Information Assurance Curricula and Certifications

Victor Piotrowski
Department of Mathematics and Computer Science
University of Wisconsin-Superior
vpiotrow@uwsuper.edu

Abstract

Although there have been several attempts to develop Information Assurance (IA) curricula, none of them meets the need of an undergraduate liberal arts education. Most of the existing IA curricula either target graduate programs, vocational education, or the need of the federal government. In this paper, we survey efforts of major players in developing or influencing IA model curricula: the government, professional organizations, and academia. This paper and an associated website http://www.LAIAC.org is an attempt to initiate collaboration in design and development of an undergraduate Liberal Arts Information Assurance Curriculum (LAIAC).

Introduction

Introducing the Cyber Security Research and Development Act, Science Committee Chairman Sherwood Boehlert said that the results of the bill would be to promote new research that will produce innovative, creative approaches to computer security, to draw more researchers into the field, and to develop a cadre of students who will become the next generation of cybersecurity researchers. It seems that in order to achieve it we need to include liberal arts colleges and universities. This paper and an associated website http://www.LAIAC.org is an attempt to initiate collaboration in design and development of an undergraduate Liberal Arts Information Assurance Curriculum (LAIAC).

Although there have been several attempts to develop Information Assurance (IA) curricula, none of them meets the need of an undergraduate liberal arts education. Most of the existing IA curriculum models either target graduate programs, vocational education, or the need of the federal government. In this paper, we survey efforts of major players in developing or influencing IA model curricula: the government, professional organizations, and academia.

Cyber Security Research and Development Act recognizes the need to increase involvment of institutions of higher education to "revise curriculum to better prepare students for careers in computer and network security" and authorizes the National Science Foundation to carry out those goals at $95,000,000 in 2003-2007. In November 2001, a group of University of Wisconsin campuses lead by UW-Milwaukee formed a steering committee for the Wisconsin Cybersecurity Program. The group organized a Curriculum Development Symposium with participants representing the National INFOSEC Education and Training Program (NIETP) within the National Security Agency; Center for Cryptography, Computer and Network Security; Army Reserve Readiness Training at Fort McCoy specializing in military cybersecurity, and business community. Currently the group is in a capacity-building stage, including curriculum development and faculty training. This paper is intended to stimulate a discussion leading to a model IA curriculum in a liberal arts environment.

Committee on National Security Systems (CNSS)

In 1990, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established to develop national policy and standards to protect national security information systems. By 1993, information systems security (INFOSEC) education, training and awareness are listed among top three priorities and NSTISSC directive 500/93 establishes the requirement for all federal departments and agencies to develop and implement INFOSEC education, training and awareness programs for national security systems. This was the origin of several training standards used by educational programs to create IA curricula eligible for federal funding:

- NSTISSI 4011: National Training Standard for INFOSEC Professionals, 1994.

- NSTISSI 4012: National Training Standard for Designated Approving Authority, 1997.
- NSTISSI 4013: National Training Standard for System Administration in Information Systems Security, 1997.
- NSTISSI 4014: National Training Standard for Information Systems Security Officers, 1997.
- NSTISSI 4015: National Training Standard for Systems Certifiers, 2000.
- NSTISSI 4016: Risk Analyst, in preparation.
- NSTISSI 4017: System Security Engineer, preparation.

Meeting these standards in a liberal arts environment is not easy since they focus on practical, low level skills. Below is a fragment of NSTISSI 4011:

Instructional Content:

- Describe agency "control points" for purchase and maintenance of AIS and telecommunications systems __
- Outline agency specific AIS and telecommunications systems __
- Review agency AIS and telecommunications security policies __

Topical Content:

- AIS: Firmware __, Hardware __, Software __
- Telecommunications Systems: Hardware __, Software __
- Agency specific security policies: Guidance __, Points of Contact __, Roles and responsibilities __
- Agency specific AIS and telecommunications policies: Points of contact __, References __

In 1996, the President's Commission on Critical Infrastructure Protection (PCCIP) was created by the Presidential Executive Order 13010. Among other, the commission was charged to establish a plan for preventing computer-based attacks on the information or communications components that control critical infrastructures (''cyber threats''), and to provide training and education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures.

