Experience Learned in Obtaining the CNSS IA Course Certification and the CAE/IAE designation at Polytechnic University of Puerto Rico (PUPR)

Alfredo Cruz, PhD
Graduate School, Polytechnic University of Puerto Rico
Hato Rey, Puerto Rico, alcruz@pupr.edu

Sandra Bonilla, MS CS
Graduate Student, Polytechnic University of Puerto Rico
Hato Rey, Puerto Rico

ABSTRACT

The authors from PUPR share their experience in obtaining the Committee on National Security Systems (CNSS) course certification and the Center of Academic Excellence in Information Assurance Eduaction (CAE/IAE) designation. IA is a field that is rapidly evolving in the IT scenario. The urgent need for information security professionals has brought together industry, government, and academic sectors, to define the requirements for IA education. Developing core courses for graduate and undergraduate IA programs with a Common Body of Knowledge (CBK) in IA is critical for new and practicing IT security professionals, including technical and managerial personnel. The CBK maps courses to information security elements required in industry, government, and academia. Standards are currently regulated by the Certified Information System Security Professional (CISSP) domains, National Security Telecommunications Information Systems Security Institution (NSTISSI) standards, and the National Institute of Standards and Technology (NIST). By obtaiing the CNSS certification and the CAE/IAE designation, an institution can compete for infrastructure, capacity building, and scholarship grants to provide exceptional educational experiences and collaboration opportunities between designated and aspiring institutions at local and national levels. This includes internships, faculty and student exchange, research and publications, funds for faculty and student research, scholarships, workshops, among other activities.

Keywords: CBK, IA, CAE/IAE, CNSS, NSTISSI

1. INTRODUCTION

Information Assurance is a new field that is rapidly evolving in the information systems and technology fields. Since the 90's the need for security professionals has become critical, bringing together industry, government, and academic sectors, to define current and upcoming requirements for information assurance and security education at the undergraduate and graduate level, and through certification.

Degrees are crucial for practicing IT professionals in information assurance; providing students with professional skills and knowledge to excel in their professions; and provides stakeholders with a clear and concise accounting of the knowledge and skills to be learned.

The development of core courses with a Common Body of Knowledge (CBK) in Information Assurance and Security (IAS) is needed to create IA curriculums. The Committee on National Security Systems (CNSS) course certification is based on mapping the courses to the information security elements that are required to fulfill the needs of: the industry, government, academia, CISSP domains, National Security Tele-communications

Information Systems Security Institution (NSTISSI) standards, and the NIST. This is a critical step in order to apply for the CAE/IAE designation. Since IA is a constantly changing field, reviewing these standards in the industry and government and applying the required changes to a CBK is imperative. The role that each course has in each of the IA knowledge areas needs to be mapped to industry and government needs (elements). Specialization areas need to be created in the programs that focus students knowledge and skills in specific areas of IA that are in great demand. The courses should combine what the industry is looking for in an employee and the learning interests of students in this area.

Finding a CBK through the CNSS course certification mapping process will lead to more effective academic programs and certifications in IA. This will contribute to increase significantly the number of competent IA faculty in academia, and IA professionals in the government and industries. It will also contribute to increase significantly the number of institutions with CAE/IAE and COE designations for the benefit of our Nation's security infrastructure, and national security organizations such as the NSA and the DHS.

2. INFORMATION ASSURANCE EDUCATIONAL BACKGROUND

In the early days, experts in the security area had military backgrounds, because the military had the technology, needs, and also the funding for the development of new technologies in the security area [1]. Military standards define numerous security disciplines, including computer security, information security, communications security, physical security, personnel security, operations security, and others, that are interrelated, but differently focused [2]. Activities like: employee awareness, operating procedures, social engineering, and system recovery, enable organizations to function in a secure manner, and need a comprehensive term to identify them. As an all-encompassing concept that covers all (safeguarding) aspects of securing information and technology, Information Assurance includes classified and non-classified systems, software, hardware, human resources, and the procedures to keep the information systems available and accurate [3].

