Chapter XVIII

Information Assurance and Security Curriculum Meeting the SIGITE Guidelines

Samuel Liles
Purdue University Calumet, USA

Reza Kamali
Purdue University Calumet, USA

ABSTRACT

Information assurance education is an interdisciplinary endeavor that only when taken as a holistic and inclusive educational activity can be successful. When considering the design and implementation of a curriculum that is set to meet standards set by outside agencies, the educational institution must use a flexible and repeatable process. Building a curriculum on top of a strong foundation will empower and facilitate success. Meeting outside agencies’ requirements, such as accrediting agencies, will close, if not eliminate any credibility gaps within an institution.

INTRODUCTION

There is a dearth within the literature of repeatable and sustainable processes or guidelines on “how to” create a curriculum that meets the requirements of outside or internal agencies making demands on the university for appropriate curriculum (R. Kamali, Liles, Winer, Jiang, & Nicolai, 2006). Further, the balance between the requirements of accrediting agencies and the stake holders in an institution may be in conflict. Preparing and creating a curriculum to meet these coordinate and conflicting requirements is a solvable task.

It is important to make insightful decision in the creation of curriculum. The sustainability of a curriculum going into the future will be predicated on the foundation of the elements and decision used to differentiate it from other curriculums.
When the overall goals and missions of the program of study are considered certain elegance can be found in the creation of a holistic curriculum model. The strength of outcome based objectives within information technology is documented strongly (Melissa J. Dark, 2004; Melissa Jane Dark, Ekstrom, & Lunt, 2005; Hazem et al., 2004; Rigby & Dark, 2006). Information assurance and security is a large interdisciplinary area of study that defies definition. The perspective of the computer scientist finds information assurance and security to be encryption and computational models. The computer engineer might find information assurance and security in the hardware security devices such as firewalls.

Information assurance and security has been defined by many authors as the practices, techniques, methods, of securing information in all of its forms from the various threats and risks that information can be subjected to in the enterprise (McKnight, 2002; National Security Telecommunications and Information Systems, 1997a). As practitioners and educators the primary subjects we deal with are confidentiality, integrity, availability, authentication, and non-repudiation and we define information assurance and security based on those topics (Maconachy, Schou, Ragsdale, & Welch, 2001). There are other ways of defining the breadth of the discipline and as an interdisciplinary area of study there will likely be more ways of defining it in the future.

The Association of Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) maintain standards bodies that assist the Accreditation Board for Engineering and Technology (ABET) in defining information technology curriculum and the information assurance and security areas required for accreditation (Liles & Kamali, 2006). Of specific interest to faculty and students are the curriculum volumes for accrediting information technology programs and specifically the topical requirements for information assurance and security. The ACM maintains special interest educations groups (SIGS) and these groups define the best curricular practices for a discipline such as computer science and specifically the special interest group for information technology education (SIGITE). (“Computing curricula 2001,” 2001) (“Curriculum: Proposed standards for IT curriculum,” 2005). It might be easier to split up information assurance and security in a few specific topical areas such as systems, software, networking, and management. These will allow us to look at the topical elements and consider them in our end solution for creating a curriculum.

Systems are all of the computing and logical devices inside the enterprise that are computational or embedded in the way the overall information systems of the enterprise works. The systems can be the sensory devices for the data center that determine the temperature of the cooling systems, or they could be the computer sitting in front of a secretary.

Software is all of the code running on the different machines. This is the code in the internal applications of the enterprise such as patches and scripts. The software we are interested in includes the operating systems of personal communication devices. There are large discussions over the validity and viability of teaching software assurance topics to undergraduates but if the techniques are baked into the first classes instructors will not be un-training students in graduate school.

Networking is the entire associated infrastructure required to make all of the different systems talk to each other. With the increase in wireless infrastructure that does not mean cables and fiber from point “A” to point “B”, but it can mean the implementation of wireless local area networks (LAN) trunks between two buildings. The networking side of the information technology budget has matured substantially in the realm of securing and inspecting data flowing on the network. The realistic creation of network redundancy and relative risk mitigation is still a new discipline in the data communication side of networking.