In 1997, PCCIP issued a report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, and asking the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the U.S. Department of Education to develop programs for education and training of information assurance specialists. The Presidential Decision Directive 63 builds on these recommendations and asks academic leaders from engineering, computer science, business and law schools to review the status of education in information security and to identify changes in the curricula and resources necessary to meet the national demand for professionals in this field. Under Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age, the President has renamed NSTISSC as the Committee on National Security Systems (CNSS). The current

structure of CNSS includes Curriculum and Certification Working group as a subgroup of the Education, Training and Awareness Working Group.

National INFOSEC Education & Training Program (NIETP)

The National Security Agency Deputy Director for Information Systems Security created the National INFOSEC Education and Training Program (NIETP) within the Information Assurance Directorate to recognize that NSA needs to play a leadership role in security education and responds to a need expressed by the NSTISSC. Its mission is to be a leading advocate for improving INFOSEC education and training nationwide.

In 2000, the White House issues the National Plan for Information Systems Protection where under Program 7 (Train and Employ Adequate Numbers of Information Security Specialists) proposes a multi-million Federal Cyber Services (FCS) training and education initiative including

> "…the creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT workers and security managers. This program will fund up to 300 students per year in their pursuit of undergraduate or graduate degrees in the information security field. In return, the students will serve in the Federal IT workforce for a fixed period following graduation. The program will also have a meaningful summer work and internship element. An important part of the SFS program is the need to identify universities for participation in the program and assist in the development of information security faculty and laboratories at these universities."

This Federal Cyber Service: Scholarship for Service (SFS) is administered by the National Science Foundation and it has two tracks:

1. The Scholarship Track provides funding to colleges and universities to award scholarships in information assurance and computer security fields. Upon graduation after their two-year scholarships, the recipients will be required to work for a federal agency for two years in fulfillment of their Federal Cyber Service commitment.

2. The Capacity Building Track provides funds to colleges and universities to improve the quality and increase the production of information assurance and computer security professionals through professional development of information assurance faculty and the development of academic programs.

In either case, the institution has to be designated by the National Security Agency as a Center of Excellence in Information Assurance Education (CAE/IAE). CAE/IAE program was established by NSA as a consequence of the Presidential Decision Directive 63 and its goal is to reduce vulnerability in the National Information Infrastructure by

promoting higher education for Information Assurance, and producing a growing number of professionals with Information Assurance expertise in various disciplines. The first criterion of measurement for a future CAE/IAE is that the academic program at the university is tied to NSTISSI Training Standards. Meeting these standards at a liberal arts college is difficult since they are vocationally focused and based on core competencies [7]. The following colleges and universities' IA curricula have been certified to meet the indicated NSTISSC training standards:

Florida State University - 4011
George Mason University - 4011
George Washington University - 4011
Idaho State University - 4011
Indiana University of Pennsylvania - 4011
Iowa State University - 4011
John Hopkins University - 4011
New Mexico Tech - 4011
Northeastern University - 4011
Norwich University – 4011, 4014
Purdue University - 4011
State University of New York at Buffalo – 4011
State University of New York at Stony Brook - 4011
Towson University - 4011
University of California, Davis - 4011
University of Idaho - 4011
University of Maryland University College - 4011
University of Nebraska at Omaha - 4011
University of Texas at San Antonio - 4011
University of Tulsa – 4011, 4012, 4013, 4014, 4015

In addition, the following 36 universities have been designated as CAE/IAE:

Air Force Institute of Technology
Carnegie Mellon University
Drexel University
Florida State University
George Mason University
George Washington University
Georgia Institute of Technology
Idaho State University
Indiana University of Pennsylvania
Information Resources Management College of the National Defense University
Iowa State University
James Madison University
Mississippi State University
Naval Postgraduate School
New Mexico Tech

