An Information Assurance and Security Curriculum Implementation

Samuel P. Liles and Reza Kamali
Purdue University Calumet, Hammond, IN, USA

sliles@purdue.edu kamalir@calumet.purdue.edu

Abstract

A holistic approach to security education is important to providing practitioners the scope of learning necessary for integration of their skills into the enterprise. Specifically domains of knowledge can easily be identified that allow for this holistic approach to be implemented into a new program of study or curriculum for information assurance and security. Within the Purdue Calumet CIT Department a new curriculum has been written and the program of study has been approved for implementation and the first students have applied to the program. The domains of systems assurance, software assurance, and operations assurance are as critical to the success as the overall goal of ABET accreditation of the program to the ACM SIGITE draft specifications when finalized.

Keywords: Information Assurance, Security, Curriculum, SIGITE, ACM

Introduction

The benefits and responsibilities having been fully weighed by *the Purdue Calumet CIT Department*, a strong case for positive acceptance was made for aligning *the Purdue Calumet CIT Department* with the ACM SIGITE (Curriculum) guidelines. The ACM SIGITE group has been working on a ABET accrediting program for information technology education in a four year program. These guidelines were mapped to multiple information technology disciplines, and specifically to a new information assurance and security program that is now accepting students. This document shows how the new program was designed and how it aligns with a variety of different certifying bodies and specifically with NTISSI 4011(NTISSI).

The process utilized wove a tapestry of the guidelines as proposed by SIGITE. The topics when given were processed into outcome based learning objectives (Bloom, 1956). These objectives were then processed as requirements against the NTISSI 4011 certification standard as a prerequisite of the program. One of the basic outcomes of this new curriculum was at the two year level all information technology students would attain the NTISSI 4011 certification as well as a broad based information technology education. This is one of the closest implementations to the newly proposed SIGITE guidelines.

Domains of knowledge

Domain areas for the entire curriculum were addressed and knowledge area requirements were examined as found in previous papers (Davis, 2003; Laswell, 1999). These were invaluable resources and allowed *the Purdue Calumet CIT Department* to evaluate and concentrate

on the most likely areas of specialization for undergraduate instruction. Having a pattern of courses put together that would advance students quickly from novice to subject matter expert was a goal. Having a framework for knowledge to be wrapped around also was part of the success strategy for *the Purdue Calumet CIT Department*.

Each of the outcome base learning objectives was processed for level of skill based on the Bloom Taxonomy (Bloom, 1956) for education. The objectives were then looked at for area of expertise as applied to the individual curricula guidelines. Balance of instructional expectation was attained by insuring that freshman and sophomore classes were balanced strongly towards the lower levels of Blooms taxonomy with fewer upper level objectives. Consequently upper level courses have higher level objectives and significantly fewer lower level objectives with an expectation that prior courses prepared the student sufficiently. As part of the preparation of that expectation course designers met and built a map of the course objectives and knowledge requirements.

Before beginning the mapping of objectives, the role of a student completing the course was discussed. What would a successful student from this program do as a career? Was the objective to create practitioners, scholars, or graduate school aspirants? These objectives were addressed within *the Purdue Calumet CIT Department* and a plan was put in place.

The Proposed Process for Certification

Starting with the documents provided by NTISSI, *the Purdue Calumet CIT Department* set up learning objectives that coincided. The first goal was to attain 4011 certification at the two year level even though *the Purdue Calumet CIT Department* is currently a four year program. Truly utilizing ad hoc methods, the learning objectives were split between the four courses known as platform technologies, operating system administration, networking, and fundamentals of information assurance and security. These four courses are split out from the objectives as set in the accreditation guidelines for 4011 certification and the outcome based learning objectives basically mirror 4011. Added to this and coinciding nicely with the draft ACM SIGITE guidelines (Curriculum) the courses also serve to help with this accreditation goal. Both of these programs sincerely support each other and help in the curriculum design process.

