College of The Pennsylvania State University. In addition, he is a Professional Associate of the Management Development Programs and Services at The Pennsylvania State University, University Park. Also, since 2009, he has been serving as an Invited Professor of Electrical Engineering at the Shanghai Normal University, China. Dr. Anwar is currently serving as the Editor-in-Chief of the ***Journal of Engineering Technology*** and as the Series Editor of the Nanotechnology and Energy Series, Taylor and Francis Group/CRC Press. Dr. Anwar recently edited a book titled ***Nanotechnology for Telecommunications*** published by the Taylor and Francis Group/CRC Press in June 2010. Moreover, he is co-editing a book titled ***Advanced Nanoelectronics and Graphene Nanoribbon Technology*** to be published by the Taylor and Francis Group/CRC Press in 2011.

Jungwoo Ryoo is an Assistant Professor of Information Sciences and Technology at the Pennsylvania State University-Altoona. His main research interests include information assurance and security, software engineering and computer networking. He conducts extensive research in software security, network/cyber security, security management (particularly in the government sector), software architecture, Architecture Description Languages (ADLs), object-oriented software development, formal methods, and requirements engineering. He is the recipient of major state and federal government grants and also has substantial industry experience in architecting and implementing secure, high-performance software for large-scale network management systems. He received his PhD in Computer Science from the University of Kansas in 2005.