Information security and information assurance fields are related and share the common goal of protecting the confidentiality, integrity and availability of information and intellectual assets. Information Security means protecting information and information systems from unauthorized access, use, modifications, damage and disruption [4]. Information Assurance (IA) is a term that covers the activities needed to assure the confidentiality, integrity, availability, and authentication; protecting and defending information and information systems. These measures include the restoration of affected information systems by incorporating protection, detection and reaction capabilities [5]. Information needs to be reliable, accurate, available at the appropriate time and verifiable as having come from a legitimate source, in order to serve the needs of the organization. Information assurance is an encompassing term, which includes hardware, software, classified and non-classified systems, human resources, and the procedures needed to keep the information in computer systems available, reliable and accurate [3].

3. JUSTIFICATION

The protection of information assets and the continuous advances in information security, pose significant challenges for academia, industry and the government sectors [6]. To address this need the President of the United States issued Presidential Decision Directive (PDD63), a Policy on Critical Infrastructure Protection, which prompted the NSA to established outreach programs like the designation as a Center of Academic Excellence in Information Assurance Education (CAE/IAE). The growing awareness for the need to protect information assets has led to a demand for Information Assurance training and education

Actually there is no standardized curriculum to teach Information Assurance in institutions of higher education in programs such as Computer Science or Computer Information Systems. Although Information Assurance educators have been looking closely at the best way to deliver the needed expertise, the only recommendation that currently exits is a draft that resulted from a workshop sponsored by the National Science Foundation (NSF) and the American Association of Community Colleges [7].

There are two dominant technology curriculum guidelines currently in use:

1) Accreditation Board for Engineering and Technology, Inc. (ABET) accreditation standard ("Criteria for Accrediting Computing Programs", 2008).
2) IS 2002 Model Curriculum Guidelines for Undergraduate Degree Programs in Information Systems, co-sponsored by: Association for Computing Machinery (ACM), Association for Information Systems (AIS) and Association for Information Technology Professionals (AITP) [8].

One major problem is that established curriculum bodies like the ACM, ABET and IEEE do not have a formal or effective standardized information security curricula model developed [9]. Furthermore, different questions arise about which and what subjects should be covered in an Information Assurance program for a graduate track level. Information Assurance is a field that has not matured sufficiently to develop processes associated with performing specific information security job tasks [10].

The main goal of universities that educate students in IT and information security are to prepare them to recognize and combat information system threats and vulnerabilities that could weaken the infrastructure of the nation [11]. The designation as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) is an asset for any university and is preceded by the CNSS course certification, where courses are evaluated through a mapping of specific required elements that apply to each course that has IA related topics.

The goals of this paper are to disseminate the experiences encountered while:

1) Acquiring the Information Assurance courseware certification from the CNSS for standards 4011 and 4013E for the Polytechnic University of Puerto Rico by doing the course mapping to understand the elements evaluated in Information Assurance education and which courses contain them. This leads to identifying the Common Body of Knowledge areas considered important for practicing information assurance professionals to provide students with the professional skills and know-how they require to excel in their professions by developing specialization areas and core courses for the design of IA programs and certifications.
2) Obtaining the DHS, NSA designation as a Center of Academic Excellence in Information Assurance Education for Polytechnic University of Puerto Rico. By complying with the required criteria for designation we can prepare professionals in computer and information security areas, which are of great demand worldwide, by understanding the overall interests and needs of the industry in the information security specialization areas.

4. RELEVANCE AND SIGNIFICANCE

In the past ten years due to world events and federal initiatives, Information Assurance has been a field that has grown rapidly. The need for knowledge and skills in Information Assurance has increased parallel to the needs in industry, government and academia [12]. When important assets of the organization (databases, networking, web applications and classified information of the computers) are attacked, damaged or threatened, business operations can be damaged or interrupted; and confidentiality and data integrity can be compromised. Bishop [13] identified the need for a standard curriculum in Information Security in two of his articles presented in the National Colloquium of Information System Security; and how these could be applied in the academia in an undergraduate, graduate, and doctoral level. In another presentation, Bishop [14] stated that at the undergraduate level, the curriculum should be focused on the application of the principles of computer security. If students want a deeper understanding and knowledge of the principles they would need to continue graduate studies or study on their own. However, graduate students will be more focused on the design and specifications to secure the systems, than on the implementation of these designs.

Kim and Choi [15] stated that in the development of an Information Security curriculum, experts in the field should determine the educational requirements for Information Security professionals. Since a formal definition of the basic principles of information security did not exist, this lack contributed to an unstructured approach to information security [16].