North Carolina State University
Northeastern University
Norwich University
Polytechnic
Purdue University
Stanford University
State University of New York, Buffalo
State University of New York, Stony Brook
Syracuse University
Towson University
University of California at Davis
University of Idaho
University of Illinois at Urbana-Champaign
University of Maryland, Baltimore County
University of Maryland, University College
University of Nebraska at Omaha
University of North Carolina, Charlotte
University of Texas, San Antonio
University of Tulsa
U.S. Military Academy, West Point
West Virginia University

Another program within NIETP is the National Colloquium for Information Systems Security Education (NCISSE) established in 1997 to influence and encourage the development of information security curricula, especially at the graduate and undergraduate levels. NCISSE is open to all desiring to advance the state of information security and information assurance education. The Colloquium sponsors an annual conference.

Finally, NIETP also includes Electronic Develop-A-Curriculum (EDACUM) program. EDACUM is an automated process that enables a group of experts to develop a curriculum for a specific course against a standard or course objective. This activity is conducted under the auspices of NSTISSC and it is conducted at Idaho State's Simplot Decision Support Center (SDSC). To date, EDACUMs have resulted in the development of the national training standards NSTISSI 4011, 4012, 4013, 4014 and 4015.

National Institute of Standards and Technology

The Computer Security Act of 1987 (Public Law 100-235) mandated NIST to create guidance on computer security Awareness and Training based on functional organizational roles described in the NIST Special Publication 800-16 *Information Technology Security Training Requirements: A Role- and Performance-Based Model* [6]. The Information Technology Security Learning Continuum modeled in this guidance, provides the relationship between awareness, training, and education.

International Information Systems Security Certifications Consortium

$(ISC)^2$ offers professional IA certifications and maintains a Common Body of Knowledge for IA. Certified Information Systems Security Professional (CISSP) examination covers the following ten knowledge areas:

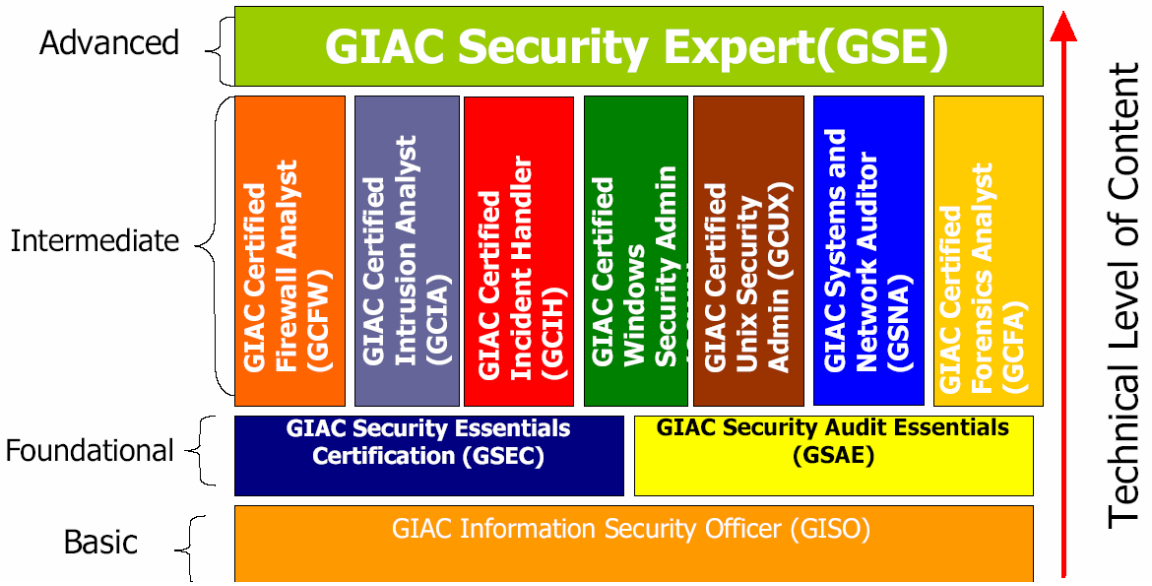
- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security