Inclusive Modularity

Multiple domains of information assurance knowledge were identified and three knowledge domains were taxonomically derived and provided the structure for the curriculum modules as areas of interest (Maconachy, 2001). The first module is systems assurance. This module is inclusive of the operating systems, networks, hardware systems, and the other mature sciences of securing systems. The second module is the software assurance module. This second module, though less holistic, is inclusive of the sub disciplines of software auditing, secure coding practices, analysis of software, and implementing software in the enterprise. The third module is a well defined module of operations assurance where the concepts of physical security, policies, procedures, risk analysis, and the other organizational non-technical controls exist.

The three domains as discussed can be sliced and defined differently depending on the perspectives of the evaluators for defining threads of knowledge through the program. The domains became increasingly important for sequencing courses and providing knowledge dependencies for curriculum design. The three domains of information assurance as identified also allow for future growth of the program as cohesive specializations. Pursuant to the goal statements of the Purdue Calumet CIT Department the final outcome of the program is to provide a student that has a well rounded information technology background with a broad based specialization in information assurance and security.

Systems Assurance

Systems assurance is the practice of hardening operating systems from known threats, analyzing and auditing hardware and devices for known threats, and remeditating the devices and computing platforms within the enterprise (Maconachy, 2001). For instance, proper configuration and defensive strategies employed for protecting a network and specifically a router would be considered systems assurance. Ensuring that user accounts are active and properly used with permissions inside of the enterprise would be considered systems assurance.

Table 1 Systems Assurance Courses

Systems Assurance Courses
Fundamentals of Information Assurance: This course covers security mechanisms, fundamental aspects, operational issues, policy, attacks, security domains, forensics, information states, security services, threat analysis, vulnerabilities, and other topics.
Systems Assurance: This course covers the implementation of systems assurance with computing systems. Topics include confidentiality, integrity, authentication, non-repudiation, intrusion detection, physical security, and encryption. Extensive laboratory exercises are assigned.
Assured Systems Design and Implementation: This course covers the design and implementation of assured systems in an enterprise environment. Topics include hardening of operating systems, choice of platforms, design criteria within the assured systems domain. Extensive laboratory exercises are assigned.
Computer Forensics: This course covers the techniques used in the forensic analysis of computerized systems for gathering evidence to detail how a system has been exploited or used. Extensive laboratory exercises are assigned.

Software Assurance

Software assurance is a selection of sub disciplines merged into a practice. Software assurance is the practice of requirements gathering, secure coding, testing, auditing, and implementation of software in the enterprise protecting against known vulnerabilities. Software assurance is the preparation of source code such that known vulnerabilities are excluded from the product. Software assurance is also about preparing robust source code so that unknown vulnerabilities create secure failure conditions (Software, 1992). Preparation can include auditing of commercial off the shelf software (COTS), or free open source software (F/OSS) being implemented within the enterprise, or third party prepared/contracted source code.

Software assurance includes normally associated computer science topics such as Software Engineering (SE), Software Quality Assurance (SQA), Highly Assured Computing (HAC), Capability Maturity Model (CMM), and other development lifecycle issues. Further software assurance elements include domain crossing topics such as end of life cycle, maintenance, retirement, reusability, and legacy adaptation strategies. Software assurance definitively includes practice oriented computing concepts including secure coding, threat modeling, vulnerability analysis, implementation, auditing, and defensive integration of software within the enterprise.

Table 2 Software Assurance Courses

Software Assurance Courses
Programming Fundamentals: This course covers fundamental data structures, fundamental programming constructs, object-oriented programming, algorithms and problem-solving, event-driven programming, recursion, and other topics.
Advanced Programming: This course covers advanced topics in programming languages, GUI development, threaded applications, components, testing and debugging methods and advanced topics in event-driven and object oriented programming techniques. Extensive laboratory exercises are assigned.
Software Assurance: This course covers defensive programming techniques, bounds analysis, error handling, advanced testing techniques, detailed code auditing, and software specification in a trusted assured environment. Extensive laboratory exercises are assigned.

Operations Assurance

Operations assurance advocates the tools of physical security and operational characteristics found in a cohesive information technology organization (Software,1999). Within the curriculums scope are the concepts of physical security, data center design, and legal and procedural reporting. Items that are of great concern to the enterprise that would be found here include disaster recovery and planning. The concept of business continuity and risk analysis are threads of knowledge that run through the domain area of operations assurance.