Standards for Information Assurance education, curriculum materials, and the process of completing the requirements for the National Center of Academic Excellence in Information Assurance and Education (CAE/IAE) have been developed by NIETP (National IA Education and Training Program). In 1999 there were seven Centers designated, the number increased to 50 in 2003, 66 in 2005, and currently there are more than 94 Centers, including the Polytechnic University of Puerto Rico (PUPR); which is one of the very few HSI's with the designation, and the only in Puerto Rico.

During the efforts of accrediting Information Technology as an academic discipline (a model curriculum), representatives of the ACM, IEEE, ABET and SIGITE stated that one of the major challenges was acquiring knowledge in the area of security. However the IT2005 Model Curriculum [17] presents Information Assurance and security as a core for any student in an Information Technology program, considering that knowledge in the area has risen sharply in importance in recent years [18].

Today, Information Assurance educators in areas like academia, government and industry are looking closely at the best way to deliver the needed expertise, success and improvements in the information assurance field.

5. RESEARCH ON INFORMATION ASSURANCE EDUCATION

The industry focuses upon applying information assurance and security to their infrastructure and proprietary information, and the government uses computer security to protect the national interest [19].
Several universities have developed programs focused on Information Assurance curricula for undergraduate levels. Programs in universities like Purdue University have resulted from collaboration and sharing among early Information Assurance educators in forums such as the Colloquium for Information Systems Security Education and governments grants, that are crucial to Information Assurance program development [20]. Mattord and Whitman [21] explain five approaches that should be analyzed and considered before developing an Information Assurance curriculum. Available resources, time, technology, faculty, money, and student demand, are elements that need to be considered before developing any of the following approaches:

1) Security elements added to existing courses
2) Security elements added to a capstone course or courses
3) Independent information security
4) Information security certificates/minors
5) Information security degree programs

When developing the IA curriculum we also have to consider that there are three types of information security programs that focus on different aspects of information assurance and security:

- Managerial Information Security – This program is not mainly focused on technical aspects and skills. It is based more on the administration and management of information security.
- Technical Information Security – This program covers the technical aspects and is one of the most popular and common IS programs.
- Balanced Information Security Program -A balanced program combines technical and managerial aspects into one program.

6. CURRENT ADVANCEMENTS IN INFORMATION ASSURANCE EDUCATION AT PUPR

Through the development of the Center of Information Assurance for Research and Education (CIARE), that is a key component for CAE designation, we have been able to make much advancement in IA education at the Graduate School, and in the undergraduate programs at the Department of Electrical and Computer Engineering and Computer Science (ECECS). CIARE has centered its efforts on the following activities: The development of technical certifications, training, workshops, conferences, and lectures, as a continuing education to professionals. This includes: special training for teachers and high school students; strengthening the Master in Science in Computer Science with a specialization in IA through the recruitment of top faculty researchers; collaborating research with the public and private sectors, including individuals; attracting and retaining outstanding PhD

faculty/researchers for the MS CS program; providing consulting services; participating in joint development partnerships; and promoting best practices in IA & cyber security.

The Center emphasizes on the participation of underrepresented groups. One of the aims is to expand our collaboration with the four-year colleges in Puerto Rico and sponsor some of their best senior students to participate in IA research projects. To encourage undergraduate participation we work closely with students in four-year colleges. We also include outreach programs to high-school students and teachers. Part of this outreach program is creating short courses in IA available to high schools, and allowing teachers to attend IA workshops.

In the last three years more than 150 graduate and undergraduate students have enrolled in Computer Forensics and Ethical Hacking courses. Actually, PUPR is the only academic institution in Puerto Rico to offer some these courses. Recently, certifications have also become very important for IT professionals as the need to up-date their knowledge and skills is constantly required.

PUPR currently has a Master in Science in Computer Science (MS CS-thesis option) and a Master in Computer Science (MCS-non-thesis option). These Master Degrees are the first in Puerto Rico, and have a specialization in Information Technology Management and Information Assurance (ITMIA).

In 2010 the Graduate School introduced a Graduate Certificate in Information Assurance and Security (GCIAS) [22] to highlight the ITMIA specialization as well as to prepare other Information Technology, Computer Engineers, and Information System professionals who are working in the development or maintenance of information and computer security systems or products, such as graduate engineers, scientists, or managers in related fields. This certificate helps these professionals develop a secure cyberspace and information structure nationwide. It prepares the student and professional with IAS skills that are already of great demand in today's fast paced, high-tech, competitive work areas. We have also been developing a Graduate Certificate in Computer Forensics that is expected to be offered soon.