System Security Certified Practitioner (SSCP) examination covers the following seven knowledge areas:

- Access Controls
- Administration
- Audit and Monitoring
- Risk, Response and Recovery
- Cryptography
- Data Communications
- Malicious Code/Malware

SANS Institute GIAC Certification Program

The SANS Institute founded GIAC (Global Information Assurance Certification) in 1999 in response to the need to validate the skills of security professionals. SANS' Security Essentials is now certified as compliant with NSTISSI's 4013 training standards. SANS training and GIAC certifications include several knowledge/skills areas like Audit, Intrusion Detection, Incident Handling, Firewalls and Perimeter Protection, Forensics, Hacker Techniques, Windows and Unix Operating System Security.



Academia

The *Information Assurance Curriculum Development* project [2] directed by Jim Davis under the 2001-2003 National Science Foundation Grant DUE #0124409:

> "… is developing a curriculum framework for undergraduate and graduate programs in Information Assurance. The framework includes: identification of broad areas of knowledge considered important for practicing professionals in information assurance, identification of key learning objectives for each of these areas, identification of a body of core knowledge and skills that all programs should contain, and a model curriculum including scope and sequence. "

After two workshops, involving about 20 military and academia experts, the project identified a list of main topics that should be covered in an undergraduate IA program. The following list uses Bloom's taxonomy [1] to indicate a desired depth level: declarative ("to know"), application ("to use"), and synthesis ("to create").

• General Information Assurance (Basic IT and traditional definitions of INFOSEC)	Declarative
• Risk Assessment (Identifying threats and vulnerabilities)	Application
• Information Security Management (Security policy; Organizational behavior, cultural, societal, and ethical implications)	Application
• Networking Fundamentals	Application
• Cryptography	Declarative
• PKI Fundamentals (cryptography PLUS implementation/usage	Declarative

issues)	
• Operating Systems	Application
• Software Engineering Practices	Declarative
• Legal, Ethical INFOSEC (have to be preparing students to FUNCTION in the current environment. This means that they have to understand what they can and cannot do.)	Declarative
• Intrusion Defense and Response	Declarative
• Emerging Technologies (what they are, what are the issues, how to evaluate and use these in a security system)	Declarative
• E-commerce related issues	Declarative
• Development of secure network applications, server, and distributed applications.	Application
• IT System and Network Security Design	Application
• Integrative experience (to address an ill-defined problem with no single correct answer. The problem has social, economical, ethical, and political constraints. Involves the consideration of more than one design alternative and requires students to work in a team environment.)	Synthesis

Remark

An updated version of this paper and additional resources on the liberal Arts Information Assurance Curriculum project can be found at LAIAC.org.

Bibliography

1. Bloom, B., Englehart, M., Furst, E., Hill, W., Krathwohl, D. *Taxonomy of Educational Objectives: Handbook I, Cognitive Domain.* New York, 1956.
2. Dark, M., Davis, J. *Report on Information Assurance Curriculum Development*. CERIAS, 2002.
3. Kabay, M. *Information Security Education Resources for Professional Development.* 5th NCISSE Proceedings, 2001.
4. Alford, K., Dunn, C., Ruocco, A. *Information Assurance Pedagogy.* Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. West Point, 2001.
5. Laswell, B., Simmel, D., Behrens, S. *Information Assurance Curriculum and Certification: State of the Practice.* CMU/SEI-99-TR-021. Pittsburgh, 1999.
6. Wilson, Mark, ed. *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* NIST Special Publication 800-16, U.S. Department of Commerce, 1998.
7. Yasinsac, A. *Information Security Curricula in Computer Science Departments: Theory and Practice.* Manuscript, 2001.