Within operations assurance you would find for example the implications of HIPPA, DMCA, or the concepts of physical security. Paradoxically items often overlooked as part of information assurance would be the concept of back up and recovery testing procedures, insurance, and other litigation aspects of operations. The ability to define, categorize, and apply financial loss expectation documents to management of an enterprise is a valuable skill.

Table 3 Operations Assurance Courses

Operations Assurance Courses
Ethical and Legal Issues of IT: This course covers professional communications, social context of computing, teamwork concepts and issues, intellectual properties, legal issues in computing, organization context, professional and ethical issues, responsibilities, privacy and civil liberties, and other topics.
Disaster recovery and planning: This course covers risk management and business continuity. Topics include disaster recovery strategies, mitigation strategies, risk analysis, and development of contingency plans for unexpected outages and component failures. Extensive laboratory exercises are assigned.
Information Assurance Risk Assessment: This course covers industry and government requirements and guidelines for information assurance and auditing of computing systems. Topics include risk assessment and implementation of standardized requirements and guidelines.

Conclusion

Developing a holistic approach to information assurance and security curriculum was an onerous task. As defined in other publications (Laswell, 1999) there are a variety of approaches to the concept of information assurance and security. With only a relatively small number of courses to deal with in developing a curriculum and not wanting to follow a standard computer science model the solution at *the Purdue Calumet CIT Department* is to focus on implementations of security strategies. These implementation strategies fit within the overall goal for *the Purdue Calumet CIT Department* to attain accreditation through SIGITE.

Developing courses that split into three domains was in consideration arbitrary but definitely necessary for defining the knowledge areas. Other divisions were considered along these same lines, or even further devolvement of the topics into common knowledge areas as defined in other people's work. Keeping in mind the practitioner approach these three domain areas served quite well at helping meet the overall goals. Further the three domain areas fit nicely at segmenting the courses and though some would argue with a particular course filling a slot often the flexibility is overlooked. This flexibility is part of the final solution to the curriculum modules and allows for growth in the overall courses.

References

Bloom, B. S. (1956). *Taxonomy of educational objectives: Handbook I: Cognitive domain*. Longmans, Green & Company

Curriculum: Proposed standards for IT curriculum. Retrieved 6/12/2005 from http://sigite.acm.org/activities/curriculum/downloads/IT%20Volume-April%202005.pdf

Crowley, E. (2003). Information system security curricula development. *Proceeding of the 4th Conference on Information Technology Curriculum*, pp. 249-255

Davis, J. & Dark, M. (2003). Defining a curriculum framework in information assurance and security. *ASEE Annual Conference*, Nashville, TN, June.

Laswell, B., Simmel, D., & Behrens, S. (1999). Information Assurance Curriculum and Certification: State of the Practice. CMU/SEI-99-TR-021, *Software Engineering Institute*, Carnegie Mellon, Pittsburg, PA, Sept.

Maconachy W. V., Schou C. D., Ragsdale D., & Welch D. (2001). A model for information assurance: An integrated approach. *Proceedings 2001 IEEE Information Assurance Workshop* , West Point, NY, 2001, pp. 306 - 310.

National Information Systems Security (INFOSEC) Glossary. (1997). NSTISSI No. 4009, National Security Telecommunications and Information Systems Security Committee, August.

NSTISSI, (1994). No. 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals.

Software Assurance Standard. (1992). NASA-STD-2201-93, NOVEMBER 10, 1992.

Biographies

Samuel P. Liles III is an Assistant Professor of Computer Information Technology at Purdue University Calumet. He is currently involved in research identifying the knowledge skills and abilities of cyber adversaries and mitigation strategies.

Dr. **Reza Kamali** is an Associate Professor and Department Head of Computer Information Technology at Purdue University Calumet, Hammond, Indiana. He was a founding member of SITE, which later became ACM's SIGITE. He was a member of the IT2006 Task Force and a member of The Joint Task Force for Computing Curricula 2005