Both certificates are supported by a state-of-the-art Computer Forensics and Investigation Laboratory that has more than $150,000.00 in Forensics Recovery of Evidence Devices (FRED) supercomputers. The FRED SC (**S**uper **C**omputer) is the first commercially available super computer designed and optimized for massive parallel processing and computation. Please see Figure 1.

Figure 1. FRED SC

7. APPLYING FOR THE CNSS CERTIFICATION AND THE CAE/IAE DESIGNATION

CNSS CERTIFICATION- MAPPING IA COURSES TO THE CNSS

This section will explain the process of applying for the CNSS Certification and the CAE/IAE designation. Before the creation of the CAE/IAE program in 1998, Information Assurance education was not common within academic programs. Information Assurance Courseware Evaluation (IACE) is a process that meticulously reviews

the courseware from commercial, government and academic sources that map to the national standards. This is determined by the National Security Telecommunications and Information Systems Security Committee, known as the Committee on National Security Systems (CNSS) [23].
The National Information Assurance Education and Training Program (NIETP) office within the Information Assurance Directorate at NSA, manages the IACE program. The NIETP operates under national authorities, serves as a National Manager for Information Assurance education, and develops training standards within the CNSS [24].

The CNSS provides a forum for the discussion of policy issues and sets the national policy, operational procedures, and guidance for the security of national security systems that is imperative. These systems contain classified information or involve: intelligence activities, cryptographic activities related to national security, and the command and control of military forces and equipment that is an integral part of a weapon or weapons system and/or critical to the direct fulfillment of military or intelligence missions.

The training/educational standards for information assurance and system security issued to date are [18]:

- NSTISSI-4011, National Training Standard for Information Systems Security (INFOSEC) Professionals
- CNSSI-4012, National Information Assurance Training Standard for Senior Systems Managers (SSM)
- NSTISSI-4013, National Information Assurance Training Standard For System Administrators (SA)
- NSTISSI-4014, Information Assurance Training Standard for Information Systems Security Officers (ISSO)
- NSTISSI-4015, National Training Standard for Systems Certifiers (SC)
- CNSSI-4016, National Information Assurance Training Standard For Risk Analysts (RA)

The standards were developed by the government as unclassified information to develop an information assurance community and to expand the education and training throughout the nation. The IACE program is located on a secure interactive website (https://app.cnss.gov/nietpcw352.nsf/), which certifies the institutions courseware, not its programs or certifications. The standards justify IA education, training, resource education, and help to increase the national security infrastructure.

Information system security professional standards (NSTISSI/CNSS 4011) need to be mapped for the CNSS certification and it is based on: Communication Basics; Automated Information System Basics; Security Basics; NSTISS Basics; System Operating Environment; NSTISS Planning and Management; NSTISS Policies and Procedures. NSTISSI 4011 responds to the need for a theoretical foundation for modeling the information systems security sciences, and addressing the needs for information systems security.

Mapping NSTISSI 4011 with CNSSI-4012, NSTISSI-4013, NSTISSI-4014, NSTISSI-4015 and/or CNSSI-4016 is the first requirement for the designation of the institution as a CAE/IAE [5]. PUPR chose the NSTISSI-4013, which requires a minimum training for the development and implementation of Information Assurance (IA) training for System Administrators (SA) and is related to the courseware of the Institution.

For NSTISSI-4013, NSTISSI-4014 and CNSSI-4016 a hierarchical level or bloom taxonomy is one of the best ways to categorize levels of questions commonly used in the educational area and to evaluate that the curriculum meets the needs of the students [25]. The levels are: 1) Entry - define, demonstrate, identify, outline, use; 2) Intermediate - design, manage, prepare, recommend, implement; and 3) Advanced - compare, evaluate, integrate, resolve, revise, verify

Entry level requires less skill and does not require any implementation or problem solving. In entry level NSTISSI-4013 the System Administrator will be able to describe and apply the appropriate actions to manage and administer an Information System in a secure manner.

IACE reviewers validate if the institution courseware covers and maps 100% of the elements; the institution should provide their course syllabus (objectives, topics, and references) as evidence. After the validation, the institution will receive a formal certification of its courseware, certifying that all of the specific standards are met. IACE certification is awarded at the annual Colloquium for Information System Security Education Conference [26].

Polytechnic University of Puerto Rico, is the first university in Puerto Rico that mapped 100% of the courseware for certification from the Committee on National Security Systems (CNSS) standards, completing the National Standards 4011 and 4013 (entry level). The CNSS courseware certification is valid for 5 years, after that the institution needs to recertify.

CAE/IAE DESIGNATION - Complying with the Nine (9) Required Criteria for the CAE/IAE Designation

Once the Institution has obtained the CNSS courseware certification, the next step is to apply for the CAE/IAE designation. To obtain the designation the institution has to comply with the nine required criteria established by the Department of Homeland Security (DHS) and the National Security Agency (NSA). The nine established criteria measure the applying institution's current IA resources, including: faculty, partnerships, IA curriculum and programs, research, collaboration, and laboratories, among others.

Criteria 1: Partnerships in IA Education

This criterion focuses on the outreach/collaboration efforts by the applying institution that extends IA education beyond the normal boundaries of the University and brings current IA practitioners into the IA Center. Institutions need to provide evidence of partnership(s) in IA education with minority colleges and universities, or K-12 schools, or 2-year community colleges, or technical schools. PUPR has always recognized the importance of partnering with business, industry, and government. Our partnerships help provide students with opportunities to work on real-world problems and networks, preparing them to seek employment in internships or post-degree jobs. PUPR has developed cooperative programs with industry and Government that also include collaborative research in Information Assurance. PUPR has professors with experience developing IA related courses for this and other academic institutions, including IA laboratories and curriculum. Some professors have collaborated in student and faculty interchange programs and have served as PI and Co-PI of various proposals to enhance research and education in IA.

Criteria 2: IA Treated as a Multidisciplinary Science

In this criterion it is required that the academic programs demonstrate that IA is not treated as a separate discipline, but as a multidisciplinary science with the body of IA knowledge incorporated into various disciplines. The School of Business at PUPR has graduate and undergraduate courses that introduce non-IA students to IA topics such as electronic commerce security, database connectivity and security, legal and ethical issues of information systems, among others. Students learn to analyze Internet business situations in which policies, ethics, and laws are put to the test. Courses cover topics such as information security and control, the ethical and social impact of information systems, e-business security planning (that includes electronic payment and e-commerce security), and security measures to protect information over communication lines with various preventive techniques. The institution should also prove that non-IA courses encourage papers in IA topics or projects, and should provide titles of thesis, dissertation, or projects in IA, or proof that IA topics are covered.

Criteria 3: University Encourages the Practice of IA

This criterion requires that the academic program demonstrates how the university encourages the practice of IA, not merely that IA is taught. The Polytechnic University has been very proactive in securing its networks. During the past year there have been significant changes on the way the networks and PUPR computers are being managed. PUPR reached the improvements needed to formalize the security policy and the procedures that go with it. The effort to enhance the information technology infrastructure and security has been a steady process.

Criteria 4: Academic Program Encourages Research in IA

This criterion focuses on encouraging student-based research and is important because research fuels the relevancy and currency of IA curricula. Institutions should provide titles and dates of thesis, dissertation, student papers, or projects in IA within 3 years of application. Our students are encouraged to participate in different research projects, thesis, and papers in the area of information assurance and security. Students have the opportunity to work with an established researcher where all of the necessary equipment and facilities are present. Working in joint research projects help the students become experts in a particular area of information assurance,

and gain valuable experience. This participation in research work will continue to enhance the current research capabilities and education of our students in IA disciplines

Criteria 5: Faculty Active in Current IA Practice and Research and Contribute to IA Literature

It should be clearly demonstrated that the faculty is active in current IA practice and research, contributes to IA literature, are members of IA professional societies or attend professional IA conferences. The depth and length of faculty expertise should be substantiated through submission of biographies. PUPR professors have participated in IA publications and papers as can be evidenced with recent publications. It is also important that the applying institution is awarded grants/funding for IA education and/or research development or lab equipment. PUPR provided a synopsis of IA related grants, funding, equipment donations, or other funding including date and approximate monetary value for the past 5 years.

Criteria 6: State-of-the-Art IA Resources

Criterion 6 states that faculty and students should have access to state-of-the-art IA resources and reference materials such as digital libraries, journals, books, links to related web sites, and laboratories. Examples of digital libraries are: ACM Digital Library, IEEE Xplorer Digital Library, and Safari Tech Books Online, among others.

PUPR has modern equipment for research and education in IA. Facilities currently available to IA students from the Graduate School and the ECECS Department include six laboratories. These laboratories have been established in the last four years with grants from the DoD, NSF, and the Puerto Rico Industrial Development Company (PRIDCO). Some are used for classroom activities and others for graduate research and studying. The basic goal of these laboratories is to support IA research and education in computer science and engineering.

Criteria 7: Focus Area or Area of Study in IA

The applicant Institution's IA program should be robust and active: It should have academic programs within a nationally or regionally accredited 4-year college or graduate-level university that has an area of study or focus area in IA. These courses should be identified for each area. Enrollment data should also be provided. At PUPR we offer a Master of Science in Computer Science with a Specialization in IA. We also offer a Graduate Certificate in Information Assurance and Security. We also plan to offer a Graduate Certificate in Computer Forensics soon. At the undergraduate level we have been offering courses in ethical hacking, computer forensics, network security, and reverse engineering, among others. Student enrollment has been increasing steadily in IA related courses.

Criteria 8: Declared Center for IA Education and Research

The applying institution must have a declared center for IA education and research from which IA curriculum is emerging. This should be a formal organization where faculty and students can share their research, collaborate, and interact. The institution should provide documentation of the designation of the Center (e.g. the charter), signed by the Dean or higher, and the mission statement.

The Center of Information Assurance for Research and Education (CIARE) at PUPR provides a forum that can be used by faculty, students, and professionals from the public and private sectors. This collaboration helps to identify the issues on IA and cyber security that need to be solved. The Center is a vehicle for: curriculum development, training, research, invention, innovation, education, public awareness, entrepreneurship, economic development, and dissemination of best practices in IA.

Criteria 9: Full-Time IA Faculty

Institutions need to report the number of IA faculty and course load to determine if there are a sufficient number of full time IA faculty members and additional faculty members (may be part-time, adjunct, visiting professor, etc.) teaching at least one IA course. This criterion requires a letter signed by the Dean or higher identifying the faculty and teaching workload, and a link to a biography or curriculum vitae for each faculty member.

The difficulty to recruit faculty in the area of information assurance is recognized nationwide. PUPR has been fortunate to attract outstanding PhD faculties to teach in our graduate programs. Their areas of research include Computer Forensics, Network Security, Cloud Computing Security and Privacy, Cryptography, among others.

8. CONCLUSIONS

The protection and security of an organization's intellectual assets has become an important challenge that should be considered in current academic curriculums. The continuously rapid change in the security field makes it extremely difficult for a university to establish a curriculum that will adequately prepare students for the professional challenges they will encounter. Nevertheless, bodies like ACM, IEEE and ABET do not have a formal or effective standardized Information Assurance curriculum model developed. Thanks to the CNSS course certification mapping, and the partnerships and collaboration that have been established through the Center of Information Assurance for Research and Education (CIARE) and the CAE/IAE designation, some information assurance educators in Puerto Rico are looking for the best ways to deliver the knowledge, skills, and expertise that is required.

With the research done at PUPR, a CBK for information assurance and security was done to set the path for the creation of Master in Information Assurance program that can be used at other institutions to promote IA education at a graduate level that includes both technical and managerial focuses in the course curriculums. Through this work, the course mapping, and the designation experiences, Polytechnic University of Puerto Rico has been able to create a CBK that is useful for graduate and undergraduate certificates and programs, enhancing current IA programs and courses, opening the path to IA programs at other institutions.

REFERENCES

[1] Longmore, C. (2002). The Orange Book Site, http://www.dynamoo.com/orange/. 02/04/12 (date accessed)

[2] Merrill, D. NOT the Orange Book, http://jya.com/ntob.htm. 02/03/12 (date accessed)

[3] Maconachy, V. (2003), "Education Training and Awareness Working Group". *Committee on National Security Systems Annual Conference: Homeland Security*.

[4] Schneider, L., Information Security - Learn About Information Security, http://jobsearchtech.about.com/od/historyoftechindustry/g/InfoSecurity.htm. 01/15/12 (date accessed)

[5] Centers of Academic of Excellence in Information Assurance Education, http://www.nsa.gov. 05/02/08 (date accessed)

[6] Pfleeger, C., and Cooper, D. (1997), "Security and Privacy: Promising Advances", *IEEE Software*, Vol. 14, No. 5, pp 27-32.

[7] NSF and American Association of Community Colleges. (2002). Protecting Information: the Role of Community Colleges in Cyber Security Education, http://www.eric.ed.gov/PDFS/ED473675.pdf. 02/04/12 (date accessed)

[8] Gorgone, J.T., Davis, G.B., Topi, Valacich, J.S., H., Feinstein, D.L., D., and Longenecker, H. (2002). IS2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems, http://www.acm.org/education/is2002.pdf. 02/05/12 (date accessed)

[9] Whitman, M. E., and Mattord, H. J. (2007). *Principles of Information Security*, 2nd edition, Thompson Learning, Inc. Canada.

[10] Reynolds, W., Report of the 1998 Annual Meeting for the National Colloquium for the Information System Security Education, http://csrc.nist.gov/nissc/1998/proceedings/panelG6.pdf.

[11] Chin, S-K., Irvine, C.E., and Frincke, D., An Information Security Education Initiative for Engineering and Computer Science, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA333216. 02/02/12 (date accessed)

[12] Bacon, T., & Tikekar, R. (2003). "Experiences with Developing a Computer Security Information Assurance Curriculum", *The Journal of Computing in Small Colleges*. Vol.18, No. 4, pp 254-267.

[13] Bishop, M. (2000). "Academia An Education in Information Security: Four Years Later", *Proceedings of the National Colloquium on Information System Security*.

[14] Bishop. M. (1997). "The State of INFOSEC Education in Academia: Present and Future Directions", *Proceedings of the National Colloquium on Information Security Education*.
[15] S. Kim & M. Choi, Educational Requirement Analysis for Information Security Professionals in Korea, Journal of Information System education, Vol. 13, no. 3, 2002.
[16] Golshani, F., Panchanathan, S., Friesen, O., Park, Y.C., and Song, J. (2001). "A Comprehensive Curriculum for IT Education and Worforce Development: An Engineering Approach", *Journal ACM SIGCES Bulletin*, Vol. 33, No. 1, pp 238-242.
[17] IT Model Curriculum. (2005). http://www.acm.org/education/curric_vols/IT_October_2005.pdf, 02/01/12 (date accessed)
[18] Dark, M., Ekstrom, J., and Lunt, B. (2005). Integration of Information Assurance and Security into the IT2005 Model Curriculum, http://www.et.byu.edu/~jekstrom/Publications/SIGITE%202005%20IAS%20Integration.pdf. 02/07/12 (date accessed)
[19] Taylor, C., and Shumba, R. Computer Security Education: Where Are We Now? http://www.iticse08.fi.upm.es/WGs/WG7.pdf. 01/14/12 (date accessed)
[20] Dark, M., and Davis, J. (2002). "Report of Information Assurance Curriculum Development". Paper presented at the meeting of the NCISSE, Washington DC, 1-22.
[21] Whitman, M.E., and Mattord, H.J., "Designing an Information Security Curriculum", *Proceedings of the 1st Annual Conference on Information Security Curriculum Development ACM*, New York, NY, USA 2004.
[22] Cruz, A. & Lopez, A. (2010). "Proposal to Submit a Graduate Certificate in Information Assurance and Security to the Council of Higher Education of Puerto Rico", Graduate School, Polytechnic University of Puerto Rico.
[23] Schweitzer, D., Humphries, J., and Baird, L. (2006). "Meeting the Criteria for a Center of Academic Excellence (CAE) in Information Assurance Education", *Journal of Computing Science in Colleges*, Vol. 22, No.1, October 2006.
[24] Malladi, S., El-Gayar, O., and Streff, K. (2007). "Experience and Lessons Learned in the Design and Implementation of an Information Assurance Curriculum", *Proceedings of the 2007 IEEE Workshop on Information Assurance,* United States Military Academy, West Point, NY, 20-22 June 2007
[25] Mucklow, T. (2008). Federal Information Systems Security Educators' Association (FISSEA) Workshop, http://csrc.nist.gov/organizations/fissea/workshops/July2008/FISSEA_July2008-workshop_TimMucklow.pdf. 02/16/12 (date accessed)
[26] Information Assurance Courseware Evaluation Program, https://app.cnss.gov. 01/12/12 (date accessed)

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.